citrix

Session Recording 2204

Contents

Session Recording 2204	4
What's new	4
Fixed issues	5
Known issues	5
Third party notices	7
System requirements	7
Get started	10
Plan your deployment	11
Security recommendations	13
Scalability considerations	19
Install, upgrade, and uninstall	31
Dynamic session recording	62
Configure	68
Configure settings on the Session Recording agent	68
Enable or disable recording	69
Configure the connection to the Session Recording server	70
Change your communication protocol	71
Configure settings on the Session Recording server	73
Authorize users	73
Customize notification messages	75
Specify where recordings are stored	75
Specify file size for recordings	81
Enable or disable digital signing	84

Configure Citrix Customer Experience Improvement Program (CEIP)	84
Policies	89
Configure session recording policies	90
Configure recording viewing policies	102
Configure event detection policies	108
Configure event response policies	139
High availability and load balancing	148
Load balance Session Recording servers	149
Configure database high availability	152
View recordings	153
Session Recording player	153
Launch the Session Recording Player	154
Enable or disable live session playback	157
Enable or disable playback protection	157
Search for recordings	158
Open and play recordings	159
Cache recordings	167
Highlight idle periods	168
Use events and bookmarks	168
Session Recording web player	171
Access the web player	171
Hide or show content on the web player home page	178
Search for recordings	180
Open and play recordings	182

Configure cache for storing recordings during playback	186
Increase the transport packet size for the web player	186
Highlight idle periods	187
Use events and comments	189
Share URLs of recordings	191
View graphical event statistics for each recording	193
View data points related to each recorded session	197
Manage recordings	198
Manage and query administrator logging	203
Best practices	208
Configure load balancing in an existing deployment	208
Deploy and load balance Session Recording in Azure	257
Troubleshoot	290
Installation of server components fails	290
Test connection to the database fails during install	291
Agent cannot connect to the server	291
Server cannot connect to the database	293
Sessions are not recording	294
Unable to view live session playback	295
Recordings are corrupted or incomplete	296
Verify component connections	296
Search for recordings using the player fails	299

Session Recording 2204

April 6, 2023

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

June 22, 2022

What's new in 2204

This release addresses issues to improve the user experience.

Fixed issues

June 22, 2022

Compared with: Session Recording 2203 LTSR

Session Recording 2204 adds the following fixes:

- This fix helps to improve the overall performance of the Session Recording web player. [SRT-7305, SRT-7430, SRT-7431, SRT-7432, SRT-7433, SRT-7435]
- The Session Recording agent might not work when Windows Management Instrumentation (WMI) calls take a long time to fetch Windows Server features. [SRT-7503]

Known issues

February 28, 2024

The following issues have been identified in this release:

- 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]
- Recording viewing policies (playback permissions) that you set might not show on the **Playback Permissions** page of the Session Recording service. The issue occurs after upgrading to Session
 Recording 2204. As a workaround, run the following script in SQL Server Management Studio
 (SSMS) that corresponds to your Session Recording database:

```
ALTER procedure [dbo].[EnumPlayerUserDeliveryGroupPoliciesOnCloud
     ]
as
begin
set nocount on
select 3 as RoleType,
a.ID as RoleAccountID,
h.principleName as PrincipleName,
```

```
9 a.IsEnabled as IsEnabled,
   e.name as PolicyType,
10
   d.DeliveryGroupID as AccountMemberAccountID,
11
    g.Name as AccountMemberName
12
13
14
    from PlayerUserCloudAccountRoleConfigure a,
15
    PlayerUserPolicyConfigSetMember b,
16
    PlayerUserPolicyDeliveryGroupSetMember d,
17
    PlayerUserPolicyType e,
18
   DeliveryGroup g,
19
   PlayerUserCloudAccount h
   where e.id=5
20
21
    and b.PlayerUserPolicyTypeID = e.ID
    and a.PlayerUserPolicyConfigSetID = b.PlayerUserPolicyConfigSetID
    and b.PolicySetID = d.PlayerUserPolicyDeliveryGroupSetID
23
24
    and g.ID=d.DeliveryGroupID
25
    and h.ID=a.CloudAccountID
27
    end
28
    <!--NeedCopy-->
```

[SRT-8028]

- 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

June 22, 2022

Session Recording Version 2204 (PDF Download)

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

System requirements

February 27, 2023

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

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

Session Recording database

Supported operating systems:

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

Supported Microsoft SQL Server versions:

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

Supported Azure SQL database services:

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

Supported AWS RDS database services:

SQL Server

Requirement: .NET Framework 4.7.2

Session Recording server

Supported operating systems:

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

Other requirements:

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

Session Recording policy console

Supported operating systems:

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

Requirement: .NET Framework 4.7.2

Session Recording agent

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

Supported operating systems:

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

Requirements:

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

Note:

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

Session Recording player

Supported operating systems:

- Windows Server 2022
- Windows Server 2019
- Windows Server 2016
- Windows 11
- 64-bit Windows 10, minimum version 1607

Requirement: .NET Framework 4.7.2

Note:

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

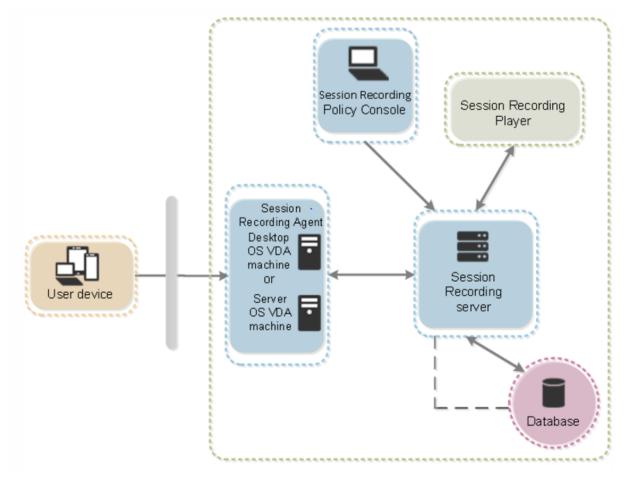
June 22, 2022

Session Recording consists of five components:

- **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 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 player.** A user interface that users access from a workstation to play recorded session files.
- 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 policy console. A console used to create policies to specify which sessions are recorded.

In the deployment example illustrated here, 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 Session Recording database. The Session

Recording player is installed on a workstation. 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

June 22, 2022

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.

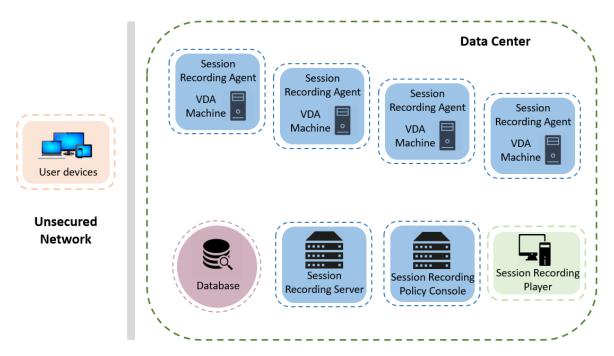
Depending upon your environment, you can deploy the Session Recording components in different scenarios.

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.

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 are installed on other servers and the Session Recording player on a workstation, all behind the firewall.



Important deployment notes

- To enable Session Recording components to communicate with each other, install them in the same domain or across trusted domains that have a transitive trust relationship. The system cannot be installed on a workgroup or across domains that have an external trust relationship.
- Considering its intense graphical nature and memory usage when playing back large recordings, we do not recommend installing the Session Recording Player as a published application.
- The Session Recording installation is configured for TLS/HTTPS communication. Install a certificate on the Session Recording server. Make sure the root certificate authority (CA) is trusted on the Session Recording components.
- For the Session Recording server on a standalone server running SQL Server, enable the TCP/IP
 protocol and run the SQL Server Browser service. These settings are disabled by default, but
 they must be enabled for the Session Recording server to communicate with the database. For
 more information, see the Microsoft articles Enable TCP/IP Network Protocol for SQL Server and
 SQL Server Browser service.
- Consider the effects of session sharing when planning your Session Recording deployment. Session sharing for published applications can conflict with Session Recording policy rules for published applications. Session Recording matches the active policy with the first published application that a user opens. After the user opens the first application, any subsequent applications opened during the same session continue to follow the policy that is in force for the first application. For example, if a policy states to record only Microsoft Outlook, the recording commences when the user opens Outlook. If the user opens a published Microsoft Word second while Outlook is running, Word also is recorded. Conversely, if the active policy doesn't specify to record Word and the user launches Word before Outlook, Outlook is not recorded.
- Though you can install the Session Recording server on a Delivery Controller, we don't recommend it because of performance issues.
- You can install the Session Recording Policy Console on a Delivery Controller.
- You can install both the Session Recording server and the Session Recording Policy Console on the same system.
- Ensure that the NetBIOS name of the Session Recording server does not exceed the limit of 15 characters. Microsoft has a 15-character limit on the host name length.
- PowerShell 5.1 or later is required for custom event logging. Upgrade PowerShell if you install the Session Recording agent on Windows Server 2012 R2 that has PowerShell 4.0 installed. Failure to comply can cause failed API calls.

Security recommendations

June 22, 2022

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.
- Session Recording server 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 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
- $\cdot \ {\sf Registry\,values\,within\,{\sf HKEY_LOCAL_MACHINE}{\sf SOFTWARE}{\sf Citrix}{\sf SmartAuditor}{\sf Server}$
- * On the Session Recording agent
 - · Process: SsRecAgent.exe
 - · Service: CitrixSmAudAgent
 - $\cdot\,$ All files in the Session Recording agent installation folder
 - Registry values under HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ SmartAuditor\Agent
- 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.
 - 1. 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.

27°	Computer Management		x
File Action View Help File Action View Help Image: Solution of the second secon	Citrixsmauddata Properties ? X General Security Citrixsm Citrixsm Group or user names: Image: Citrix Security More Society Image: Citrix Security More More Image: Citrix Security More Society Image: Citrix Security More More Image: Citrix Security More More Image: Citrix Security More Add Remove Permissions for Everyone Add Penditions for Everyone Alow Denty Image: Citrix Security Full Control Image: Citrix Security Image: Citrix Security Image: Citrix Security Pendition Image: Citrix Security Image: Citrix Security Image: Citrix Security Provide Message Image	auddata Actions	×
	Receive Journal Message Image: Construction of advanced settings, click For special permissions or advanced settings, click Advanced Advanced. OK Cancel		

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

2	Computer Management	_ 🗆 X
File Action View Help		
(+ ->) 2 📷 🗙 🖾 @ 🕞 🛛 📷		
Computer Management (Local) Storage S	citrixsmauddata Properties 2 General Security	Actions citrixsmauddata More Actions
L		

- 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

January 5, 2023

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. To use this functionality, 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
yo	Edit Setting
verview Settings Assigned to • Use video codec for compression User setting - ICA\Graphics For actively changing regions (Default: Use when preferred)	Use video codec for compression Value: for actively changing regions Image: Colspan="2">Image: Colspan="2">Colspan=CS, 7:3 Desktop OS, 7:3 Server OS, 7:1 Desktop OS, 7:15 Server OS, 7:15 Desktop OS, 7:15 Server OS, 7:15 Desktop OS, 7:15 Desktop OS, 7:17 Desktop OS, 7:17 Desktop OS, 7:18 Desktop OS, 7:1903 Server OS, 1905 Desktop OS, 7:190 Desktop OS, 1905 Desktop OS, 7:19 Desktop OS, 7:17 Desktop OS, 7:10 Desktop OS, 7:19 Desktop OS, 7:19 Desktop
	Select 'For the entire screen' to optimize for cases with heavy use of server-rendered video and 3D graphics, especially in low bandwidth.

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 ses-

sions 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 3.5 Mbps. (5,000 sessions times 20 MB divided by 8 hours, divided by 3,600 seconds per hour.) 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 higher than the input rate (3.5 Mbps), so recording the 5,000 Outlook sessions is feasible.

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. Instead of recording 5,000 Outlook sessions that generate 3.5 Mbps on one Session Recording server, reduce to 3,500 sessions that generate only about 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.

Performance Object	Counter Name	Description
Citrix Session Recording Storage Manager	Active Recording Count	Similar to the Citrix Session Recording agent counter excep for the Session Recording server. Indicates the total number of sessions currently being recorded for all servers.
Citrix Session Recording Storage Manager	Message bytes/sec	The throughput of all recorded sessions. Can be used to determine the rate at which the Storage Manager is processing data. If MSMQ is backlogged with messages, the Storage Manager runs at full speed. This value can be used to indicate the maximum processing rate of the Storage Manager.
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
MSMQ Queue	Bytes in Queue	observed. 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.

Performance Object	Counter Name	Description
MSMQ Queue	Message in Queue	Similar to the Bytes in Queue counter but measures the number of messages.
Network Interface	Bytes Total/sec	Can be used to measure on both sides of the link to observe how much data is generated when sessions are recorded. When measured on the Session Recording server, this counter indicates the rate at which incoming data is received. Contrasts with the Citrix Session Recording Storage Manager Message bytes/sec counter that measures the processing rate of data. If the network rate is greater than 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 2204

		Minimum Number 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
			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 fo
			Session Recording.
			RAID 3 can be
			deployed at a similar
			cost but with better
			write performance.

		Minimum Number 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

July 10, 2023

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.

This article includes the following sections:

- Installation checklist
- Use Citrix scripts to install the Windows roles and features prerequisites
- Install the Session Recording administration components

- Install the Session Recording database
- Install the Session Recording server
- Install the Session Recording agent
- Install the Session Recording player and the web player
- Automate installation
- Upgrade Session Recording
- Uninstall Session Recording
- Integrate with Citrix Analytics for Security

Installation checklist

You install the Session Recording components by using the following files:

- Broker_PowerShellSnapIn_x64.msi
- SessionRecordingAdministrationx64.msi
- SessionRecordingAgentx64.msi
- SessionRecordingPlayer.msi
- SessionRecordingWebPlayer.msi

Before you start the installation, complete this list:

X	Step
	Install the prerequisites before starting the
	installation. See System requirements and Use
	Citrix scripts to install the Windows roles and
	features prerequisites.
	Select the machines on which you want to install
	each Session Recording component. Make sure
	that each machine meets the hardware and
	software requirements for the component or
	components to be installed on it.
	Use your Citrix account credentials to access the
	Citrix Virtual Apps and Desktops download page
	and download the product file. Unzip the file.

8	Step
	To use the TLS protocol for communication
	between the Session Recording components,
	install the correct certificates in your
	environment.
	Install any hotfixes required for the Session
	Recording components. The hotfixes are
	available from the Citrix Support.
	Configure Director to create and activate the
	Session Recording policies. For more
	information, see Configure Director to use the
	Session Recording server.

Note:

- We recommend that you divide the published applications into separate Delivery Groups based on your recording policies. Session sharing for published applications can conflict with the active policy if the applications are in the same Delivery Group. Session Recording matches the active policy with the first published application that a user opens. Starting with version 7.18, you can use the dynamic session recording feature to start or stop recording sessions at any time during the sessions. For more information, see Dynamic session recording.
- If you plan to use Machine Creation Services (MCS) or Citrix Provisioning, prepare a unique QMId. Failure to comply can cause recording data losses.
- SQL Server requires that you enable TCP/IP, the SQL Server Browser service is running, and Windows Authentication is used.
- To use HTTPS, configure server certificates for TLS/HTTPS.
- Make sure that users under Local Users and Groups > Groups > Users have write permission to the C:\windows\Temp folder.

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</pre>

```
Installs Prereqs for Session Recording Administration
4
    .Description
5
        Supports Windows Server 2022, Windows Server 2019 and Windows
             Server 2016.
6
        Install below windows feature on this machine:
7
        -Application Development
        -Security - Windows Authentication
8
9
        -Management Tools - IIS 6 Management Compatibility
             IIS 6 Metabase Compatibility
11
            IIS 6 WMI Compatibility
12
            IIS 6 Scripting Tools
            IIS 6 Management Console
13
        -Microsoft Message Queuing (MSMQ), with Active Directory
14
            integration disabled, and MSMQ HTTP support enabled.
15
    #>
16
    function AddFeatures($featurename)
17
    {
18
19
        try
20
        {
21
22
             $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"
32
             Exit 1
         }
34
        Write-Host "Addition of Windows feature $featurename
            succeeded"
     }
37
38
39
    $system= gwmi win32_operatingSystem | select name
40
    if (-not (($system -Like '*Microsoft Windows Server 2022*') -or (
41
        $system -Like '*Microsoft Windows Server 2019*') -or ($system
        -Like '*Microsoft Windows Server 2016*')))
42
    {
43
44
        Write-Host("This is not a supported server platform.
            Installation aborted.")
45
        Exit
46
     }
47
48
```

```
# Start to install Windows feature
49
    Import-Module ServerManager
51
    AddFeatures('Web-Asp-Net45') #ASP.NET 4.5
52
    AddFeatures('Web-Mgmt-Console') #IIS Management Console
53
54
    AddFeatures('Web-Windows-Auth') # Windows Authentication
55
    AddFeatures('Web-Metabase') #IIS 6 Metabase Compatibility
    AddFeatures('Web-WMI') #IIS 6 WMI Compatibility
57
    AddFeatures('Web-Lgcy-Scripting')#IIS 6 Scripting Tools
58
    AddFeatures('Web-Lgcy-Mgmt-Console') #IIS 6 Management Console
59
    AddFeatures('MSMQ-HTTP-Support') #MSMQ HTTP Support
    AddFeatures('web-websockets') #IIS Web Sockets
61
    AddFeatures('NET-WCF-HTTP-Activation45') #http activate
    <!--NeedCopy-->
```

InstallPrereqsforSessionRecordingAgent.ps1

```
1
    <#
2
    .Synopsis
3
        Installs Prereqs for Session Recording Agent
4
    .Description
5
        Supports Windows Server 2022, Windows Server 2019, Windows
            Server 2016, windows 11, and Windows 10.
6
        Install below windows feature on this machine:
        -Microsoft Message Queuing (MSMQ), with Active Directory
7
            integration disabled, and MSMQ HTTP support enabled.
    #>
8
    function AddFeatures($featurename)
9
10
    ſ
11
        try
13
        {
14
15
             $feature=Get-WindowsFeature | ? {
    $_.DisplayName -eq $featurename -or $_.Name -eq $featurename }
16
17
             Add-WindowsFeature $feature
18
19
         }
20
21
        catch
22
        {
23
            Write-Host "Addition of Windows feature $featurename
24
                failed"
25
             Exit 1
26
         }
27
28
        Write-Host "Addition of Windows feature $featurename
            succeeded"
29
     }
31
    # Start to install Windows feature
```

```
$system= gwmi win32_operatingSystem | select name
34
    if (-not (($system -Like '*Microsoft Windows Server 2022*') -or (
        $system -Like '*Microsoft Windows Server 2019*') -or ($system
        -Like '*Microsoft Windows Server 2016*') -or ($system -Like '*
        Microsoft Windows 11*') -or ($system -Like '*Microsoft Windows
         10*')))
    {
37
        Write-Host("This is not a supported platform. Installation
            aborted.")
        Exit
     }
40
41
42
43
    if ($system -Like '*Microsoft Windows Server*')
44
    {
45
46
        Import-Module ServerManager
        AddFeatures('MSMQ') #Message Queuing
47
48
        AddFeatures('MSMQ-HTTP-Support')#MSMQ HTTP Support
     }
49
51
    else
52
    {
53
54
        try
55
        {
56
             dism /online /enable-feature /featurename:MSMQ-HTTP /all
         }
59
        catch
61
        {
62
63
            Write-Host "Addition of Windows feature MSMQ HTTP Support
                 failed"
64
             Exit 1
65
         }
        write-Host "Addition of Windows feature MSMQ HTTP Support
67
            succeeded"
     }
    <!--NeedCopy-->
```

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.



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
2 <!--NeedCopy-->
```

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 the Session Recording administration components

Note:

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

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

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

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

Note:

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

- 1. Install Microsoft OLE DB Driver for SQL Server.
- Under the HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4
 .0.30319 registry key, add the SchUseStrongCrypto DWORD (32-bit) value and set
 the value data to 1.
- 3. Restart Windows Server 2016.
- 1. Install Broker_PowerShellSnapIn_x64.msi.

Important:

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

- 2. Start the Windows command prompt as an administrator, and then run the msiexec /i SessionRecordingAdministrationx64.msi command or double-click the .msi file.
- 3. On the installation UI, click **Next** and accept the license agreement.
- 4. On the **Session Recording Administration Setup** screen, select the Session Recording administration components you want to install.

👷 Citrix Session Recording Administration Setup	- 🗆 X
Select Features Please select which features you would like to install.	citrix
🗇 🥽 – Cossian Decembra Server	Bession Recording Database
drive.	eature will be installed on the local hard eature requires 12MB on your hard drive.
< >	
Current location: C:\Program Files\Citrix\SessionRecording\Database\	Browse
Disk Cost Reset <	Back Next > Cancel

Note:

Installing all Session Recording administration components on a single server is fine for a proof of concept. However, for a large production environment, we recommend that you install the Session Recording policy console on a separate server and the Session Recording server, Session Recording Administrator Logging, and Session Recording database on another separate server. 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.

Install the Session Recording database

Note:

• The Session Recording database isn't an actual database. It's a component for creating and configuring the required databases in the Microsoft SQL Server instance. Session Recording

supports three solutions for database high availability based on the Microsoft SQL Server. For more information, see Database high availability.

• You can deploy the Session Recording database on Azure SQL Managed Instance, on SQL Server on Azure Virtual Machines (VMs), and on AWS RDS. For more information, see Deploy the Session Recording database on Azure SQL Managed Instance or on AWS RDS and Deploy the Session Recording database on SQL Server on Azure VMs.

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

- Deployment 1: Install the Session Recording server and Session Recording database on the same machine and the Microsoft SQL Server on a remote machine. (**Recommended**)
- Deployment 2: Install the Session Recording server, Session Recording database, and Microsoft SQL Server on the same machine.
- Deployment 3: Install the Session Recording server on a machine and install both the Session Recording database and Microsoft SQL Server on another machine. (**Not recommended**)
- 1. On the **Database and Server Configuration** page, specify the instance name and database name of the Session Recording database and the computer account of the Session Recording server. Click **Next**.
 - Instance name: If the database instance isn't a named instance, you can use only the computer name of the SQL Server. If you've named the instance, use computer-name\instancename as the database instance name. To determine the server instance name that you're using, run **select @@servername** on the SQL Server. The return value is the exact database instance name. If your SQL server listens on a custom port other than the default port 1433, set the custom listener port by appending a comma to the instance name. For example, type **DXSBC-SRD-1,2433** in the **Instance name** text box, where 2433, following the comma, denotes the custom listener port.
 - **Database name**: Type a custom database name in the **Database name** text box or use the default database name preset in the text box. Click **Test connection** to test the connectivity to the SQL Server instance and the validity of the database name.

Important:

A custom database name must consist of only A-Z, a-z, 0–9, and underscores, and can't exceed 123 characters.

- You must have the **securityadmin** and **dbcreator** server role permissions of the database. If you do not have the permissions, you can:
 - * Ask the database administrator to assign the permissions for the installation. After the installation completes, the **securityadmin** and **dbcreator** server role permissions are no longer necessary and can be safely removed.

* Or, during the msi installation, a dialog box prompts for the credentials of a database administrator with the **securityadmin** and **dbcreator** server role permissions. Type the correct credentials and then click **OK** to continue the installation.

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

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

Note:

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

2. Follow the instructions to complete the installation.

Install the Session Recording server

1. Select Session Recording Server and Session Recording Administrator Logging.

Note:

- The Session Recording Administrator Logging is an optional subfeature of the Session Recording server. Select the Session Recording server before you can select the Session Recording Administrator Logging.
- We recommend that you install the Session Recording Administrator Logging together with the Session Recording server at the same time. If you don't want the Administrator Logging feature to be enabled, you can disable it on a later page.
- 2. On the Database and Server Configuration page, specify the settings.
 - Instance name: Type the name of your SQL Server in the Instance name text box. If you're using a named instance, type computer-name\instance-name; otherwise, type computer-name only. If your SQL server listens on a custom port other than the default port 1433, set

the custom listener port by appending a comma to the instance name. For example, type **DXSBC-SRD-1,2433** in the **Instance name** text box, where 2433, following the comma, denotes the custom listener port.

- Database name: Type a custom database name in the Database name text box or use the default database name CitrixSessionRecording that is preset in the text box.
 You must have the securityadmin and dbcreator server role permissions of the database.
 If you do not have the permissions, you can:
 - Ask the database administrator to assign the permissions for the installation. After the installation completes, the **securityadmin** and **dbcreator** server role permissions are no longer necessary and can be safely removed.
 - Or, during the msi installation, a dialog box prompts for the credentials of a database administrator with the **securityadmin** and **dbcreator** server role permissions. Type the correct credentials and then click **OK** to continue the installation.
- After typing the correct instance name and database name, click **Test connection** to test the connectivity to the Session Recording database.
- Type the Session Recording server computer account, and then click **Next**.
- 3. On the **Administration Logging Configuration** page, specify configurations for the Administration Logging feature.
 - Logging database is installed on the SQL Server instance: This text box isn't 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.
 - Logging database name: 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.

- Use default database name: Selecting this option uses the default logging database name.
- **Enable Logging service**: 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.
- 4. Click **Next** and complete the installation.

Note:

The Session Recording server default installation uses HTTPS/TLS to secure communications. If TLS isn't 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. Navigate to the Session Recording Broker site, open the SSL settings, and clear the **Require SSL** check box.

Install the Session Recording agent

Install the Session Recording agent on the VDA or VDI machine on which you want to record sessions.

- On the Session Recording Agent Configuration page: If you've installed the Session Recording server in advance, type the computer name of the machine where you installed the Session Recording server. Type the protocol and port information for the connection to the Session Recording server. If you haven't installed Session Recording yet, you can change such information later in Session Recording Agent Properties.
- 2. Follow the instructions to complete the installation.

Note:

When Machine Creation Services (MCS) or Citrix Provisioning Services (PVS) creates VDAs with the Microsoft Message Queuing (MSMQ) installed, those VDAs can have the same QMId under certain conditions. This case might cause various issues, for example:

- Sessions might not be recorded even if the recording agreement is accepted.
- The Session Recording server might not receive session logoff signals and as a result, 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 for single-session OS VDAs that are created using PVS 7.7 or later and MCS 7.9 or later in the static desktop mode.

For multi-session OS VDAs created using MCS or PVS and single-session OS VDAs 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 make sure enough VDAs are running before user logon.

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

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

1 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.

1 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
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 $depServices = Get-Service -name MSMQ -dependentservices | Select -
      Property Name
10
11 # Restart MSMQ to get a new QMId
13 Restart-Service -force MSMQ
14
15 # Start dependent services
16
17 if ($depServices -ne $null) {
18
19
       foreach ($depService in $depServices) {
21
```

```
$startMode = Get-WmiObject win32_service -filter "NAME = '$
23
       ($depService.Name)'" | Select -Property StartMode
24
25
            if ($startMode.StartMode -eq "Auto") {
26
27
28
                Start-Service $depService.Name
29
             }
31
    }
32
34
    }
35
36 <!--NeedCopy-->
```

Install the Session Recording player and the web player

Install the Session Recording player on the Session Recording server or on workstations in the domain. Install the web player on the Session Recording server only.

Double-click SessionRecordingPlayer.msi and SessionRecordingWebPlayer.msi and follow the instructions to complete the installation.

Automate installation

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

Automate installation of the Session Recording administration components

Install the complete set of the Session Recording administration components by using a singlecommand For example, either of the following commands installs the complete set of the SessionRecording 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"
2 <!--NeedCopy-->
```

```
1 msiexec /i "SessionRecordingAdministrationx64.msi" ADDLOCAL="
    SsRecServer,PolicyConsole,SsRecLogging,StorageDatabase"
    DATABASEINSTANCE="CloudSQL" DATABASENAME="CitrixSessionRecording"
```

```
LOGGINGDATABASENAME="CitrixSessionRecordingLogging"
AZURESQLSERVICESUPPORT="1" AZUREUSERNAME="CloudSQLAdminName"
AZUREPASSWORD="CloudSQLAdminPassword" /q /l*vx "c:\WithLogging.log"
2 <!--NeedCopy-->
```

Note:

```
The SessionRecordingAdministrationx64.msi file is located on the Citrix Virtual Apps and Desktops ISO under \layout\image-full\x64\Session Recording.
```

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-sqlsupport.public.ca7b16b60789.database.windows.net,3342 if you're using Azure SQL Managed Instance.
- DATABASENAME is the database name of the Session Recording database.
- LOGGINGDATABASENAME is the name of the Administrator Logging database.
- **AZURESQLSERVICESUPPORT** determines whether cloud SQL is supported. To use cloud SQL, set it to 1.
- **DATABASEUSER** is the computer account of the Session Recording server.
- AZUREUSERNAME is the cloud SQL admin name.
- AZUREPASSWORD is the cloud SQL admin password.
- /q specifies quiet mode.
- /l*v specifies verbose logging.
- yourinstallationlog is the location of your installation log file.

Create a master image for deploying the Session Recording server You might already have the Session Recording database and the Administration Logging database in place from an existing deployment. For such scenarios, you can now forego database checks when you're 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 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 eases 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"
2 <!--NeedCopy-->
```

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're 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
4 <!--NeedCopy-->
```

The commands connect the Session Recording server installed earlier to an existing Session Recording database and Administration Logging database.

The SsRecUtils.exe file is stored in \Citrix\SessionRecording\Server\bin\. Set the **DATABASEINSTANCE**, **DATABASENAME**, and **LOGGINGDATABASENAME** parameters as needed.

Keep databases when uninstalling the Session Recording administration components With **KEEPDB** set to **True**, the following command keeps the Session Recording database and the Administration Logging database when uninstalling the Session Recording administration components:

```
1 msiexec /x "SessionRecordingAdministrationx64.msi" KEEPDB="True"
2 <!--NeedCopy-->
```

Automate installation of the Session Recording player and web player

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

Note:

The SessionRecordingPlayer.msi file is located on the Citrix Virtual Apps and Desktops ISO under \layout\image-full\x86\Session Recording.

The SessionRecordingWebPlayer.msi file is located on the Citrix Virtual Apps and Desktops ISO under \layout\image-full\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
3 <!--NeedCopy-->
```

Note:

The SessionRecordingAgentx64.msi file is located on the Citrix Virtual Apps and Desktops ISO under \layout\image-full\x64\Session Recording.

Where:

- yourservername is the NetBIOS name or FQDN of the machine hosting the Session Recording server. If not specified, this value defaults to localhost.
- **yourbrokerprotocol** is HTTP or HTTPS that the Session Recording agent uses to communicate with the Session Recording Broker. If not specified, this value defaults to HTTPS.
- **yourbrokerport** is the port number that the Session Recording agent uses to communicate with the Session Recording Broker. If not specified, this value defaults to zero, which directs the Session Recording agent to use the default port number for your selected protocol: 80 for HTTP or 443 for HTTPS.

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

Upgrade Session Recording

You can upgrade certain deployments to later versions without having to first set up new machines or sites. You can upgrade from the latest CU of Session Recording 7.15 LTSR, and from any later version, to the latest version of Session Recording.

Note:

When you upgrade Session Recording administration from 7.6 to 7.13 or later and choose **Modify** 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 can't upgrade from a Technical Preview version.

Requirements, preparation, and limitations

- Use the Session Recording installer's graphical interface or command line to upgrade the Session Recording 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 identified after the database upgrade.
- In addition to being a domain user, you must be a local administrator on the machines where you're 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 file 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.

- Session Recording agent 7.6.0 and later are compatible with the latest version of Session Recording server. However, some new features and bug fixes might not take effect.
- Any sessions started during the upgrade of a Session Recording server aren't 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 isn't installed after you upgrade Session Recording from a previous version 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's little chance that the recording can be complete.
- Review the following upgrade sequence, so that you can plan and mitigate potential outages.

Upgrade sequence

- 1. When the Session Recording database and Session Recording server are installed on different servers, stop the Session Recording Storage Manager service manually on the Session Recording server. Then upgrade the Session Recording database first.
- 2. Through the Internet Information Services (IIS) Manager, make sure that the Session Recording Broker is running. Upgrade the Session Recording server. If the Session Recording database and Session Recording server are installed on the same server, the Session Recording Database is also upgraded.
- 3. The Session Recording service is back online automatically when the upgrade of the Session Recording server is completed.
- 4. Upgrade the Session Recording agent (on the master image).
- 5. Upgrade the Session Recording policy console with or after the Session Recording server.
- 6. Upgrade the Session Recording player.

Deploy the Session Recording database on cloud SQL database services

This section describes how to deploy the Session Recording database on Azure SQL Managed Instance, on AWS RDS, and on SQL Server on Azure VMs.

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

Tip:

You can also run a single command similar to the following to deploy the Session Recording database on Azure SQL Managed Instance or on AWS RDS. For more information, see the preceding Automate installation section in this article.

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

- 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, marketpla
Amazon RDS \times	
Dashboard	Connectivity & security Monitoring Logs & events Configu
Databases	
Query Editor	Connectivity & security
Performance Insights	
Snapshots	Endpoint & port
Automated backups	Endpoint
Reserved instances	database-2.ccjfaeoogg0g.us-east-2.rds.amazonaws.com
Proxies	Port
Subnet groups	1433
Parameter groups	
Option groups	
Events	
Event subscriptions	
Recommendations	
Certificate update	
	Security group rules (2)
	, 3.oup
	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 cloud SQL** check box and fill in the cloud SQL admin name and password. Make other required configurations.

🖟 Citrix Session Reco	ording Administration Setup		-		×
Database and Serve	r Configuration			citr	ιż
	e name and database name of the Se f the Session Recording Server.	ssion Recording	Databa	se and the	
<u>I</u> nstance name	Example: .\SQLEXPRESS,computer-name tcp:xxxx.database.windows.net,3342	\SQLEXPRESS, co	mputer-na	me,	
<u>D</u> atabase name	Use default database name				
<u>C</u> loud SQL admin name					
<u>C</u> loud SQL admin password]
Session Recording Server computer account	Example: localhost, domain\computer-nam	e			
	< Ba	ck Next	>	Cance	el

Note:

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

Azure AD authentication isn't supported.

🐴 Session	Recording Se	rver Pro	perties			_		×
Playback	Notifications	CEIP	Logging	RBAC	Email	Cloud	DB	We 💶
	QL Managed Ir tion allows you			QL.				
🗹 Ena	ble cloud SQL							
Cloud	d SQL admin	srtsqsl	admin					
Cloud	d SQL admin word:	•••••						
			0	K	Can	cel		Apply

Migrate an on-premises database to cloud SQL Managed Instance

- 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.

Deploy the Session Recording database on SQL Server on Azure VMs

On SQL Server on Azure VMs, you can deploy the Session Recording database.

- 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: When you're using SessionRecordingAdministrationx64.msi for the installation, clear the **Enable cloud SQL** check box.

4. Follow instructions to complete the installation.

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 isn't 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.

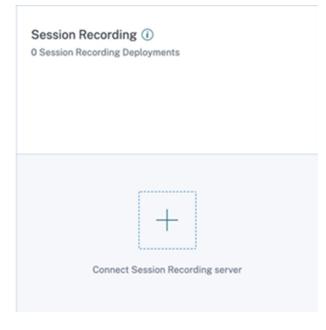
Prerequisites

Before you begin, meet the following prerequisites:

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

Connect your Session Recording server to Citrix Analytics for Security

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



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

Connect Sess	ion Recording Server	×
Configure and	connect your Session Recording server to Citrix Analytics.	
1	Prerequisites What is your Session Recording version? Image: Can your Session Recording server connect to the following addresses? Session recording server should meet service connectivity requirements Session recording server should have connectivity to https://api.analytics.cloud.com 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.

The configuration file is located at <Session Recording server installation path>\bin\SsRecStorageManager.exe.config

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

🔚 SsRe	cStorageManager exe.config E3							
1	xml version="1.0" encoding="utf-8"?							
2	<pre>G<configuration></configuration></pre>							
3	<pre><startup uselegacyv2runtimeactivationpolicy="true"></startup></pre>							
4	<supportedruntime version="v4.0.30319"></supportedruntime>							
5	<supportedruntime version="v2.0.50727"></supportedruntime>							
6	-							
7	<pre>cappSettings></pre>							
8	<pre>- </pre>							
9	c <system.net></system.net>							
10	<pre>cmailSettings></pre>							
11	<pre>classes com > classes class</pre>							
12	<pre><network <="" host="your.smtp.server" password="yourpase" port="587" pre="" username="yourEmail@address.com"></network></pre>	word"						
	enableSsl="true"/>							
13	-							
14	<pre></pre>							
15	<pre>cdefaultProxy enabled="true"></pre>							
16	<pre><pre>cypassonlocal="True"/></pre></pre>							
17	-							
18	<pre>- </pre>							
19	Q <runtime></runtime>							
20	<pre><generatepublisherevidence enabled="false"></generatepublisherevidence></pre>							
21	-							
22	L							
23								

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.

If there're more than one Session Recording server in your deployment, you must copy the file to each server that you want to connect and follow the steps to configure each server.

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

For example:

```
1 C:\Program Files\Citrix\SessionRecording\Server\bin\ SsRecUtils.
exe -Import_SRCasConfigurations C:\Users\administrator \
Downloads\SessionRecordingConfigurationFile.json
2 <!--NeedCopy-->
```

- 10. Restart the following services:
 - Citrix Session Recording Analytics Service
 - Citrix Session Recording Storage Manager
- 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're 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 isn't applicable for Session Recording server version 2106 and later.

View the connected deployments

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

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

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

← Con	nected Sessior	n Recording De	ployments						
	Session recording se	rvers							
	 Session Record 	ding deployment							:
	The Session red	cording server is success	fully configured and connected	1.					
	BASE URL		SESSION RECORDING DEPLOYMENT		CONFIGURATION STATUS		LAST UPDATED		
	Site-2-v2103.sm	narttools.clm	No.071 101 804 415 4114		Success		Sep 21 2021 11:26 AM		
					Showing 1-1 of 1 items	Pa	ge 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've 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 hasn't 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 Sessi	on Recording Deployments					
	Session recording servers V 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 0 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 Session Recording Deployments

\sim	Session Recording deployment					
	The Session recording server is s	ucces	sfully configured and connected.		Remove Session recording s	server from Analytic
	BASE URL		SESSION RECORDING DEPLOYMENT	CONFIGURATION STATUS	 LAST UPDATED 	
	Session-Recording-Server-		NAMES AND ADDRESS OF A DATABASE.	Success	Nov 13 2021 1:02 AM	
				Showing 1-1 of 1 items	Page 1 of 1 < >	5 rows 🗸

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

```
1 <Session Recording server installation path>\bin\SsRecUtils.exe -
Remove_SRCasConfigurations
2 <!--NeedCopy-->
```

For example:

```
1 C:\Program Files\Citrix\SessionRecording\Server\bin\ SsRecUtils.
exe -Remove_SRCasConfigurations
2 <!--NeedCopy-->
```

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. As a result, 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 <!--NeedCopy-->
```

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

Registry name	Registry path	Key type	Value
AuditorUniqueID	Computer\ HKEY_LOCAL_MACHIN \SOFTWARE\ Citrix\ SmartAuditor\ Server\	String NE	Enter your UUID.
EnableCASUseAudi	to CompigtetD HKEY_LOCAL_MACHIN /SOFTWARE/ Citrix/ SmartAuditor/ Server/	REG_DWORD	1

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

Dynamic session recording

June 22, 2022

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

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

Note:

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

Enable or disable dynamic session recording

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

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

- 1. After the Session Recording installation is complete, log on as an administrator to the machine where you installed the Session Recording agent.
- 2. Open the Registry Editor.
- 3. Browse to HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor.
- 4. Set the value of DynamicControlAllowed to 0 or use the default value, 1.
 1: enable dynamic recording
 0: disable dynamic recording
- 5. Restart the Session Recording agent to make your setting take effect. If you are using MCS or PVS for deployment, change the setting on your master image and perform an update to make your change take effect.

Warning:

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

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

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

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

Delivery Group or Machine Name Queries Create Query Site Address: Citrix Cloud Controller Enter a site address Delivery Groups Machines	\times
🖳 Create Query X]
Site Address: Citrix Cloud Controller	
Enter a site address	
Delivery Groups O 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. For more information, run Get-			
	Help Start-BrokerSessionRecording			
	to see the command online help.			
Stop-BrokerSessionRecording	Lets you stop recording a specific active session,			
	a list of active sessions, or sessions launched by			
	a specific user. For more information, run Get-			
	Help Stop-BrokerSessionRecording			
	to see the command online help.			
Get-BrokerSessionRecordingStatus	Lets you get the recording status of a specific			
	active session. For more information, run			
	Get-Help Get-			
	BrokerSessionRecordingStatus to see			
	the command online help.			

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

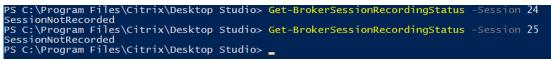
1. (For Citrix Virtual Apps and Desktops PowerShell SDK only) Launch PowerShell from the Citrix Studio console.

Console Root	a farmer and a second se	Actions
 Citrix Studio (BVT_DB) Search 	citrix	Citrix Studio (BVT_DB)
Machine Catalogs	Common Taxis Actions PowerShell	View +
AppDisks	# Register the certificate for the Licensing Service	* Refresh
Applications	# 4/9/2018 2:31 AM	Pielp
Policies	# Get-JonNite -AdminAddreas Twkson-ddn-1.but.inosi:#07 -RearerToken *******	
 Configuration Administrators 	Start-LopHighLevelOperation -MdminAddress "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"	
Controllers Hosting	Set-ConflySiteMetedata -AdminAddress "wksoe-ddo-1.bvt.looal:80" -BearerToken ****** -LogpingId "of62600e-e2ef-4164-9eb6-00225324d85" -Name "OrrtificateMash" -Value "skiGqiyuBu48160EqTaxgANoDpoSTOTF+kKEZEMISeDgB86M857200e0hilmUCof+cG816DyJBxt5/S01d10-+	-
Licensing StoreFront App-V Publishing AppDNA	Stop-Confident Devention - Anniaddream 'Wine-do-Llow.lookis' -SearerTokes ****** -EndTime "4/9/2015 6:31:19 NM" -HiphlevelOperation1d **ENDEV-Ent-Al-Net-Office/1012024055 -Inforcement1 fTree 5 Stops Completed mercentally	
Zones		
44 Citra StoreFront	# Get the certificate for the Licensing Service #	
	# 4/9/2018 2:31 AM	
	Get-LicCertificate -kLminAddrews "https://wkase-ddc-1.kvt.local:8085/" # Script completed successfully	
	Get the certificate for the Licensing Service	
	4/9/2018 9:49 TM	
	<pre>det-lioCertificate =Adminkdress "https://wkace-ddo-1.kvt.local:8085/" # Script completed successfully</pre>	
	* . Get the certificate for the Licensing Service	
	we the destillate for the licensing period	
	Get-lioGertificate -AdminAddress "https://Wkace-ddo-1.bvt.local:8083/" # Fortific.completed successfully	
	Get the certificate for the Licensing Service	
	\$ 4/9/2018 10:06 PM	
	* Ger-LioCerrificate -AdminAddress "https://wkace-ddc-1.bvt.local:8083/* # Script completed successfully	
	Laurch PowerSite	ă)

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

2 Select Administrator C:\Windows/System32\WindowsPowerShell\v1.0\Powershell.ee - X
PS C:\Program Files\Citrix\Desktop Studio> \$sessions_get=brokersession -username WKAOE\testuser6
PS C:\Program Files\Citrix\Desktop Studio> \$sessions.sessionstate
Active
Active
PS C:\Program Files\Citrix\Desktop Studio> \$sessions.sessiontype
Desktop
Application
PS C:\Program Files\Citrix\Desktop Studio> \$sessions.OStype
Windows 2016
PS C:\Program Files\Citrix\Desktop Studio> _______

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



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.

🔿 🖄 🖬 👔 🖬								_
Console Root						Acti	0.05	-
Citrix Studio (dDDC3)			Last 7 days	~ Search	Q	Log		
Search Machine Catalogs	Administrator	Main Task	Start 1	End	Status		Preferences	
Delivery Groups	▼ Today						Create Cust	
Applications	APRQ\qh	Stop Recording of Session '5DAE93E5-E14E	8/20/2020 : 3:56:13	8/20/2020 : 3:56:13	Successful	8	Delete Logs	
Policies	APRQ\qh	Stop Recording of Session '4DD677B7-DDE	8/20/2020 : 3:56:09	8/20/2020 : 3:56:09	Successful		View	
Logging Configuration	APRQ\qh	Start Recording of Session '5DAE93E5-E14E	8/20/2020 : 3:56:05	8/20/2020 : 3:56:05	Successful			
Administrators	APRQ\qh	Start Recording of Session '4DD677B7-DDE	8/20/2020 : 3:56:02	8/20/2020 : 3:56:02	Successful	-	Refresh	
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			
a Licensing	APRQ\qh	Create Machine 'Styx_VDA1_1' in Delivery G	8/20/2020 : 1:22:55	8/20/2020 : 1:22:55	Successful			
StoreFront	APRQ\qh	Create Delivery Group 'Styx_VDA1'	8/20/2020 : 1:22:54	8/20/2020 : 1:22:55	Successful			
👍 App-V Publishir Q Zones	APRQ\qh	Create Machine Catalog 'Styx_VDA1'	8/20/2020 : 1:22:24	8/20/2020 : 1:22:24	Successful			
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			
	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 22, 2022

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

- Settings on the Session Recording agent
 - Enable or disable recording
 - Configure the connection to the Session Recording Server
 - Configure the communication protocol
- Settings on the Session Recording server
 - Authorize users
 - Customize notification messages
 - Specify where recordings are stored
 - Specify file size for recordings
 - Enable or disable digital signing
 - Configure CEIP
- 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 22, 2022

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

June 22, 2022

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

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

Enable or disable recording on a VDA

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

Note:

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

Enable custom event recording

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

For example, an event might contain the following text: "User opened a browser."Each time a user opens a browser during a session being recorded, the text inserts to the recording at that point. When a viewer plays back the recorded session, the viewer can locate and count the times that the user opened a browser by noting the number of markers.

To insert custom events to recordings on a server:

• Use **Session Recording Agent Properties** to enable a setting on each server where you want to insert custom events. Enable each server separately. You can't globally enable all servers in a site.

• Write applications built on the Event API that runs within each user's Citrix Virtual Apps and Desktops or Citrix DaaS (formerly Citrix Virtual Apps and Desktops service) 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, do the following:

- 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.

Configure the connection to the Session Recording server

June 22, 2022

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 22, 2022

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 22, 2022

This section guides you through the following settings:

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

Authorize users

June 22, 2022

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.
- **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.

Customize notification messages

March 20, 2024

If the active recording policy records sessions with notification, users receive recording notifications after typing credentials. The default notification message is **Your activity with the desktop or program(s) you recently started is being recorded. If you object to this condition, close the desktop or program(s).** Users can click **OK** to dismiss the window and continue their sessions.

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

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

Create a notification message

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

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

Specify where recordings are stored

April 3, 2023

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

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

Note:

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

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

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

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

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

5. In the **Restore directory for archived files** field, type your folder for restoring archived recordings.

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

🐴 Sessio	n Record	ing Server	Properties	;	_		×
Storage	Signing	Rollover	Playback	Notifications	CEIP	Logging	RE • •
	ad-balanc			he directories ultiple directo			
Filest	orage dire	ctories:					_
	The defau	List of fo It folder C:		pty. cordings will	be	Add. Modify	
			used.			Remo	ve
them a	vailable f	or playbac	k.	rchived sessi	ion record	lings and n	nake
		y for archi ordingsRest				Brows	
				ОК	Cancel		Apply

Configure an Azure file share to store recordings

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

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

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

Recording File Size MB/hour	Session Quantity	File Share Type	File Share Quota (TB)	Session Recording Server Quantity	Session Recording Server Size
< 6.37	< 1,000	HDD Standard (StorageV2)	2	1	Standard D4as_v4
< 6.37	1,000–2,000	SSD Premium	3	1	Standard D4as_v4
< 6.37	2,000–3,000	SSD Premium	5	1	Standard D4as_v4
< 6.37	3,000–4,000	SSD Premium	6	1	Standard D4as_v4
Approx.10	< 1,000	HDD Standard (StorageV2)	3	1	Standard D4as_v4
Approx.10	1,000–2,500	SSD Premium	6	1	Standard D4as_v4
Approx.10	2,500–4,000	SSD Premium	10	2	Standard D4as_v4

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

- 2. Add the Azure file share credentials to the host where you installed the Session Recording server.
 - a) Start a command prompt as an administrator and change the drive to the **<Session Recording Server installation path>\Bin** folder.

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

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

Where,

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

There are two ways to obtain your storage account key:

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

🛁 sessionrecordings		Connect ×
SMB File share		-
	Ø Connect ↑ Upload + Add directory	Secure transfer required' is enabled on the storage account. SMB clients connecting to this share must support SMB protocol version 3 or higher in order to handle the encryption
Cverview	Search files by prefix	requirement. Click here to learn more.
Access Control (IAM)	Name	
Settings	No files found.	Windows Linux macOS
Properties		To connect to this Azure file share from Windows, choose from the following authentication methods and run the PowerShell commands from a normal (not elevated)
Operations		PowerShell terminal:
역 Snapshots		Drive letter
🚰 Backup		
Monitoring		Authentication method Active Directory
Métrics		Storage account key
		Connecting to a share using the storage account key is only appropriate for admin access. Utilizing Active Directory allows to differentiate file and folder access, per AD account, within a share. Learn more
		<pre>\$connectTestResult = Test-NetConnection -ComputerName srcmdstg.file.core.windows.net -Port 445 if (sconnectTestResult.TcpTestSucceeded) (</pre>
		This script will check to see if this storage account is accessible via TCP port 445, which is the port SMB uses. If port 445 is available, your Azure file share will be persistently mounted. Your organization or internet service provider (JSP) may block port 445, however you may use Azure Point-to-Sife (PS) VPA. JAzure Site-to-Site (SS) VPN, or ExpressRoute to tunnel SMB traffic to your Azure file share over a different port. Learn how to circumvent the port 445 problem (VPN)

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

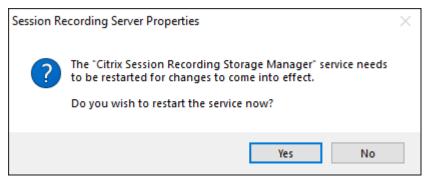
■ Microsoft Azure	P Search resources, services, and docs (G+/)
Home > srcmd >	
<pre></pre>	eys
	Use access keys to authenticate your applications when making requests to this Azure storage account. Store your access keys so that you can maintain connections using one key while regenerating the other.
Cverview	When you regenerate your access keys, you must update any Azure resources and applications that access this storage acc
Activity log	
🗳 Tags	Storage account name srcmdstg
Diagnose and solve problems	
Access Control (IAM)	Hide keys
💕 Data migration	key1 🗘
🚡 Storage Explorer (preview)	
Settings	DSjcn/SOpzwPxhckjTgGZUZtolh8A3PA0H8W0e+J9kuid6p7xX11eqNMu0Xkx7R352f2GHRFU2PllFi11vbE/A==
Access keys	Connection string DefaultEndpointsProtocol=https;AccountName=;AccountKey=DSjcn/SOpzwPxhckjTgGZUZtolh8A3PA0H8W0e+.
S CORS	
Configuration	key2 🗘
Encryption	Key O97VNcAmv+WpgFYYO6r3OfMyaD20sSGGpJuBgfkDYv3Z27j19TYOMbWFaz1N6riO81c2qF5JZOQVxqydmysO2A==
 Shared access signature 	
	Connection string DefaultEndpointsProtocol=https;AccountName=;AccountKey=O97VNcAmv+WpqFYYO6r3OfMyaD20sSGGpJuBi
Networking	ревынствропосно-теродесовликате-
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.

torage				Notifications									
	d-balanc			ne directories ultiple directo									
File sto	orage dire	ctories:											
		List of fo	lders is em	ptv.		Add							
Т	he defau	It folder C:	SessionRe used.	cordings will	be	Modify		File	e Storage	Directory			
						Remov	'e	E	Enter a dir	rectory for	storing recor	ded session files:	
									unt.file.co	e.windows	.net\sessionre	ecording\recordings	Browse
												OK	Cance
them a	vailable fo	or playbac	k.	chived sessi	on recordi	ngs and m	ake					ОК	Cance
Restore	vailable fo e director	to tempora or playbac y for archi ordingsRest	k. ved files:	chived sessi	on recordi	ngs and m Browse						OK	Cance
Restore	vailable fo e director	or playbac y for archi	k. ved files:	chived sessi	on recordi							OK	Cance
Restore	vailable fo e director	or playbac y for archi	k. ved files:	chived sessi	on recordii							ОК	Cance
Restore	vailable fo e director	or playbac y for archi	k. ved files:	chived sessi	on recordi							OK	Cance
Restore	vailable fo e director	or playbac y for archi	k. ved files:	chived sessi	on recordi							ОК	Cance
Restore	vailable fo e director	or playbac y for archi	k. ved files:	chived sessi	on recordi							OK	Cance
Restore	vailable fo e director	or playbac y for archi	k. ved files:	chived sessi	on recordi							OK	Cance
Restore	vailable fo e director	or playbac y for archi	k. ved files:	Chived sessi	Cancel	Browse						OK	Cance

- 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.



Specify file size for recordings

November 24, 2022

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	R[• •
before record not roll than 30	a new file ing durationed over if 00MB. File	is started on specifie the record	Files are r d, whicheve ling duration	num limit to wh olled over who er occurs first n is less than ver when the s	en the file , is reach 1 hour ar	e size or hed. Files a hd size is l	are ess
Files	size thres	hold (MB):			50		
Reco	rding dura	ation thres	hold (hours):	12		
				OK	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.

Enable or disable digital signing

June 22, 2022

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.

Configure Citrix Customer Experience Improvement Program (CEIP)

March 21, 2024

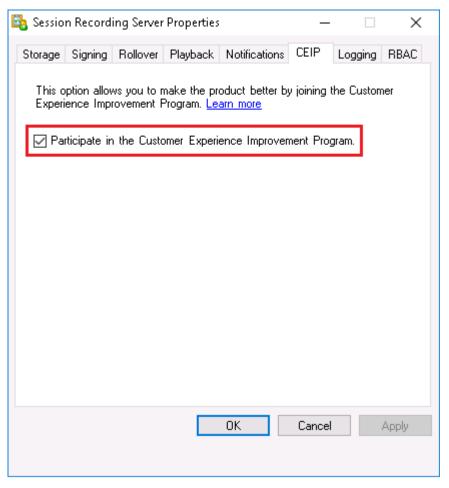
When you participate in the Citrix Customer Experience Improvement Program (CEIP), anonymous configuration and usage data is collected and sent to Citrix. The data helps improve the product quality and performance. In addition, a copy of the anonymous data is sent to Google Analytics for fast and efficient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

Settings

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 to make the setting take effect.



Google Analytics setting

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

Registry setting that enables or disables Google Analytics (default = 0):

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

Name: CeipHeartBeatDisable

Value: 1 = disabled, 0 = enabled

When unspecified, Google Analytics is enabled.

To disable Google Analytics:

- 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. Add a registry value and name it **CeipHeartBeatDisable**.
- 5. Set the value data of **CeipHeartBeatDisable** to 1.
- 6. Restart the Citrix Session Recording Analytics Service to make the setting take effect.

Data collected from the Session Recording server

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

Data Point	Key Name	Description
Machine GUID	machine_guid	Identifying the machine where the data originates. With Google Analytics enabled, heartbeat data is sent to Google Analytics regardless of whether CEIP is enabled.

Data Point	Key Name	Description
Operating System version	OS_version	Text string denoting the machine's operating system. With Google Analytics enabled, heartbeat data is sent to Google Analytics regardless of whether CEIP is enabled.
Session Recording server version	SRS_version	Text string denoting the installed version of the Session Recording server. 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.

Session Recording 2204

Data Point	Key Name	Description
Number of recordings	event-logging-	Integer denoting the number of
containing logged events	recording-number	recording files that contain
		logged events. The data is sent
		when both Google Analytics
		and CEIP are enabled.
Administrator logging	admin-logging-status	Digit indicating the
enablement		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-	Integer denoting the number of
	number	logged events. The data is sent
		when both Google Analytics
		and CEIP are enabled.
Number of custom policies	customized-policies-	Integer denoting the number of
	number	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	rbac-status	Digit indicating the enablement
enablement		of recording viewing policies.
		"1"means enabled. "0"means
		disabled. The data is sent when
		both Google Analytics and CEIP
		are enabled.

Policies

March 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 (\layout\image-full\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 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 you want to modify, right-click, and choose **Properties**. Use the **Rules** wizard to modify the rule.
 - Select the rule 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

June 22, 2022

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

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

System-defined recording policies

Session Recording provides the following system-defined recording policies:

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

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

Create a custom recording policy

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

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

For each rule, choose one recording action:

- **Enable session recording with notification**. This option records entire sessions (screens and events). Users receive recording notifications in advance.
- **Enable session recording without notification**. This option records entire sessions (screens and events). Users do not receive recording notifications.
- Enable event only session recording with notification. 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. 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.

Rules Wizard	×
Step 1: Select a recording option to specify if, and how, a session is recorded.	
O Enable session recording with notification	
O Enable session recording without notification	
C Enable event only session recording with notification	
O Enable event only session recording without notification	
Disable session recording	
	1
< Back Next >	Cancel

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

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

action of the rule applies. On the **Select IP Address and IP Range** screen, add a valid IP address or IP range for which recording is enabled or disabled. The IP addresses mentioned here are the IP addresses of the Citrix Workspace apps.

🕎 Rules Wizard		Х
Step 2: Select the rule criteria.		
Users or Groups		
Published Applications or Desktop		
Delivery Groups or Machines		
IP Address or IP Range		
1		1
Step 3: Edit the rule criteria.		
Selecting a rule criterion above activates the option here. To edit	t, click the underlined value.	
Users / Groups: All Users		
Published Resources: All Applications and Desktop		
Delivery Groups / Machines: All Delivery Groups and Machines IP Address / IP Range: All IP Addresses		
	< Back Next >	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 **Do not record** action have the highest priority.
- Rules with the Record with notification action have the second-to-highest priority.

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

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

To create a custom recording policy:

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

🖳 Rule	es Wizard	\times
Step	1: Select a recording option to specify if, and how, a session is recorded.	
OEr	nable session recording with notification	
	nable session recording without notification	
OEr	nable event only session recording with notification	
	nable event only session recording without notification	
💿 Di	sable session recording	
	< Back Next > Cancel	

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

🖢 Rules Wizard		×
Step 2: Select the rule criteria.		
Users or Groups		
Published Applications or Desktop		
Delivery Groups or Machines		
IP Address or IP Range		
		1
Step 3: Edit the rule criteria.		
Selecting a rule criterion above activates the option here. To edit	, click the underlined value.	
Users / Groups: All Users		
Published Resources: All Applications and Desktop		
Delivery Groups / Machines: All Delivery Groups and Machines IP Address / IP Range: All IP Addresses		
IF Address / IF Nange, All IF Addresses		
	< Back Next >	Cancel

6. Edit the rule criteria - To edit, click the underlined values. The values are underlined based on the criteria 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.

Step 2: Select the rule criteria. Users or Groups Published Applications or Desktop Delivery Groups or Machines IP Address or IP Range
 ✓ Published Applications or Desktop ✓ Delivery Groups or Machines ☐ IP Address or IP Range
Delivery Groups or Machines IP Address or IP Range
IP Address or IP Range
Step 3: Edit the rule criteria.
Selecting a rule criterion above activates the option here. To edit, click the underlined value.
Users / Groups: All Users
Published Resources: Select Published Applications or Desktop
Delivery Groups / Machines: <u>Select Delivery Groups or Machines</u> IP Address / IP Range: All IP Addresses
< Back Next > Cancel

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

Relivery 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		₽ 4 4 ⁰	0
 Identity and Access Management 			
Authentication Administrators API Access Domains			
To use this secure client in a sile	Secure Clients are used to interact w ent connector install or to access any of our AP Name your Socure Client	ith Citrix Cloud APIs. Is, use the customer ID	r.
Name			Actions

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 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 have reached the maximum size. For more information about the maximum file size for recordings, see Specify file size for recordings.

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

If the previous recording policy		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	Recording stops.
Record without notification	Record with notification	Recording continues and a notification message appears.
Record with notification	Do not record	Recording stops.

If the previous recording policy		After a rollover, the recording
was	And the new recording policy is	policy will be
Record with notification	Record without notification	Recording continues. No message appears the next time
		a user logs on.

Configure recording viewing policies

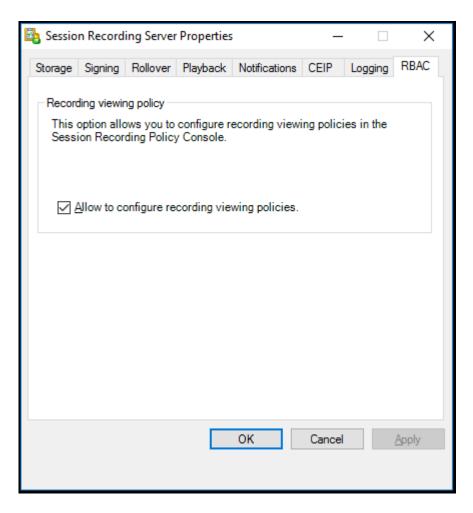
June 22, 2022

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 determines which user or group can view recordings that originate from other users and groups, published applications and desktops, and delivery groups and VDAs you specify.

Create a custom recording viewing policy

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

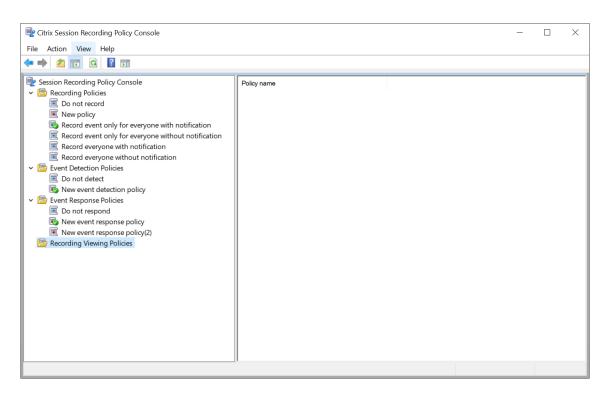
- 1. Log on to the machine hosting the Session Recording server.
- 2. From the Start menu, choose Session Recording Server Properties.
- 3. In Session Recording Server Properties, click the RBAC tab.
- 4. Select the Allow to configure recording viewing policies check box.



To create a custom recording viewing policy:

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

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



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

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

🖳 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	o who can view recordings				
				Add.	
	Select Users or Groups			×	
	Select this object type:				
	Users or Groups			Object Types	
	From this location:				
	AWDDC1-0001			Locations	
	Enter the object names to select (exam	nples):			
	AWDDC1-0001\Administrator;			Check Names	
	Advanced		OK	Carreel	
	Advanced		UK	Cancel	
		< 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

Session Recording 2204

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	
< Back Next > Cancel	ł

Note:

For recording viewing policies, 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	d					×
Complete the r	ule setup.					
Recording view						
AWDDC1-0001	Administrator					
<i>Rule criteria:</i> Users / Groups	Published Resources	Delivery Groups / Machir	nes			
Name	Location	1				
🔒 Administrato	or AWDDC	:1-0001				
			< Back	Next >	Finish	Cancel

Configure event detection policies

March 13, 2023

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

Events that can be detected

Session Recording detects target events and tags those events in recordings for later search and playback. You can search for events of interest from large amounts of recordings and locate those events during playback.

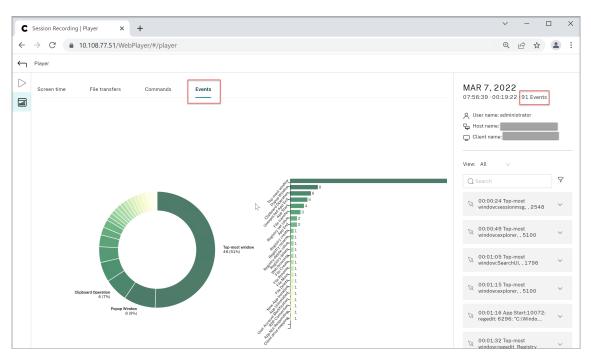
System-defined events

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

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

For example:

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



• Events in a screen recording in the web player:

C Session Recording Player ×	+	✓ - □ ×
← → C	layer/#/player	€ ☆ ≰ 🛔
← Player		
Image: Second secon	€ Ox12 arms	MAR 7, 2022 08:01:47:00:01:00:22 Events Set User name: Client name: Uiev: All Search
	If Process Disposing and Dis	00:00:12 Registry create:1904:C.Program Files:CL 00:00:12 Registry create:1904:C.Program Files:CL
a p o a é O b	Construction Don't miss what's happening Key in Sprug Propil in Nettors at the fact is boost	00:00:12 Registry ~ Files(CL ~ 00:00:12 Registry ~
► <2 00:00:07/	700-01:00 Comments Cf Share Current Playback X1 Show stats 55 FULL SCREEN	Create1304:C.Program Files/C 00:00:12 Registry create1304:C.Program Files/C

• Events in the Session Recording player:

ପ୍ରିକSession Recording Player File Edit View Play Tools Helo	
🔁 🕨 🛅 🗐 🗓 🖬 🚱 Search: 🔹 Anytime 🔽 👘 🕼 🔯 Advanced Search	
Workspace	
Now Playing	
Events and Bookmarks	
1:17:04 AM App Start: 10072: regedit: 6296: "C:\Windows\regedit.exe"	
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\SOFTWARE\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\SOFTWARE\regtest\name New Value #1	
1:18:36 AM Registry Delete Value: 10072: C:\Windows\regedit.exe: HKEY_LOCAL_MACHINE\SDFTWARE\regtest\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	
2 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	
11330 AM Unexpected App Exit: 6644: C:\Program Files\Google\Chrome\Application\chrome.exe: C:\Windows\System32\KERNELBASE.dll	
113:32 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: W/Shell, CtxDnDSourceProxy, 7260	
1:19:53 AM Top-most window: explorer, , 5100	
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	
1:20:52 AM File Hename: 5100: C::Windows\New Text Document.(2).81 [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, 1:21:09 AM Clipboard Operation: File, explorer, C:\Windows\document.txt,	
121:09 AM Clippolard Uperation: File, explorer, C:\Windows\document.txt, 121:11 AM File Move: 5100: C:\Windows\document.txt C:\Users\administratorXF485\Desktop\document.txt: 0 Bytes	
1:21:11 AM File Move: 5100: C:\Windows\document.txt C:\Users\administratorXF485\Desktop\document.txt: 0 Bytes 1:21:11 AM Clipboard Doeration: Text, explorer, .	
12/12 AM. Eiko Dakes 5100 - DV:risdow Alexa Text Decrement bit: 0.Rutes	

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.

Events and Bookmarks	
1:26:54 AM Clipboard Operation: Text, cmd, , Administrator: Command Prompt	
🗢 1:27:03 AM - File Transfer: 7260: Client:Applicationhang.exe: Host:Applicationhang.exe: 7.5 KB	N
1:27:09 AM Top-most window: Applicationhang, Form1, 3996	2
1:27:21 AM Top-most window: WerFault, , 5956	
1:27:58 AM Top-most window: explorer, , 5100	
1:27:59 AM App Not Responding: 3996: C:\Users\administrator.XF4B5\Desktop\Applicationhang.exe	
1:28:03 AM Top-most window: explorer, , 5100	
◯ 1:28:03 AM Top-most window: Taskmgr, Task Manager, 6844	
1:30:02 AM Client drive mapping: D	

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.

User: administrator Domain: LK6WA Application: Desktop Delivery Group: TSVDA2 VDA Machine: AWTSVDA-0002 Site: BVT_DB Status: Complete	File Edit V	new Play Tools Help	
Workspace	🖕 i 🕨 📰 i d	🗊 📅 🚓 🔊 Search: 🔹 Anvtime 🔹 🕅 🍈 🕅 Advanced Search	
Workspace - schnistatator Search Result Pavortes	_ , ,		
Search Results Favorites Now Playing Jsea: administator Domain: LK6WA Applicabir: Desktop Delivery Group: TSVA2 Other Status: Complete Status: Complete Status: Sonplete Status: Sonpleter Status: Sonpleter Status: Sonpleter Status: Sonpleter Status: Sonpleter Sonpleter Status: Sonpleter Sonpleter Status: Sonpleter Sonpleter Sonpleter Status: Sonpleter Sonpleter Sonpleter Sonpleter	•		
User: administrator Domain: LKBWA Application: Desktop Delevery Group: TSVDA2 VDA Machine: AVTSVDA:0002 Site: BVT_D8 Statu: Complete Stat: 9/14/2020.1:57.AM Events and Bookmarks 1:58:36 AM App End: 8976: chrome 1:58:36 AM App End: 9164: chrome 1:58:36 AM App End: 9000: software_reporter_tool 1:58:36 AM App End: 9200: software_reporter_tool 1:58:37 AM App End: 9200: corthoat: 8116: 1/?/C:\Windows\system32\conhost.exe 0x4 1:58:37 AM App Stat: 5020: MessageQueuingTool 1:58:37 AM App Stat: 5020: MessageQueuingTool 1:59:34 AM App Stat: 5020: MessageQueuingTool 1:59:34 AM App Stat: 5020: MessageQueuingTool 1:59:34 AM App Stat: 5020: MessageQueuingTool 2:00:43 AM App Stat: 5020: MessageQueuingTool 2:00:43 AM App Stat: 5020: MessageQueuingTool 2:00:44 AM App Stat: 5020: MessageQueuingTool 2:00:44 AM App Stat: 1:044: ConsoleApplication10 2:00:144 AM App Stat: 1:024: chrome: 9560: "C\Program Files (x86)\Google\Chrome\Application\chrome.exe" -\ype=renderer -field+tiid+handle=1540,575. 2:01:144 AM App Stat: 1:024: chrome: 9560: "C\Program Files (x86)\Google\Chrome\Application\chrome.exe" -\ype=renderer -field+tiid+handle=1540,575. 2:01:144 AM App Stat: 1:024: chrome: 9560: "C\Program Files (x86)\Google\Chrome\Application\chrome.exe" -\ype=renderer -field+tiid+handle=1540,575. 2:01:144 AM App Stat: 1:024: chrome: 9560: "C\Program Files (x86)\Google\Chrome\Application\chrome.exe" -\ype=renderer -field+tiid+handle=1540,575. 2:01:144 AM App Stat: 1:024: chrome: 9560: "C\Program Files (x86)\Google\Chrome\Application\chrome.exe" -\ype=renderer -field+tiid+handle=1540,575. 2:01:144 AM App Stat: 1:024: chrome: 9560: "C\Program Files (x86)\Google\Chrome\Applica	🐻 👌 Search Re		
Domain: LKSWA Application: Desktop Delivery Group: TSVDA-0002 VDA Machine: AWTSVDA-0002 Site: BVT_DB Status: Complete Status: Complete Status: Supprise PVA 40201-157 AM Events and By End: 8976: chrome 1:58:36 AM App End: 99164: chrome 1:58:36 AM App End: 99302: software_reporter_tool 1:58:36 AM App End: 98760: chrome 1:58:36 AM App End: 98760: chrome 1:58:36 AM App End: 98760: chrome 1:58:36 AM App End: 98700: chrome 1:58:36 AM App End: 98700: chrome 1:58:36 AM App End: 98700: chrome 1:58:37 AM App Stat: 19840: chrome 1:58:38 AM App End: 98700: chrome 1:58:37 AM App Stat: 19840: chrome 1:58:37 AM App Stat: 19840: chrome: 9300: "C:\Vindows/system32\conhost exe 0x4 1:58:37 AM App End: 93200: cml 4816: cml -help 1:58:37 AM App End: 9320: cml 48200: ping 1:58	Now Playing		
Application: Desktop Delivery Group: TSVDA2 VDA Machine: AVTSVDA:0002 Site: BVT_DB Statu: Complete Statu: Sy14/2020 1:57 AM Events and Bookmarks:	User:	administrator	١,
Delivery Group: TSVDA2 VDA Machine: AVTSVDA.0002 Site: BVT_DB Statux: Complete Statu: Sy14/2020 1:57 AM Events and Bookmarks: 1:58:36 AM App End: 8976: chrome 1:58:36 AM App End: 19164: chrome 1:58:36 AM App End: 19008: software_reporter_tool 1:58:36 AM App End: 10008: software_reporter_tool 1:58:36 AM App End: 10008: software_reporter_tool 1:58:36 AM App End: 10164: software_reporter_tool 1:58:36 AM App End: 7500: MessageQueuingTool 1:58:37 AM App Statt: 5080: cornhoat: 8416: (rr/?/C:///windows/system32/cornhost.exe 0x4 1:58:38 AM App End: 7260: MessageQueuingTool 2:00:34 AM App Statt: 7260: MessageQueuingTool 2:00:34 AM App Statt: 7260: MessageQueuingTool 2:00:34 AM App End: 9300: chrome 9300: "C:/Vorgram Files (x86/NGoogle/Chrome/Application/Chrome.exe" -type=renderer -fieldHiahande=1540.5975 2:00:14 AM App Statt: 9342: PNIG<	Domain:	LK6WA	l
VDA Machine: AWTSVDA-0002 Site:: BVT_DB Statu:: Complete Statu:: Syl14/2020 1:57 AM Events and Bookmarks:	Application	Desktop	
Site: BVT_DB Statu: Complete Statu: 9/14/2020 1:57 AM Events and Bookmarks Instatut Statu: 1:58:36 AM App End: 8976: chrome 1:58:36 AM App End: 9164: chrome 1:58:36 AM App End: 9000: software_reporter_tool 1:58:37 AM App End: 8000: chrome 1:58:37 AM App Stat: 5000: combost: 8416: (rrd/-help 1:58:37 AM App Stat: 5000: combost: 8416: (rrd/-help 1:58:37 AM App Stat: 7200: MessageQueuingTool 9300: C:\Users\Administator.LK6WA\Desktop\MessageQueuingTool exe 1:58:37 AM App Stat: 7200: MessageQueuingTool 9300: C:\Users\Administator.LK6WA\Desktop\MessageQueuingTool exe 1:58:37 AM App Stat: 7200: MessageQueuingTool 9300: C:\Users\Administator.LK6WA\Desktop\MessageQueuingTool exe 1:58:37 AM App Stat: 7200: MessageQueuingTool 9300: C:\Users\Administator.LK6WA\Desktop\MessageQueuin			ľ
Statux: Complete 9/14/2020 1:57 AM Events and Bookmarks 1:58:36 AM App End: 876: chrome 1:58:36 AM App End: 9164: chrome 1:58:36 AM App End: 9000: software_reporter_tool 1:58:36 AM App End: 8000: corome 1:58:37 AM App Statt: 5000: coronest: 8416: \??\C\:Windows\system32\conhost.exe 0x4 1:58:37 AM App Statt: 9800: cordme 1:58:36 AM App End: 8000: cordme 8416: \??\C\:Windows\system32\conhost.exe 0x4 1:58:37 AM App Statt: 9800: cord: 9800: C\:Users\Administrator.LK6WA\Desktop\MessageQueuingTool.exe 1:58:37 AM App Statt: 9800: cord: 8416: \??\C\:Windows\system32\conhost.exe 0x4 1:58:37 AM App Statt: 9800: cord: 9810: C\:Users\Administrator.LK6WA\Desktop\MessageQueuingTool.exe 1:58:37 AM App Statt: 9800: cord: 9800: C\:Users\Administrator.LK6WA\Desktop\MessageQueuingTool.exe 1:58:37 AM App Statt: 9800: cord: 9800: C\:Users\Administrator.LK6WA\Desktop\MessageQueuingTool.exe 2:00:44 AM App Statt: 9800: cord: 9800: C\:			
Start 9/14/2020 1:57 AM Events and Bokmarks 1:58:36 AM App End: 8976: chrome 1:58:36 AM App End: 9164: chrome 1:58:36 AM App End: 9164: chrome 1:58:36 AM App End: 9000: software_reporter_tool 1:58:36 AM App End: 9700: software_reporter_tool 1:58:36 AM App End: 9700: software_reporter_tool 1:58:36 AM App End: 8700: chrome 1:58:36 AM App End: 9800: chrome 1:58:37 AM App Statt: 9800: chrome 1:58:37 AM App Statt: 9800: chrome 1:58:37 AM App Statt: 9800: chrome 1:58:38 AM App End: 9144: ConsoleApplication10: 9380: C:\Users\Administrator.LK6WA\Desktop\MessageQueuingTool.exe 1:58:37 AM App Statt: 9200: mdt: 9380: C:\Users\Administrator.LK6WA\Desktop\MessageQueuingTool.exe 1:58:38 AM App Statt: 9200: mdt: 9380: C:\Users\Administrator.LK6WA\Desktop\MessageQueuingTool.exe 1:58:37 AM App Statt: 9200: mdt: 9380: C:\Users\Administrator.LK6WA\Desktop\MessageQueuingTool.exe 1:58:38 AM App End: 9144: ConsoleApplication10: 9380: C:\Users\Administrator.LK6WA\Desktop\MessageQueuingTool.exe 2:00:34 AM App Statt: 9540: Chrome: 9390: 'C:\Program Files (x86\Nocogle\Chrome\Application\chrome.exe'' -Upe=rendere		-	
Events and Bookmarks 1:58:36 AM App End: 976: chrome 1:58:36 AM App End: 9164: chrome 1:58:36 AM App End: 9104: software_reporter_tool 1:58:36 AM App End: 9300: software_reporter_tool 1:58:36 AM App End: 9300: software_reporter_tool 1:58:36 AM App End: 9500: chrome 1:58:37 AM App Statt: 5080: conhost: 8416: \r??\C:\Windows\system32\conhost.exe 0x4 1:58:37 AM App Statt: 9800: cml: 8416: cmd: 8092: 'C:\Windows\system32\conhost.exe 0x4 1:58:37 AM App Statt: 9800: cml: 8416: cmd: 9800: C:\Users\Administrator.LK&WA\Desktop\MessageQueuingTool.exe 1:59:34 AM App Statt: 9200: MssageQueuingTool 2:00:34 AM App End: 7200: MessageQueuingTool 2:00:34 AM App Statt: 944: ConsoleApplication10. 2:00:34 AM App Statt: 944: ConsoleApplication10. 2:01:34 AM App Statt: 9544: PING: 9580. 'C:\Program Files (x86)\Google\Chrome\Application\chrome.exe'' 2:01:34 AM App Statt: 932: chrome: 9560. 'C:\Program Files (x86)\Google\Chrome\Application\chrome.exe'' 2:01:30 AM App Statt: 9342: PING: 9380. 'C:\Program Files (x86)\Google\Chrome\Application\chrome.exe'' 2:01:34 AM App Statt: 932: chrome: 9560. 'C:\Program Files (x86)\Google\Chrome\Application\chrome.exe'' -\ype==mdererfie		·	
 158:36 AM App End: 9376: chrome 158:36 AM App End: 9376: chrome 158:36 AM App End: 9320: software_reporte_tool 158:36 AM App End: 9580: chrome 158:36 AM App End: 8580: chrome 158:36 AM App End: 8580: chrome 158:36 AM App Stat: 5080: conhost 8416: \c?\C\Windows\system32\conhost.exe 0x4 158:37 AM App Stat: 5080: conhost 8416: \c?\C\Windows\system32\conhost.exe 0x4 158:37 AM App Stat: 5080: conhost 8416: \c?\C\Windows\system32\conhost.exe 0x4 158:37 AM App Stat: 7260: MessageQueuingTool: 9980: C:\Users\Administrator.LK6WA\Desktop\MessageQueuingTool.exe 158:34 AM App End: 7260: MessageQueuingTool: S980: C:\Users\Administrator.LK6WA\Desktop\MessageQueuingTool.exe 158:34 AM App Stat: 5144: ConsoleApplication10: 9960: C:\ConsoleApplication10.exe 200:34 AM App Stat: 9144: ConsoleApplication10: 9960: C:\ConsoleApplication10.exe 201:30 AM App Stat: 9544: FING: 9980: ping: www.baidu.com -t 201:30 AM App Stat: 1332: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" 201:44 AM App Stat: 1332: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" -type=renderer -field-trial-handle=1540,5975 201:44 AM App Stat: 1256: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" -type=utility -utility-sub-type=stratoge.enjom 201:44 AM App Stat: 116: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" -type=utility -utility-sub-type=stratoge.enjom 201:44 AM App Stat: 11172: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\c		5/14/2020 1.5/ AIM	
 1:58:36 AM App End: 9164: chrome 1:58:36 AM App End: 9320: software_reporter_tool 1:58:36 AM App End: 8760: chrome 1:58:36 AM App End: 8680: chrome 1:58:36 AM App Start: 5080: conhost 8416: \??\C\Windows\system32\conhost.exe 0x4 1:58:37 AM App Start: 5080: conhost 8416: \??\C\Windows\system32\conhost.exe 0x4 1:58:37 AM App Start: 9300: cml: 8416: cmd :=help 1:58:38 AM App End: 7260: MessageQueuingTool 1:58:34 AM App Start: 7260: MessageQueuingTool 2:00:34 AM App End: 7260: MessageQueuingTool 2:00:34 AM App End: 9144: ConsoleApplication10: 9380: C:\Users\Administrator.LK&WA\Desktop\MessageQueuingTool.exe 2:01:44 AM App Start: 9560: chrome: 9380: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" -type=renderer -field-trial-handle=1540.5975 2:01:44 AM App Start: 132: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" -type=renderer -field-trial-handle=1540.5975 2:01:44 AM App Start: 1418: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" -type=renderer -field-trial-handle=1540.5975 2:01:	Events and Bo	ookmarks	
 1:58:36 AM App End: 10008: software_reporter_tool 1:58:36 AM App End: 9900: software_reporter_tool 1:58:36 AM App End: 9900: software_reporter_tool 1:58:36 AM App End: 9900: software_reporter_tool 1:58:36 AM App End: 8760: chrome 1:58:36 AM App End: 8680: chrome 1:58:37 AM App Stat: 5080: conhost: 8416: \??\C:\Windows\system32\conhost.exe 0x4 1:58:37 AM App Stat: 5080: conhost: 8416: \??\C:\Windows\system32\conhost.exe 0x4 1:58:37 AM App Stat: 9800: cml: 8416: cmd: 8092: "C:\Windows\system32\conhost.exe 0x4 1:58:37 AM App Stat: 9800: cml: 8416: cmd: 9920: C:\Users\Administrator.LKEWA\Desktop\MessageQueuingTool.exe 1:58:37 AM App Stat: 7260: MessageQueuingTool 1:59:34 AM App Stat: 7260: MessageQueuingTool 2:00:34 AM App End: 19144: ConsoleApplication10: 9980: C:\ConsoleApplication10.exe 2:00:34 AM App End: 9544: PING 2:01:34 AM App Stat: 9544: PING 2:01:34 AM App Stat: 1392: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" -type=renderer -field-trial-handle=1540.5975 2:01:44 AM App Stat: 1392: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" -type=renderer -field-trial-handle=1540.5975 2:01:44 AM App Stat: 1416: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" -type=renderer -field-trial-handle=1540.5975 2:01:44 AM App Stat: 1416: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" -type=renderer -field-trial-handle=1540.5975 2:01:44 AM App Stat: 1416: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" -type=renderer -field-trial-handle=1540.5975 2:01:44 AM App Stat: 1416: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" -type=renderer -field-trial-handle=1540.5975 2:01:44 AM App Stat: 1416: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\App			,
 1:58:36 AM App End: 9920: software_reporter_tool 1:58:36 AM App End: 9900: software_reporter_tool 1:58:36 AM App End: 10164: software_reporter_tool 1:58:36 AM App End: 10164: software_reporter_tool 1:58:36 AM App End: 8680: chrome 1:58:36 AM App End: 8680: chrome 1:58:37 AM App Stat: 5080: conhost 8416: \??\C:\Windows\system32\conhost.exe 0x4 1:58:37 AM App Stat: 5080: conhost 8416: \??\C:\Windows\system32\conhost.exe 0x4 1:58:37 AM App Stat: 9800: cmd: 8092: "C:\Windows\system32\conhost.exe 0x4 1:58:37 AM App Stat: 9980: cmd: 8416: cmd -help 1:59:34 AM App End: 7260: MessageQueuingTool: 9980: C:\Users\Administrator.LK6WA\Desktop\MessageQueuingTool.exe 1:59:42 AM App End: 7260: MessageQueuingTool 2:00:34 AM App End: 9144: ConsoleApplication10: 9980: C:\ConsoleApplication10.exe 2:00:34 AM pEnd: 9144: ConsoleApplication10: 9980: C:\ConsoleApplication10.exe 2:01:44 AM App Stat: 9560: chrome: 9980: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" -type=renderer -field-trial-handle=1540.5975 2:01:44 AM App Stat: 132: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" -type=renderer -field-trial-handle=1540.5975 2:01:44 AM App Stat: 132: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" -type=renderer -field-trial-handle=1540.5975 2:01:44 AM App Stat: 132: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" -type=renderer -field-trial-handle=1540.5975 2:01:44 AM App Stat: 1256: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" -type=renderer -field-trial-handle=1540.5975 2:01:44 AM App Stat: 1256: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" -type=renderer -field-trial-handle=1540.5975 2:01:44 AM App Stat: 10172: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Applica	-		
 1:58:36 AM App End: 9900: software_reporter_tool 1:58:36 AM App End: 10164: software_reporter_tool 1:58:36 AM App End: 8760: chrome 1:58:36 AM App End: 8680: chrome 1:58:36 AM App End: 8680: conhost: 8416: \??\C\\Windows\system32\conhost.exe 0x4 1:58:37 AM App Stat: 5080: conhost: 8416: \??\C\\Windows\system32\conhost.exe 0x4 1:58:37 AM App Stat: 9980: cmd: 8416: cmd: 8092: "C\\Windows\system32\conhost.exe 0x4 1:58:37 AM App Stat: 7260: MessageQueuingTool: 9980: C\\Users\Administrator.LK6WA\Desktop\MessageQueuingTool.exe 1:59:34 AM App Stat: 7260: MessageQueuingTool 2:00:34 AM App Stat: 7260: MessageQueuingTool 2:00:34 AM App Stat: 9144: ConsoleApplication10: 9980: C\\ConsoleApplication10.exe 2:00:49 AM App Stat: 9544: PING 2:01:44 AM App Stat: 1392: chrome: 9560: "C\Program Files (x86)\Google\Chrome\Application\chrome.exe" -type=renderer -field-triah-handle=1540.5975 2:01:44 AM App Stat: 2564: chrome: 9560: "C\Program Files (x86)\Google\Chrome\Application\chrome.exe" -type=renderer -field-triah-handle=1540.5975 2:01:44 AM App Stat: 2564: chrome: 9560: "C\Program Files (x86)\Google\Chrome\Application\chrome.exe" -type=renderer -field-triah-handle=1540.5975 2:01:44 AM App Stat: 2564: chrome: 9560: "C\Program Files (x86)\Google\Chrome\Application\chrome.exe" -type=renderer -field-triah-handle=1540.5975 2:01:44 AM App Stat: 2564: chrome: 9560: "C\Program Files (x86)\Google\Chrome\Application\chrome.exe" -type=renderer -field-triah-handle=1540.5975 2:01:44 AM App Stat: 1172: chrome: 9560: "C\Program Files (x86)\Google\Chrome\Application\chrome.exe" -type=renderer -field-triah-handle=1540.5975 2:01:44 AM App Stat: 1172: chrome: 9560: "C\Program Files (x86)\Google\Chrome\Application\chrome.exe" -type=renderer -field-triah-handle=1540.5975 2:01:44 AM App Stat: 10172: chrome: 9560: "C\Program Files (x86)\Google\Chrome\App			
 1:58:36 AM App End: 10164: software_reporter_tool 1:58:36 AM App End: 8760: chrome 1:58:36 AM App End: 8680: chrome 1:58:37 AM App Stat: 5080: conhost: 8416: \??\C:\Windows\system32\conhost.exe 0x4 1:58:37 AM App Stat: 9980: cmd: 8092: "C:\Windows\system32\conhost.exe 0x4 1:58:37 AM App Stat: 9980: cmd: 8416: cmd -help 1:58:37 AM App Stat: 7260: MessageQueuingTool 2:59:34 AM App Stat: 7260: MessageQueuingTool 2:00:34 AM App Stat: 7260: MessageQueuingTool 2:00:34 AM App End: 7260: MessageQueuingTool 2:00:34 AM App Stat: 9144: ConsoleApplication10: 9980: C:\ConsoleApplication10.exe 2:00:49 AM App Stat: 9544: PING 2:01:30 AM App Stat: 9544: PING 2:01:40 AM App Stat: 9560: chrome: 9980: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" -type=renderer -field-trial-handle=1540.5975 2:01:44 AM App Stat: 256: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" -type=renderer -field-trial-handle=1540.5975 2:01:44 AM App Stat: 2256: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" -type=renderer -field-trial-handle=1540.5975 2:01:44 AM App Stat: 2256: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" -type=renderer -field-trial-handle=1540.5975 2:01:44 AM App Stat: 2256: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" -type=renderer -field-trial-handle=1540.5975 2:01:44 AM App Stat: 10172: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" -type=renderer -field-trial-handle=1540.5975 2:01:44 AM App Stat: 10172: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" -type=renderer -field-trial-handle=1540.5975 2:01:44 AM App Stat: 10172: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" -type=renderer -field-trial-handle=1540.5975	_		
 1:58:36 AM App End: 8760: chrome 1:58:36 AM App End: 8680: chrome 1:58:37 AM App Statt: 5080: conhost: 8416: \??\C:\Windows\system32\conhost.exe 0x4 1:58:37 AM App Statt: 9980: cmd: 8416: cmd -help 1:58:38 AM App Statt: 7260: MessageQueuingTool: 9980: C:\Users\Administrator.LK6WA\Desktop\MessageQueuingTool.exe 1:59:34 AM App Statt: 7260: MessageQueuingTool: 9980: C:\Users\Administrator.LK6WA\Desktop\MessageQueuingTool.exe 1:59:34 AM App Statt: 7260: MessageQueuingTool: 9980: C:\Users\Administrator.LK6WA\Desktop\MessageQueuingTool.exe 2:00:34 AM App End: 7260: MessageQueuingTool 2:00:49 AM App End: 9144: ConsoleApplication10: 9980: C:\ConsoleApplication10.exe 2:00:49 AM App End: 9544: PING: 9980: ping_www.baidu.com -t 2:01:40 AM App Statt: 9544: PING 2:01:44 AM App Statt: 3924: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" -uppe=renderer -field-trial-handle=1540.5975 2:01:44 AM App Statt: 1416: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" -uppe=rulity -utility-sub-type=storage.mojon 2:01:44 AM App Statt: 1416: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" -uppe=rulity -utility-sub-type=storage.mojon 2:01:44 AM App Statt: 1416: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" -uppe=rulity -utility-sub-type=storage.mojon 2:01:44 AM App Statt: 1416: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" -uppe=rulity -utility-sub-type=storage.mojon 2:01:44 AM App Statt: 1416: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" -uppe=rulity -utility-sub-type=storage.mojon 2:01:44 AM App Statt: 10172: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" -uppe=guting-storage.mojon 2:01:44 AM App Statt: 10048: chrome: 9560: "C:\Program Files (x86)\G	<u> </u>		
 1:58:36 AM App End: 8680: chrome 1:58:37 AM App Start: 5080: conhost: 8416: \??\C:\Windows\system32\conhost.exe 0x4 1:58:37 AM App Start: 8416: cmd: 8092: "C:\Windows\system32\conhost.exe 0x4 1:58:37 AM App Start: 9980: cmd: 8416: cmdhelp 1:59:34 AM App Start: 7260: MessageQueuingTool: 9980: C:\Users\Administrator.LK6WA\Desktop\MessageQueuingTool.exe 1:59:42 AM App End: 7260: MessageQueuingTool 2:00:34 AM App Start: 9144: ConsoleApplication10: 9980: C:\ConsoleApplication10.exe 2:00:49 AM App Start: 9144: ConsoleApplication10 2:01:01 AM App Start: 9544: PING: 9980: mmw.baidu.com -t 2:01:30 AM App Start: 9544: PING: 9980: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe"type=rendererfield-trial-handle=1540,5975 2:01:44 AM App Start: 256: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe"type=rendererfield-trial-handle=1540,5975 2:01:44 AM App Start: 2256: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe"type=rendererfield-trial-handle=1540,5975 2:01:44 AM App Start: 2256: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe"type=rendererfield-trial-handle=1540,5975 2:01:44 AM App Start: 1416: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe"type=rendererfield-trial-handle=1540,5975 2:01:44 AM App Start: 12256: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe"type=rendererfield-trial-handle=1540,5975 2:01:44 AM App Start: 1416: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe"type=rendererfield-trial-handle=1540,5975 2:01:44 AM App Start: 1416: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe"type=rendererfield-trial-handle=1540,5975 2:01:44 AM App Start: 10172: chrome: 9560: "C:\Program Files (x			
 1:58:37 AM App Start: 5080: conhost: 8416: \??\C:\Windows\system32\conhost.exe 0x4 1:58:37 AM App Start: 8416: cmd: 8092: "C:\Windows\system32\conhost.exe" 1:58:37 AM App Start: 9980: cmd: 8416: cmdhelp 1:59:34 AM App Start: 7260: MessageQueuingTool: 9980: C:\Users\Administrator.LK6WA\Desktop\MessageQueuingTool.exe 1:59:42 AM App End: 7260: MessageQueuingTool 2:00:34 AM App Start: 9144: ConsoleApplication10: 9980: C:\ConsoleApplication10.exe 2:00:49 AM App End: 9144: ConsoleApplication10 2:00:49 AM App Start: 9542: PING: 9980: mini strator.LK6WA\Desktop\MessageQueuingTool.exe 2:00:49 AM App Start: 9144: ConsoleApplication10 2:01:01 AM App Start: 9544: PING: 9980: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" 2:01:44 AM App Start: 9560: chrome: 9580: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" -type=rendererfield-trial-handle=1540,5975 2:01:44 AM App Start: 2256: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" -type=tuility -utility-sub-type=storage.mojom 2:01:44 AM App Start: 1416: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" -type=tuility -utility-sub-type=storage.mojom 2:01:44 AM App Start: 1416: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" -type=tuility -utility-sub-type=storage.mojom 2:01:44 AM App Start: 1416: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" -type=tuility -utility-sub-type=storage.mojom 2:01:44 AM App Start: 1416: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" -type=tuility -utility-sub-type=storage.mojom 2:01:44 AM App Start: 1416: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" -type=tuility -utility-sub-type=storage.mojom 2:01:44 AM App Start: 10172: chrome: 9560: "C:\Program Files (x86)\Google\Ch	-		
 1:58:37 AM App Start: 8416: cmd: 8092: "C:\Windows\system32\cmd.exe" 1:58:58 AM App Start: 9980: cmd: 8416: cmd -help 1:59:34 AM App Start: 7260: MessageQueuingTool: 9980: C:\Users\Administrator.LK6WA\Desktop\MessageQueuingTool.exe 1:59:42 AM App End: 7260: MessageQueuingTool 2:00:34 AM App Start: 9144: ConsoleApplication10: 9980: C:\ConsoleApplication10.exe 2:00:49 AM App End: 9144: ConsoleApplication10 2:00:49 AM App Start: 9544: PING 2:01:30 AM App Start: 9544: PING 2:01:30 AM App Start: 9560: chrome: 9580: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" -type=renderer -field-trial-handle=1540,5975 2:01:44 AM App Start: 2256: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" -type=tuility -utility-sub-type=storage.mojom 2:01:44 AM App Start: 1416: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" -type=tuility -utility-sub-type=storage.mojom 2:01:44 AM App Start: 1416: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" -type=tuility -utility-sub-type=storage.mojom 2:01:44 AM App Start: 1416: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" -type=tuility -utility-sub-type=storage.mojom 2:01:44 AM App Start: 1416: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" -type=tuility -utility-sub-type=storage.mojom 2:01:44 AM App Start: 1416: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" -type=tuility -utility-sub-type=storage.mojom 2:01:44 AM App Start: 10172: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" -type=gu-process -field-trial-handle=1540, 2:01:44 AM App Start: 10048: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" -type=gu-process -field-trial-handle=1540, 2:01:44 AM App Start: 10162: chrome:	_		
 1:59:34 AM App Start: 7260: MessageQueuingTool: 9980: C:\Users\Administrator.LK6WA\Desktop\MessageQueuingTool.exe 1:59:42 AM App End: 7260: MessageQueuingTool 2:00:34 AM App Start: 9144: ConsoleApplication10: 9980: C:\ConsoleApplication10.exe 2:00:49 AM App End: 9144: ConsoleApplication10 2:01:01 AM App Start: 9544: PING: 9980: ping: www.baidu.com -t 2:01:30 AM App End: 9544: PING: 9980: C:\Program Files (x86)\Google\Chrome\Application\chrome.exe'' 2:01:44 AM App Start: 1392: chrome: 9560: 'C:\Program Files (x86)\Google\Chrome\Application\chrome.exe''type=rendererfield-trial-handle=1540,5975 2:01:44 AM App Start: 2256: chrome: 9560: 'C:\Program Files (x86)\Google\Chrome\Application\chrome.exe''type=rendererfield-trial-handle=1540,5975 2:01:44 AM App Start: 1416: chrome: 9560: 'C:\Program Files (x86)\Google\Chrome\Application\chrome.exe''type=rendererfield-trial-handle=1540,5975 2:01:44 AM App Start: 1416: chrome: 9560: 'C:\Program Files (x86)\Google\Chrome\Application\chrome.exe''type=rendererfield-trial-handle=1540,5975 2:01:44 AM App Start: 1416: chrome: 9560: 'C:\Program Files (x86)\Google\Chrome\Application\chrome.exe''type=rendererfield-trial-handle=1540,5975 2:01:44 AM App Start: 1416: chrome: 9560: 'C:\Program Files (x86)\Google\Chrome\Application\chrome.exe''type=rendererfield-trial-handle=1540,5975 2:01:44 AM App Start: 10172: chrome: 9560: 'C:\Program Files (x86)\Google\Chrome\Application\chrome.exe''type=gpu-processfield-trial-handle=1540, 2:01:44 AM App Start: 10048: chrome: 9560: 'C:\Program Files (x86)\Google\Chrome\Application\chrome.exe''type=gpu-processfield-trial-handle=1540, 2:01:44 AM App Start: 10172: chrome: 9560: 'C:\Program Files (x86)\Google\Chrome\Application\chrome.exe''type=gpu-processfield-trial-handle=1540, 2:01:44 AM App Start: 10048: chrome: 9560: 'C:\Program	_	··· ·	
 1:59:42 AM App End: 7260: MessageQueuingTool 2:00:34 AM App Start: 9144: ConsoleApplication10: 9980: C:\ConsoleApplication10.exe 2:00:49 AM App End: 9144: ConsoleApplication10 2:01:01 AM App Start: 9544: PING: 9980: ping_www.baidu.com -t 2:01:30 AM App End: 9544: PING 2:01:30 AM App End: 9544: PING 2:01:44 AM App Start: 1392: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe"type=rendererfield-trial-handle=1540,5975 2:01:44 AM App Start: 2564: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe"type=rendererfield-trial-handle=1540,5975 2:01:44 AM App Start: 1416: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe"type=rendererfield-trial-handle=1540,5975 2:01:44 AM App Start: 1416: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe"type=rendererfield-trial-handle=1540,5975 2:01:44 AM App Start: 1416: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe"type=rendererfield-trial-handle=1540,5975 2:01:44 AM App Start: 1416: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe"type=utilityutility-sub-type=storage.mojom 2:01:44 AM App Start: 10172: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe"type=gu-processfield-trial-handle=1540, 2:01:44 AM App Start: 1072: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe"type=gu-processfield-trial-handle=1540, 2:01:44 AM App Start: 10048: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe"type=gu-processfield-trial-handle=1540, 2:01:44 AM App Start: 10048: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe"type=gu-processfield-trial-handle=1540, 2:01:44 AM App Start: 10048: chrome: 9560: "C:\Program Fi	😑 1:58:58 AM A	pp Start: 9980: cmd: 8416: cmdhelp	
 2:00:34 AM App Start: 9144: ConsoleApplication10: 9980: C:\ConsoleApplication10.exe 2:00:49 AM App End: 9144: ConsoleApplication10 2:01:01 AM App Start: 9544: PING: 9980: ping_www.baidu.com -t 2:01:30 AM App End: 9544: PING 2:01:30 AM App End: 9544: PING 2:01:44 AM App Start: 1392: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe"	<mark>O</mark> 1:59:34 AM .	App Start: 7260; MessageQueuingTool: 9980; C:\Users\Administrator.LK6WA\Desktop\MessageQueuingTool.exe	
 2:00:49 AM App End: 9144: ConsoleApplication10 2:01:01 AM App Start: 9544: PING: 9980: ping_www.baidu.com.et 2:01:30 AM App End: 9544: PING 2:01:43 AM App Start: 9560: chrome: 9980: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" 2:01:44 AM App Start: 1392: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" -type=renderer -field-trial-handle=1540,5975 2:01:44 AM App Start: 2644: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" -type=renderer -field-trial-handle=1540,5975 2:01:44 AM App Start: 2256: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" -type=renderer -field-trial-handle=1540,5975 2:01:44 AM App Start: 2256: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" -type=utility -utility-sub-type=storage.mojom 2:01:44 AM App Start: 11416: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" -type=utility -utility-sub-type=network.mojom 2:01:44 AM App Start: 10172: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" -type=gpu-process -field-trial-handle=1540, 2:01:44 AM App Start: 10172: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" -type=gpu-process -field-trial-handle=1540, 2:01:44 AM App Start: 10048: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" -type=gpu-process -field-trial-handle=1540, 2:01:44 AM App Start: 10048: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" -type=gpu-process -field-trial-handle=1540, 2:01:44 AM App Start: 10048: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" -type=crashpad-handler "-user-data-direC\ 			
 2:01:01 AM App Start: 9544; PING: 9980; ping: www.baidu.com-t 2:01:30 AM App End: 9544; PING 2:01:30 AM App End: 9544; PING 2:01:43 AM App Start: 9560; chrome: 9980; "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" 2:01:44 AM App Start: 1392; chrome: 9560; "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe"type=rendererfield-trial-handle=1540,5975 2:01:44 AM App Start: 2644; chrome: 9560; "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe"type=rendererfield-trial-handle=1540,5975 2:01:44 AM App Start: 2256; chrome: 9560; "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe"type=utilityutility-sub-type=storage.mojom 2:01:44 AM App Start: 1416; chrome: 9560; "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe"type=utilityutility-sub-type=network.mojom 2:01:44 AM App Start: 10172; chrome: 9560; "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe"type=gpu-processfield-trial-handle=1540,5975 2:01:44 AM App Start: 10172; chrome: 9560; "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe"type=gpu-processfield-trial-handle=1540,5975 2:01:44 AM App Start: 10048; chrome: 9560; "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe"type=tilityutility-sub-type=network.mojom 2:01:44 AM App Start: 10048; chrome: 9560; "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe"type=gpu-processfield-trial-handle=1540, 2:01:44 AM App Start: 10048; chrome: 9560; "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe"type=gpu-processfield-trial-handle=1540, 	-		
 2:01:30 AM App End: 9544: PING 2:01:43 AM App Start: 9560: chrome: 9980: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" 2:01:44 AM App Start: 1392: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe"type=rendererfield-trial-handle=1540,5975 2:01:44 AM App Start: 2644: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe"type=rendererfield-trial-handle=1540,5975 2:01:44 AM App Start: 2644: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe"type=rendererfield-trial-handle=1540,5975 2:01:44 AM App Start: 2256: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe"type=utilityutility-sub-type=storage.mojom 2:01:44 AM App Start: 1416: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe"type=utilityutility-sub-type=network.mojom 2:01:44 AM App Start: 10172: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe"type=gpu-processfield-trial-handle=1540,5975 2:01:44 AM App Start: 10172: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe"type=gpu-processfield-trial-handle=1540, 2:01:44 AM App Start: 10048: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe"type=gpu-processfield-trial-handle=1540, 2:01:44 AM App Start: 10048: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe"type=gpu-processfield-trial-handle=1540, 	-		ł
 2:01:43 AM App Start: 9560: chrome: 9980: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe"type=rendererfield-trial-handle=1540,5975 2:01:44 AM App Start: 1392: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe"type=rendererfield-trial-handle=1540,5975 2:01:44 AM App Start: 2644: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe"type=rendererfield-trial-handle=1540,5975 2:01:44 AM App Start: 2256: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe"type=utilityutility-sub-type=storage.mojom 2:01:44 AM App Start: 1416: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe"type=utilityutility-sub-type=network.mojom 2:01:44 AM App Start: 10172: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe"type=utilityutility-sub-type=network.mojom 2:01:44 AM App Start: 10048: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe"type=utilityutility-sub-type=network.mojom 2:01:44 AM App Start: 10048: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe"type=gpu-processfield-trial-handle=1540, 2:01:44 AM App Start: 10048: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe"type=gpu-processfield-trial-handle=1540, 	-		
 2:01:44 AM App Start: 1392: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe"type=rendererfield-trial-handle=1540,5975 2:01:44 AM App Start: 2644: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe"type=rendererfield-trial-handle=1540,5975 2:01:44 AM App Start: 2256: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe"type=utilityutility-sub-type=storage.mojom 2:01:44 AM App Start: 1416: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe"type=utilityutility-sub-type=storage.mojom 2:01:44 AM App Start: 1416: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe"type=utilityutility-sub-type=network.mojom 2:01:44 AM App Start: 10172: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe"type=gpu-processfield-trial-handle=1540, 2:01:44 AM App Start: 10048: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe"type=gpu-processfield-trial-handle=1540,	-		
 2:01:44 AM App Start: 2644: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe"type=rendererfield-trial-handle=1540,5975 2:01:44 AM App Start: 2256: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe"type=utilityutility-sub-type=storage.mojom 2:01:44 AM App Start: 1416: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe"type=utilityutility-sub-type=network.mojom 2:01:44 AM App Start: 1416: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe"type=utilityutility-sub-type=network.mojom 2:01:44 AM App Start: 10172: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe"type=gpu-processfield-trial-handle=1540, 2:01:44 AM App Start: 10048: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe"type=gpu-processfield-trial-handle=1540, 2:01:44 AM App Start: 10048: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe"type=gpu-processfield-trial-handle=1540, 2:01:44 AM App Start: 10048: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe"type=crashpad-handler "user-data-dir=C:\ 			
 2:01:44 AM App Start: 1416: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe"type=utilityutility-sub-type=network.mojom 2:01:44 AM App Start: 10172: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe"type=gpu-processfield-trial-handle=1540, 2:01:44 AM App Start: 10048: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe"type=gpu-processfield-trial-handle=1540, 2:01:44 AM App Start: 10048: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe"type=crashpad-handler "user-data-direC:\ 	-		
 2:01:44 AM App Start: 10172: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe"type=gpu-processfield-trial-handle=1540, 2:01:44 AM App Start: 10048: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe"type=crashpad-handler "-user-data-dir=C:\ 			
2:01:44 AM App Start: 10048: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe"type=crashpad-handler "user-data-dir=C:\	-	App Start: 1416: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" -type=utility -utility-sub-type=network.mojom	
	O 2:01:44 AM		
🔾 2:01:44 AM App Start: 8960: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe"type=rendererfield-trial-handle=1540,5975	 2:01:44 AM 2:01:44 AM 	App Start: 10172: chrome: 9560: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe"type=gpu-processfield-trial-handle=1540,	
	 2:01:44 AM 2:01:44 AM 2:01:44 AM 2:01:44 AM 		

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 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.dl
 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: WfShell, CtxDnDSourceProxy, 7260

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

L	
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: SearchUl, , 1796	
○ 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	12 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	

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

1.23.00 Am Popup Window, 11132, lusting: "[Local Osers and Groups (Local/Osers], Built-in account for administering the computer/
 1:23:08 AM Popup Window: 11132, lusting: - [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.

		Popup Window: 2192, Remote Desktop Connection, The remote computer could not be authenticated due
0	1:24:50 AM	RDP Connection: 2192: IP address
\circ	1:25:19 AM	Top-most window: cmd, Administrator: Command Prompt, 10776
$^{\circ}$	1:25:38 AM	Top-most window: explorer, , 5100
0	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 or not 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

ι.	~	1.20.00 AM	r op most	******	CAPIOICI, , 0100

1:25:40 AM Clipboard Operation: File, explorer, C:\Users\administrator.XF4B5\Desktop\confidential.docx,

1:25:45 AM File Transfer: 7260: Host:C:\Users\administrator.XF4B5\Desktop\confidential.docx: Client:confidential.docx: 0

- C 1:26:18 AM Top-most window: WfShell, CtxDnDSourceProxy, 7260
- 😑 1:26:19 AM Top-most window: explorer, , 5100
- O 1:26:21 AM File Transfer: 7260: Client:confidential.docx: Host:confidential.docx: 0 Bytes
- O 1:26:54 AM Clipboard Operation: Text, cmd, , Administrator: Command Prompt
- 🔾 1:27:03 AM File Transfer: 7260: Client:Applicationhang.exe: Host:Applicationhang.exe: 7.5 KB -

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

O 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:

Browser	Version
Chrome	69 and later
Internet Explorer	11
Firefox	61 and later

Note:

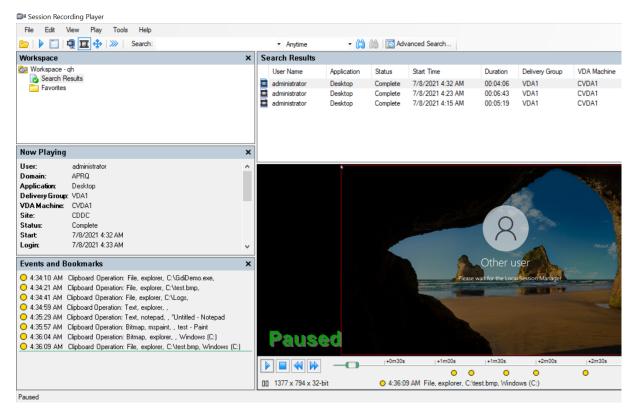
This feature requires Session Recording Version 1906 or later.

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 I	3ookmarks ×
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
😑 1:56:39 AM	Top-most window: explorer, Application.evtx, 7212
😑 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, Bisijisbb j.docx, 8896
😑 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
-	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	

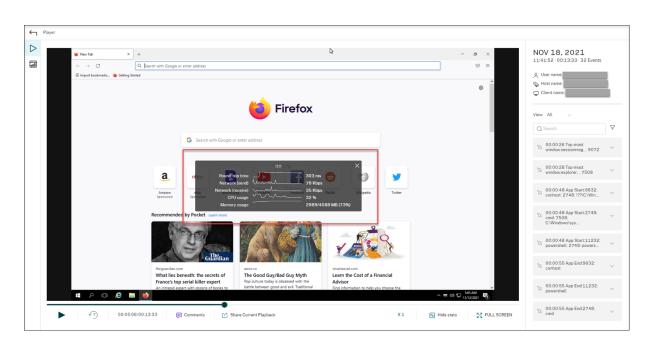
For example:

lookmarks
Registry Set Value: 8452: C:\Windows\System32\csrss.exe : HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Tablet PC IsTabletPC
Registry Create: 8452: C:\Windows\System32\csrss.exe: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Tablet PC
Registry Set Value: 8452: C:\Windows\System32\csrss.exe : HKEY_LOCAL_MACHINE\SOFTWARE\WDW6432Node\Microsoft\Windows\Tablet PC IsTabletPC
Registry Create: 8452: C:\Windows\System32\csrss.exe: HKEY_LOCAL_MACHINE\SOFTWARE\WDW6432Node\Microsoft\Windows\Tablet PC
Registry Set Value: 8452: C:\Windows\System32\csrss.exe : HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\AutoRotation LastOrientation
Registry Create: 8452: C:\\windows\System32\csrss.exe: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\\Windows\CurrentVersion\AutoRotation
Registry Set Value: 8452: C:\Windows\System32\csrss.exe : HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\AutoRotation\NonPreserve LastAutoRequest
Registry Create: 8452: C:\Windows\System32\csrss.exe: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\AutoRotation\NonPreserve
Registry Set Value: 8452: C:\Windows\System32\csrss.exe : HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\AutoRotation LastOrientation
Registry Create: 8452: C:\Windows\System32\csrss.exe: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\AutoRotation
Registry Set Value: 9992: C:\Program Files\Citrix\HDX\bin\CtxGfx.exe : HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics\3\LLIndicator
Registry Delete Value: 9992: C:\Program Files\Citrix\HDX\bin\Ctxgfx.exe : HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics\3 SessionHeight
Registry Delete Value: 9992: C:\Program Files\Citrix\HDX\bin\Ctx6fx.exe : HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics\3] SessionWidth
Registry Delete Value: 9992: C:\Program Files\Citrix\HDX\bin\Ctxgfx.exe : HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics\3] NumMonitors
Registry Create: 9992: C:\Program Files\Citrix\HDX\bin\CtxGfx.exe: HKEY_LOCAL_MACHINE\SOFTWARE\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



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. Note that 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: 2192. Remote Desktop Connection. Connecting to: [Peddress | Initiating remote connection...
 1:24 05 AM Popup Window: 2192. Remote Desktop Connection, Remote Desktop can't connect to the remote computer for one of these reasons: \n\n] Remote access to the server is not enabled\n2] The remote computer is turned off\n3] The remote.

Custom events

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

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

Session Recording 2204

🔐 Session Reco	rding Plaver										- 0	×
	View Play Tools Help											
🗁 I 🕨 🛅 IP	🗐 🎞 💠 💓 🛛 Search:		 Anytime 	- 😭	()). 🔀 Adv	ranced Search						
Workspace		×	Search Results									×
Workspace - Search R Favorites	esults		User Name administrator administrator administrator	Application Desktop Desktop Desktop	Status Complete Complete Complete	Start Time 7/8/2021 4:32 AM 7/8/2021 4:23 AM 7/8/2021 4:15 AM	Duration 00:04:06 00:06:43 00:05:19	Delivery Group VDA1 VDA1 VDA1	VDA Machine CVDA1 CVDA1 CVDA1 CVDA1	Events Only No No No	Size 1,134 KB 796 KB 776 KB	
Now Playing		×										
User: Domain: Application: Delivery Group VDA Machine: Site: Status: Status: Start Login:		~				Co	ntent b	locked				
	ookmarks Volepad++,Sentive content detected;; Volepad++,Sentive content detected;;	×				Sentive	e conte	nt detecte	ed			
					+0h	01m +0h02	m	+0h02m	_+0h04m	+0h05m	+0h06m	
								<u> </u>				/

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.

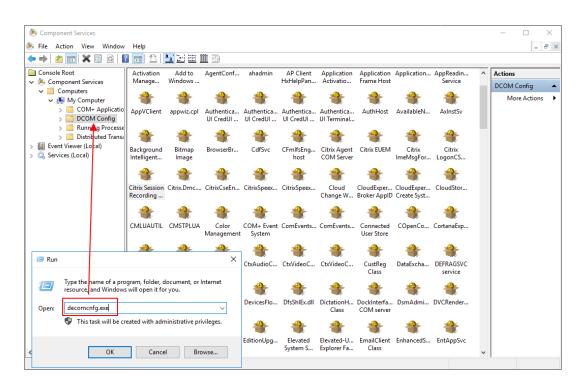
😳 Session	Recording Ager	nt Properties	_		\times			
Recording	Connections							
Session recording Select this option to enable policy-based session recording on this VDA machine. If this option is not selected, session recording is disabled on this machine.								
Custom event recording Select this 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	Cancel	A	pply			

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

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

Local administrators are granted with this permission by default. To grant other users this permission, use the Windows DCOM configuration tool:

a) Open the Windows DCOM configuration tool on the Session Recording agent by running dcomcnfg.exe.



b) Right-click Citrix Session Recording Agent and choose Properties.

Citrix Session Recording	CitrixCseEn CitrixSpeex CitrixSpee	ء x (Cha
Citrix Session Recording	Agent Properties ?	×
-	curity Endpoints Identity	
20001011 000	this DCOM application	
Application Name:		
Application ID:	{07c6c101-d1ac-4429-be2e-5ecb7ce98012}	
Application Type:		_
Authentication Level		~
Service Name:	CitrixSmAudAgent	
Leam more about <u>setting</u>	<u>q these properties</u> .	
	OK Cancel App	bly

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

Launch and Activation Permission	?	×	CustReg Class
Group or user names:			-
SYSTEM Administrator			DockInterfa. COM serve
Administrator (AWTSVDA-0001\Administrator)	Remove		EmailClient Class
Select Users, Computers, Service Accounts, or Group			×
Select this object type:	13		<u>^</u>
Users, Groups, or Built-in security principals			Object Types
From this location:			
bvt.local			Locations
Enter the object names to select (examples):			
			Check Names
<u>A</u> dvanced	0	К	Cancel

Launch and Activation Permission	n	?	\times
Security			
Group or user names:			_
SYSTEM			
Administrator)1\ Administrator)		
Administrator (AWTSVDA-000 guoxiangzh (UQYEB\guoxian			
	3-17		
	Add	Remove	
	L		
		-	
Permissions for guoxiangzh	Allow	Deny	_
Permissions for guoxiangzh Local Launch	Allow	Deny	
	Allow	Deny	
Local Launch		Deny	
Local Launch Remote Launch	Allow	Deny	1
Local Launch Remote Launch Local Activation	Allow	Deny	
Local Launch Remote Launch Local Activation		Deny	
Local Launch Remote Launch Local Activation		Deny	
Local Launch Remote Launch Local Activation		Deny	
Local Launch Remote Launch Local Activation		Deny	
Local Launch Remote Launch Local Activation		Deny	

Note:

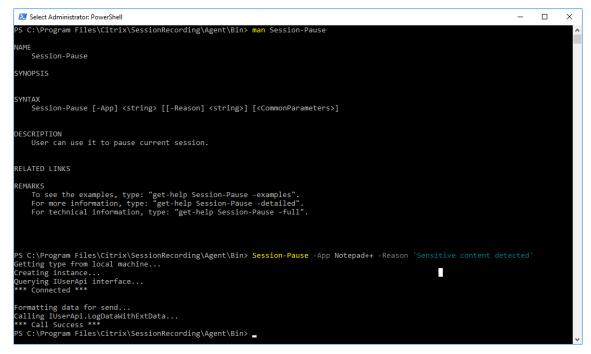
DCOM configuration takes effect immediately. There is no need to restart any services or the machine.

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

Parameter	Description	Required or Optional
-APP	The app name that calls the cmdlet.	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.	

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



Search for and play back recordings with tagged events

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

In the Session Recording player, click Advanced Search on the tool bar or choose Tools > Advanced Search.

2. Define your search criteria in the **Advanced Search** dialog box.

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

🗊 Advanced Search	×
Saved Searches Save As Reset Values	
Search Criteria	
Common Date/Time Events Other	
Citrix-defined events and events inserted by third-party applica recordings with target events tagged, set the search criteria be	ations can be tagged while a session is being recorded. To search for low.
Event text:	
Event type: Citrix. Event Monitor. App End Citrix. Event Monitor. App Start Citrix. Event Monitor. CDMUSBDriveAttac Citrix. Event Monitor. Clipboard Citrix. Event Monitor. FileCreate Citrix. Event Monitor. FileDelete Citrix. Event Monitor. FileBove Citrix. Event Monitor. FileRename Citrix. Event Monitor. Generic. USBDriveAttac	
Query Builder Citrix. Event Monitor. TopMost Citrix. Event Monitor. Web Browsing Find the 200 most relevant re Citrix. UserApi.SessionPause Citrix. UserApi.SessionResume Any Citrix-defined event	
Search Stop	Close

Note:

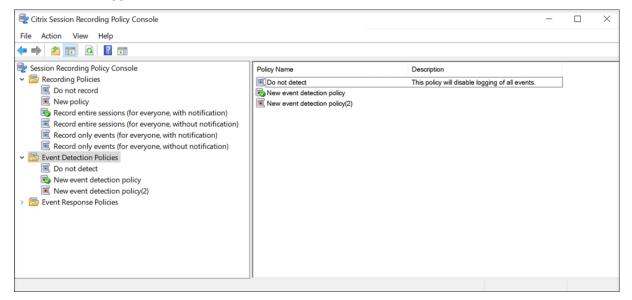
- The **Event type** list itemizes all event types. You can select an event type to search. Selecting **Any Citrix-defined event** means to search for all recordings with any type of events logged by Citrix Session Recording.
- The **Event text** filter supports partial match. Wildcards are not supported.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

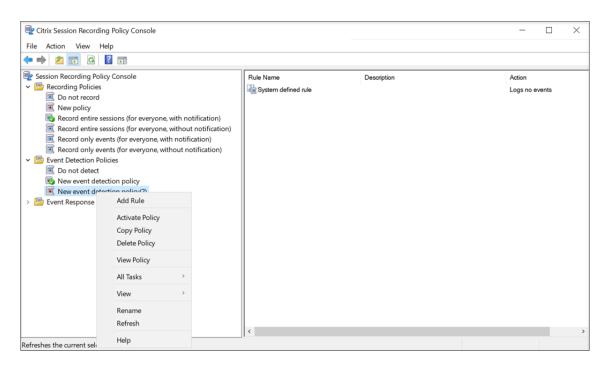


You cannot modify or delete the system-defined event detection policy.

Create a custom event detection policy

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.

Session Recording 2204

🕎 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	~
	Cruch
< Back Next >	Cancel

Rules Wizard	×
Step 1: Select one or more of the following options to specify whether to log the related events.	
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	
Log user account modifications	
Log RDP connections	
Log app installs and uninstalls	
Log performance data	
Log popup windows	~
< 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.

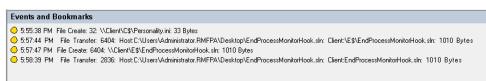
• App monitoring list: When you select Log app start events and Log app end events, use the App monitoring list to specify target applications to monitor and to avoid an excessive number of events from flooding the recordings.

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

View: Events \lor	
Q file	Υ
00:01:32 File transfer:1080 Host:C:\Users\	
© 00:01:40 File transfer:1080 Client:GAHear	
© 00:01:56 File transfer:1080 Text Docu	4: Client:New 💙
© 00:01:59 File transfer:1080 Client:DataVisu	
. 00.02.03 File	
File overte procent	tod in the Session Decording

- File events presented in the Session Recording Player



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

Note:

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

\Documents in the File monitoring list.

- Separate monitored paths with a semicolon (;).
- Only exact matches are supported. Wildcards aren't supported.
- Path strings are case-insensitive.

Limitations:

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

Events and E	3ookmarks		
😑 5:42:32 AM	Web browsing:	https://www.google.com,	Google - Google Chrome, chrome

List of supported browsers:

Browser	Version
Chrome	69 and later
Internet Explorer	11
Firefox	61 and later

• 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	
😑 1:56:39 AM	Top-most window: explorer, Application.evtx, 7212	
😑 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, Bisijisbb j.docx, 8896	
🕒 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	
O 1:57:51 AM	Top-most window: regedit, FileOperationMonitorList, 6584	
😑 1:58:04 AM	Top-most window: notepad++, shi, 4940	
O 1:58:25 AM	Top-most window: explorer, Task Switcher, 7212	
<mark>O</mark> 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 target registries you want to monitor and separate the paths with a semicolon (;). Start a path with HKEY_USERS, HKEY_LOCAL_MACHINE, or HKEY_CLASSES_ROOT. For example, you can type HKEY_LOCAL_MACHINE\ SOFTWARE\Microsoft\Windows; HKEY_CLASSES_ROOT\GuestStateVDev. If you leave this list unspecified, no registry modification is captured.
- Log app failures: Logs unexpected app exits and unresponsive apps. This rule applies to all apps.
- Log user account modifications: Logs the following user account modifications: account creation, enablement, disablement, deletion, lockout, name changes, and password modification attempts.
- Log RDP connections: Logs RDP connections initiated from the VDA hosting the recorded session.
- Log app installs and uninstalls: Logs app installs and uninstalls during the recorded session. This rule applies to all apps.
- Log performance data: Enables the session data overlay feature. Select this check

box to view data points related to the recorded session.

- **Log popup windows**: Logs popup windows that might appear when users open or close a confidential file or access a folder.
- b) Select and edit the rule criteria.

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

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

Note:

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

c) Follow the wizard to complete the configuration.

	e for this rule:			
ile1				
rovide a desc	ription for this rule:	:		
pecific user rule	filter			
Enable this rul	e			
ummary (click	Back to edit):			
otions selected:				
g &CDM mappe	d USB events			
ule criteria:				
Jsers / Groups	Published Resources	Delivery Groups / Machines	IP Address / IP Range	
_	Location			
Name 🎖 user	Location JZUAI-SI	RS-1		
_		RS-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:

EDIE VH	liew Favorites Help				 	
	Location	^ Name	Type	Data		
		🙈 (Default)	REG_SZ	(value not set)		
	> - MSLicensing	AppMonitorList	REG_MULTI_SZ	regedit.exe cmd.exe powershell.exe wsl.exe		
	> - PortICA Print	#EnableAccountChangeEvents	REG_DWORD	0x00000001 (1)		
		#EnableAppChangeEvents	REG_DWORD	0x00000001 (1)		
	> - ServerFTA	# EnableAppFaultEvents	REG_DWORD	0x00000001 (1)		
	> Agent	# EnableAppLaunchEvents	REG_DWORD	0x00000002 (2)		
	SessionEvents	# EnableCDMUSBDriveEvents	REG_DWORD	0x00000001 (1)		
	3	# EnableClipboardEvents	REG_DWORD	0x00000001 (1)		
	> - StackAgentinfo	EnableFileOperationMonitorEve.	REG_DWORD	0x00000001 (1)		
	SvcHost	EnableGenericUS8DriveEvents	REG_DWORD	0x00000001 (1)		
	Telemetry	# EnableIdleEvent	REG DWORD	0x00000001 (1)		
	> - UniversalPrintDrivers	# EnablePerfDataEvents	REG_DWORD	0x00000001 (1)		
		# EnablePopupWindowEvents	REG_DWORD	0x00000001 (1)		
	> - Versions	# EnableRDPConnectionEvents	REG DWORD	0x00000001 (1)		
	> - VirtualDesktopAgent	# EnableRegistryOperationMonito.	REG DWORD	0x00000001 (1)		
	— WebAuthnAllowedProcesses	Second Se	REG_DWORD	0x00000001 (1)		
	> - XenTools	# EnableTopMostEvents	REG_DWORD	0x00000001 (1)		
	— XenToolsInstaller	EnableWebBrowsingActivities	REG_DWORD	0x00000001 (1)		
	> - XenToolsNetSettings	FileOperationMonitorList	REG_MULTI_SZ	c/windows \\		
5.	Classes	HoleEventActivePktNumThrottle	REG_DWORD	0x00000000 (0)		
2.	Clients	HideEventActivePktSizeThrottle	REG_DWORD	0x00000000 (0)		
5.	Google	# IdleEventActiveThrottle	REG DWORD	0x00000000 (0)		
2.	Intel	# IdleEventThrottle	REG DWORD	0x00000000 (0)		
	malicious	RegistryOperationMonitorList	REG_MULTI_SZ	\REGISTRY\MACHINE		
5.	Martin Prikryl	Contractory operation and the	neograe. Gae			
2.	Microsoft					
1.51	MozillaPlugins	~				

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).

Registry Value	Description
EnableAppChangeEvents	 1: enables detecting app installs and uninstalls; 0: disables detecting app installs and uninstalls (default value data).
EnableAppFaultEvents	 1: enables detecting app failures; 0: disables detecting app failures (default value data).
EnableAppLaunchEvents	 1: enables detecting only app starts; 2: enables detecting both app starts and ends; 0: disables detecting app starts and ends (default value data).
AppMonitorList	Specifies target apps to monitor. No app is specified by default, which means no app is captured by default.
EnableCDMUSBDriveEvents	1: enables detecting the insertion of CDM mapped USB mass storage devices; 0: disables detecting the insertion of CDM mapped USB mass storage devices (default value data).
EnableClipboardEvents	 1: enables detecting clipboard activities; 0: disables detecting clipboard activities (default value data).
EnableFileOperationMonitorEv	ent 1 : enables detecting file operations; 0 : disables detecting file operations (default value data).

Registry Value	Description	
FileOperationMonitorList EnableGenericUSBDriveEvents	Specifies target folders to monitor. No folder is specified by default, which means no file operation is captured by default. 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	
EnablePerfDataEvents	 data). 1: enables the session data overlay feature; 0: disables the session data overlay feature 	
EnablePopupWindowEvents	(default value data). 1 : enables detecting popup window events; 0 : disables detecting popup window events (default value data).	
EnableRDPConnectionEvents	1: enables detecting RDP connections; 0: disables detecting RDP connections (default value data).	
EnableRegistryOperationMonito	rEleettables 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.	

Registry Value	Description
EnableWebBrowsingActivities	 1: enables detecting web browsing activities; 0: disables detecting web browsing activities (default value data).

Here are some compatible scenarios:

- If your Session Recording is newly installed or upgraded from a release earlier than 1811 that doesn't support event detection (logging), the related registry values on each Session Recording agent are the default. Because there is no active event detection policy by default, no events are logged.
- If your Session Recording is upgraded from a release earlier than 1811 that supports event detection but has the feature disabled before your upgrade, the related registry values on each Session Recording agent remain the default. Because there is no active event detection policy by default, no events are logged.
- If your Session Recording is upgraded from a release earlier than 1811 that supports event detection and has the feature partially or fully enabled before your upgrade, the related registry values on each Session Recording agent remain the same. Because there is no active event detection policy by default, the event detection behavior remains the same.
- If your Session Recording is upgraded from 1811, the event detection (logging) policies configured in the policy console remain in use.

Caution:

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

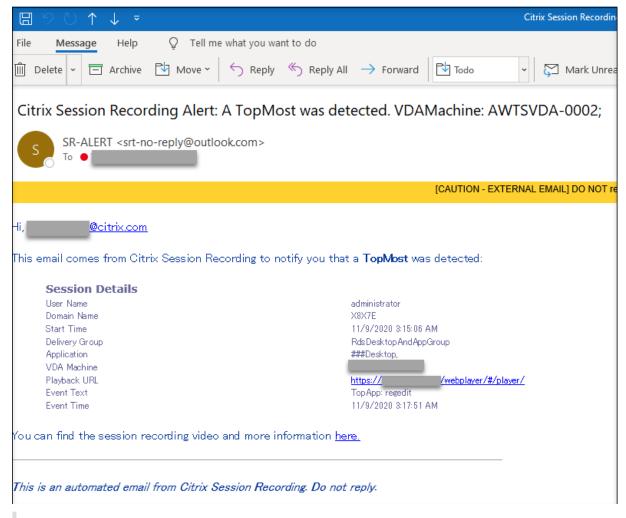
Configure event response policies

August 16, 2022

This policy setting lets you send email alerts and start screen recording immediately in response to logged events in recorded sessions. If you record only specific events without capturing any screens, you can configure an event trigger to start screen recording immediately when a specific event occurs. This feature is called event-triggered dynamic screen recording.

The only system-defined event response policy is **Do not respond**. You can create custom event response policies as needed. Only one event response policy can be active at a time.

For an example email alert, see the following screen capture:



Tip:

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

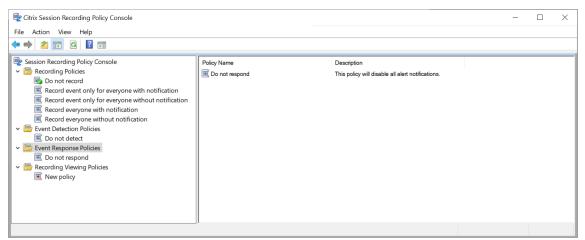
System-defined event response policy

Session Recording provides one system-defined event response policy:

• **Do not respond**. By default, neither email alerts nor dynamic screen recording is provided 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.

Email alert when a session start is detected		
Use event triggers to specify how to respond when a	a session event is detected.	
Configure event triggers (0)		
tep 1-2: Enter email addresses for the alert n	ecipients and set time spans for dynamic screen recording.	
mail recipients:		
	ling to this rule. Separate the addresses with a semicolon (;).	
creen recording time span after we detect an event:		
low many minutes do you want us to record the screer	after we detect an event?	
creen recording time span before we detect an event	(available only for virtual desktop sessions):	
low many seconds of the screen recording do you wai	nt us to keep before we detect an event?	

- 7. (Optional) Set email recipients and the email sender properties.
 - a) Type email addresses for the alert recipients in the **Rules** wizard.
 - b) Configure outgoing email settings in the Session Recording Server Properties.

Session Recording 2204

ollover	Playback	Notfications	CEIP	Logging	RBAC	Email	Cloux	• •
SMTP s	erver:	smtp.office365	.com					
Port:		587	$\mathbf{\nabla}$	Enable S	SL.			
Display	name:	Session Rec	ording /	Vert System				
Email a	ddress:	srt-no-reply@o	utlook)	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		🗹 Deliv	very group			
	Applicat	ion		🗹 Appl	ication			
	VDA Ma	chine		VDA	Machine			
				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 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 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.

After you select **Use event triggers to specify how to respond when a session event is de-tected**, the **Configure Event Triggers** button becomes available. Click it to specify logged events that can trigger email alerts, dynamic screen recording, or both.

_			_		Dimension 1					Dimension 2	_		-		Send email	Start screen recording	Description
	Event type is	File Create	~	and	Path	~	Equals	~	and	File size (MB)	~	Greater th	~	then			
	Or event type is	Top Most	~	and	App name	~	Equals	~	and	Window title	~	Equals	~	then			
	Or event type is	CDM USB	~	and	Drive letter	~	Equals	~	and		~		~	then			
	Or event type is	File Rename	~	and	Path	~	Equals	~	and	Name	~	Equals	~	then			
	Or event type is		~	and		~		~	and		~		~	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 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 rules. 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. Set the time spans for dynamic screen recording:

- Screen recording time span after a session event is detected: 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 a session event is detected: You can configure how many seconds of the screen recording you want to keep before events are detected. This feature is available only for virtual desktop sessions. The value ranges from 1 to 120. Setting the value to any of 1 through 10 makes the value 10 effective. If you leave the value unspecified, the feature does not take effect. The actual length of the screen recording that Session Recording keeps might be a little longer than your configuration.

🕎 Rules Wizard	×
Step 1-1: Select one or more of the following options.	
Email alert when a session start is detected.	
Use event triggers to specify how to respond when a session event is detected.	
Configure event triggers (0)	
Step 1-2: Enter email addresses for the alert recipients and set time spans for dynamic screen recordin	ig.
Email recipients:	
Type the email addresses who will receive alerts according to this rule. Separate the addresses with a semicolon (;).	
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 (available only for virtual desktop sessions):	
How many seconds of the screen recording do you want us to keep before we detect an event?	
< Back Next >	Cancel

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

vent type	Dimension	Option
p Start		
		App name
		Full command line
o End		
		App name
Most		
		App name
		Windows title
Browsing		
		URL
		Tab title
		Browser name
Create		
		Path
		File size (MB)
Rename		
		Path
		Name
Move		
		Source path
		Destination path
		File size (MB)
Delete		
		Path
		File size (MB)
M USB		
		Drive letter
neric USB		
		Device name

Event type	Dimension	Option
dle		
		idle duration (Hrs)
File Transfer		
		File source
		File size (MB)
		File name
Registry Create		
		Key name
Registry Delete		
		Key name
Registry Set Value		
		Key name
		Value name
Registry Delete Value		
		Key name
		Value name
Registry Rename		
		Key name
User Account Modification		
Union and Anna Faith		User name
Unexpected App Exit		A a a a a a a a a a a
App Not Desperding		App name
App Not Responding		Ann name
New App Installed		App name
vew App installed		App name
App Uninstalled		עראין ארא
ημη oninstatieu		App name
RDP Connection		

Event type	Dimension	Option
		IP address
Popup Window		
		Process name
		Window content
Performance Data		
		CPU usage (%)
		Memory usage (%
		Net send (MB
		Net receive (MB)
		RTT (ms)
Clipboard Operation		
		Data type
		Process name
		Content

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

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

Rules Wizard	×
Step 2: Select the rule criteria.	
Users or Groups	٦
Published Applications or Desktop	
Delivery Groups or Machines	
IP Address or IP Range	
Step 3: Edit the rule criteria.	
Selecting a rule criterion above activates the option here. To edit, click the underlined value.	
Users / Groups: All Users	
Published Resources: All Applications and Desktop	
Delivery Groups / Machines: All Delivery Groups and Machines IP Address / IP Range: All IP Addresses	
In Audress / In Mange, Air In Addresses	
< Back Next > Cancel	

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 22, 2022

This section guides you through the following settings:

- Load balance Session Recording servers
- Configure database high availability

Load balance Session Recording servers

June 22, 2022

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:

```
<redirections xmlns="msmq-queue-redirections.xml">
2
           <redirection>
3
                        <from>http://<ADCHost>*/msmq/private$/
                           CitrixSmAudData</from>
4
                        <to>http://<LocalFqdn>/msmq/private$/
                           CitrixSmAudData</to>
5
           </redirection>
6
           <redirection>
                        <from>https://<ADCHost>*/msmq/private$/
7
                           CitrixSmAudData</from>
8
                        <to>https://<LocalFqdn>/msmq/private$/
                           CitrixSmAudData</to>
9
           </redirection>
10 </redirections>
11 <!--NeedCopy-->
```

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

June 22, 2022

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

June 22, 2022

Use the Session Recording player or the Session Recording web player to view, search, and bookmark recorded sessions.

If sessions are recorded with the live playback feature enabled, you can view sessions that are in progress, with a delay of 1-2 seconds.

Sessions that have a longer duration or larger file size than the limits configured appear in more than one session file.

Note:

Grant users the right to access the recorded sessions of VDAs.

Session Recording player

June 22, 2022

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

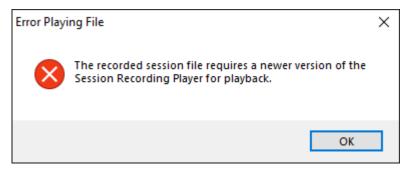
Launch the Session Recording Player

June 22, 2022

Launch the Session Recording player

Note:

- If a recording contains blocked content, Session Recording skips it. However, if you navigate to the blocked period, your playback shows a black screen and a message indicating that that content is blocked. To use this feature, use Session Recording 2012 and later.
- If you are using the Session Recording player 2009 and earlier to play back a recording, the following error message appears. The web player is not impacted.



- 1. Log on to the workstation where the Session Recording player is installed.
- 2. From the **Start** menu, choose **Session Recording Player**. The Session Recording player appears.

Be Edit We Rey Tools Help Complete Search. Complete Sea	Workspace - Administrator Workspace - Administrator Search Results User Name Application Status Status S														Contra -	
Image: Search: Revuls: Workspace: A wor	Vorspace - Administrator Vorspace - Administrator Search Results Vorspace - Administrator Pektop Gomplete Status Sacutal Results Vorspace - Administrator Dektop Complete Status Sacutal Results Sacutal Results Vorspace - Administrator Dektop Complete Status Sacutal Results Vorspace - Administrator Dektop Complete Status Sacutal Results Vorspace - Administrator Dektop Complete Status Sacutal Results Vorspace - Administrator Dektop Complete Status Sacutal Results Vorspace - Administrator Dektop Complete Status Stat		- 1											ording Player	ession Rec	CPP Se
Workspace X Search Results Vertice Search Results User Finder Search Results Complete Search Results Search Results User Finder administrator Deading Complete Search Results Search Results User Finder Search Results Search Results Complete Search Results Search Results User Finder Search Results Search Result Complete	Workspace > Administrator													/lew Play Tools Help	Edit	File
Worksgaber - Administrator Worksgaber - Administrator Delivery Group VDA Machine EventOrly Worksgaber - Administrator Delivery Group VDA Machine EventOrly Warksgaber - Administrator Warksgaber - Administrator Delivery Group VDA Machine EventOrly Mainimitation Delivery Group VDA Machine EventOrly Warksgaber - Administrator Warksgaber - Administrator Warksgaber - Administrator Delivery Group VDA Machine EventOrly Mainimitator Delikap Complete S/8/2021 E 23 AM 00.02.54 TSAgert0 Warksgaber - Administrator Delikap Complete S/8/2021 E 27 AM 00.01.64 TSAgert0 Warksgaber - Administrator Delikap Complete S/8/2021 E 27 AM 00.01.64 TSAgert0 Warksgaber - Administrator Delikap Complete S/8/2021 E 27 AM 00.01.62 TSAgert0 Warksgaber - Administrator Delikap Complete S/8/2021 E 27 AM 00.01.62 TSAgert0 Warksgaber - Administrator Delikap Complete S/8/2021 E 27 AM 00.01.62 TSAgert0 Warksgaber - Administrator Delikap Complete S/8/2021 E 27 AM 00.01.62 TSAgert0 Warksgaber - A	Workspace - Administrator Workspace - Administrator Delvey Group VDA Machine Provides Seacch Resulti Parvides Structor 1527 AM 010148 TSAgert0 W2K16517-730C3/G administrator Desktop Complete Structor 1527 AM 001444 TSAgert0 W2K16517-730C3/G administrator Desktop Complete Structor 1527 AM 001444 TSAgert0 W2K16517-730C3/G administrator Desktop Complete Structor 1227 AM 0001441 TSAgert0 W2K16517-730C3/G Domain: UYSE Administrator Desktop Complete Structor 1227 AM 0005:37 TSAgert0 W2K16517-730C3/G Domain: UYSE Application Desktop Complete Structor 127 AM 00.05:37 TSAgert0 W2K16517-730C3/G Statu: Complete Structor 136 M M Nove Playing Nove Playing M Nove Playing Nove Playing Nove Playing Nove							d Search	💧 [[Advance	- 🗯 🕯	 In last 24 hours 			🚇 🎞 💠 ≫ 🛛 Search:		b
Search Results Desktop Complete 5/8/2021 527 AM 010148 T34,pert0 W2X1651730CLGG Yee Administrator Desktop Complete 5/8/2021 518 AM 000244 T34,pert0 W2X1651730CLGG No Administrator Desktop Complete 5/8/2021 518 AM 000144 T34,pert0 W2X1651730CLG No Administrator Desktop Complete 5/8/2021 227 AM 001022 T34,pert0 W2X1651730CLG No Mow Playing Administrator Desktop Complete 5/8/2021 227 AM 0001537 T34,pert0 W2X1651730CLG Yee Mow Playing Administrator Desktop Complete 5/8/2021 227 AM 0001537 T34,pert0 W2X1651730CLG Yee Now Machine: W2X1651730CLG Situ Complete 5/8/2021 227 AM 0001537 T34,pert0 W2X1651730CLG Yee Status: Complete Situ Complete Situ Complete Yee Yee Yee Yee 22834 AM Apponted window: frefox Xee Yee Yee Yee Yee <t< td=""><td>Search Result Output Output Output Output Output Output Output Output W2R(15ST-73BCG)G Fevorites administrator0 Deletop Complete 5/8/2021 523 AM 00.024 TSAgent0 W2R(15ST-73BCG)G M2R(15ST-73BCG)G W2R(15ST-73BCG)G W2R(15ST-73BCG)G</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>Search Results</td><td>×</td><td></td><td></td><td></td></t<>	Search Result Output Output Output Output Output Output Output Output W2R(15ST-73BCG)G Fevorites administrator0 Deletop Complete 5/8/2021 523 AM 00.024 TSAgent0 W2R(15ST-73BCG)G M2R(15ST-73BCG)G W2R(15ST-73BCG)G											Search Results	×			
Favortes Favortes Low Low Complete 5/8/2021 2/2/4 M U10146 Experior W241551738GCJG No administrator Deaktop Complete 5/8/2021 2/2/2/21 1/2/4 M000244 TSAgent0 W241551738GCJG No administrator Deaktop Complete 5/8/2021 2/2/21 1/4/4 M000244 TSAgent0 W241551738GCJG No Mow Playing X X Deaktop Complete 5/8/2021 2/27.4M 00.05.37 TSAgent0 W241551738GCJG No Now Playing X X Deaktop Complete 5/8/2021 2/27.4M 00.05.37 TSAgent0 W241551738GCJG Yes Now Playing X X Deaktop Complete 5/8/2021 2/27.4M 00.05.37 TSAgent0 W241551738GCJG Yes Now Playing X X State Complete 5/8/2021 2/27.4M 00.05.37 TSAgent0 W241551738GCJG Yes 2/28.44 Mapo State State Control State State State State S	Section and the section of the sectin of the section of the section of the s	EventOnly	Eve	Machine	VD	Delivery Group	ration	Du	Start Time	Status	Application	User Name				
 	administrator Desktop Complete 5/8/2021 5124 M 00.0254 TSAgent0 W2K165T-738CGJG administrator Desktop Complete 5/8/2021 5124 M 00.0140 TSAgent0 W2K165T-738CGJG administrator Desktop Complete 5/8/2021 5124 M 00.0140 TSAgent0 W2K165T-738CGJG Now Playing ************************************	Yes	CGJG Yer	K16ST-738C0	W	TSAgent0	:01:48.	M 01	5/8/2021 5:27 A	Live	Desktop	administrator0		esults		
Administrator Desktop Complete \$19/2021 516 AM 00.01.40 T5Agent0 W2K165T-330C.G.G No Now Playing Administrator Desktop Complete \$19/2021 2.27 AM 00.02.37 T5Agent0 W2K165T-330C.G.G Yes Now Playing Administrator Desktop Complete \$19/2021 2.17 AM 00.05.37 T5Agent0 W2K165T-330C.G.G Yes Now Charles W3K165T-330C.G.G T5Agent0 W2K165T-330C.G.G Yes Yes Yes Domains U0YEB Starts Complete \$19/2021 2.17 AM 00.05.37 T5Agent0 W2K165T-330C.G.G Yes Starts Complete Starts Starts Complete \$19/2021 2.27 AM 100.05.37 Yes Yes Yes 2.2854 AM Applications Model Topmoti vindow: fretox Model Yes Yes Yes Yes 2.2324 AM Applications Yes Yes Yes Yes Yes Yes 2.2324 AM App field 1006: fretox Model Jeso Jeso Yes Yes <td< td=""><td>Image: administrator Desktop Complete 5/8/2021 5:16 AM 00:01:40 TSAgent0 W2K165T-7380C3/G Now Playing: Pesktop Complete 5/8/2021 2:27 AM 00:02:20 TSAgent0 W2K165T-7380C3/G User: administrator Desktop Complete 5/8/2021 2:17 AM 00:01:40 TSAgent0 W2K165T-7380C3/G User: administrator Desktop Desktop Desktop Desktop Desktop Desktop Domain: UVYEB Application: V2K165T-7380C3/G V2K165T-7380C3/G V2K165T-7380C3/G Statu: Statu: Complete Stafur Complete Stafur Statu: Complete Stafur Complete Stafur Stafur 228854 AM App Stat: 1968. firefox: 228:028 CVPL Complete 228054 M Topmont window: firefox, K028E CVPL Complete 228054 M Topmont window: firefox, C188E Complete Stafut 228054 M Topmont window: firefox, C188E Complete 228054 M Topmot window: firefox, C188E Complete 228054 M</td><td>No</td><td>CGJG No</td><td>(16ST-738CC</td><td>W:</td><td>TSAgent0</td><td>:02:54</td><td>M 00</td><td>5/8/2021 5:23 A</td><td>Complete</td><td>Desktop</td><td>administrator0</td><td></td><td></td><td>Favorites</td><td></td></td<>	Image: administrator Desktop Complete 5/8/2021 5:16 AM 00:01:40 TSAgent0 W2K165T-7380C3/G Now Playing: Pesktop Complete 5/8/2021 2:27 AM 00:02:20 TSAgent0 W2K165T-7380C3/G User: administrator Desktop Complete 5/8/2021 2:17 AM 00:01:40 TSAgent0 W2K165T-7380C3/G User: administrator Desktop Desktop Desktop Desktop Desktop Desktop Domain: UVYEB Application: V2K165T-7380C3/G V2K165T-7380C3/G V2K165T-7380C3/G Statu: Statu: Complete Stafur Complete Stafur Statu: Complete Stafur Complete Stafur Stafur 228854 AM App Stat: 1968. firefox: 228:028 CVPL Complete 228054 M Topmont window: firefox, K028E CVPL Complete 228054 M Topmont window: firefox, C188E Complete Stafut 228054 M Topmont window: firefox, C188E Complete 228054 M Topmot window: firefox, C188E Complete 228054 M	No	CGJG No	(16ST-738CC	W:	TSAgent0	:02:54	M 00	5/8/2021 5:23 A	Complete	Desktop	administrator0			Favorites	
Automistrator Desktop Complete 5/9/2021 2:17 AM 00.02:20 TSAgent0 W2K16ST-738CGJG Yes Uter: administrator Desktop Complete 5/9/2021 2:17 AM 00.05:37 TSAgent0 W2K16ST-738CGJG Yes Domain: UUYEB administrator Desktop Complete 5/9/2021 2:17 AM 00.05:37 TSAgent0 W2K16ST-738CGJG Yes Domain: UUYEB administrator Desktop Complete 5/9/2021 2:17 AM 00.05:37 TSAgent0 W2K16ST-738CGJG Yes Domain: UUYEB administrator Desktop Complete S/9/201 2:27 AM S/9/201 2:27 AM <td>Now Playing administrator Desktop Complete 5/8/2021 2.27 AM 00.02.20 TSAgent0 W2K16ST-380CsJG User: administrator Desktop Complete 5/8/2021 2.17 AM 00.05.37 TSAgent0 W2K16ST-380CsJG Domain: U/YEB Application: Desktop Desktop Desktop Desktop Desktop Denain: U/YEB Outrop State: S</td> <td>No</td> <td>CGJG No</td> <td>(16ST-738CC</td> <td>W:</td> <td>TSAgent0</td> <td>:04:44</td> <td>M 00</td> <td>5/8/2021 5:18 A</td> <td>Complete</td> <td>Desktop</td> <td>administrator</td> <td></td> <td></td> <td></td> <td></td>	Now Playing administrator Desktop Complete 5/8/2021 2.27 AM 00.02.20 TSAgent0 W2K16ST-380CsJG User: administrator Desktop Complete 5/8/2021 2.17 AM 00.05.37 TSAgent0 W2K16ST-380CsJG Domain: U/YEB Application: Desktop Desktop Desktop Desktop Desktop Denain: U/YEB Outrop State: S	No	CGJG No	(16ST-738CC	W:	TSAgent0	:04:44	M 00	5/8/2021 5:18 A	Complete	Desktop	administrator				
Image: State: State: State	Now Playing administrator Desktop Complete 5/8/2021 2.17 AM 00.05.37 TSAgent0 W2K16ST-330CGJG Use:: administrator Application: Outor Application: App	No	CGJG No	(16ST-738CC	W:	TSAgent0	:01:40	M 00	5/8/2021 5:16 A	Complete	Desktop	administrator				
Now Playing User: administrator Domain: UUYEB Application: Desktop Delivery Group: TSAper10 VDA Machine: WX:1851-7380G/IG Site: site: site: site: site: site: Statu: Complete Statu: Statu: <t< td=""><td>Now Playing × Uer: administrator Domain: UQYEB Application: Desktop Delivery Group: TSAgent0 VDA Machine: V/2X16S1-739CGJG Site: site Statu: Complete Statu: Solution: Outmain: 1927 27 AM Ionim: FiR/2001 227 AM Ionim: FiR/2001 227 AM Ionim: FiR/2001 227 AM 22854 AM Topmost window: firefox, Mozilla Fin 22854 AM Topmost window: firefox, Mozilla Fin 22805 AM Topmost window: SelficepreinceH 22805 AM Pape Ind 10385: firefox 22820 A</td><td>Yes</td><td>CGJG Yes</td><td><16ST-738C0</td><td>W</td><td>TSAgent0</td><td>:02:20</td><td>M 00</td><td>5/8/2021 2:27 A</td><td>Complete</td><td>Desktop</td><td>administrator</td><td></td><td></td><td></td><td></td></t<>	Now Playing × Uer: administrator Domain: UQYEB Application: Desktop Delivery Group: TSAgent0 VDA Machine: V/2X16S1-739CGJG Site: site Statu: Complete Statu: Solution: Outmain: 1927 27 AM Ionim: FiR/2001 227 AM Ionim: FiR/2001 227 AM Ionim: FiR/2001 227 AM 22854 AM Topmost window: firefox, Mozilla Fin 22854 AM Topmost window: firefox, Mozilla Fin 22805 AM Topmost window: SelficepreinceH 22805 AM Pape Ind 10385: firefox 22820 A	Yes	CGJG Yes	<16ST-738C0	W	TSAgent0	:02:20	M 00	5/8/2021 2:27 A	Complete	Desktop	administrator				
User: administrator Denktop Desktop Desktop Desktop Desktop Delivery Group: TSAgent0 VDA Machine: W2K16517380.GJG Site: site Statu: Complete Statu: Complete Statu: SPR/2021 2:27 AM Prior Strate S168: (frefox: 2282 TAM App: State 1968: (frefox: 2282 "C-VPL. 22854 AM App: State 1968: (frefox: 2282 "C-VPL. 22855 SAM Veb browsing: https://bjl88.com_[58 22830 AM App: State 1968: frefox: 2282 "C-VPL. 22830 AM App: State 1968: (frefox: 2382 "C-VPL. 22831 AM Topmost window: explorer, 10772 22832 TAM Topmost window: frefox, [SBE] 22832 AM App End: 10168: frefox 22832 AM App End: 1026: frefox 22	User: administrator A Domain: UQYEB Application: Deaktop Delivery Group: TSAgentu F VDA Machime: W2K1S51-730CGJG Site: site Statu: Complete Story Story Story Statu: Complete Story Story Story Statu: Story Story Story Story 2284 4M App Stat: Story Model Fr. Story 2285 4AM Top-most window: fields, Modila Fr. Story Story Story 2280 5AM Top-most window: explore: , 10772 Story Story Story Story 2280 5AM Top-most window: explore: , 10772 Story Story Story Story Story 2280 5AM Top-most window: fields, (Stift) Story Story Story Story Story 2280 5AM Top-most window: fields, (Stift) Story Story Story Story Story 2280 5AM Top-most window: fields, (Stift) Story Story Story Story Story 2280 5AM	Yes	CGJG Yes	<16ST-738C0	W:	TSAgent0	:05:37	M 00	5/8/2021 2:17 A	Complete	Desktop	dministrator				
User: administrator Denktop Desktop Desktop Desktop Desktop Delivery Group: TSAgent0 VDA Machine: W2K16517380.GJG Site: site Statu: Complete Statu: Complete Statu: SPR/2021 2:27 AM Prior Strate S168: (frefox: 2282 TAM App: State 1968: (frefox: 2282 "C-VPL. 22854 AM App: State 1968: (frefox: 2282 "C-VPL. 22855 SAM Veb browsing: https://bjl88.com_[58 22830 AM App: State 1968: frefox: 2282 "C-VPL. 22830 AM App: State 1968: (frefox: 2382 "C-VPL. 22831 AM Topmost window: explorer, 10772 22832 TAM Topmost window: frefox, [SBE] 22832 AM App End: 10168: frefox 22832 AM App End: 1026: frefox 22	User: administrator Domain: UQYEB Application: Desktop Delivery Group: TSAgentU VDA Machine: V2X1651-730CGJG Site: site Statu: Complete Statu: Complete Statu: S/8/2021-227 AM Loninr 5/8/2021-227 AM Loninr 5/8/2021-227 AM 2284 AM App Stat: 9168; firefor: 2328: "C.VPL. ^ 2 228 54 AM Top-most window: Kifetor, Mocilla Fin. 2 228 54 AM Top-most window: Kifetor, 10772 2 228 02 AM Top-most window: Splore: , 10772 2 228 02 AM Top-most window: splore: , 10772 2 228 12 AM App End 11056: firefox 2 228 20 AM App End 11056: firefox 2 228 20 AM App End 11056: firefox 2 228 21 AM App End 11056: firefox												×		Plaving	Now
Domain: UQYEB Application: Desktop Debrivey Group: TSAgent0 VDA Machine: W2X16ST-7380C3/G Site:: site Statu:: Complete Statu:: Statu:: Statu:: Statu:: Statu:: Statu:: VDA Machine: Y2X16ST-7380C3/G VEnts and Bookmarks: X 22849 MM App Stat: 9168: firefox: 2328: "C.PL:	Domain:UQYEBApplication:DesktopDelivey Group:TSAgent0VDA Machine:V2X1651-730CGJGSite:siteStatu:CompleteStatu:5/8/2021 227 AMInnir:F/8/2021 227 AMInnir:F/8/2021 227 AM22849 AMApp Stat: 9168: firefox: 2328: "C.VPL.22849 AMApp Stat: 9168: firefox: 2328: "C.VPL.22859 AMVeb browsing: https://bistoc.mc.fise.22859 AMTop-most window: Splete., 107722280 AMTop-most window: Splete., 1077222812 AMFile Rename: 10772: C.VestVS.bt.I 5 L.228251 AMTop-most window: Splete., 1077222812 AMFile Rename: 10772: C.VestVS.bt.I 5 L.228251 AMTop-most window: Splete., 1077222821 AM App End: 10365: firefox2282 SAM App End: 1036: firefox2282 SAM App End: 1036: firefox <t< td=""><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>administrator</td><td></td><td></td></t<>													administrator		
Application: Desktop Deliverginou: TSAgent0 VDM Machine: V2K15ST73060.06 Site: ate Statu: Complete Statu: Site: 5/8/2021 2.27 AM V VEXENST model: V 22843 AM App Stat: Site: 228454 AM Top-most window: firefox. Mozilla Fir 228355 AM Verbowsing: fittp://bj8.6com, f58 228301 AM Top-most window: seplorer, 10772 228302 AM Top-most window: seplorer, 10772 228320 AM pp End: 1085; firefox 22832 22832 AM App End: 108; firefox 22832 22832 AM App End: 128; pirgenedee: 280 22832 AM App End: 128; pirgenedee: 280	Application: Desktop Defivery Group: TSAgentU VDA Machine: W2K15817380CB/G Site: site Site: site Stat: 5/8/2021 2:27 AM Stat: 5/8/2021 2:27 AM Site: 5/8/2021 2:27 AM 2:28:54 AM Topmost window: firefox, firefox, firefox 2:28:54 AM Topmost window: splore, 10772 2:28:05 AM Veb browsing: http://bj8.com. [58. 2:28:55 AM Topmost window: splore, 10772 2:28:50 AM Topmost window: splore, 10772 2:28:51 AM Topmost window: splore, 10772 2:28:51 AM Topmost window: splore, 10772 2:28:20 AM Topmost window: splore, 10772 2:28:20 AM Topmost window: firefox 2:28:21 AM App End: 10356; firefox 232:21 AM 2:28:22 AM App End: 10356; firefox 2:28:22 AM App End: 10356; firefox 2:28:22 AM App End: 10356; firefox 228:21 AM 2:28:22 AM App End: 10356; firefox 228:21 AM 2:28:22 AM App End: 1056; firefox 228:21 AM 2:28:22 AM App End: 1056; firefox 228:21 AM															
Delivery Group: TSAgert0 VDA Machine: W2K157-730CGJG Statu: Complete Statu: Complete Statu: StaP/2021 2.27 AM L roirr 5/8/2021 2.27 AM 2 2849 AM App Statt: 1968: firefox: 2328: "C.VP. 2 2845 AM Top-most window: firefox, Mosters Fri. 2 2855 AM Vebrowsing: http://bj8.com, f58. 2 2830 AM Top-most window: seplorer, 10772 2 2831 AM Top-most window: seplorer, 10772 2 2831 AM Top-most window: firefox, [SB@WR] 5 2 2831 AM Top-most window: seplorer, 10772 2 2832 AM App End: 1086: firefox 2 2832 AM App End: 1286: firefox 2 2832 AM App End: 1286	Delivery Group: TSAgent0 VDA Machime: V/2K1551-7380GJG Site: ale Stat: Complete Stat: StaVD21227 AM Lonim: F38/D721272 AM V Events and Bookmarks × 2 228:49 AM App Stat: 9168. firefox: 2328. "C.VPL: A 2 228:54 AM Top-most window: kifefox, Mozilla Fr 2 228:54 AM Top-most window: explorer., 10772 2 228:02 AM Top-most window: explorer., 10772 2 229:01 AM Top-most window: explorer., 10772 2 229:01 AM Top-most window: explorer., 10772 2 229:02 AM Top-most window: explorer., 10772 2 229:02 AM Top-most window: explorer., 10772 2 229:05 AM Top-most window: firefox, [58] mg 5 2 229:15 AM Top-most window: firefox, [59] mg 5 2 229:04 App End: 1036; firefox 2 229:04 App End: 1036; firefox															
VDA Machine: W2K16ST-7380C6JG Site::::::::::::::::::::::::::::::::::::	VDA Machine: W2K16S17-380CGJG Site:: alte Statu:: Complete Statu:: 5/8/2021 227 AM Panire: 10/96 Stat: Panire: 10/97 AM Panire: 10/72 Panire: 10/72 Panire: 10/72 Panire: 10/97 AM Panire: 10/97 AM Panire: 10/97 AM Panire: 10/77 AM Panire: 10/97 AM Panire: 10/97 AM Panire: 10/97 AM P															
Statux Complete Statux SP8/2021 2.27 AM Vectors and Bowmarks X 2 284.94 M App Stat: 9168: frefox 2328: "C:VPL A 2 285.95 AM Top-most window: frefox, Moalls Fin. 2 285.95 AM Top-most window: septore, .10772 2 283.02 AM Top-most window: septore, .10772 2 283.15 AM Top-most window: Spetigris fielox 2 283.22 AM App End: 1058: fielox 223.23 AM App End: 1058: fielox 2 283.22 AM App End: 1985. fielox 223.23 AM App End: 1985. fielox 2 283.22 AM App End: 1985. fielox 223.23 AM App End: 1985. fielox 2 283.22 AM App End: 1985. fielox 223.23 AM App End: 1985. fielox 2 283.22 AM App End: 1985. fielox 223.23 AM App End: 1985. fielox 2 283.23 AM App End: 1928. conhost 2276: N72. 2283.24 M App End: 1928. conhost 2276: N72. 2 283.23 AM App End: 1928. conhost 2276: N72. 2283.24 M App End: 1928. conhost 2276: N72. 2 283.23 AM App End: 1928. fielox 1 2 283.24 M App End: 1928. fielox 1 2 283.23 AM	Statur: Domplete Statt 5/8/2021 2:27 AM Statt 5/8/2021 2:27 AM Events and Borkmarks × 2 288 49 AM App Statt: 9168: firefox: 2328: "CVPL: A 2 288 54 AM Top-most window: firefox, Mozila Fir × 2 285 54 AM Top-most window: explore:, 10772 × 2 283 54 AM Top-most window: explore:, 10772 × 2 283 54 AM Top-most window: explore:, 10772 × 2 283 54 AM Top-most window: Shell ExperienceH × 2 283 54 AM Top-most window: explore:, 10772 × 2 283 55 AM Top-most window: Shell ExperienceH × 2 283 55 AM Top-most window: Shell ExperienceH × 2 283 55 AM Top-most window: Shell Statt 5 2 283 20 AM App End: 10166: firefox × × 2 283 20 AM App End: 10136: firefox × × 2 283 21 AM App End: 10136: firefox × 2 283 21 AM App End: 10166: firefox × 2 283 21 AM App End: 1016: firefox × 2 283 21 AM App End: 10160: firefox ×															
Stat: 5/8/2021 227 AM Lowine 5/8/2021 277 AM Parite 5/8/2021 277 AM Value 5/8/2021 277 AM Value 5/8/2021 277 AM Value 5/8/2021 277 AM Value Xalue V	Stat: 5/8/2021 2.27 AM × Loninr 5/8/2021 2.57 AM × Events and Bookmarks × C284 9AM App Stat: 9168. firstox 2328. "C.VPL. ^ 2284 9AM Top-most window: Kellscover, Mozilla Fir. 2289 1AM Top-most window: spleter, 10772 2291 0AM Top-most window: spleter, 10772 2291 2AM Top-most window: firstox, [S6F] #5. 2292 5AM Top-most window: spleter, 10772 2293 1AM Top-most window: spleter, 10772 2293 1AM Top-most window: spleter, 10772 2293 2AM Top-most window: spleter, 10772 2293 1AM Top-most window: spleter, 10772 2293 2AM App End: 10365; firefox 2293 2AM App End: 1036; firefox 2293 2AM App End: 106; firefox 2293 2AM App													site		Site:
1 nair 5.08/0012 272 AM V Vertes and Bookmarks X 2 2849 AM App Start: 9168: firefox: 2328: "C.VPL X 2 2854 AM Top-most window: firefox, folds: Fire. 2 2 2859 AM Veb browsing: http://bj.86 com, f58 X 2 2859 AM Veb browsing: http://bj.86 com, f58 X 2 2805 AM Top-most window: seplorer, 10772 X 2 2815 AM Top-most window: seplorer, 10772 X 2 2815 AM Top-most window: firefox, [58@] \$K\$ X 2 2815 AM Top-most window: firefox, [58@] \$K\$ X 2 2815 AM Top-most window: firefox, [58@] \$K\$ X 2 2815 AM Top-most window: firefox, [58@] \$K\$ X 2 2817 AM Top-most window: firefox, [10772 X 2 2823 AM App End: 1086: firefox X 2 2823 CM App End: 1086: firefox X 2 2823 ZM App End: 1986: firefox Y 2 2823 ZM <td>Innir 5/8/2021 2-22 AM V Events and Borkmarks X 2.2849 AM App Statt: 9168: firefox 2328: "CVPLA 2.2849 AM App Statt: 9168: firefox 2328: "CVPLA 2.2859 AM Veb browsing: https://bj8c.com.[58 2.2830 AM Top-most window: explorer, 10772 2.2901 AM Top-most window: shellExperienceH 2.2830 AM Top-most window: firefox, [587])% 5 2.2812 AM File Renam: 10772: C/vetAlS.bt I S.L. 2.2820 AM App End: 10366: firefox 2.2821 AM App End: 10366: firefox 2.2822 AM App End: 10366: firefox 2.2823 AM App End: 10366: firefox 2.2824 AM<</td> <td></td> <td>Complete</td> <td>18:</td> <td>Statu</td>	Innir 5/8/2021 2-22 AM V Events and Borkmarks X 2.2849 AM App Statt: 9168: firefox 2328: "CVPLA 2.2849 AM App Statt: 9168: firefox 2328: "CVPLA 2.2859 AM Veb browsing: https://bj8c.com.[58 2.2830 AM Top-most window: explorer, 10772 2.2901 AM Top-most window: shellExperienceH 2.2830 AM Top-most window: firefox, [587])% 5 2.2812 AM File Renam: 10772: C/vetAlS.bt I S.L. 2.2820 AM App End: 10366: firefox 2.2821 AM App End: 10366: firefox 2.2822 AM App End: 10366: firefox 2.2823 AM App End: 10366: firefox 2.2824 AM<													Complete	18:	Statu
Charler SAXAD12 276 BM Events and Bookmarks X 22849 AM App Start: 9168: firefox: 2328: "C.VPL. 22859 AM Top-most window: firefox, Mozilla Fir 22830 AM Top-most window: shell specienceH 22830 AM Top-most window: shell specienceH 22831 AM Top-most window: shell specienceH 22831 AM Top-most window: shell specienceH 22832 AM Top-most window: firefox 22832 AM Top-most window: shell specienceH 22832 AM Top-most window: splereH 22832 AM	Control Stat/2011 2012 MM Events and Bookmarks X 2 284 94 M Top-most window: firefox: 2328: "CVPL													5/8/2021 2:27 AM	:	Start
22849 AM App Stat: 9168: firefox 2328: "C.VPL. ▲ 228554 AM Top-most window: firefox, Moalla Fir 228559 AM Veb browsing: https://bij58.com, [58 229310 AM Top-most window: Shell: BpeinneeH 228351 AM Top-most window: Shell: BpeinneeH 229310 AM Top-most window: Shell: BpeinneeH 229312 AM Top-most window: Shell: BpeinneeH 229313 AM Top-most window: Bield: SpeinneeH 229314 M Pap End: 10185: Intelox 229324 22932 JM App End: 10185: Intelox 2293214 M pap End: 10185: Intelox 22932 JM App End: 10185: Intelox 2293214 M pap End: 10185: Intelox 22932 JM App End: 19185 Intelox 2293214 M pap End: 19185: Intelox 22932 JM App End: 1928: Intelox 2293214 M pap End: 19185: Intelox 22932 JM App End: 1928: Intelox 2293214 M pap End: 19185: Intelox 22932 JM App End: 1928: Intelox 2293214 M pap End: 1928: Intelox 22932 JM App End: 1928: conhost: 2276: V?? 229324 M pap End: 1928: Intelox 22932 JM App End: 1928: conhost: 2276: V?? 229324 M pap End: 1928: conhost: 2276: V?? 22932 JM App End: 1928: conhost: 2276: V?? 229324 M pap End: 1928: Intelox 22933 JM App End: 1928: conhost: 2276: V?? 229324 M pap End:	 228:49 AM App Start: 3168: firefox: 2328: "C.VPL. ^ 228:54 AM Top-most window: firefox: Modille Fir 228:59 AM Web browsing: https://bj.58.com, [56] 229:01 AM Top-most window: ShellExperienceH 229:02 AM Top-most window: ShellExperienceH 229:03 Fireformat: Window: ShellExperienceH 229:04 AM App End: 1058: fireformat: ShellExperienceH 229:04 App End: 10396: fireformat: ShellExperienceH 229:04 App End: 1000; explore: 10772 												×	5/8/2021 2-27 AM	n .	l onin
22854 AM Top-most window: firefox, Mozila Fir. 22859 AM Web browsing: https://bj.8c.om, [58 22850 AM Top-most window: seplore:, 10772 2290 AM Top-most window: seplore:, 10772 22930 AM Top-most window: firefox [588]% 5 229315 AM Top-most window: firefox [588]% 5 229315 AM Top-most window: seplore:, 10772 22920 AM App End: 10356; firefox 229320 AM App End: 10256; firefox 229320 AM App End: 2026; conhost 229320 AM App End: 2026; conhost 229320 AM App End: 2026; firefox 229320 AM App End: 2026; firefox 229320 AM App End: 2026; conhost 22932	22854 AM Top-most window: firefox, Mozilla Fit 22859 AM Web browsing: https://bj8.com, [58 22901 AM Top-most window: septore:, 10772 22902 AM Top-most window: Shell SuperiorceH 22915 AM Top-most window: Shell SuperiorceH 22915 AM Top-most window: Shell SuperiorceH 22915 AM Top-most window: Signer, 10772 22915 AM Top-most window: Signer, Staff Staff St 2292 22804 M App End: 10356; firefox 229204 App End: 10356; firefox 2292 2304 App End: 10356; firefox 229214 App End: 10366; firefox 2292 2304 App End: 1056; firefox 229214 App End: 1056; firefox 2292 24 AM App End: 1056; firefox 229214 App End: 1050; firefox 2292 24 AM Top-most window: explore:, 10772												×	ookmarks	nts and B	Even
228:59 AM Web browsing: https://bj58.com,[58 22901 AM Top-most window: explorer, .10772 229:12 AM File Rename: 107272. C:Vest/6.kbt 15.t. 229:220 AM App End: 10188: firefox 229:220 AM App End: 10188: firefox 229:220 AM App End: 10158: firefox 229:220 AM App End: 10158: firefox 229:220 AM App End: 9168: firefox 229:220 AM App End: 926: conhost: 2276: 177. 229:222 AM App End: 9276: pingender: 2282: " 229:23 AM App End: 9276: pingender: 2282: " 229:24 AM App End: 9276: pingender: 2282: "	228:59 AM Web browsing: https://bj.58.com, [58 22901 AM Top-most window explore:, 10772 22902 AM Top-most window: spleter, 10772 22912 AM File Rename: 10772: C:\Uset\S.txt I 5.t. 22912 AM File Rename: 10772: C:\Uset\S.txt I 5.t. 22912 AM App End: 10168: filefox 2292 229 AM App End: 10168: filefox 2292 229 AM App End: 10156: filefox 2292 229 AM App End: 10156: filefox 2292 229 AM App End: 10168: filefox 2292 229 AM App End: 10168: filefox 2292 220 AM App End: 10168: filefox 2292 221 AM App End: 1026: filefox 2292 21 AM App End: 1026: filefox												"C:\Pr 🔺	App Start: 9168: firefox: 2328: "C:	28:49 AM	0 2:2
229301 AM Top-most window: explore; , 10772 229302 AM Top-most window: Shell ExperienceH 229305 AM Top-most window: Shell ExperienceH 229305 AM Top-most window: Shell ExperienceH 229315 AM Top-most window: Interox, [\$\$90385 5 229312 AM Pap End: 10586; firefox 229320 AM App End: 10586; firefox 229320 AM App End: 90586; firefox 229321 AM App End: 90586; firefox 229322 AM App End: 90586; firefox 229322 AM App End: 90586; firefox 229322 AM App End: 9056; firefox 229322 AM App End: 9258; conhost 2276; 1/77 2293222 AM App End: 9228; conhost 2276; 1/77 2293232 AM App End: 9228; conhost 2276; 1/77 2293234 M App End: 9228; conhost 2276; 1/77 229324 M App End: 9228; conhost 2276; 1/77 2293	229.01 AM Top-most window: explorer, .10772 229.02 AM Top-most window: Shell ExperienceH 229.05 AM Top-most window: explorer, .10772 229.12 AM File Rename: 10772: C:veat/S.bt I 5 L. 229.15 AM Top-most window: Infelox, [S9593# 5 229.20 AA App End: 10165: firefox 229.20 AA App End: 10165: firefox 229.20 AA App End: 10165: firefox 229.21 AM App End: 9588; firefox 229.22 AM App End: 10165: firefox 229.23 LAM App End: 10165: firefox 229.21 AM App End: 10165: firefox 229.22 AM App End: 10165: firefox 229.21 AM App End: 1016; firefox															
22302 AM Top-most window: ShellExperienceH 22305 AM Top-most window: explorer, 10772 22315 AM Top-most window: fields. (Slif) % 5 22315 AM Top-most window: fields. (Slif) % 5 22320 AM App End: 10356: firefox 22320 AM App End: 10356: firefox 22321 AM App End: 1056: firefox 22322 AM App End: 1056: firefox 22322 AM App End: 1267: firefox 22322 AM App End: 1267: firefox 22322 AM App End: 226: conhost: 2276: 1/Y7 22323 AM App End: 2276: pingeneter: 2328 " 22323 AM App End: 2276: pingeneter: 22323 AM App End: 2276: pingeneter: 22323 AM App End: 2276: pingeneter: 22323 AM App End: 1208: infox 22332 AM App End: 2276: pingeneter: 22333 AM App End: 2276: pingeneter: 2233 AM App End: 1208: infox 2233 AM App End: 1208: infox 2233 AM App End: 1208: infox	2:2902 AM Top-most window: ShellExperienceH 2:2905 AM Top-most window: explorer, 10772 2:2912 AM Tipe Remains: 10772: Chueth Skit 15 L 2:2913 FAM Top-most window: fields, [Stif] bit 5 2:2912 AM App End: 10356; firefox 2:292 202 AM App End: 10356; firefox 2:292 202 AM App End: 10356; firefox 2:292 202 AM 2:292 202 AM App End: 10356; firefox 2:292 202 AM 2:292 202 AM App End: 1056; firefox 2:292 214 App End: 1050; firefox 2:292 214 Am 2:292 214 Am App End: 100; firefox 2:292 214 Am 2:292 214 Am												om, (58	Web browsing: https://bj.58.com,	28:59 AM	0 2:2
229305 AM Top-most window: explorer, 10772 229312 AM File Rename: 107272 C:Vest6.btt 15 t 229312 AM App End: 10188: firefox 229320 AM App End: 10188: firefox 229320 AM App End: 10158: firefox 229321 AM App End: 9188: firefox 229322 AM App End: 9188: firefox 229322 AM App End: 9189: firefox 229322 AM App End: 928: conhost t2276: jringender: 2286: " 229323 AM App End: 928: conhost t2276: jringender: 2288: " 229323 AM App End: 928: conhost t2276: jringender: 2288: " 229323 AM App End: 928: conhost t 1001 10155: jringender: 2288: " 229324 AM App End: 928: conhost t 10155: jringender: 2288: " 229324 AM App End: 928: conhost t 10155: jringender: 2288: " 229324 AM App End: 928: conhost t 10172 229324 AM App End: 928: conhost t 10155: jringender: 2288: " 229324 AM App End: 928: conhost t 10155: jringender: 2288: " 229324 AM App End: 928: conhost t 10155: jringender: 2288: " 229324 AM App End: 928: conhost t 10155: jringender: 2288: " 0001 000000	22305 AM Top-most window: explorer, , 10772 22312 AM File Rename: 10727: C/Uset%Ext [5 L. 22315 AM Top-most window: frietox, [59司號 5 2232 AM App End: 10168: friefox 2232 AM App End: 10356: friefox 2232 AM App End: 10368: friefox 2232 AM App End: 10372: C/Uset App End: 1															
22312 AM File Rename: 10772 C.VastAsht 15 L. 22312 AM AppEnd: 10585; fieldox 22320 AM AppEnd: 10585; fieldox 22320 AM AppEnd: 10585; fieldox 22321 AM AppEnd: 1058; fieldox 22321 AM AppEnd: 1058; fieldox 22321 AM AppEnd: 1058; fieldox 22321 AM AppEnd: 1050; fieldox 22321 AM AppEnd: 120; fieldox 22323 AM AppEnd: 120; fieldox	22312 AM File Rename: 10772. C:Vest\Stat I S L. 22315 AM Top-most window: firefox, [SIGBI\$ 5 22320 AM App End: 10165; firefox 22320 AM App End: 10156; firefox 22320 AM App End: 958; firefox 22321 AM App End: 956; firefox 22321 AM App End: 160; firefox															
229.15 AM Top-most window: firefox, [\$6000 5: 229.20 AM App End: 10168; firefox 229.20 AM App End: 10168; firefox 229.21 AM App End: 9168; firefox 229.21 AM App End: 9168; firefox 229.22 AM App End: 9168; firefox 229.22 AM App End: 9160; firefox 229.22 AM App End: 9276; origoender: 2276; 1/72 229.22 AM App End: 9276; pingender: 2276; 1/72 229.23 AM App End: 9276; pingender: 2276; 1/72 229.23 AM App End: 9276; pingender: 228; " 229.23 AM	22915 AM Top-most window: firefox, [59司城 5 22920 AM App End: 10168; firefox 22920 AM App End: 10168; firefox 22920 AM App End: 9168; firefox 22920 TAM App End: 9168; firefox 22921 AM App End: 160; firefox 22921 AM App End: 160; firefox 22921 AM App End: 160; firefox															
22920 AM App End: 10168: firefox 22920 AM App End: 10056: firefox 22920 AM App End: 10056: firefox 22921 AM App End: 9158: firefox 22922 AM App End: 9158: firefox 22922 AM App End: 9226: conhost: 2276: 177. 22922 2M App End: 9226: conhost: 2276: 177. 22922 2M App End: 9226: conhost: 2276: 177. 22923 2M App End: 9226: conhost: 276: 177. 22923 2M App End: 9226: conhost: 4 times +times +	229.20 AM App End: 10168: firefox 229.20 AM App End: 10356: firefox 229.20 AM App End: 10356: firefox 229.21 AM App End: 9168: firefox 229.21 AM App End: 160: firefox 229.21 AM App End: 160: firefox 229.21 AM App End: 160: firefox															
22320 AM App End: 10356: firefox 22320 AM App End: 10356: firefox 22321 AM App End: 9988: firefox 22321 AM App End: 9186: firefox 22321 AM App End: 9186: firefox 22322 AM App End: 9282: conhost: 2276: \??\. 22322 AM App End: 2282: conhost: 2276: \??\. 22322 AM App End: 2282: conhost: 2276: \??\. 22322 AM App End: 2282: conhost: 2276: \??\. 22323 AM App End: 2276: pingender 22332 AM App End: 2276: pingender 22332 AM App End: 2276: pingender	22520 AM App End: 10356: firefox 22920 AM App End: 10356: firefox 22921 AM App End: 1056: firefox 22321 AM App End: 1160: firefox 22321 AM App End: 1160: firefox 22321 AM App End: 1160: firefox												同城 5			
229:20 AM App End: 9968; firefox 229:21 AM App End: 9168; firefox 229:21 AM App End: 9106; firefox 229:21 AM App End: 9208; conhost: 1276; V?L. 229:22 AM App Stat: 1276; pingender: 1226; V?L. 229:22 AM App End: 9227; conhost: 12276; V?L. 229:23 AM App End: 9227; conhost: 12276; vingender: 1226; vin	229.20 AM App End: 9968. firefox 229.21 AM App End: 9168. firefox 229.21 AM App End: 9168. firefox 229.21 AM App End: 160. firefox 229.21 AM Toronast window explorer: 10772															-
22921 AM App End: 9168; firefox 22921 AM App End: 9169; firefox 22921 AM App End: 160; firefox 22921 AM App End: 920; conhost: 2276; 1772. 22922 AM App Start: 2276; pingsender: 2328: " 22932 AM App End: 9226; conhost: 2276; 1772. 22932 AM App End: 9226; conhost: 2276; 1772. 22932 AM App End: 9226; conhost: 276; pingsender: 2328: " 22932 AM App End: 9226; conhost: 4 molts: +1m0s: +1m15s: +1m30s: +1m45s: +2m00s 22932 AM App End: 9276; pingsender: 2328: " 22932 AM App End: 9276; pingsender: 2328; " 22932 AM App End: 9276; pingsender: 2328; " 22932 AM App End: 9276; pingsender: 2328; " 22932 AM App End: 9276; pingsender: 9276; ping	2:29:21 AM App End: 9168: firefox 2:29:21 AM App End: 160: firefox 2:29:21 AM App End: 160: firefox 2:29:21 Am App End: 100: firefox															
22921 AM App End 100: fieldox 22921 AM App End 100: fieldox 22922 AM App Ends 2276: tyr2. 22922 AM App Start 2276: pingsender: 2328: " 229322 AM App Ends 2276: pingsender: 2328: " 229323 AM App Ends 2276: pingsender: 238: " 229323 AM App Ends 2276: pingsender: 238: " 22932 AM App Ends 2276: pingsender: 238: " 22933 AM App Ends 2276: pingsender: 238	229.21 AM App End: 160: firefox 229.21 AM Ton-most window evolver, 10772															
229.21 AM Top-most window: explorer, , 10772 229.22 AM App Statt 9228: conhost 12276: 177. 229.22 AM App End: 9228: conhost 12276: pingender 229.32 AM App End: 92276: pingender 229.32 AM App End: 92276: pingender 229.32 AM App End: 9276: pingender	O 22921 AM Top-most window explorer 10772															
22322 AM App Start 9228: conhost 2276: 177. 22322 AM App End 9228: conhost 2276: 177. 22323 AM App End 9228: conhost 22333 AM App End 92276: pingender 22333 AM App End 9276: pingender 22333 AM App End 9276: pingender 0 00 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	22322 AM TopTilda Window, explore, 7:0722 22322 AM App Stat: 3225 confust 2276 V72.												770			
229.22 AM App Start 2276: pingsender: 2328: " 229.23 AM App End: 9228: conhost 1 +0m15s 1+0m30s 1+0m45s 1+1m00s 1+1m15s 1+1m30s 1+1m45s 1+2m00s 229.23 AM App End: 92276: pingsender 229.23 AM App End: 9276: pingsender 229.23 AM App End: 9276: pingsender 229.23 AM App End: 9276: pingsender												End				
229.23 AM App End: 9228. conhost 229.32 AM App End: 9228. conhost 1 → □ → □ → □ → □ → □ → □ → □ → □ →	2:29:22 AM App Start: 2276: pingsender: 2328: "															
○ 2233 AM App End 22% pingender	2:29:23 6M (App End: 9229: cophoet	5	+2m00=	+1m45s	+1m30s	1+1m15s	005	(+1m)	+0m45s	1+0m20						
- 910/2017 2.23.20				0 0000	000 0	o anno		0		23 AM 8608	-	W2K16ST-738CG	~			
	E VIZKIGST AGCGGG ZZSZSAW BOOL MERAX SIGOL	L 1 2.23.20 F	5/6/2021		_			_	III OIUX	20 Min 0000	0 2.23	W21(1001-700CG				-

Tip: The **EventOnly** column indicates a screen recording or an event-only recording.

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

Session Reco										-		×
	New Play Tools Help											
	🧕 🎞 💠 ≫ Search:			• In last 2	24 hours 👻 💭	🕍 [🔀 Advanced	Search					
Vorkspace		×	Search Resu	lts								
Workspace - / Search Re Pavorites			User Name administrator administrator adminis adminis adminis adminis		Status Live Complete Complete Complete Complete	Start Time 5/8/2021 5:27 Al 5/8/2021 5:23 Al 5/8/2021 5:18 Al 5/8/2021 5:16 Al 5/8/2021 2:27 Al 5/8/2021 2:27 Al	M 00:02:54 M 00:04:44 M 00:01:40 M 00:02:20	Delivery Group TSAgent0 TSAgent0 TSAgent0 TSAgent0 TSAgent0 TSAgent0	W2K W2K W2K W2K W2K	Machine 16ST-738CGJG 16ST-738CGJG 16ST-738CGJG 16ST-738CGJG 16ST-738CGJG 16ST-738CGJG 16ST-738CGJG	EventOnly Yes No No No Yes Yes	y
Now Playing		×		Move to Folder								
User: Domain: Application: Delivery Group: VDA Machine: Site: Site: Status: Status: Login:	edministrator UQYEB Desktop TSAgen0 W/2K16S1-738CGJG šie Complete 5/8/2021 2.27 AM 5/8/2021 2.72 AM	< >	3	Copy to Folder Properties								
Events and Bo	ookmarks	×										
 228.54 AM 228.59 AM 229.01 AM 229.02 AM 229.02 AM 229.12 AM 229.15 AM 229.20 AM A 229.20 AM A 229.20 AM A 229.21 AM A 	App Start: 9168: firefox 2328: "C-VPL. Top-most window: firefox, Mozilla Fin- web horwsing: https://bis8c.com, [58: op-most window: explorer, 10772 Top-most window: ShellExperienceH op-most window: shellExperienceH op-most window: firefox, [58]前後 5 pp End: 10168: firefox pp End: 10168: firefox pp End: 9168 firefox pp End: 160: firefox pp End: 928 conhost: 2276: V77. Vap Start: 2276: opmost window: explorer, 10772 vap Start: 2276: 077.		End									
2:29:23 AM A	pp End: 9228: conhost pp End: 2276: pingsender			→	+0m15s +0m		+1m00s				2m00s	4
	pp End: 2328: firefox		Desktop		2:29:23 AM 86	0 00	• •		0 000		0 0 000 3/2021 2:29:1	

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 22, 2022

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:

- A digital signature can't be assigned and you can't view the certificate until recording is completed.
- Playback protection can't be applied until recording is complete. If playback protection is enabled, you can view live playback sessions. But they are not encrypted until the session is completed.
- You can't cache a file until recording is completed.

By default, live session playback is enabled.

- 1. Log on to the computer hosting the Session Recording server.
- 2. From the Start menu, choose Session Recording Server Properties.
- 3. In Session Recording Server Properties, click the Playback tab.
- 4. Select or clear the Allow live session playback check box.

Enable or disable playback protection

June 22, 2022

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 22, 2022

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**.

Open and play recordings

June 22, 2022

Open recordings

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

- Perform a search using the Session Recording player. Recorded sessions that meet the search criteria appear in the search results area.
- Access recorded session files directly from your local disk drive or a shared drive.
- Access recorded session files from a Favorites folder.

When you open a file that was recorded without a digital signature, a warning message appears. It says that the origin and integrity of the file were not verified. If you are confident of the integrity of the file, click **Yes** in the warning window to open the file.

The Session Recording player checks the Citrix Workspace app version before playing back a recorded session. If the player doesn't support the Citrix Workspace app version, an error is returned. To eliminate the error, select **Skip Citrix Workspace app version check** in **Session Recording Server Properties**.

🔖 Sessio	n Record	ling Server P	roperties		_		×
Storage	Signing	Rollover F	layback	Notifications	CEIP	Logging	RI + +
Live se This still in	ession play option per n progres	/back rmits the play	back of s	ession record			
This Sess viewe	ion Playe ed by use	crypts sessio r. This prever rs other than	nts sessio the user t	ng files before on recordings hat originally downloaded fo	from beir download	ng copied led the file	
This befor	option all e the Ses	sion Recordi	skip the C ng Player	Citrix Workspa plays back a on check befo	recording	g.	eck
				ОК	Cancel		<u>A</u> pply

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.
- 4. From the menu bar, choose **File > Folder > New Folder**. A new folder appears under the **Fa-vorites** folder.
- 5. Type the folder name, then press **Enter** or click anywhere to accept the new name.

Use the other options that appear in the **File > Folder** menu to delete, rename, move, copy, import, and export the folders.

Play recordings

After you open a recorded session in the Session Recording player, you can navigate through the recorded sessions using these methods:

- Use the player controls to play, stop, pause, and increase or decrease playback speed.
- Use the seek slider to move forward or backward.

You can also navigate through the recorded session by going to the inserted markers and custom events.

Note:

- During playback of a recorded session, a second mouse pointer might appear. The second pointer appears at the point in the recording when the user navigated within Internet Explorer and clicked an image that was originally larger than the screen but was scaled down automatically by Internet Explorer. While only one pointer appears during the session, two might appear during playback.
- This version of Session Recording doesn't support SpeedScreen Multimedia Acceleration and the Flash quality adjustment policy setting. When this option is enabled, playback displays a black square.
- When you record a session with a resolution higher than or equal to 4096 x 4096, there might be fragments in the recording appearance.

Use the player controls

You can click the player controls in the lower part of the player window or access them by choosing **Play** from the **Session Recording Player** menu bar.

Player Control	Function
	Plays the selected session file.
	Pauses playback.

Player Control	Function
	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.

Keyboard Key	Function
Home	Seeks to the beginning.
End	Seeks to the end.
Right Arrow	Seeks forward five seconds.
Left Arrow	Seeks backward five seconds.
Move the mouse wheel one notch down	Seeks forward 15 seconds.
Move the mouse wheel one notch up	Seeks backward 15 seconds.
Ctrl + Right Arrow	Seeks forward 30 seconds.
Ctrl + Left Arrow	Seeks backward 30 seconds.
Page Down	Seeks forward one minute.
Page Up	Seeks backward one minute.
Ctrl + Move the mouse wheel one notch down	Seeks forward 90 seconds.
Ctrl + Move the mouse wheel one notch up	Seeks backward 90 seconds.
Ctrl + Page Down	Seeks forward six minutes.
Ctrl + Page Up	Seeks backward six minutes.

You can also use the following keyboard keys to control the seek slider:

To adjust the speed of the seek slider: From the Session Recording Player menu bar, choose Tools >

Options > Player and drag the slider to increase or decrease the seek response time. A faster response time requires more memory. The response might be slow depending on the size of the recordings and your machine's hardware.

Change the playback speed

You can set a playback speed in exponential increments from one-quarter normal playback speed to 32 times normal playback speed.

- 1. Log on to the workstation where the Session Recording player is installed.
- 2. From the Start menu, choose Session Recording Player.
- 3. From the **Session Recording Player** menu bar, choose **Play > Play Speed**.
- 4. Choose a speed option.

The speed adjusts immediately. Text indicating the exponential rate appears briefly in green in the lower part of the player window.

Highlight the idle periods of recorded sessions

Idle periods of a recorded session are the portions in which no action takes place. The Session Recording player can highlight the idle periods of recorded sessions during playback. The option is **On** by default. For more information, see Highlight idle periods.

Skip over spaces where no action occurred

Fast review mode allows you to set the player to skip the portions of recorded sessions where no action takes place. This setting saves time for playback viewing. However, it doesn't skip animated sequences such as animated mouse pointers, flashing cursors, or displayed clocks with second hand movements.

- 1. Log on to the workstation where the Session Recording player is installed.
- 2. From the Start menu, choose Session Recording Player.
- 3. From the **Session Recording Player** menu bar, choose **Play > Fast Review Mode**.

The option toggles on and off. Each time you choose it, its status appears briefly in green in the player window.

Change the playback display

You can do the folloing to change how recorded sessions appear in the player window:

- Pan and scale the image.
- Show playback in full screen
- Display the player window in a separate window
- Display a red border around the recorded session to differentiate it from the player window background.

Display the player window in full screen

- 1. Log on to the workstation where the Session Recording player is installed.
- 2. From the Start menu, choose Session Recording Player.
- 3. From the **Session Recording Player** menu bar, choose **View > Player Full Screen**.
- 4. To return to the original size, press Esc or F11.

Display the player window in a separate window

- 1. Log on to the workstation where the Session Recording player is installed.
- 2. From the Start menu, choose Session Recording Player.
- 3. From the **Session Recording Player** menu bar, choose **View > Player in Separate Window**. A new window appears, containing the player window. You can drag and resize the window.
- 4. To embed the player window in the main window, choose **View > Player in Separate Window**, or press **F10**.

Scale the session playback to fit the Player window

- 1. Log on to the workstation where the Session Recording player is installed.
- 2. From the Start menu, choose Session Recording Player.
- 3. From the Session Recording Player menu bar, choose Play > Panning and Scaling > Scale to Fit.
 - Scale to Fit (Fast Rendering) shrinks images while providing good quality. Images are drawn quicker than using the High Quality option but the images and texts are not sharp. Use this option if you are experiencing performance issues when using the High Quality mode.
 - Scale to Fit (High Quality) shrinks images while providing high quality. Using this option can cause the images to be drawn more slowly than the Fast Rendering option.

Pan the image

- 1. Log on to the workstation where the Session Recording player is installed.
- 2. From the Start menu, choose Session Recording Player.

- 3. From the **Session Recording Player** menu bar, choose **Play > Panning and Scaling > Panning**. The pointer changes to a hand. And a small representation of the screen appears in the top right of the player window.
- 4. Drag the image. The small representation indicates where you are in the image.
- 5. To stop panning, choose one of the scaling options.

Display a red border around Session Recording

- 1. Log on to the workstation where the Session Recording player is installed.
- 2. From the Start menu, choose Session Recording Player.
- 3. From the Session Recording Player menu bar, choose Tools > Options > Player.
- 4. Select the Show border around session recording check box.

If the **Show border around session recording** check box is not selected, you can temporarily view the red border by clicking and holding down the left mouse button while the pointer is in the player window.

Cache recordings

June 22, 2022

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 22, 2022

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 22, 2022

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 you insert in a recorded session during session playback using the Session Recording player. After insertion, bookmarks are associated with the recorded session until you delete them. However, they are not saved as part of the session file but stored as separate .iclb files in the **Bookmarks** cache folder on the Session Recording player, for example, C:\Users\SpecificUser\AppData\Local\Citrix\SessionRecording\Player\Bookmarks, with the same file name as the .icl recording file. To play back a recording using bookmarks on a different player, copy the .iclb files to the **Bookmarks** cache folder on that player. By default, each bookmark is labeled with the text "Bookmark,"but you can change it to any text annotation up to 128 characters long.

Events appear as yellow dots and bookmarks appear as blue squares in the lower part of the player window. Moving the mouse over the dots and squares displays the text label associated with them. You can also display the events and bookmarks in the **Events and Bookmarks** list of the Session Recording player. They appear in this list with their text labels and the times in the recorded session at which they appear, in chronological order.

You can use events and bookmarks to help you navigate through recorded sessions. By going to an event or bookmark, you can skip to the point in the recorded session where the event or bookmark is inserted.

Display events and bookmarks in the list

The **Events and Bookmarks** list displays the events and bookmarks inserted in the recorded session that is currently playing. It can show events only, bookmarks only, or both.

- 1. Log on to the workstation where the Session Recording player is installed.
- 2. From the Start menu, choose Session Recording Player.
- 3. Move the mouse pointer to the **Events and Bookmarks** list area and right-click to display the menu.
- 4. Choose Show Events Only, Show Bookmarks Only, or Show All.

Insert a bookmark

- 1. Log on to the workstation where the Session Recording player is installed.
- 2. From the Start menu, choose Session Recording Player.
- 3. Begin playing the recorded session to which you want to add a bookmark.
- 4. Move the seek slider to the position where you want to insert the bookmark.
- 5. Move the mouse pointer to the player window area and right-click to display the menu.
- 6. Add a bookmark with the default **Bookmark** label or create an annotation:
 - To add a bookmark with the default **Bookmark** label, choose **Add Bookmark**.
 - To add a bookmark with a descriptive text label that you create, choose **Add Annotation**. Type the text label 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 22, 2022

The web player lets you use a web browser to view and play back recorded sessions. Using the web player, you can:

- Search for recordings by using filters.
- View and play back both live and completed recordings with tagged events listed in the right pane.
- configure cache memory for storing recordings during playback.
- Highlight idle periods.
- Leave comments about a recording and set comment severities.
- Share URLs of recordings.
- View graphical event statistics for each recording.
- View data points related to each recorded session.

Access the web player

June 22, 2022

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:

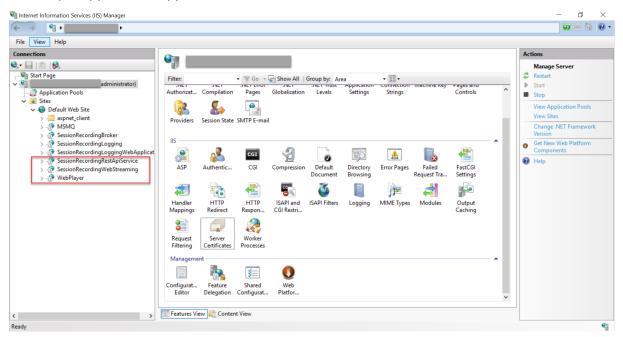
- When logging on to the web player website, domain users do not need to enter credentials while non-domain users must.
- Supported browsers include Google Chrome, Microsoft Edge, and Firefox.
- To have the web player function properly, make sure you enable WebGL in Firefox.

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.

Session Recording 2204

dit View Favorites Help				
uter\HKEY_LOCAL_MACHINE\SOFTWARE\Cit				
SOFTWARE	Hanne	Type	Data	
- 7-Zip	atabase Failover Partner	REG_SZ		
> Business Objects	atabaseName	REG_SZ	CitrixSessionRecording2	
V Citrix	BeferredHashCalcFileSizeThreshold	REG_DWORD	0x00200000 (2097152)	
Citrix Desktop Delivery Controller InstallAgent	200 DormantTimeInHours	REG_DWORD	0x00000030 (48)	
	200 EnableAnalytics	REG_DWORD	0x00000001 (1)	
MetaInstall SmartAuditor	20 EnableAzureSQLService	REG_DWORD	0x00000000 (0)	
SmartAuditor	201 EnableRecordingActionLogging	REG_DWORD	0x00000001 (1)	
> XenDesktop	2010 EnableSRStorageLogging	REG_DWORD	0x00000001 (1)	
XenDesktop XenTools	30 EnableWebBasedSrPlayer	REG_DWORD	0x00000001 (1)	
XenToolsInstaller	and LinkEmail	REG_SZ		
XenToolsInstaller XenToolsNetSettings	and LinkExpire	REG_SZ	172800000000	
> Classes	and LinkHost	REG_SZ		
> Classes	ab LinkSalt	REG_SZ	kk2od974	
DefaultUserEnvironment	80 LoggingBlockState	REG_DWORD	0x00000000 (0)	
> dotnet	ab Logging Database Failover Partner	REG_SZ		
GitForWindows	ab Logging Database Name	REG_SZ	CitrixSessionRecordingLogging	
> Google	20 LoggingLoggingState	REG_DWORD	0x00000001 (1)	
> Intel	20 MaxOpenFiles	REG_DWORD	0x00002710 (10000)	
> JavaSoft	28 MaxRolloverFileSizeInMB	REG_DWORD	0x0000012c (300)	
	200 PlaybackProtection	REG DWORD	0x00000001 (1)	
> Microsoft	200 PlayerUserRBACEnabledKey	REG_DWORD	0x00000000 (0)	
MozillaPlugins	ab PolicyFilePath	REG_SZ	C:\Program Files\Citrix\SessionRecording\Server\\A	
> ODBC	20 PolicyFileRefreshPeriodInSeconds	REG_DWORD	0x0000012c (300)	
> OpenSSH	100 RoleBasedSecurityEnabled	REG_DWORD	0x00000001 (1)	
> 📙 Partner	20 RolloverFileSizeInMB	REG_DWORD	0x00000032 (50)	
> Policies	20 RolloverTimeInHours	REG_DWORD	0x0000000c (12)	
> 📕 Python	3 SkipReceiverVersionCheck	REG DWORD	0x00000001 (1)	
> 📙 Qualys	ab SmAudDatabaseInstance	REG SZ	10.108.92.40	
- RegisteredApplications	WebPlayerDisableAllRecording	REG DWORD	0x00000000 (0)	
> Setup		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:

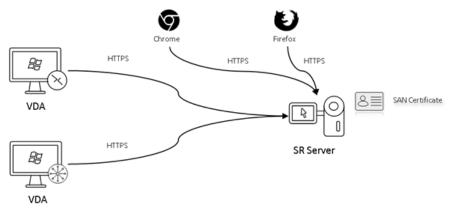
1. Add an SSL binding in IIS.

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

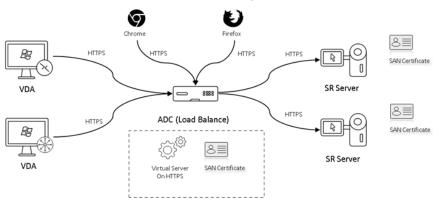
Note:

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-

s	ite Bindin	?	×				
	Type http	Host Name	Port 80	IP Address *	Binding Informa	Add Edit Remove Browse	
						Close	

- 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	?	×
Iype: IP address: Port: http All Unassigned 80 https Image: state of the state		
OK	Cancel	

Add Site Binding		? ×
Ip address: https All Unassigned Host name: Image: Imag	P <u>o</u> rt: ✓ 443]
SSL certi <u>f</u> icate:	_	
Not selected ~	Se <u>l</u> ect	<u>V</u> iew
Not selected		
test	ОК	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) (Optional) For Session Recording 2103 and later that host the WebSocket server in IIS, enable TLS by editing TLSEnable=1 and ignore the **ServerPort**, **SSLCert**, and **SSLKey** fields.
- c) (Optional) For Session Recording 2012 and earlier, enable TLS by editing TLSEnable=1, and fill in the paths to the SSL certificate and its key, respectively.

Note:

Only the PEM format of SSL certificates and key files is supported. The **ServerPort** field indicates the port number that the web player uses to collect recording files. In the following screen capture, it is set to the default value (22334). SsRecWebSocketServer.exe.config - Notepad

```
File Edit Format View Help
#1-enable TLS
#0-disable TLS
TLSEnable=0
#default-enable web socket server on all ip address
#x.x.x.vonly enable server on the given ip address
ServerAddress=default
#default-enable web socket server on tcp port 22334
#[0-65535]-enable server on the given tcp port
ServerPort=default
#cert file path and name, only config it when TLSEnable=1
SSLCert=C:\aSRS2.pem
#key file path and name, only config it when TLSEnable=1
SSLKey=C:\newaSRS2key.pem
```

To extract the separate certificate and key files used in the WebSocket server configuration:

- i. Ensure that OpenSSL is installed on your Session Recording Server that contains the SSL certificate.
- ii. Export the SSL certificate as a .pfx file. The .pfx file includes both the certificate and the private key.
- iii. Open the command prompt and go to the folder that contains the .pfx file.
- iv. Start OpenSSL from the OpenSSL\bin folder.
- v. Run the following command to extract the certificate:

Enter the import password that you created when exporting the .pfx file.

vi. Run the following command to extract the private key:

Enter the import password that you created when exporting the .pfx file. Provide a new password for protecting your key file when prompted for the PEM pass phrase.

vii. Run the following command to decrypt the private key:

- d) Save your changes.
- e) Check your firewall settings. Allow SsRecWebSocketServer.exe to use the TCP port (22334 by default) and allow access to the web player URL.
- f) Run the SsRecUtils -stopwebsocketserver command.

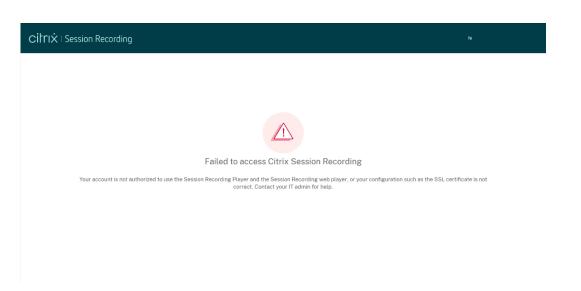
Hide or show content on the web player home page

June 22, 2022

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	-		\times						
Notifications CEIP Logging RBAC Email Cloud DB	We	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 Car	ncel	Ap	ply						

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.

CITIX Session Recording			Q Search by host name, user, start time, and so on				\checkmark		hi manana k atala	
► 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 Loggin	is v	May 19, 2021 5:20 PM				1	True	SERVER	00:02:28	lacksquare
Onfiguration	v	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	lacksquare
		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	ightarrow
		May 14, 2021 5:58 PM	Administrator			0	False	SERVER	00:02:14	lacksquare
		May 14, 2021 3:00 PM	Administrator			0	False	SERVER	00:00:37	lacksquare
		May 14, 2021 2:58 PM	Administrator			0	False	SERVER	00:00:31	lacksquare
		May 14, 2021 2:56 PM	Administrator			0	False	SERVER	00:00:40	lacksquare

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 Re	COrding Show all recordings of this session	Q Search by host	name, user, start time, and	l so on		\sim		hi H	_
► Recordings ^	Follow 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	\odot
🗐 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	lacksquare
	May 14, 2021 6:20 PM	Administrator			0	False	SERVER	00:00:41	ightarrow

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 22, 2022

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.

Session Recording 2204

Cilri× Session Re	ecording	Q Search by host name, user, start Ime, and so on					hi P	
Recordings	Follow up	Host name	🛆 User name					
All Recordings	🗌 Start Time 👙	🗄 Application	🖵 Client name			Recording Server 👙	Duration 👙	Action
Comments ~	May 19, 2021 5:20 PM	① Client IP address	🖓 Event text			SERVER	00:02:28	ightarrow
Administrator Logging 🗸	May 19, 2021 5:23 PM	Event type	Time 🕄			SERVER	00:01:57	ightarrow
Configuration	March 3, 2021 10:43 AM					SERVER	00:08:05	ightarrow
	March 3, 2021 12:39 PM	Administrator		5 False		SERVER	00:01:22	$\mathbf{\bullet}$
	March 31, 2021 3:35 PM	Administrator		19 False		SERVER	00:04:37	\mathbf{b}
	March 31, 2021 3:47 PM	Administrator		1 False		SERVER	00:01:34	(\mathbf{b})

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.

CilrIX Session Re	ecording	Q Search by ho	Q Search by host name, user, start time, and so on			\sim			hi	
► Recordings ▲										
All Recordings	FILTER							Search	Clear All	
Comments ~	Host name Enter on	ne Host name							$+ \times$	
Eg Administrator Logging 👻	E 🖉 User name									
Configuration V	Client name	User 🌲	Host 🖕	Client 🌲	Events 👙	Events Only 👙	Recording Server 👙	Duration 👙	Action	
	🗋 🛛 🌐 Client IP address				1	True	SERVER	00:02:28	\mathbf{b}	
	🕞 i 🧏 Event text				23	True	SERVER	00:01:57	ightarrow	
	Comments	Administrator			0	False	SERVER	00:08:05	\mathbf{b}	
	D L Time M	Administrator			5	False	SERVER	00:01:22	\mathbf{b}	
	March 31, 2021 3:35 PM	Administrator			19	False	SERVER	00:04:37	\mathbf{b}	
									\sim	

You can also click the + symbol to add filters.

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

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 da	ate ect date				
	Start Time	End ti					×
	Duration At least		Seconds 🗸				3
Start Time 👙		User 🜲	Host 🔶	Client 🌲	Events 🌲	Duration 🔶	Action
February 9, 2021 5:2	2 PM	qh			5	00:30:07	

The **Time** filter consists of recording start date, start time, and duration.

Open and play recordings

June 22, 2022

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.

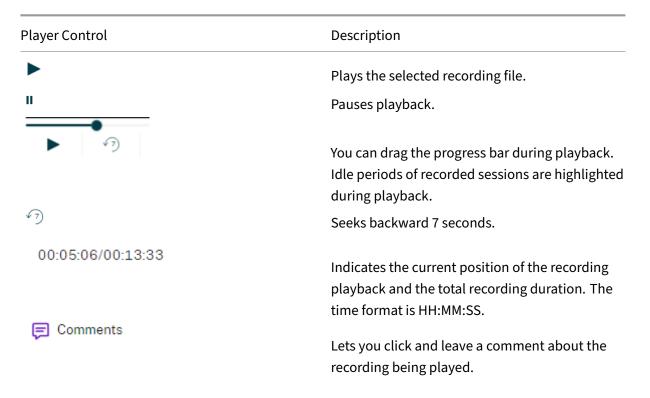
CilriX Session	n Re	cording	Q Search by host	name, user, start time, a	and so on		\sim		hi	
Recordings	^	Start Time 🍦	User 🎄	Host 👙	Client 👙	Events 👙	Events Only 👙	Recording Server 🜲	Duration 👙	Action
All Recordings		May 19, 2021 5:36 PM	Administrator			0	False	SERVER	Live	\mathbf{E}
Comments	v	May 19, 2021 5:23 PM				23	True	SERVER	00:01:57	∢
Administrator Logging	~	May 19, 2021 5:20 PM				1	True	SERVER	00:02:28	►
Configuration	v	May 14, 2021 6:48 PM	Administrator			0	False	SERVER	00:00:58	€
		May 14, 2021 6:46 PM	Administrator			0	False	SERVER	00:00:50	►
		May 14, 2021 6:31 PM	Administrator			0	False	SERVER	00:00:35	►
		May 14, 2021 6:20 PM	Administrator			0	False	SERVER	00:00:41	►
		May 14, 2021 5:58 PM	Administrator			0	False	SERVER	00:02:14	►
		May 14. 2021 3:00 PM	Administrator			0	False	SERVER	00:00:37	►
		May 14, 2021 2:58 PM	Administrator			0	False	SERVER	00:00:31	∢
		May 14, 2021 2:56 PM	Administrator			0	False	SERVER	00:00:40	\mathbf{b}

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

÷	Player					
\triangleright			N			
		😢 New Tab 🛛 🗙	+	- o ×	NOV 18, 2021 11:41:52 · 00:13:33 · 32 Events	
000		$\leftarrow \ \rightarrow \ \mathbf{G}$	Q. [search with Google or enter address	\odot =	11.41.52 · 00.15.55 · 52 Events	
		🕀 Import bookmarks 👋 Getting Sta	ted		Q User name:	
				* Î	Se Host name:	
			ii Firefox		Client name: View: All ∨ Q Search	▽
			G Search with Google or enter address		00:00:26 Top-most window:sessionmsg, , 9072	~
			303 ms **** Network (send) 78 Kbps		© 00:00:28 Top-most window:explorer. , 7508	~
			Ameson Sponsord Metwork (proceive)		© 00:00:48 App Start:9632: conhost: 2748: \??\C:\Win	~
			Recommended by Pocket LISIN POOR		© 00:00:48 App Start:2748: cmd: 7508: C:\Windows\sys	~
					© 00:00:48 App Start:11232: powershell: 2748: powers	~
			Wind Utanu aconco smartastet.com Wind Use beneath: the secrets of The Good Guy/Bad Guy Myth Learn the Cost of a Financial		© 00:00:55 App End:9632: conhost	~
		# 2 0 🤅 🗖	France's top serial killer expert Pop culture today is obsessed with the Advisor An intrepid expert with dozens of books to battle between good and evil. Traditional Find information to help you choose the	= 40 ₽ 505 AM	00:00:55 App End:11232: powershell	~
	•	√7) 00:05:0	6001333 🔄 Comments 🕜 Share Current Playback. X 1 🕢 Hide	e stats 🔀 FULL SCREEN	© 00:00:55 App End:2748: cmd	~

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
Share Current Playback	Lets you click and copy the URL of the current recording to the clipboard.
Show stats	
	Shows the overlay that features data points
	related to the recorded session.
Hide stats	
	Hides the session data overlay.
Xı	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:

AUG 20, 2021 18:50:50 · 01:37:00 · 359 Events					
 ∧ User name: c ⊷ Host name: A □ Client name: 7 					
View: All					
Q All	\bigtriangledown				
Events Comments admin: Cet	~				
00:00:40 Top-most window:sessionmsg, , 8412	~				
© 00:00:53 Clipboard Operation:Text, sessionmsg, ,	~				
	\sim				
© 00:00:54 Top-most window:explorer, , 8944	~				
♥ 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 displays of events. For example:

Session Recording 2204

ß	00:18:29 Top-most window:setup_wm, Windows Media P	~
ß	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 cache for storing recordings during playback

June 22, 2022

On the **Configuration** page of the web player, click the slider to set up the cache memory for storing recordings during playback.

Tip:

You can access the **Configuration** page directly through **http(s)://<FQDN of Session Recording** Server>/WebPlayer/#/configuration/cache.

Recordings * Set up recording cache Comments Administrator Logging Administrator Logging Configuration Amments Storage	CITIX Session Recording				Q Search	by host name, user, start t	time, and so on
Administrator Logging ~ Image: Configuration ^ 2MB 20MB 50MB 70MB	Recordings	¥	Set up rec	cording cache			
Image: Configuration 2MB 20MB 50MB 70MB 100MB	Comments	~	You can set up cao	he memory to store reco	rdings while playing.		
2MB 20MB 50MB 70MB 100MB	Administrator Logging	Ŷ		0			
Storage	O Configuration	^	2MB	20MB	50MB	70MB	100MB
	Storage						

Increase the transport packet size for the web player

June 22, 2022

- 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).

HKEY_LOCAL_MACHINE\SOFTWAR	\Citrio	\SessionRecording\CloudClientServi	ce			
Local Registry X						4
eys	×	Name	Type	Data		
V Citrix	^	🕂 (Default)	REG_SZ	(value not set)		
Auditor Cloud CloudClientService		BlockSizeMultiple	REG_DWORD	0x00000004 (4)		
Citrix Desktop Delivery O Citrix Desktop Delivery O	or	A SessionRecordingUUID	REG_SZ	99a59354-1c99-d923-9de9-2c0a3736a960		
> - Qualys	~	<				

Highlight idle periods

June 22, 2022

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.

Session Recording 2204

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.
dleEventActiveThrottle	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.
dleEventActivePktSizeThrottle	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 22, 2022

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

	AUG 20, 2021 18:50:50 · 01:37:00 · 359 Events							
ςĻΗ	 Q User name: c G Host name: A G Client name: C 							
View:	All	n						
Q	All		\bigtriangledown					
Ţ	Events Comments cei	admin: mentaire sur	\sim					
	00:00:40 Top- window:session	·most nmsg, , 8412	~					
	00:00:53 Clip Operation:Text		~					
F	• 00:00:53 ct	xadmin:	~					
	00:00:54 Top- window:explor		~					
Ţ	• 00:00:54 ct dqwdwd	xadmin:	~					
	00:01:13 Top- window:ipconf		\sim					

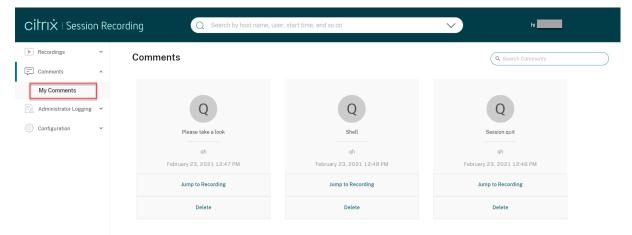
Comment on recordings

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 you left, refresh your webpage, expand the comment, and then click **Delete**.

← Player	
	NOV 17 0001
	NOV 17, 2021 15:43:44 · 00:12:51 · 30 Events
	0. Ukas name
	🖉 User name:
	Client name
	•
	View: Comme V
	view. comme V
	Q Search
	D0:00:00 ctxuser1: test
Session Recording	Delete
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).	• 00:00:00 ctxuser1: test 2
Round trip time 0 me	💬 • 00:00:00 ctxuser1: test 3 🗸
Network (scena) 452 Kbps Network (scena) 90 Kbps	
Verwork (Peeder) 00 Kdpa	L
Memory usage 2471/4088 MB (60%)	
Amor Agent - AMTTND	
1 47 00.00.30/00.12.51 🔄 Comments 🗗 Share Current Playback X1 🔛 Hide stats 💱 Exit full screes	

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.

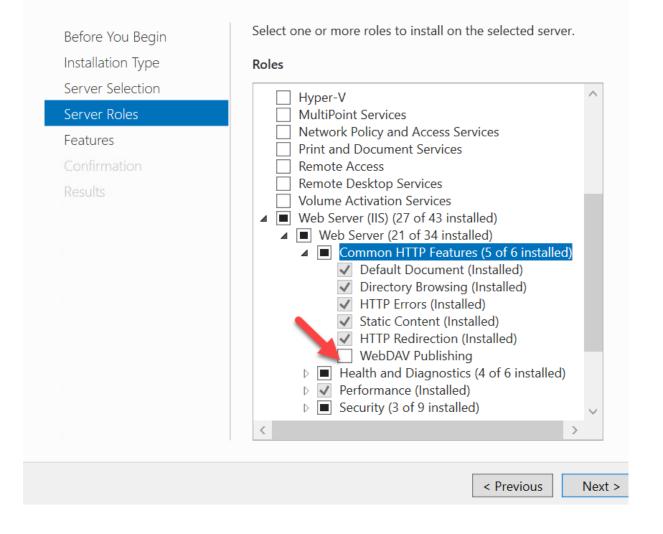


Note:

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 URLs of recordings

June 22, 2022

Clicking **Share Current Playback** on the playback page of a recording copies the recording URL to the clipboard. You can share the URL with other users for them to access the recording directly without the need to search in all recordings.

\leftarrow	Player				
\triangleright		🗉 New Tab 🛛 🗙	+	- a ×	NOV 18, 2021
		< → C	Q. [search with Google or enter address		11:41:52 · 00:13:33 · 32 Events
		- Import bookmarks 🍓 Getting Sta			Q User name:
				*	G Host name:
				193	Client name:
			🝅 Firefox		View: All V Q Search
			G Search with Google or enter address		
					© 00:00:26 Top-most window:sessionmsg., 9072
			303 ms (1) X Honor Units (1		© 00:00:28 Top-most ∨ window:explorer. , 7508
			Amazon Sensors Sa CPU ang Control Cont		© 00:00:48 App Start:9632: conhost: 2748:\??\C:\Win ~
			Recommended by Pocket Learn more		00:00:48 App Start:2748:
					C:\Windows\sys
					© 00:00:48 App Start:11232: powershell: 2748: powers ~
			Giliedian		
			theguardian.com aeon.co smarfasset.com		© 00:00:55 App End:9632:
			What lies beneath: the secrets of The Good Guy/Bad Guy Myth Learn the Cost of a Financial		
			France's top serial killer expert Pop culture today is obsessed with the Advisor An intrepid expert with dozens of books to battle between good and evit. Traditional Find information to help you choose the	~	© 00:00:55 App End:11232:
		# P 🗇 ಿ ╞	• ^	₩ 44) ₩ 505 AM 11/12/2021	
	►	√7) 00:05:0	VI00.13.33 @ Comments [7] Share Current Playback X1 💽 Hi	de stats	

After you click **Share Current Playback**, 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

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

For 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 shared URL 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 protect the preceding URL expiration time	Kk2od974	Change the default value to an arbitrary string that preferably ends with digits.

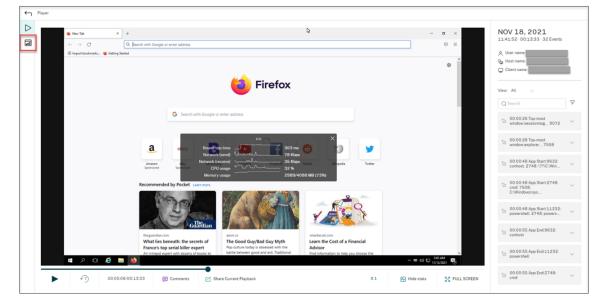
View graphical event statistics for each recording

June 22, 2022

Event data visualization is available in the web player for each recording. It provides graphical event statistics for you to quickly comprehend the events inserted in recordings.

To view graphical event statistics, complete the following steps:

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



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

Screen time

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

Υ	Player		
	Screen time File transfers	Commands Events	*
	XenDesktopVdaSetup explorer chrome	00:20:52 00:19:14 00:16:52	
	firefox csrss	00:11:55 00:10:30	
	ConfigurationWizard	00:07:46	- 1
	powershell	00:03:00	- 1
	cmd	00:02:58	- 1
	mmc	00:00:35	- 1
	iexplore	00:00:35 00:00:16	- 1
	JonasAgentSystray	00:00:15	- 1
	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:

Player			
▷ Screen time	File transf	sfers Commands Events power	rshell
		as the	top-most window
000		(All	> 20 minutes) (5-20 minutes) (< 5 minutes)
			time Duration
XenDesktopVdaSe		00:20:52	0 00:00:04
expl	orer	00:19:14 00:28:2	
chr	ome 🛛	00:16:52 00:29:0	2 00:00:15
fir	efox	00:11:55 00:30:0	4 00:00:03
с	srss	00:10:30 00:30.2	
ConfigurationWi	zard	00:07:46	
powers		0030.4	
	cinic	00.02.58	
r		00:00:35 00333	
iexp	lore	00:00:35 00:33:5	3 00:00:09 🛑
Task	mgr	00:00:16 00:36:3	8 00:00:06 📟
JonasAgentSys	trav	00:00:15	
session	-	00:37:2	
	0	00:00:14 00:37:4 00:00:12 00:42:3	
setup_			
WfS		00:00:11	
wmpla	ayer	00:00:10	
Citrix	iles	00:00:07	
Open	With	00:00:06	
msp	aint	00:00:05	
msedgewebvi		• 00:00:05 •	
meedgeneeri			

• File transfers

The File transfers tab provides graphical statistics about bidirectional file transfers be-

tween 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.

\leftarrow	Player
\triangleright	Screen time File transfers Commands Events
••0	Per 1 minute V All transfers V
	Number of files 🗸
	Number of files File size (Bytes) Z
	File size (MB) 6 - 6 -
	5 - 5 - 4 -
	2 - 2 - 1 -
	1 0 10:25 10:30 10:35 10:40 10:45 10:50 10:55 11:00 11:05 11:10 11:15 11:20 11:25 11:30
	Transfer from host to client Transfer from client to host

• 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.

\leftarrow	Player			
\triangleright	Screen time	File trans	fers Comm	ands Events
00				
		Custom searc	h	Type a search string or use a regular expression
		Saved search		Select a saved search
	15 / 15 Commands			IPv4 Address
	00:01:14	cmd	powershell: power CDFTraceTask.ps1	
			CDF Hacelask.ps.	comprigmt taskmgr
	00:01:23	powershell	logman: "C:\Windc	mmc
	00:28:16	cmd	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"

• Events

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

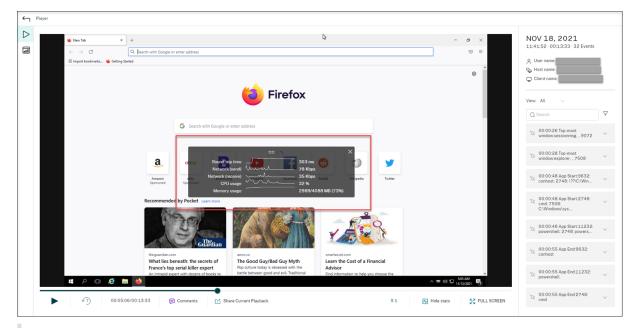


View data points related to each recorded session

June 22, 2022

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

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



Note:

- Session Recording collects round trip time every 15 seconds and the rest of the data points every second.
- Theoretically, Session Recording refreshes data on round trip times every five seconds. However, round trip time data actually refreshes every 15 seconds because of the collection cycle.
- Session recording refreshes the rest of the data points every 5 seconds and presents their average values on the overlay.

The overlay is semi-transparent. You can relocate and hide it.

- To relocate the overlay, hover your mouse over the eight dots and then do a drag and drop.
- To hide the overlay, click **Hide stats**.

You can enable the overlay by selecting **Log performance data** when creating your event detection policy. For more information, see Configure event detection policies.

Manage recordings

June 22, 2022

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 \Program Files\Citrix\SessionRecording\Server\Bin folder on the server hosting the Session Recording server.

Quick reference chart

The following table lists the commands and options that are available for the ICLDB utility. Type the commands using the following format:

```
icldb [version | locate | dormant | import | archive | remove |
removeall] command-options [/l] [/f] [/s] [/?]
```

Note:

More extensive instructions are available in the help associated with the utility. To access the help, from a command prompt, type the \Program Files\Citrix\SessionRecording \Server\Bin folder, and type icldb /?. To access help for specific commands, type icldb *command* /?.

Command	Description
archive	Archives the session recording files older than the retention period specified. Use this command to archive recordings and events in the recordings. The events are archived in the ArchivedEvent database table.

Command	Description
dormant	Displays or counts the session recording files
	that are considered dormant. Dormant files are
	session recordings that were not completed due
	to data loss. Use this command to verify if you
	suspect that you are losing data. You can check
	whether session recording files are becoming
	dormant for the entire database, or only
	recordings made within the specified number of
	days, hours, or minutes.
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).
locate	Locates and displays the full path to a session
	recording file using the file ID as the criteria. Use
	this command when you are looking for the
	storage location of a session recording file. It is
	also one way to verify if the database is
	up-to-date with a specific file.
remove	Removes the references to session recording
	files from the database. Use this command (with
	caution) to clean up the database. Specify the
	retention period to be used as the criteria. You
	can also remove the associated physical file.
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.
voration	Displays the Session Recording database
version	Displays the session needfalling database

Command	Description
/1	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.

Archive session recording files

To maintain an adequate level of spare disk capacity in the recording storage locations, archive session recording files regularly. Depending on the amount of available disk space and typical size of recording files, archiving intervals differ. Session recording files must be older than two days from the start date before a session recording file can be archived. This rule is to prevent any live recordings from being archived before they become complete.

Two methods are available when you archive session recordings. The database record for a recording file can be updated to have a status of archived while the file remains in the recording storage location. This method can be used to reduce the search results in the player. The other method is to update the database record for a recording file to the archived status and move the file from the recording storage location to another location for backup to alternative media. When the ICLDB utility moves session recording files, the files are moved to the specified directory where the original file folder structure of year/month/day no longer exists.

The session recording record in the Session Recording database contains two fields associated with archiving—the archive time and archive note. The archive time represents the current date and time a recording was archived. The archive note is an optional text note that can be added during archiving. The two fields indicate that a recording has been archived and the time of archiving.

In the Session Recording player, archived session recordings show a status of Archived and the date and time of archiving. Session recordings that have been archived might still be played if the files have not been moved. If a session recording file was moved during archiving, a file not found error is displayed. The session recording file must be restored before the session can be played. To restore a session recording file, provide the File ID and Archive Time of the recording file. Restoring archived files is discussed further in the following Restore session recording files section.

The **archive** command of the ICLDB utility has several parameters that are described as follows:

 /RETENTION:<days> - The retention period in days for session recordings. Recordings older than the number of days specified are marked as archived in the Session Recording database. The retention period must be an integer number greater than or equal to 2 days.

- **/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, 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>/Server/Bin).
- 4. Run the ICLDB ARCHIVE /RETENTION: <days> /LISTFILES /MOVETO: <directory > /NOTE: <note> /L command where 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>/Server/Bin).
- 4. Run the ICLDB ARCHIVE /RETENTION: <days> /LISTFILES /NOTE: <note> /L command where **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 Session Recording 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 Session Recording 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 Session Recording player for playback. If the file is not found, the Session Recording Broker sends a file not found error to the Session Recording 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 can also 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 are described as follows:

- **/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.
- /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.

To restore session recording files by using the restore directory for archived files

- 1. Log on to the server where the Session Recording server is installed as a local administrator.
- 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.

To restore session recording files by using the ICLDB import command

- 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>/Server/ 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.

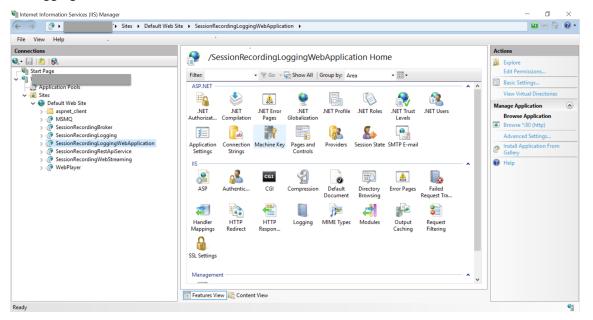
Manage and query administrator logging

June 22, 2022

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.

			Search by host name, user, start time,				hi APRQ\qh	3 x x
CİİTIX Session Re	ecording	0	Search by host name, user, start time,	and so on		~	hi APRQ\qh	
 Recordings 	ID ‡	Logging Time	Task Category T	Component Affected	Ψ	Task Details	Task Excuted By	Authorized
Comments ~	63	1/30/2022 2:12 AM	Recording File Play Back	Session Recording Player	+	Action = Session File Path and Size Query	APRQ/qh	true
Administrator Logging 🔺	62	1/30/2022 2:11 AM	Recording File Play Back	Session Recording Player	+	Action = Session File Path and Size Query	APRQ/qh	true
Configuration Logging	61	1/30/2022 2:09 AM	Recording File Play Back	Session Recording Player	+	Action = Session File Path and Size Query	APRQ/qh	true
Record Reason Logging	60	1/30/2022 2:08 AM	Server Config Change	Session Recording Server	+	WebPlayerDisableAllRecording:False	APRQ/qh	true
Configuration 👻	59	1/30/2022 2:07 AM	Recording File Play Back	Session Recording Player	+	Action = Session File Path and Size Query	APRQ/qh	true
	58	1/30/2022 2:06 AM	Server Config Change	Session Recording Server	+	WebPlayerDisableAllRecording:True	APRQ/qh	true
	57	1/30/2022 2:04 AM	Recording File Play Back	Session Recording Player	+	Action = Session File Path and Size Query	APRQ/qh	true
	56	1/30/2022 2:03 AM	Recording File Play Back	Session Recording Player	+	Action = Session File Path and Size Query	APRQ/qh	true
	55	1/30/2022 2:02 AM	Recording File Play Back	Session Recording Player	+	Action = Session File Path and Size Query	APRQ/qh	true
	54	1/30/2022 2:01 AM	Server Config Change	Session Recording Server	+	WebPlayerDisableAllRecording:False	APRQ/qh	true

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 two parts –configuration logging and recording reason logging.

citri×∣Session Re	cording	9	Search by host name, user, sta	rt time, and	so on		\checkmark	
Recordings ~	ID ÷	Logging Time	Task Category	Ψ	Component Affected	Ŧ	Task Details	Task E
Comments ~	63	1/30/2022 2:12 AM	Recording File Play Back		Session Recording Player	+	Action = Session File Path and Size Query	API
Administrator Logging 🔺	62	1/30/2022 2:11 AM	Recording File Play Back		Session Recording Player	+	Action = Session File Path and Size Query	APF
Configuration Logging	61	1/30/2022 2:09 AM	Recording File Play Back		Session Recording Player	+	Action = Session File Path and Size Query	APF
Record Reason Logging	60	1/30/2022 2:08 AM	Server Config Change		Session Recording Server	+	WebPlayerDisableAllRecording:False	APF
Configuration V	59	1/30/2022 2:07 AM	Recording File Play Back		Session Recording Player	+	Action = Session File Path and Size Query	APR
	58	1/30/2022 2:06 AM	Server Config Change		Session Recording Server	+	WebPtayerDisableAllRecording:True	APR
	57	1/30/2022 2:04 AM	Recording File Play Back		Session Recording Player	+	Action = Session File Path and Size Query	APR
	56	1/30/2022 2:03 AM	Recording File Play Back		Session Recording Player	+	Action = Session File Path and Size Query	APR
	55	1/30/2022 2:02 AM	Recording File Play Back		Session Recording Player	+	Action = Session File Path and Size Query	APF
	54	1/30/2022 2:01 AM	Server Config Change		Session Recording Server	+	WebPlayerDisableAllRecording:False	APR

Configuration logging

This part logs the following administrator activities:

- **Policy Document Change** Changes to policies on the Session Recording policy console or Citrix Director
- Server Config Change Changes in Session Recording Server Properties
- Recording File Play Back Playback of recorded sessions
- 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.

CitriX Session	Re	cording	0	Search by host name, user, start time, and	so on	~
Recordings	~	ID \$	Logging Time	Task Category	Component Affected	Task Details
Comments	×	32	2/9/2021 1:26 AM	Event Logging Reason	Session Recording Agent	+ Applications = GDDC/Desktop===Desktop
Eg Administrator Logging	^	31	2/9/2021 1:26 AM	Email Alert Reason	Session Recording Agent	+ Applications = GDDC/Desktop/###Desktop
Configuration Logging		30	2/9/2021 1:26 AM	Record Reason	Session Recording Agent	+ Applications = GDDC/Desktop/###Desktop
Record Reason Logging		29	2/9/2021 1:24 AM	Event Logging Reason	Session Recording Agent	+ Applications = GDDC/Desktop===Desktop==
Configuration	ř	28	2/9/2021 1:24 AM	Email Alert Reason	Session Recording Agent	+ Applications = GDDC/Desktop/###Desktop
		27	2 2 2021 1:24 AM	Record Reason	Session Recording Agent	+ Applications = GDDC/Desktop/###Desktop
		26	2/9/2021 1:21 AM	Event Logging Reason	Session Recording Agent	+ Applications = GDDC/Desktop/###Desktop
		25	2:9/2021 1:21 AM	Email Alert Reason	Session Recording Agent	+ Applications = GDDC/Desktop/###Desktop
		24	2/9/2021 1:21 AM	Record Reason	Session Recording Agent	+ Applications = GDDC/Desktop/###Desktop
		23	2/9/2021 1:18 AM	Event Logging Reason	Session Recording Agent	+ Applications = GDDC/Desktop/###Desktop

Recording reason logging

This part logs which policies have triggered recordings.

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

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 case might generate a large number of 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 22, 2022

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

June 22, 2022

This article guides you through the process of adding load balancing nodes using Citrix ADC in an existing Session Recording deployment. The following servers are used as an example throughout the process. 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 Shar										~ 🕐
← → × ↑ 🏪 > 1	This PC > Windows (C:)						~ Ū	Search Windows (C:)		P
	Name	^	Date modified	Туре	Size					
📌 Quick access	46c2a726da860f	f96b3b8c5f458e292	10/29/2020 3:25 AM	A File folder						
📃 Desktop 🛛 🖈	PerfLogs	5055555511562252	10/29/2020 6:00 AM							
👆 Downloads 🛛 🤘	Program Files		11/23/2020 2:13 AM							
🔮 Documents 🛛 🖈		x86)	11/23/2020 2:22 AM							
📰 Pictures 🛛 🚿	SessionRecordir	ng		/I File folder						
💻 This PC	SQLServer2017N	Open Me		1 File folder						
	Users	Open in new wind		1 File folder						
💣 Network	Windows	Pin to Quick acce	55	1 File folder						
	💿 ip	Give access to	>	🔒 Remove access		KB				
		Restore previous v	rsions	🙍 Specific people						
		Include in library	> -							
		Pin to Start								
		Send to	>							
		Cut								
		Сору								
		Create shortcut								
		Delete								
		Rename								
		Properties								
9 items 1 item selected										
								MACAddpo	cc · A	6 22 Fg
🏪 🛃 📙 🖛 Windov	ws (C:)							_		×
File Home Sha	re View									~ 🕐
$\leftarrow \rightarrow \rightarrow \uparrow \blacksquare \rightarrow$	This PC > Windows (C:)	1					v ⊙	Search Windows (C:)		ρ
		^					¢ U	Scaren mildons (ei)		~
📌 Quick access	Name		Date modified	Туре	Size					
Desktop 🔊		f96b3b8c5f458e292	10/29/2020 3:25 AN							
Downloads	PerfLogs		10/29/2020 6:00 AN							
•	Program Files		11/23/2020 2:13 AN							
i occanicito y	Program Files (>		11/23/2020 2:22 AN							
Pictures 🕫	SessionRecordir		11/25/2020 3:06 AN							
💻 This PC	SessionRecordia	narPortorod	11/15/2020 2.00 AK	1 Eile telder		- 0	x c			
🔿 Network	SQLServer20									
- NELWOIK	Windows	 Network access 								
	ip									
		Choose people or	n your network to	o share with						
		-								
		Type a name and then	click Add, or click the	arrow to find someone.						
					~	∠ <u>A</u> dd				
		Name			Permissio		-			
		& Administrator			Read/Wri					
		Administrator &			Owner	ile +				
		LB\SRSERVER1\$			Read/Wri	ite 🔻	7			
10 items 1 item selecte	ed	I'm having trouble sha	ring						[
						Share	Cancel			

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

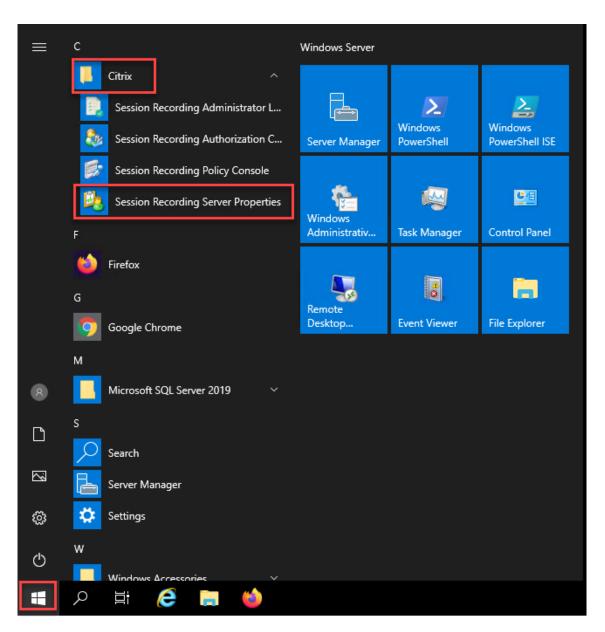
🔒 🏹 📙 🗸 Sessi	onRecording						- 0	×
File Home S	ihare View							~ 🕐
← → • ↑ <mark> </mark> :	This PC > Windows (C:) → SessionRecording →				νÖ	Search SessionRecording	Q
Quick access Desktop Downloads Documents Pictures This PC Network	Name Marne Mar	^	Date modified 11/25/2020 5:24 AM	Type File folder	Size		Joint Jestion Colonary	~
1 item State: 🎎 Sha	ared							

- 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 (\$) unless you install the player and the Session Recording server on the same machine.

🔄 Sessio	n Record	ing Server	Properties		-		×
Storage	Signing	Rollover	Playback	Notifications	CEIP	Logging	RI •
	ad-balanc			he directories ultiple director			
	orage dire		N 1		1		_
NSR:	5QL\Sess	ionRecordi	ng\share			A <u>d</u> d.	
						<u>M</u> odify	/
						<u>R</u> emo	ve
Specif	v a folder	to tempora	rilv store a	rchived sessio	on record	lings and n	nake
them a	vailable f	or playbac	k.			2	
		y for archi					_
\\SRS	6QL\Sessi	onRecordir	ngsRestored	l\share		Brows	e
				ОК	Cancel		Apply
				5	Carloot		

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)

ter\HK	EY_LOCAL_MACHINE\SOFTWARE\Citri	x\SmartAuditor\Server		
omput	ter	Name	Туре	Data
HKE	Y_CLASSES_ROOT	ab (Default)	REG SZ	(value not set)
HKE	Y_CURRENT_USER	8 _Installed	REG_DWORD	0x00000001 (1)
·	Y_LOCAL_MACHINE	Real AllowLivePlayback	REG DWORD	0x00000001 (1)
	CD0000000	ab AzureSQLServiceAdminPasswo	-	
	ARDWARE	ab AzureSQLServiceAdminUserna	-	
	AM	ab DatabaseFailoverPartner	REG SZ	
_	ECURITY	ab DatabaseName	REG_SZ	CitrixSessionRecording
	OFTWARE	DeferredHashCalcFileSizeThres	-	0x00200000 (2097152)
× -	Citrix	B DormantTimeInHours	REG_DWORD	0x00000030 (48)
Ļ	Citrix Desktop Delivery Controller	Bill EnableAnalytics	REG_DWORD	0x00000001 (1)
2	InstallAgent		REG_DWORD	0x00000000 (0)
>	MetaInstall		REG DWORD	0x00000001 (1)
~	SmartAuditor	EnableRecordingActionLogging	REG DWORD	0x0000001 (1)
Ť	Server	EnableSRStorageLogging	REG DWORD	
	XenTools	EnableWebBasedSrPlayer	-	0x00000001 (1)
	XenToolsInstaller		REG_DWORD	0x00000001 (1)
	XenToolsNetSettings	FileStorageDirectories	REG_MULTI_SZ	\\SRSQL\SessionRecording\share
50	Classes	ab LinkEmail	REG_SZ	
51	Clients	ab LinkExpire	REG_SZ	172800000000
1.	DefaultUserEnvironment	ab LinkHost	REG_SZ	
>	Google	ab LinkSalt	REG_SZ	kk2od974
3	Intel	8 LoggingBlockState	REG_DWORD	0x00000001 (1)
3	Microsoft	b LoggingDatabaseFailoverPartner	-	
3	Mozilla	ab LoggingDatabaseName	REG_SZ	CitrixSessionRecordingLogging
>	mozilla.org	at LoggingLoggingState	REG_DWORD	0x00000001 (1)
>	ODBC	100 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	100 PlaybackProtection	REG_DWORD	0x00000001 (1)
>	Qualys	PlayerUserRBACEnabledKey	REG_DWORD	0x00000000 (0)
	RegisteredApplications	赴 PolicyFilePath	REG_SZ	C:\Program Files\Citrix\SessionRecording\Server\\
>	Setup	🕮 PolicyFileRefreshPeriodInSeco	REG_DWORD	0x0000012c (300)
>	WOW6432Node	🕮 RoleBasedSecurityEnabled	REG_DWORD	0x00000001 (1)
S)	YSTEM	100 RolloverFileSizeInMB	REG_DWORD	0x00000032 (50)
HKE	Y_USERS	RolloverTimeInHours	REG_DWORD	0x0000000c (12)
HKE	Y_CURRENT_CONFIG	BipReceiverVersionCheck	REG DWORD	0x00000001 (1)

5. Restart the Citrix Session Recording Storage Manager service.

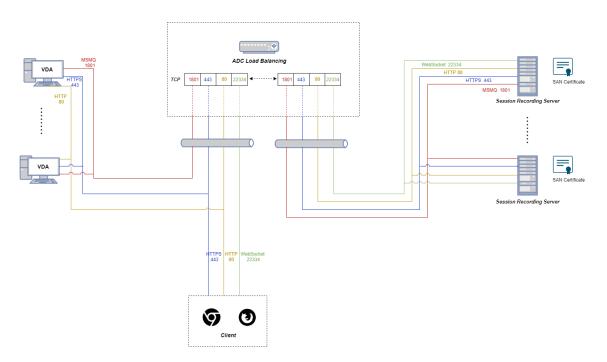
Step 3: Configure load balancing in Citrix ADC

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

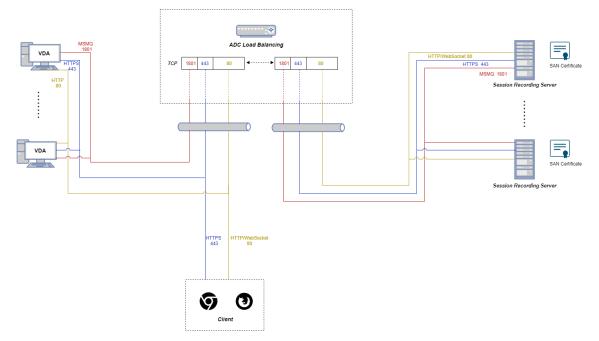
Configure load balancing through TCP passthrough

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.

Dashboard	Configuration	Reporting	Documentation	Downloads					
G Configur	re Basic Feat	ures							
SSL Offloading		HTTP Compressi	on						
🗸 Load Balancing		Content Switchin	ng						
Content Filter		Integrated Cachi	ng						
Rewrite		Citrix Gateway							
Authentication, Au	uthorization and Auditing								
ОК С	lose								

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:

citrix. Ad	C VPX (1000)			
Dashboard	Configuration	Reporting	Documentation	Downloads
Croato S	orvor			

Create Server

Name* srv-1	\odot
IP Address Domain Name	
IPAddress*	
10.63.32.55	\bigcirc
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 ~			
\mathbf{Q} Click here to search or you can ent	er Key : Value format			0
NAME	STATE	IPADDRESS / DOMAIN	C TRAFFIC DOMAIN	
🗸 srv-1	ENABLED	10.63.32.55		0
Total 1				25 Per Page ∨ Page 1 of 1 < ▶

5. For WebSocket server Version 1.0, add load balancing services of ports 80, 1801, 22334, and 443 for each Session Recording server. For WebSocket server Version 2.0, add load balancing services of ports 80, 1801, and 443 for each Session Recording server.

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

citrix. add v	VPX (100	00)					
Dashboard	Configurat	tion	Reportir	ng l	Documentation	Downloa	ads
Q Search in Menu		Traffic Ma	nagement	/ Load B	alancing / Service	s / Services	
System AppExpert	>	Servi	ces				
Traffic Management	~	Services	s 🚺	Auto Dete	ected Services 0	Internal Se	ervices 6
Load Balancing Virtual Servers	~	Add	Edit	Delete	Rename	Statistics	No action $ \checkmark $
☆ Services		Q Click	here to sea	rch or you o	an enter Key : Value	format	
Service Groups			NAME			\$ S	ERVER 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 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**.

Deebbaard	Configuration	Depenting	Desumentation	Develorde
Dashboard	Configuration	Reporting	Documentation	Downloads
Load Bal	ancing Serv	ice		
Basic Settings				
Service Name*				
srv-1-80		(j)		
New Server	• Existing Server			
Server*				
srv-1 (10.63.32	2.55) 🗸			
Protocol*				
TCP	~	()		
Port*				
80		()		
► More				

Bind the TCP protocol monitor to each load balancing service.

	Configuration	Reporting	Documentation	Downloads	
Load Balar	ncing Servi			ad Balancing Monitor Binding / Load Balancing Monitor Binding alancing Monitor Binding	5
			Select Monit		
			tcp	> Add Edit	Ō
			Binding Deta	tails	
				taito	
	OOWN		Weight		
			1		
			✓ State		
			✓ State		
			Bind	Close	

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

Traffic Manage	ment / Load Balancing / Services / Ser	vices							
Services 🗘									
Services 4	Auto Detected Services 0 Inter	nal Services 6							
Add	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 balancing virtual servers of ports 80, 443, and 1801. For example:

Traffic Manage	ement / Load Balancing / Virtual Servers									
Virtual	Servers									ي 🕲 🛃
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 F	Reporting	Documentat	ion (Downloads				
Q Search in Menu		Traffic Mar	nagement / Lo	ad Balancing / Vir	tual Servers					
System	>	Virtua	al Serve	rs 🕕						
AppExpert	>	virtue								
Traffic Management	~	Add	Edit Dele	ete Enable	Disable	Rename	Statistic	s Select Ac	tion 🗸	
Load Balancing	~	Q Click h	ere to search or y	rou can enter Key : V	alue format					
☆ Virtual Servers		-					A			
Services			NAME			STATE	♦ EFI	FECTIVE STATE	\$	IP ADDRESS
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 based on the TCP protocol.

citrix. Add	: 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)	P address.	plication is accessible from the Internet, the virtual server IP (VIP) address is a pub ailability of resources to process client requests.
Name*				
vsrv-80		Ō		
Protocol*				
TCP		Ó		
IP Address Type*				
IP Address		·		
IP Address*				
10 . 63 .	32 . 60	(i)		
Port*				
80		()		
► More				
ОК	Cancel			

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

С	itriż. 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				Listen Priority Listen Policy Expression Redirection Mode Range IPset RHI State AppFlow Logging Retain Connections on Cluster TCP Probe Port	- IP 1 - PASSIV ENABL NO -
	Services and	d Service Groups					
	A service grou Note: Bind at le	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, any other configuration detail	to a virtual server, and you can ac eed.	ld service
	No Load Bala	ncing Virtual Server Servio	ce Binding				
	No Load Bala	ncing Virtual Server Servio	eGroup Binding				
	Continue						

Session Recording 2204

С	itriż. ad	C VPX (1000)			
	Dashboard	Configuration	Reporting	Documentation	Downloads
_	Lood Po	lopoing Virtu	ol Corvor	Service Bind	ling / Service
		lancing Virtu		Service	4
				Select	Add Edit
				Q Click here	to search or you can enter Key : Value format
					NAME
					srv-1-80
					srv-1-443
					srv-1-22334
				Total 4	
	Done				

Choose a load balancing method.

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

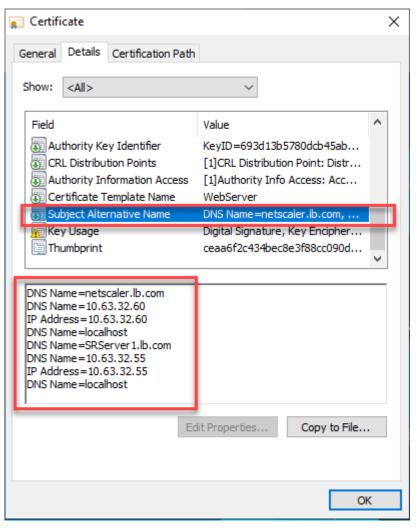
Configure persistence on each virtual server. We recommend you select **SOURCEIP** as the persistence type. For more information, see Persistence settings.

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.

File Action Yiew Help 	
BDNS Name Type Data Timestamp JEDC □ moder	
V ELBDC	
 Reverse Lookup Zones Tust Points Conditional Forwarders Game as parent folder) Name Server (NS) Ibdc.Ib.com, hostma static (same as parent folder) Host (A) 10.63.32.82 11/19/2020 2:00:00 AM Ibdc Ibdc Host (A) 10.63.32.82 static IBDC Host (A) 10.63.32.60 static SServer1 Host (A) 10.63.32.68 11/19/2020 2:00:00 AM SServer2 Host (A) 10.63.32.68 11/19/2020 1:00:00 PM SServer2 Host (A) 10.63.32.61 11/19/2020 2:00:00 AM SServer2 Host (A) 10.63.32.61 11/23/2020 2:00:00 AM TSVDA Host (A) 10.63.32.215 11/23/2020 2:00:00 AM 	

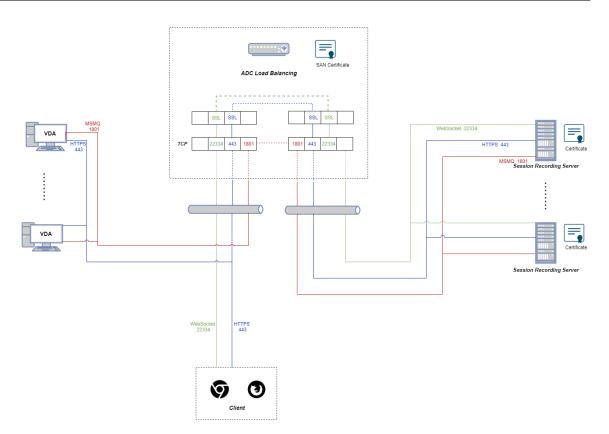
8. To access the web player over HTTPS, ensure that a SAN certificate is available both on Citrix ADC and on each Session Recording server. A SAN certificate contains the FQDNs of the Citrix ADC and of each Session Recording server.



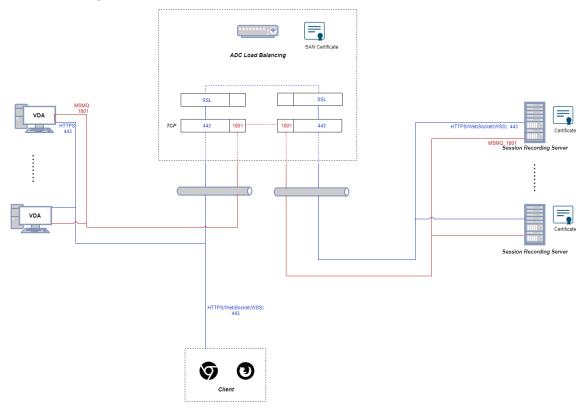
Configure load balancing through SSL offloading

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	PX (100	0)
Dashboard Co	onfigurat	ion Reporting Documentation Downloads
Q Search in Menu		System / Settings
System Licenses	~	Settings
 Settings Diagnostics High Availability NTP Servers 	>	Modes and Features Configure Modes Configure Basic Features Configure Advanced Features Configure Extra Management CPU
Reports Profiles		
Partition Administration	>	
User Administration	>	
Authentication	>	
Auditing	>	
SNMP	>	ADM
AppFlow	<u> </u>	Configure ADM Parameters

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

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

citrix. Add	C VPX (1000)			
Dashboard	Configuration	Reporting	Documentation	Downloads
Configur	e Basic Feat	ures		
SSL Offloading		HTTP Compress	sion	
✓ Load Balancing		Content Switch	ing	
Content Filter		Integrated Cach	ning	
Rewrite		Citrix Gateway		
Authentication, Au	thorization 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:

citrix. Ad	C VPX (1000)			
Dashboard	Configuration	Reporting	Documentation	Downloads
Croate S	Convor			

Create Server

Name*	
srv-1	\bigcirc
IP Address Domain Name	
IPAddress*	
10.63.32.55	
Traffic Domain	
	V 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 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:

	: Management /	/ Load Balancing / Services / Services								
Add Edit Delete Statistics Action	vices									Q R
Name State IP Address/Domain Name Port Protocol Max Clients Max Requests Cache Type Traffic ○ ○ \$\string{1-443}\$ ● UP 10.6332.55 443 \$\string{1-443}\$ 0 0 \$\string{1-443}\$ 0 \$\string{1-443}\$ \$1-	vices 3 Au	Auto Detected Services 0 Internal Servi	rices 6							
① ⊙ □ \$Nv-1-443 ● UP 10.63.32.55 443 55L 0 0 5ERVER	Add Edit Delete Statistics Action •								Search 🕶	
	Name	me	State	IP Address/Domain Name	Port	Protocol	Max Clients	Max Requests	Cache Type	Traffic Domain
□ srv-1-1801 ● UP 10.6332.55 1801 TCP 0 0 SERVER	srv-1-	-1-443	• UP	10.63.32.55	443	SSL	0	0	SERVER	0
	srv-1-	-1-1801	• UP	10.63.32.55	1801	TCP	0	0	SERVER	0
□ 3/v-1-2234 ● UP 10.63.32.55 22334 5SL 0 0 5 SERVER	srv-1-	-1-22334	• UP	10.63.32.55	22334	SSL	0	0	SERVER	0

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

citrix. adc	VPX (100	0)		
Dashboard	Configurati	ion Reporti	ing Documentation	Downloads
Q Search in Menu		Traffic Managemen	nt / Load Balancing / Services	/ Services
System	>	Services		
AppExpert	>			
Traffic Management	~	Services 0	Auto Detected Services 0	Internal Services 6
Load Balancing	~	Add Edit	Delete Rename St	tatistics No action 🗸
Virtual Servers				
☆ Services		Q Click here to se	earch or you can enter Key : Value f	ormat
Service Groups		NAM	E	
Monitors		No items		
Metric Tables				
Servers				
Persistency Groups	3			
Radius Nodes				
Priority Load Balancir	ng 🧵 >			
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. add	VPX (1000)		
Dashboard	Configuration	Reporting	Docum
🖯 Load Bal	ancing Serv	vice	
Basic Settings			
Service Name* srv-1-22334		Ō	
O New Server	• Existing Server		
Server* srv-1 (10.63.32	.55)	/	
Protocol*			
SSL Port*		/ (Ì)	
22334		(j)	
► More			
ОК	Cancel		

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

	CİTIX. ADC VPX (1000)								
Dashboard Config	guration Re	porting	Documentation	Downloads					
load Balancin	g Service			alancing Monitor Binding /		itor Binding			
			Select Monitor*	*	Add	Edit			
	srv-1 10.63.32.55		Binding Details	3					
	• DOWN SSL 22334		Weight 1 ✓ State		Ō				
			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	C VPX (1000)	
Dashboard	Configuration	Reporting Do
Contemporal Con	ancing Serv	/ice
Basic Settings		
Service Name*		
srv-1-443		Ō
O New Server	• Existing Server	
Server*		
srv-1 (10.63.32	2.55)	\sim
Protocol*		
SSL		~
Port*		
443		(i)
► More		
ОК	Cancel	

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

	PX (1000)		
Dashboard C	onfiguration Rep	orting Documentation	Downloads
		Service Load	Balancing Monitor Binding / Load Balancing Monitor Binding
Load Balan	cing Service	Load Bal	ancing Monitor Binding
		Select Monit	or*
		https	> Add Edit (j
		Binding Deta	ils
	10.63.32.55 • DOWN	Weight	
		1	
		✓ State	
Comments		✓ otate	
		Bind	Close

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 add	VPX (1000)		
Dashboard	Configuration	Reporting	Documentat
😋 Load Bala	ancing Serv	vice	
Basic Settings			
Service Name*			
srv-1-1801		(j)	
O New Server	• Existing Server		
Server*			
srv-1 (10.63.32	.55)	~	
Protocol*			
TCP	`	i)	
Port*			
1801		<u>(</u>)	
► More			
ок	Cancel		

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

arvice Load Balancing Monitor Binding / Load Balancing Monitor Binding arvice Load Balancing M
ielect Monitor* tcp > Add Edit (inding Details Veight 1 State
tcp > Add Edit (inding Details //eight 1 ? State
inding Details Veight 1 2 State
1 State
1 State
State
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. adc	CİTIX. ADC VPX (1000)								
Dashboard	Configurat	tion R	eporting	Documentatio	n Do	ownloads			
Q Search in Menu		System /	Profiles /	HTTP Profiles					
System	\sim	Profil	es						
Licenses Settings		TCP Prof		HTTP Profiles 3	Databas	e Profiles 0	SSL Profil		
Diagnostics High Availability	>	Add)elete					
NTP Servers Reports		Q Click h	ere to search NAME	or you can enter Key : Val		INVALID 🗢 INV	ALIDATE HTT		
🔄 Profiles			nshttp_	default_profile	×	×			
Partition Administrat	ion >		nshttp_	default_strict_validation	~	~			
User Administration	>		nshttp_	default_internal_apps	~	~			
Authentication Auditing	>	Total 3							
SNMP	>								

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

Session Recording 2204

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 Inv
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 (j)	Enable RTSP Tunnel
Drop extra data from server	✓ HTTP Weblogging	Persistent ETag
Adaptive Timeout		
Create		

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 vpx	(1000)				HA Status Not configured	Parti defau	tion 🗸 It	nsroot \vee
	Dashboard Conf	figuration	Reporting	Documentation	Downloads				\$
¢	Load Balanci	ng Servi	ce						
	Basic Settings						/	Help	
	Service Name Server Name IP Address Server State Protocol Port Comments Monitoring Connection Close	srv-1-2233 srv-1 10.63.32.59 • DOWN SSL 22334 Bit NONE		Traffic Domain Number of Active Connecti Hash ID Server ID Clear Text Port Cache Type Cacheable Health Monitoring AppFlow Logging	0 - - None - SERVEI NO YES ENABL			+ Thre + Prot + Poli	cies
	Service Settings					/	×	+ SSL	Policies
	Sure Connect Surge Protection OFF Use Proxy Port YES			Client Keep-Alive	NO NO NO				lificate

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

Profiles	
Net Profile	
	★ +
TCP Profile	
	✓ +
HTTP Profile	
websocket_SSL	✓ + ⑦
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.

File Action Yiew Help Image: State of the state of	â DNS Manager				_	×
 Image: Second Secon	File Action View Help					
 IbDC IbDC Insdcs sites sites tcp udp DomainDnsZones Trust Points Conditional Forwardes ForestDnsZones Game as parent folder) Name Server (NS) Ibdc.lb.com, hostma static (same as parent folder) Notes (A) Io63.32.82 It/19/2020 2:00:00 AM Ibdc Host (A) Io63.32.82 It/19/2020 11:00:00 PM Ibdc Ibdc (A) Ibdc (A) Io63.32.65 It/19/2020 11:00:00 PM Netscaler Most (A) Io63.32.65 It/19/2020 2:00:00 AM Ibdc Host (A) Io63.32.65 It/19/2020 11:00:00 PM Netscaler Most (A) Io63.32.65 It/19/2020 11:00:00 PM Netscaler Host (A) Io63.32.60 static SRServer1 Host (A) Io63.32.60 It/19/2020 11:00:00 PM Netscaler Host (A) Io63.32.61 It/19/2020 11:00:00 PM SRServer2 Host (A) Io63.32.61 It/19/2020 3:00:00 AM 	♦ ≥					
		 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 10.63.32.55 10.63.32.55 10.63.32.56 10.63.32.68 10.63.32.91	static static 11/19/2020 2:00:00 AM static 11/19/2020 11:00:00 PM static 11/19/2020 11:00:00 AM 11/19/2020 11:00:00 AM 11/23/2020 3:00:00 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.

raffic Manag	ement / Load Balancing / Virtual Servers								
/irtual	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

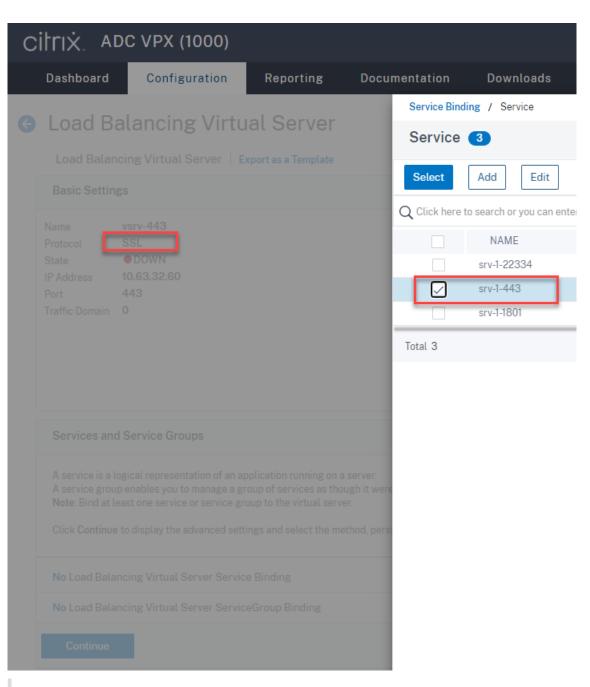
Navigate to Traffic Management > Load Balancing > Virtual Servers and click Add.

Citrix add	VPX (100)0)								
Dashboard	Configurat	ion f	Reporting	Documentation	n Do	wnloads				
Q Search in Menu		Traffic Ma	nagement / Loa	d Balancing / Virtua	al Servers					
System	>	Virtua	al Server	s 🚹						
AppExpert	>	virtat		5						
Traffic Management	~	Add	Edit Delet	e Enable	Disable	Rename	Statis	stics Select	Action 🗸	
Load Balancing	~	Q Click h	ere to search or yo	ou can enter Key : Valu	ue format					
☆ Virtual Servers			NAME			STATE	\$	EFFECTIVE STATE	\$	IP ADDRESS
Services		No items								
Service Groups										
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. Type a server name, select **TCP** or **SSL**, and select the relevant port number as described earlier.

triż adc	VPX (1000)			
Dashboard	Configuration	Reporting	Documentation	Downloads
Load Bala	ancing Virtu	al Server		
Basic Settings				
network (WAN), the	VIP is usually a private (CANN non-routable)	IP address.	oplication is accessible from the Internet, the virtual server IP (VIP) address is a p ailability of resources to process client requests.
vsrv-80		(j)		
		U		
Protocol*		()		
IP Address Type*	•	\bigcirc		
IP Address	~			
IP Address*				
10 . 63 .	32 60	(j)		
Port*		U		
80		(i)		
00		\bigcirc		

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 algorith	m that the Citrix ADC	uses to
Load Balancing Method*		
LEASTBANDWIDTH	~ (i)	
New Service Startup Request Rate		
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

(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 serv	ver or service. You can apply the same profile to multiple entities of the same type.	
Net Profile	HTTP Profile	
TCP Profile	DB Profile	
LB Profile	DNS Profile Name	
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 Certificate
4	
Certificat	e-Key Pair Name*
lbcard	
Certificat	e File Name*
Choose	e File 🔻 Ibcard.cer
Key File N	lame*
Choos	e File 🔻 Ibcard.key
Password	*
••••	C C C C C C C C C C C C C C C C C C C
🖌 Notif	fy When Expires
No SNM	P Trap destination found. Notification will not be sent until a trap destination is configured.
Notificati	ion Period
30	
L	
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
G	Load B	alancing Virtu	al Server		
	Load Balan	icing 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		
	<mark>No</mark> 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 \checkmark			
HTTP/HTTPS port:	Default \vee			
Port Number:				
Message life specifies the pe message queue.	riod during which dat	a remains	in the	
Message life (seconds):	7200			
Session Recording Broker				
Protocol:	HTTPS \sim			
HTTP/HTTPS port:	Custom ~			
Port Number:	443			
	OK (Cancel	Ap	ply

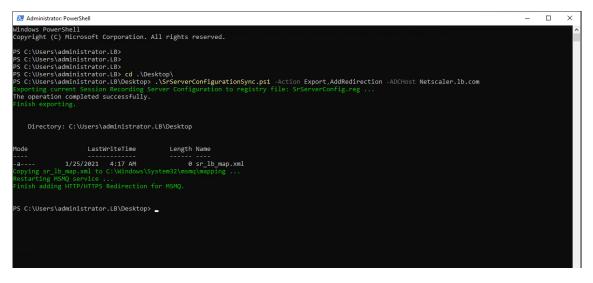
On each Session Recording server, add and set the IgnoreOSNameValidation DWORD value to 1 under HKEY_LOCAL_MACHINE\ SOFTWARE\Microsoft\MSMQ\ Parameters. For more information, see Knowledge Center article CTX248554.

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	eue		
Protocol:	HTTP ~]		
HTTP/HTTPS port:	Default 🗸 🗸			
Port Number:	80			
Message life specifies the p message queue. Message life (seconds):	7200	ata remains	in the	
Session Recording Broker				
Protocol:	HTTPS ~			
HTTP/HTTPS port:	Custom ~			
Port Number:	443]		
	ОК	Cancel	Δη	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

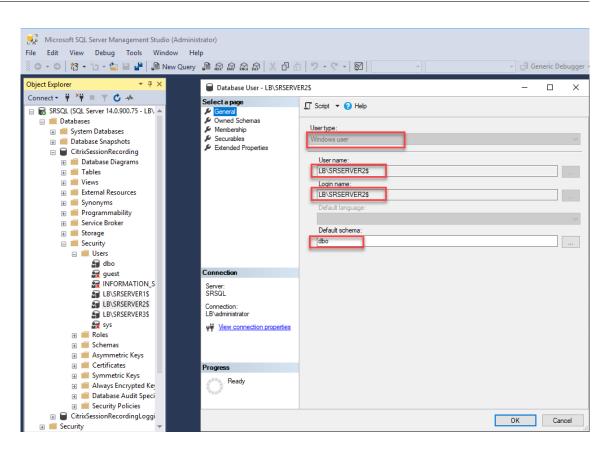
1. Prepare a machine in the same domain and install only the Session Recording server and Session Recording Administrator Logging modules on the machine.

	Features
[*] Licensing Agreement [*] Core Components	Feature (Select all)
Features	Session Recording Policy Console Citrix Session Recording Policy Console
Database and Server Administrator Logging	Session Recording Server Citrix Session Recording Broker and Storage Management.
Summary Install Finish	 Session Recording Administrator Logging Administrator Logging captures Session Recording Server configuration changes and recording activities to the Session Recording Database.
	Session Recording Database Citrix 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 Administrator Logging Summary Install Finish 	The Administrator Logging database is installed on the SQL Server instance:
	SRSQL
	Administrator Logging database name:
	CitrixSessionRecordingLogging 🗸
	Test connection
	 Enable Administrator Logging This option enables the Session Recording Administrator Logging service.
	 Enable mandatory blocking This option blocks policy and server property changes if logging fails.

- 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 (1000))			
Dashboard	Configuration	n Reporting	Documentation	Downloads	
Q Search in Menu	1	Traffic Management / Lo	ad Balancing / Servers		
System AppExpert	> S	Servers 🝳			
Traffic Management	~	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	(() 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					

CITIX ADC VP	X (100	00)					
Dashboard Co	nfigurat	ion Report	ing Documentation [Downloads			
Q Search in Menu		Traffic Managemer	t / Load Balancing / Services / Se	rvices			
System AppExpert	> >	Services					
Traffic Management	\sim	Services 8	Auto Detected Services 0 In	ternal Services 6			
Load Balancing Virtual Servers	~	Add Edit	Delete Rename Statistic	s No action V			
☆ Services		Q Click here to se	earch or you can enter Key : Value format				
Service Groups		N	IAME	♦ SERVER STATE	IP ADDRESS/DOMAIN NAME	○ PORT	PROTOCOL
Monitors		s	rv-1-80	• UP	10.63.32.55	80	TCP
Metric Tables		s	rv-1-443	● UP	10.63.32.55	443	TCP
Servers		s	rv-1-1801	• UP	10.63.32.55	1801	TCP
Persistency Groups		s	rv-1-22334	• UP	10.63.32.55	22334	TCP
Radius Nodes		s	rv-2-443	• UP	10.63.32.74	443	TCP
Priority Load Balancing	•	s	rv-2-80	• UP	10.63.32.74	80	TCP
Content Switching	•	s	rv-2-1801	• UP	10.63.32.74	1801	TCP
Cache Redirection	•	s	rv-2-22334	• UP	10.63.32.74	22334	TCP
DNS	>	Total 8					
GSLB	•						
SSL	>						
Subscriber	>						
Service Chaining	>						
User	>						

Dashboard C	onfiguration	Reporting	Documentation	Downloads		
Search in Menu	Traffic	Management / Load	d Balancing / Virtual Serve	rs		
System AppExpert	> Virt	ual Server	S 4			
Traffic Management	~ Add	I Edit Delet	e Enable Disable	e Rename Stat	istics Select Action	\sim
Load Balancing		ick here to search or yo	ou can enter Key : Value form	at		
Services		NAME			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	1	• UP	• UP	10.63.32.60
Persistency Groups	Tota	4				
Radius Nodes						
Priority Load Balancing	•					
Content Switching	() >					
Cache Redirection	() >					
DNS	>					
GSLB	•					
SSL	>					
Subscriber	>					
Service Chaining	>					
User	>					
Optimization	>					

Session Recording 2204

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 © IP ADDRESS © PORT © PROTOCO
	srv-1-22334 10.63.32.55 22334 TCP
	Close
Services and Service Groups 2 Load Balancing Virtual Server Service Bindings	
2 Load Balancing Virtual Server Service Bindings	
2 Load Balancing Virtual Server Service Bindings No Load Balancing Virtual Server ServiceGroup Binding	
2 Load Balancing Virtual Server Service Bindings No Load Balancing Virtual Server ServiceGroup Binding Method Load Balancing Method LEASTBANDWIDTH	

- 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 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

June 22, 2022

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.

Session Recording 2204

▲ Create storage account - Micros × +		
← → C 🔒 portal.azure.com/#create/Micro	osoft.StorageAccount	
■ Microsoft Azure	𝒫 Search resources, services, and docs (G+/)	
Home > Storage accounts >		
Create storage account	t	
redundant. Azure Storage includes Azure	Blobs (objects), Azure Data Lake Storage Gen2, Azure Files, Azure Queues, and Azure lepends on the usage and the options you choose below. 업	
Project details		
Select the subscription to manage deploy your resources.	ed resources and costs. Use resource groups like folders to organize and manage all	
Subscription *	cse-dev-03-ca 🗸 🗸	
Resource group *	×	
	Create new	
Instance details		
The default deployment model is Resourc using the classic deployment model inste	e Manager, which supports the latest Azure features. You may choose to deploy ad. Choose classic deployment model	
Storage account name * 🕕		
Location *	(US) East US V	
Performance ①	● Standard 🔿 Premium	
Account kind ①	StorageV2 (general purpose v2)	
Replication 🕕	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.

			№ 10-	🞐 🏟 ? 🙄 📕
Home > Co	ontainers 🖈 …			
Search (Ctrl+/) Access keys Geo-replication	≪ + Container A Change access level ⇒ Search containers by prefix	Restore containers 🗸 🖒 Refresh 🛛 🗎 Delete		Show deleted containers
 CORS Configuration Encryption 	Name You don't have any containers yet. Click '+ Cont	Last modified tainer' to get started.	Public access level	Lease state
 Shared access signature Networking 				
 Security Static website Properties 				
Blob service				
 Containers 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.

Session Recording 2204

Microsoft Azure	$\mathcal P$ Search resources, services, and docs (G+/)	
services > Virtual machines >		
reate a virtual mac	hine	
elect the subscription to manage de	eployed resources and costs. Use resource groups like folders to organize	and manage all
our resources.		
ubscription * 🕕	cse-dev-03-ca	\sim
Resource group * 🛈	(New) Resource group	\sim
	Create new	
stance details		
rtual machine name * 🕕		
egion * 🕕	(US) East US	
gion ()		
vailability options 🕕	No infrastructure redundancy required	\checkmark
nage * 🕕	Windows Server 2019 Datacenter - Gen1	\sim
	See all images	
zure Spot instance 🕕		
ze * 🕕	Standard_D4s_v3 - 4 vcpus, 16 GiB memory (\$83.22/month)	\sim
	See all sizes	
dministrator account		

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

Microsoft Azure					🎐 🐵 📍	©
Container	≪ ↑ Upload 合 Change access level ○ Refresh 1 0 Delet	a → Change ting Ø Argui	re lesse - x ^Q Break lesse	View spanskate	Create and	shat
Overview Access Control (IAM)	Authentication method: Access key (Switch to Azure AD User Accou Location: yuchunblob		release y break lease	· view snapshots		anot
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						Properties
						Cenerate SAS
						 View previous versions
						 View snapshots
						Create snapshot
						∠ Change tier
						Acquire lease
						S Break lease

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.

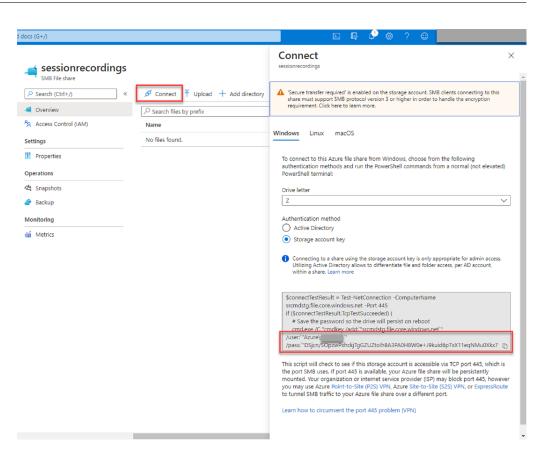
b) Run the SsRecUtils.exe -AddAzureFiles <storageAccountName> <fileShareName> <accesskey> command.

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.

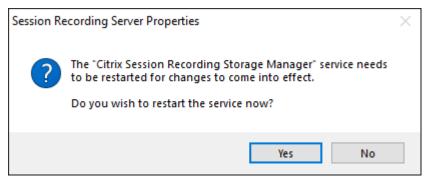
■ Microsoft Azure	P Search resources, services, and docs (G+/)
Home > srcmd >	
<pre></pre>	eys
	Use access keys to authenticate your applications when making requests to this Azure storage account. Store your access keys so that you can maintain connections using one key while regenerating the other.
Cverview	When you regenerate your access keys, you must update any Azure resources and applications that access this storage acc
Activity log	
🗳 Tags	Storage account name srcmdstg
Diagnose and solve problems	
Access Control (IAM)	Hide keys
💕 Data migration	key1 🗘
🚡 Storage Explorer (preview)	
Settings	DSjcn/SOpzwPxhckjTgGZUZtolh8A3PA0H8W0e+J9kuid6p7xX11eqNMu0Xkx7R352f2GHRFU2PllFi11vbE/A==
Access keys	Connection string DefaultEndpointsProtocol=https;AccountName=;AccountKey=DSjcn/SOpzwPxhckjTgGZUZtolh8A3PA0H8W0e+.
S CORS	
Configuration	key2 🗘
Encryption	Key O97VNcAmv+WpgFYYO6r3OfMyaD20sSGGpJuBgfkDYv3Z27j19TYOMbWFaz1N6riO81c2qF5JZOQVxqydmysO2A==
 Shared access signature 	
	Connection string DefaultEndpointsProtocol=https;AccountName=;AccountKey=O97VNcAmv+WpqFYYO6r3OfMyaD20sSGGpJuBi
Networking	ревынствропосно-терудесовликате-
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.

torage	Signing	Rollover	Playback	Notifications	CEIP	Logging	RE • •						
				ne directories ultiple directo									
volume													
File st	orage dire	ctories:											
						Add							
1	The defau	List of fo	Iders is em	pty. cordings will	he	Modify.							
		in folder e.	used.	corolligo uni				File	e Storage	e Directory	,		
						Remov	/e	E	Enter a di	rectory for	storing recor	ded session files:	
										e.windows	s.net\sessionn	ecording\recordings	Browse
												OK	Canc
Specify them a	y a folder vailable fo	to tempora	rily store a k.	chived sessi	on recordi	ngs and m	ake					ОК	Canc
them a	ivailable fo	or playbac	k.	chived sessi	on recordir	ngs and m	ake					ОК	Canc
them a	vailable for	or playbac y for archi	k. ved files:	chived sessi	on recordin	-						ОК	Canc
them a	vailable for	or playbac	k. ved files:	chived sessi	on recordir	ngs and m Browse						ОК	Canc
them a	vailable for	or playbac y for archi	k. ved files:	chived sessi	on recordin	-						ОК	Canc
them a	vailable for	or playbac y for archi	k. ved files:	chived sessi	on recordin	-						ОК	Canc
them a	vailable for	or playbac y for archi	k. ved files:	chived sessi	on recordin	-						ОК	Canc
them a	vailable for	or playbac y for archi	k. ved files:	chived sessi	on recordin	-						ОК	Canc
them a	vailable for	or playbac y for archi	k. ved files:	rchived sessi	on recordir	-						ОК	Canc
them a	vailable for	or playbac y for archi	k. ved files:	chived sessi	on recordir	-						ОК	Canc
them a	vailable for	or playbac y for archi	k. ved files:	chived sessi	on recordii	-						ОК	Canc
them a	vailable for	or playbac y for archi	k. ved files:			Browse						ОК	Canc
them a	vailable for	or playbac y for archi	k. ved files:	OK	on recordin	Browse						OK	Canc

- 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	😝 LiveArena Broadcast	🙆 Citrix ADC		
	Name	Resources	🐴 Citrix ADC 13.0 - Azure Stack		at Viewed
	🚍 yu	No results were found.	Citrix ADC 12.1		ew seconds ago
			👌 Citrix ADC VPX FIPS		ew seconds ago
			Documentation	See all	minutes ago
	📰 yu 🗇 SR 🔇 SR		Tutorial: Azure Active Directory single sign-on		-
	SR		Tutorial: Azure Active Directory integration with Citrix		minutes ago
			Azure AD secure hybrid access Microsoft Docs		ay ago
	<↔> SR		Linux virtual desktops with Citrix - Azure Example		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
	 VN 	Try searching in Azure Active Directory			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**.

Home >				
Citrix ADC	\$ ···			
Citrix				
c	Citrix ADC 🗇 Add to Favorites			
citrix.	itrix 1 ☆ ☆ ☆ ①.0 (0 ratings)			
	Azure benefit eligible ⊡ ⁿ			
se	elect a plan Citrix ADC VPX Bring Your Own License V Create			
Overview Plans	Usage Information + Support Reviews			
Overview Plans	Usage Information + Support Reviews			
Citrix ADC is an enter	Usage Information + Support Reviews prise-grade application delivery controller that delivers your applications quickly, reliably, and securely, with the deployment and pricing flexibility to unique needs. Designed to provide operational consistency and a smooth user experience, Citrix ADC eases your transition to the hybrid cloud.			
Citrix ADC is an enter	prise-grade application delivery controller that delivers your applications quickly, reliably, and securely, with the deployment and pricing flexibility to			
Citrix ADC is an enterp meet your business' u	prise-grade application delivery controller that delivers your applications quickly, reliably, and securely, with the deployment and pricing flexibility to			
Citrix ADC is an enter meet your business' u Why Citrix?	prise-grade application delivery controller that delivers your applications quickly, reliably, and securely, with the deployment and pricing flexibility to unique needs. Designed to provide operational consistency and a smooth user experience, Clrrix ADC eases your transition to the hybrid cloud.			
Citrix ADC is an entery meet your business' u Why Citrix? Citrix ADC offers high	prise-grade application delivery controller that delivers your applications quickly, reliably, and securely, with the deployment and pricing flexibility to unique needs. Designed to provide operational consistency and a smooth user experience, Citrix ADC eases your transition to the hybrid cloud.			
Citrix ADC is an entery meet your business' u Why Citrix? Citrix ADC offers high	prise-grade application delivery controller that delivers your applications quickly, reliably, and securely, with the deployment and pricing flexibility to unique needs. Designed to provide operational consistency and a smooth user experience, Clrrix ADC eases your transition to the hybrid cloud.			
Citrix ADC is an enter meet your business' u Why Citrix? Citrix ADC offers high applications across dk	prise-grade application delivery controller that delivers your applications quickly, reliably, and securely, with the deployment and pricing flexibility to unique needs. Designed to provide operational consistency and a smooth user experience, Citrix ADC eases your transition to the hybrid cloud.			
Citrix ADC is an enter meet your business' u Why Citrix? Citrix ADC offers high applications across dk	prise-grade application delivery controller that delivers your applications quickly, reliably, and securely, with the deployment and pricing flexibility to unique needs. Designed to provide operational consistency and a smooth user experience, Citrix ADC eases your transition to the hybrid cloud.			
Citrix ADC is an entery meet your business' u Why Citrix? Citrix ADC offers high applications across cl step of the way. Key Benefits:	prise-grade application delivery controller that delivers your applications quickly, reliably, and securely, with the deployment and pricing flexibility to inique needs. Designed to provide operational consistency and a smooth user experience, Citrix ADC eases your transition to the hybrid cloud.			
Citrix ADC is an entery meet your business' u Why Citrix? Citrix ADC offers high applications across ck step of the way. Key Benefits: • Flexible & Cor capacity licensi	prise-grade application delivery controller that delivers your applications quickly, reliably, and securely, with the deployment and pricing flexibility to inique needs. Designed to provide operational consistency and a smooth user experience, Citrix ADC eases your transition to the hybrid cloud.			
Citrix ADC is an entery meet your business' u Why Citrix? Citrix ADC offers high applications across ck step of the way. Key Benefits: • Flexible & Cor capacity licensi • Best User Exp	prise-grade application delivery controller that delivers your applications quickly, reliably, and securely, with the deployment and pricing flexibility to inique needs. Designed to provide operational consistency and a smooth user experience, Citrix ADC eases your transition to the hybrid cloud.			
Citrix ADC is an entery meet your business' u Why Citrix? Citrix ADC offers high applications across ck step of the way. Key Benefits: • Flexible & Con capacity licensi • Best User Exp users to the be	prise-grade application delivery controller that delivers your applications quickly, reliably, and securely, with the deployment and pricing flexibility to inique needs. Designed to provide operational consistency and a smooth user experience, Clrix ADC eases your transition to the hybrid cloud.			
Citrix ADC is an entern meet your business' u Why Citrix? Citrix ADC offers high applications across ck step of the way. Key Benefits: • Flexible & Con capacity licens • Best User Exp users to the be • Integrated Ap Comprehensiv	prise-grade application delivery controller that delivers your applications quickly, reliably, and securely, with the deployment and pricing flexibility to inique needs. Designed to provide operational consistency and a smooth user experience, Citrix ADC eases your transition to the hybrid cloud.			

4. Set VM configurations.

Session Recording 2204

▲ Create Citrix ADC - Microsoft Azu × +	
← → C	netscalervpx-1vm-3nicnetscalervpx-1vm-3nic-byol
\equiv Microsoft Azure	Search resources, services, and docs (G+/)
Home > Citrix ADC >	
Create Citrix ADC	
A Changes on this step may reset later se	lections 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 * 🛈	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 * 🛈	d28e81a280 ✓
Azure Monitoring Metrics ①	C Enabled
5	Disabled
Backend Autoscale ①	C Enabled
	Disabled
Review + create < Previous	Next : Network and Additional Settings >

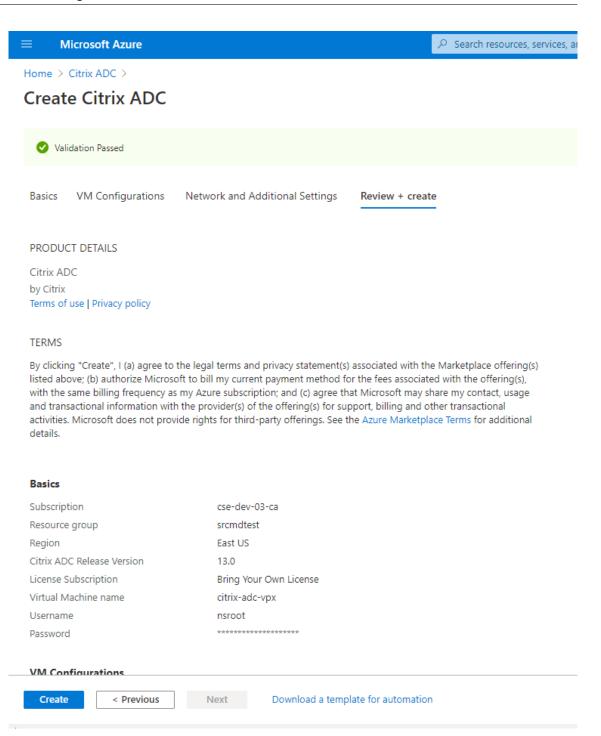
5. Check and modify network settings if necessary. Choose **ssh (22), http (80), https (443)** for public inbound ports.

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, a	nd docs (G+/)
Home > Citrix ADC >			
Create Citrix ADC			
Configure virtual networks			1
Virtual network * ii	(new) citrix-adc-vpx-virtual-network	\sim	
	Create new		
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)			
Management Public IP (NSIP) * 🛈	(new) citrix-adc-vpx-nsip Create new	\sim	
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	
	Create new		
Clientside Domain Name 🕡	citrix-adc-vpx-vip-23f12ee6b2	 	
		.eastus.cloudapp.azure.com	
Public Inbound Ports (Management o	nly)		
Ports open for Management public IP ①			
1	() ssh (22)		
	 ssh (22), http (80), https (443) 		
Review + create < Previous	Next : Review + create >		

■ Microsoft Azure		$ \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
Accelerated Networking		
Accelerated Networking (Management	On	
Interface) (i)	O off	
Accelerated Networking (Client Interface)	• On	
	○ off	
Accelerated Networking (Server	• On	
Interface) 🛈	O off	
Public IP (Management)		
Management Public IP (NSIP) * 🛈	(new) citrix-adc-vpx-nsip	~
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.

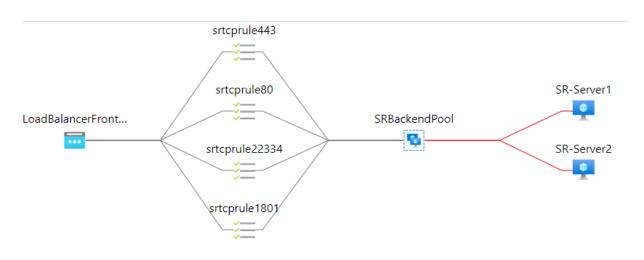
Session Recording 2204

Microsoft Azure) adc	
lome > srlb > citrix-adc-vpx-nic1	1				
🚽 citrix-adc-vpx-ni	c11 IP conf	figurations			
Network interface		•			
Search (Ctrl+/)	« 🕂 Add 🛛	🛛 Save 🗡 Dise	card 🕐 Refresh		
Overview	IP forwardin	ig settings			
Activity log	IP forwarding	9			Disabled Enabled
Access control (IAM)	Virtual netwo	ork			srazureautovnet
Tags	IP configura	tions			
ettings	Subnet	litona			srazureautosubnet2 (192.168.2.0/24)
IP configurations					
DNS servers					
Network security group	🚺 The as	ssociated virtual mac	hine 'citrix-adc-vpx' n	nust be either stopped or deallocated	in order to be able to edit the subnet.
Properties					
Locks		P configurations	True	Delvete ID eddeses	Dublic ID address
utomation	Name	IP Version	Туре	Private IP address	Public IP address
Tasks (preview)	vip	IPv4	Primary	192.168.2.4 (Dynamic)	Unassigned (citrix-adc-vpx-vip) ***
Export template					
pport + troubleshooting					
Effective security rules Effective routes New support request					
Effective security rules			우 adc		
Effective security rules Effective routes New support request Microsoft Azure me > srlb > citrix-adc-vpx-nic11			P adc		
Effective security rules Effective routes New support request Microsoft Azure me > srlb > citrix-adc-vpx-nic11 citrix-adc-vpx-nic1	1 IP configu	urations	ନ adc		
Effective security rules Effective routes New support request Microsoft Azure me > srlb > citrix-adc-vpx-nic11 citrix-adc-vpx-nic11 Network interface	· -	-			
Effective security rules Effective routes New support request Microsoft Azure me > srlb > citrix-adc-vpx-nic11 citrix-adc-vpx-nic11 Network interface Search (Ctrl+/) 《	1 IP configu + add ᠍ s	-			
Effective security rules Effective routes New support request Microsoft Azure Microsoft Azure Citrix-adc-vpx-nic11 Citrix-adc-vpx-nic11 Network interface Search (Ctrl+/) « Overview	+ Add 🗔 s	Save X Discard	🕐 Refresh		
Effective security rules Effective routes New support request Microsoft Azure me > srlb > citrix-adc-vpx-nic11 citrix-adc-vpx-nic1 Network interface Search (Ctrl+/)	+ Add 🗔 s	Save X Discard	🕐 Refresh	ce will be restarted to utilize the new su	ibret.
Effective security rules Effective routes New support request Microsoft Azure me > srlb > citrix-adc-vpx-nic11 citrix-adc-vpx-nic1 Network interface Search (Ctrl+/)	+ Add 🗔 s	Save X Discard	🕐 Refresh	ce will be restarted to utilize the new su	ibnet.
Effective security rules Effective routes Microsoft Azure Microsoft Azure Microsoft Azure Citrix-adc-vpx-nic1 Citrix-adc-vpx-nic1 Network interface Search (Ctrl+/) « Overview Activity log Access control (IAM) Tags	+ Add 🔚 S	Save X Discard	🕐 Refresh	_	ubnet.
 Effective security rules Effective routes New support request Microsoft Azure Microsoft Azure otrix-adc-vpx-nic1 citrix-adc-vpx-nic1 Network interface search (Ctrl+/) « Overview Activity log Access control (IAM) Tags tings 	+ Add 🔙 S	Save X Discard	🕐 Refresh		
Effective security rules Effective routes Effective routes New support request Microsoft Azure Come > srlb > citrix-adc-vpx-nic11 Citrix-adc-vpx-nic11 Citrix-adc-vpx-nic1 Network interface Search (Ctrl+/) « Activity log Access control (IAM) Tags ttings IP configurations	+ Add 💽 S	ave X Discard	🕐 Refresh		sabled Enabled
Effective security rules Effective routes Chicrosoft Azure Microsoft Azure Microsoft Azure Microsoft Azure Chicrosoft Azure Contrix-adc-vpx-nic1 Cottrix-adc-vpx-nic1 Network interface Search (Ctrl+/) Coverview Activity log Access control (IAM) Tags tings IP configurations DNS servers	+ Add 💽 S	ave X Discard	🕐 Refresh	D ST	sabled Enabled
Effective security rules Effective routes Chicrosoft Azure Microsoft Azure Microsoft Azure Microsoft Azure Chicrosoft Azure Coverview Activity log Access control (IAM) Tags UP configurations DNS servers Network security group	+ Add 🖃 s The virtual IP forwarding set IP forwarding Virtual network IP configurations Subnet *	machine associated w titings	🕐 Refresh	D ST	sabled Enabled
Effective security rules Effective routes New support request Microsoft Azure me > srib > citrix-adc-vpx-nic11 Citrix-adc-vpx-nic11 Network interface Search (Ctrl+/) 《 Overview Activity log Access control (IAM) Tags tings IP configurations DNS servers Network security group Properties	+ Add 🖃 s	machine associated wittings	 Refresh ith this network interfe 	Sta Sta	sabled Enabled izureautovnet zureautosubnet (192.168.1.0/24)
Effective security rules Effective routes New support request Microsoft Azure me > srlb > citrix-adc-vpx-nic11 citrix-adc-vpx-nic11 Network interface Search (Ctrl+/)	+ Add 💽 S	s vigurations Teverson T	Refresh	sr sr Private IP address	sabled Enabled zzureautovnet zureautosubnet (192.168.1.0/24) Public IP address
Effective security rules Effective routes Effective routes New support request Nicrosoft Azure Citrix-adc-vpx-nic11 Citrix-adc-vpx-nic11 Network interface Search (Ctrl+/) 《 Overview Activity log Access control (IAM) Tags IP configurations DNS servers Network security group Properties Locks omation	+ Add 🖃 s	s vigurations Teverson T	 Refresh ith this network interfe 	Sta Sta	sabled Enabled izureautovnet zureautosubnet (192.168.1.0/24)
Effective security rules Effective routes New support request Microsoft Azure me > srlb > citrix-adc-vpx-nic11 citrix-adc-vpx-nic11 Network interface Search (Ctrl+/)	+ Add 💽 S	s vigurations Teverson T	Refresh	sr sr Private IP address	sabled Enabled zzureautovnet zureautosubnet (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 Citrix-adc-vpx-nic1 Citrix-	+ Add 💽 S	s vigurations Teverson T	Refresh	sr sr Private IP address	sabled Enabled zzureautovnet zureautosubnet (192.168.1.0/24) Public IP address
Effective security rules Effective routes Effective routes Microsoft Azure Mic	+ Add 💽 S	s vigurations Teverson T	Refresh	sr sr Private IP address	sabled Enabled zzureautovnet zureautosubnet (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 Citrix-adc-vpx-nic1 Citrix-	+ Add 💽 S	s vigurations Teverson T	Refresh	sr sr Private IP address	sabled Enabled zzureautovnet zureautosubnet (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	× 🛛 🖓 O 🍩	? ©) Yuchun.Jiang@citrix.com
Azure servic	Services See all	Marketplace	See all	
Create a resource	 Load balancing - help me choose (Preview) Application gateways Front Doors 	 Load Balancer / ADC aiScaler Load Balancer & Site Acceleration Ishlangu Load Balancer ADC IS-5000 (SGbps) 		More services
Recent resou	CloudAMQP CloudAMQP CloudAMQP	Documentation Load Balancer Microsoft Docs What is Azure Load Balancer	See all	
Name SRAppGV1 Suchun,jiang SRLoadBalan	Workload Insights CloudSimple Nodes CloudSimple Services Resources	Azure Load Balancer concepts Microsoft Docs Quickstart: Create a public load balancer - Azure portal Resource Groups		3
 SRVnet srtest 	No results were found. Didn't find what you were looking for?	No results were found.		
 LB-hubtest-Ty asfazuretests srazureauto 	Try searching in Activity Log Try searching in Azure Active Directory Searching al subscriptions. Change			
↔ VNet-hubtest	Virtua	l network 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 .

Create load balance		
	s, or internal where it is only accessible from a virtual network. Azure I on (NAT) to route traffic between public and private IP addresses. Let	
Project details		
Subscription *	cse-dev-03-ca	\sim
Resource group *	sribtest Create new	\checkmark
Instance details		
Name *	SRLoadBalance	\checkmark
Region *	(US) East US	\sim
Type * 🕡	Internal Public	
SKU * 🛈	Basic Standard Standard Load Balancer is secure by default. This means I	Network Service
	Groups (NSGs) are used to explicitly permit and whitelist a do not have an NSG on a subnet or NIC of your virtual me traffic is not allowed to reach this resource. Please configu communication if needed. For outbound communication outbound rule is needed. Learn more about outbound co	allowed traffic. Ìf you achine resource, ure an NSG to ensure , an explicit
Configure virtual network.		
Virtual network * 🕕	srazureautovnet	\sim
Subnet *	srazureautosubnet (192.168.1.0/24)	\sim
	Manage subnet configuration	
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.

		${\cal P}$ Search resources, services, and docs (0	\$+/)	
Home > SRLoadBalance				
SRLoadBalance Bac	kend pools			
✓ Search (Ctrl+/) «	+ 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				
š≡ Load balancing rules				
Inbound NAT rules				
Properties				
🔒 Locks				
Monitoring				
III Alerts				
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, a
Home > SRLoadBalance > Add backend pool SRLoadBalance		
Name * Virtual network ③ IP version	SRBackendPool srazureautovnet (sribtest) IPv4 IPv6	~
Virtual machines You can only attach virtual machines in d All IP configurations must be on the sam + Add X Remove		configuration or no public IP configuration.
Virtual machine ↑↓	IP Configuration \uparrow_{\downarrow}	Availability set \uparrow_{\downarrow}
	ime location as Load Balancer. Only IP cont in be selected. All of the IP configurations l	
 No virtual machine scale set is foun 	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	$\mathcal P$ Search resources, services, and docs	(G+/)		📃 🗵 🕼 🗳 🎯 ? 😳 📃	
Home > SRLoadBalance					
SRLoadBalance	Health probes				>
P 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					
🖬 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.

≡ Microsoft Azure	$\mathcal P$ Search resources, services, and docs (G+/)
Home > SRLoadBalance >	
SRHealthProbe SRLoadBalance	
🔚 Save 🗙 Discard 📋 Delete	
Name *	
SRHealthProbe80	\checkmark
Protocol (i)	
ТСР	\sim
Port* ①	
80	
Interval * ① 5	
5	seconds
Unhealthy threshold * ①	
2	
	consecutive failures
Used by 🕠	
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		℅ Search resources, services, and docs (G+/)
Home > SRLoadBalance		
SRLoadBalance Loa	d balancing rules	
	+ Add	
🚸 Overview		
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		
III 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.

	$\mathcal P$ Search resources, services, and docs (G+/)
Home > SRLoadBalance >	
Add load balancing rule	
SRLoadBalance	
Name *	
SRTCPRule80	✓
IP Version *	
● IPv4 ◯ IPv6	
Frontend IP address * (i)	
192.168.1.23 (LoadBalancerFrontEnd)	\checkmark
HA Ports ()	
Protocol	
● TCP ◯ UDP	
Port *	
80	~
Backend port * ①	
80	✓
Backend pool ①	
SRBackendPool	\checkmark
Health probe ① SRHealthProbe80 (TCP:80)	~
	V
Session persistence ① Client IP	~
	`
Idle timeout (minutes) ①	
0	4
TCP reset Disabled Image: Enabled	
Floating IP ①	
ок	

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

Microsoft Azure			℅ Search r	esources, services, and	docs (G+/)
Home > SRLoadBalance					
SRLoadBalance Backend	pools				
P Search (Ctrl+/) ≪ + Add	🕐 Refresh				
Overview					
Activity log Backen	d pool	1	Virtual machi	ne	Virtual machine status
Access control (IAM)	ckendPool				
✓ Tags					
Diagnose and solve problems					
Settings					
Frontend IP configuration					
Backend pools					
P Health probes					
≆ Load balancing rules					
lnbound NAT rules					
Properties					
A Locks					
Monitoring					
Alerts					
Microsoft Azure Search resou Home > SRLoadBalance >	rces, services, and docs (G+/)	machines to bac	and neal		₽ç 🖉 @ ? ©
SRBackendPool	Aud virtual	machines to bac	lena poor		
IP Address	You can only attach Virtual machines m	virtual machines that are in the ust have a standard SKU public	same location and on the P or no public IP.	same virtual network as the loadbaland	er.
IP Version Prv4	P Filter by name		Location == eastus	Virtual network == SRVnet	Resource group == all Availability set == all
	Virtual machine	↑↓ Resource group ↑↓	IP Configuration $\uparrow \downarrow$	Availability set ↑↓ Tags	Notes
	sr-server1	_	ipconfig1 (10.7.1.5) ipconfig1 (10.7.1.6)		· · ·
Virtual machines You can only attach virtual machines in eastus that have a standard SKU public IP configuration o					
All IP configurations must be on the same virtual network. + Add					
Virtual machine ↑↓ IP Configuration ↑↓ Availabilit	· *** *				
No virtual machines selected					
Virtual machine scale sets					
Virtual Machine Scale Sets must be in same location as Load Balancer. Only IP configurations that (Basic/Standard) as the Load Balancer can be selected. All of the IP configurations have to be in th	have th e same				
No virtual machine scale set is found in eastus that matches the above criteria					
•					
Virtual machine scale set IP address	_				
Save Cancel		and .			
	Add Can	ter			

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.

ľ	Vame		
	AGbackendpool		
(E	Add backend pool without targets Yes No Backend targets		
	Target type	Target	
	IP address or FQDN	192.168.1.13	<u>î</u>
	IP address or FQDN	192.168.1.18	â ···
	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

	Microsoft Azure	$\mathcal P$ Search resources, services, and docs (G+/)		🖂 🕼 🖉 🛞 ? 😳 Yuchun Jiang@	citrix.com CITRIX
*=	SRAppGV1 SRAppGV1 HTTP s Application gateway	ettings		Add HTTP setting	;
,⊳ s	earch (Ctrl+/) «	+ Add		HTTP settings name SRHttpSetting80 Backend protocol	
🔷 Ti	-	Name	Port		
PD	iagnose and solve problems	SRHttpSetting80	80	Backend port *	
Settin	gs	SRHttpSetting443	443	80	
💼 c	onfiguration	SRHttpSetting22334	22334		
🖲 V	eb application firewall			Additional settings Cookie-based affinity ()	
🧐 B	ackend pools			Cookerbased annual () Enable Disable	
8⊟ н	TTP settings			Connection draining ()	
🖬 F	ontend IP configurations			C Enable Disable	
Ξυ	steners			Request time-out (seconds) * ()	
📥 R	ules			20	
👎 н	ealth probes			Override backend path ①	
P	roperties				
βu	ocks			Host name	
Moni	oring			By default, Application Gateway does not change the incoming HTTP host header from the client and sends the header unaltered to the backend. Multi-tenant services like App service or API management rely on a specific host header or SNI	
💵 A	lerts			unaltered to the backend. Multi-tenant services like App service or API management rely on a specific host header or SNI extension to resolve to the correct endpoint. Change these settings to overwrite the incoming HTTP host header.	
nii N	letrics			Save	
a D	iaqnostic settings				

• 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 docs	(G+/)	E E E 2 8 7 C
Home > SRAppGV1 SRAppGV1 HTTP s	settings …		Add HTTP setting
Approcision guteway	+ Add Search HTTP settings Name SRHttpSetting80 SRHttpSetting22334	Port 80 443 22334	HTTP settings name SRHUpSetting443 Backend protocol
Listeners Listeners Listeners Listeners Listeners Listeners Monitoring Listens Monitoring Listens Mi Metrics Diagnostic settings			Certificate srb Add certificate Additional settings Cookle-based affinity Trable Disable Cookle-based affinity Cookle-based affinit

	Search resources, services, and docs	(G+/)	
Microsoft Azure Home > SRAppGV1 ¥= SRAppGV1 HTTP S Application gateway P Search (Crl+/) × Acclass control (wm) * Tags Diagnose and solve problems Settings © Configuration © Web application firewall © Backend pools E HTTP settings E Listenes Luis Web apple and solve problems		Port 80 443 22334	Image: Section of the section of t
Monitoring Alerts Mi Metrics Diagnostic settings			Ves No

• 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.

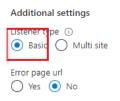
Home > SRAppGV1					
SRAppGV1 Fronte	end IP config	gurations			
		end IP configurations			
	* Туре	Status	Name	IP address	Associated listeners
Tags	Public	Not configured			
Diagnose and solve problems	Private	Configured	appGwPrivateFrontendIp	10.7.0.6	SRListener80, 2 more
ettings					
Configuration					
Web application firewall					
Backend pools					
∃ HTTP settings					
Frontend IP configurations					
E Listeners					
Rules					
Health probes					
Properties					
Locks					
Ionitoring					
Alerts					
Metrics					

5. Add listeners.

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

Automation Automation							
		, P Search resources, services, and do	cs (G+/)			📭 🗳 🎯 ? 😳 📕	
	Home > SRAppGV1						
		ners					×
• Pari Application observations application of the parity back and the parity b		🛛 🕂 Add listener 💍 Refresh					
Without Book Dot Book Dot Book Proceed Interme Image: Image	Tags	Application Gateway, it is automatic	ally directed to the WebSocket er	Il gateway sizes. There is no ac abled backend server using th	ditional configuration required to enable or d e appropriate backend pool as specified in ap	isable WebSocket support. If a WebSocket 1 splication gateway rules.	traffic is received on the
Configuration Wite weed to If TTP B0 Stemptidue to If TTP Bit backword point Bit backword point Bit backword point If TTP 44.3 Stemptidue to: If TTP Bit backword point Bit backword point Bit backword point Bit backword point If TTP 44.3 Stemptidue to: If TTP If TTP 44.3 Stemptidue to: If TTP	Diagnose and solve problems						
We spikulation from an analysis of the section of the section of the section security policy to match your operational security registered. We spikulation from an analysis of the section of the section of the section security policy to match your operational security registered. We spikulation from an analysis of the section of the section of the section security policy to match your operational security registered. We spikulation from an analysis of the section of the section of the section security policy to match your operational security registered. We spikulation from an analysis of the section of the section of the section security policy to match your operational security registered. We spikulation from an analysis of the section of the section of the section security policy to match your operational security registered. We spikulation from an analysis of the section of the section of the section security policy to match your operational security registered. We spikulation from an analysis of the section of the section of the section security policy to match your operational security registered. We spikulation from an analysis of the section of the section of the section of the section of the section security policy to match your operational security registered. We spikulation from an analysis of the section of the section of the section security policy to match your operational security registered. We spikulation from an analysis of the section of the section of the section of the section of the section of the section of the section of the section of the section of the section of the section of the section of the section of the section of	Settings	Name	Protocol	Port	Associated rule	Host name	
Witcheld (Markan) Imma Witcheld (Markan) Imma Imma<	Configuration	SRListener80	HTTP	80	SRHttpRule80		
With With With With With With With With	Web application firewall	SRListener443	HTTPS	443	SRHttpRule443		
Tertered II only and IIII only and III on	Backend pools	SRListener22334	HTTPS	22334	SRHttpRule22334	-	•••
Extension Extension International State St	8 HTTP settings	SSL Policy					
I there is a factor of the state is a fact	Frontend IP configurations	The SSL policy defines the SSL proto	col version and available ciphers.	Choose from one of the pred	efined policies or create a custom security poli	icy to match your organizational security re	auirements.
■ Reis	🔁 Listeners	Learn more about SSL policy. 🕫					
Il hopentie C tasks Menting Liscoler, RAX, WITH, 4AS, 2KB, GOM, SHAASH TIS, COLE, RAX, WITH, 4AS, 2KB, GOM, SHAASH TIS, COLE, RAX, WITH, 4AS, 2KB, GOM, SHAASH TIS, COLE, RAX, WITH, 4AS, 2KB, GOM, SHAASH TIS, COLE, RAX, WITH, 4AS, 2KB, COC, SHAASH TIS, COLE, RAX, WITH, 4AS, 2KB, COC, SHAASH TIS, COLE, RAX, WITH, 4AS, 2KB, COC, SHAA LIS, COLE, RAX, WITH, SHAA, COC, SHAA LIS, COLE, RAX, WITH, SHAA, COC, SHAA, SHAA, COC, SHAA, SHAA, SHAA, COC,	📥 Rules						
i projekti Circle Star Star Star Star Star Star Star Star	Health probes	Min protocol version					
A tods Ciperative Microsoft Azure	Properties	TLSv1_0					
Meetering Its.Cold:Raw,WithABS.JBS.COLS:MARKA Its.Cold:Raw,WithABS.JBS.COLS:MARKA Its.Cold:Raw,WithABS.JBS.COLS:MARKA Its.Cold:Raw,WithABS.JBS.COLS:MARKA Its.Cold:Raw,WithABS.JBS.COLS:MARKA Its.Cold:Raw,WithABS.JBS.COLS:MARKA Its.Cold:Raw,WithABS.JBS.COLS:MARKA Its.Cold:Raw,WithABS.JBS.COLS:MARKA Its.Cold:Raw,WithABS.JBS.COLS:MARKA Its.Cold:Raw,WithABS.JBS.COLS:MARKA Its.Cold:Raw,WithABS.JBS.COLS:MARKA Its.Cold:Raw,WithABS.JBS.COLS:MARKA Its.Cold:Raw,WithABS.JBS.COLS:MARKA Its.Cold:Raw,WithABS.JBS.COLS:MARKA Its.Cold:Raw,WithABS.JBS.COLS:MARKA Its.Cold:Raw,WithABS.JBS.COLS:MARKA Its.Cold:Raw,WithABS.JBS.COLS:MARKA Its.Cold:Raw,WithABS.JBS.COLS:MARKA Its.Cold:Raw,WithABS.JBS.COLS:MARKA Its.Cold:Raw,WithABS.JBS.ColS:MARKA Its.Cold:Raw,WithABS.JBS.ColS:MARKA Its.Cold:Raw,WithABS.JBS.ColS:MARKA Its.Cold:Raw,WithABS.JBS.ColS:MARKA Its.Cold:Raw,WithABS.JBS.ColS:MARKA Its.Cold:Raw,WithABS.JBS.ColS:MARKA SRAppGV1 SRListener80 Frontend IP * ① Private Its.Cold:Raw,WithABS.JBS.ColS:MARKA Bold:Raw,WithABS.JBS.ColS:MARKA Bold:Raw,WithABS.JBS.ColS:MARKA Bold:Raw,WithABS.JBS.ColS:MARKA Bold:Raw,WithABS.JBS.ColS:MARKA Bold:Raw,WithABS.JBS.ColS:MARKA Bold:Raw,WithABS.JBS.ColS:MARKA Bold:Raw,WithABS.JBS.ColS:MARKA Bold:Raw,WithABS.JBS.ColS:MARKA Bold:Ra		Cipher suites					
Alerst 11,5COHE,RSA,WITH,AES,28C,GSA4384 13,5COHE,RSA,WITH,AES,28C,GSA4384 13,5COHE,RSA,WITH,AES,28C,GSA4384 15,5COHE,RSA,WITH,AES,28C,GSA4384 5,5COHE,RSA,WITH,AES,28C,GSA444 15,5COHE,RSA,WITH,AES,28C,GSA444 15,5COHE,RSA,WITH,AES,28C,GSA444 15,5COHE,RSA,WITH,AES,28C,GSA444 15,5COHE,RSA,WITH,AES,28C,GSA444 15,5COHE,RSA,WITH,AES,28C,GSA444 15,5COHE,RSA,WITH,AES,28C,GSA444 15,5COHE,RSA,WITH,AES,28C,GSA444 15,5COHE,RSA,WITH,AES,28C,GSA444 15,5COHE,RSA,WITH,AES,28C,GSA444 15,5COHE,RSA,WITH,AES,28C,GSA444 15,5COHE,RSA,WITH,AES,28C,GSA444 16,5COHE,RSA,WITH,AES,28C,GSA444 16,5COHE,RSA,WITH,AES,28C,GSA444 16,5COHE,RSA,WITH,AES,28C,GSA444 16,5COHE,RSA,WITH,AES,28C,GSA444 17,5COHE,RSA,WITH,AES,28C,GSA444 17,5COHE,RSA,WITH,AES,28C,GSA444 17,5COHE,RSA,WITH,AES,28C,GSA444 17,5COHE,RSA,WITH,AES,28C,GSA444 17,5COHE,RSA,WITH,AES,28C,GSA444 17,5COHE,RSA,WITH,AES,28C,GSA444 17,5COHE,RSA,WITH,AES,28C,GSA4444 17,5COHE,RSA,WITH,AES,28C,GSA4444 17,5COHE,RSA,WITH,AES,28C,GSA4444 17,5COHE,RSA,WITH,AES,28C,GSA4444 17,5COHE,RSA,WITH,AES,28C,GSA44444 17,5COHE,RSA444444 17,5COHE,RSA444444444444444444444444444444444444							
In Score, Sax, With, ABS, 138, CGC, SHA256 Tis, Score, Sax, With, ABS, 138, CGC, SHA256 Tis, Score, Sax, With, ABS, 138, CGC, SHA256 Tis, Score, Sax, With, ABS, 138, CGC, SHA256 Tis, Score, Sax, With, ABS, 138, CGC, SHA256 Tis, Score, Sax, With, ABS, 138, CGC, SHA256 Tis, Score, Sax, With, ABS, 138, CGC, SHA256 Tis, Score, Sax, With, ABS, 138, CGC, SHA256 Tis, Score, Sax, With, ABS, 138, CGC, SHA256 Tis, Score, Sax, With, ABS, 138, CGC, SHA256 Tis, Score, Sax, With, ABS, 138, CGC, SHA256 Tis, Score, Sax, With, ABS, 138, CGC, SHA256 Tis, Score, Sax, With, ABS, 138, CGC, SHA256 Tis, Score, Sax, With, ABS, 138, CGC, SHA256 Tis, Score, Sax, With, ABS, 138, CGC, SHA256 Tis, Score, Sax, With, ABS, 138, CGC, SHA256 Tis, Score, Sax, With, ABS, 138, CGC, SHA256 Tis, Score, Sax, With, ABS, 138, CGC, SHA256 Tis, Score, Sax, With, ABS, 138, CGC, SHA256 Tis, Score, Sax, With, ABS, 138, CGC, SHA256 Sax, Spore, Sax, With, ABS, 138, CGC, SHA25 Sax, Spore, Sax, With, ABS, 138, CGC, Sha4 Sax, Spore, Sax, Spore, Sax, Spore, Sax, Spore, Sax, Spore, Sax, Spore, Sax, Spore, Sax, Spore, Sax, Spore, Sax, Spore, Sax, Spore, Sax, Spore, Sax, Spor							
Method TIS ECOME REAL WITH ARS 255.08C.93A Diagnomic settings Its ECOME REAL WITH ARS 255.08C.93A </td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td>							
• Listener on port 80 Microsoft Azure Microsoft Azure Home > SRAppGV1 > SRListener80 SRListener80 Frontend IP * ① Private Protocol ②							
Microsoft Azure Microsoft Azure Search resources, services, and docs (G+/) Home > SRAppGV1 > SRListener80 Frontend IP * () Private Private Protocol ()	Diagnostic settings	 TLS ECDHE RSA WITH AES 128 CB 	C SHA				
SRListener80 SRAppGV1 Listener name ① SRListener80 Frontend IP * ① Private \checkmark Port * ① 80 \checkmark		•			₽ Search re	sources, services, and do	ocs (G+/)
SRAppGV1 Listener name ① SRListener80 Frontend IP * ① Private ✓ Port * ① 80 ✓	Home > SRAppGV1	>					
SRListener80 Frontend IP * ① Private V Protecol ①	SRListener80)					
Frontend IP * ① Private Port * ① 80 Protocol ①	Listener name 🛈						
Private V Port * (i) 80 V Protocol ①	SRListener80						
Port * (i) 80 V Protocol ①	Frontend IP * 🕠						
80 V	Private				\sim		
Protocol ①	Port * (i)						
Protocol ①	80				×		
					×		
	Protocol (i)						
	-						
	HTTP O HTTPS						

Associated rule SRHttpRule80



• 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 >	
SRListener443 SRAppGV1	
Listener name () SRListener443	
Frontend IP * 🕠	
Private	~
Port* ()	•
443	\checkmark
Protocol () HTTP HTTPS	
Choose a certificate Create new Select existing	
Certificate *	
Ibdc	\sim
Renew or edit selected certificate	
Associated rule	
SRHttpRule443	
Additional settings	
Basic Multi site	
Error page url Ves No	

• 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 Searc	ch resource
Home > SRAppGV1 >		
SRListener22334 SRAppGV1		
Listener name 🕕		
SRListener22334		
Frontend IP * ()		-
Private	\sim]
Port * (i)		1
22334	~]
Protocol ① O HTTP		
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 Yes No		

6. Create request routing rules.

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

Session Recording 2204

Microsoft Azure	, ○ Search resources, services, and docs (G+/)		🗖 🖬 🖓 🕼 ? 😳	
ome > <u>SRAppGV1</u>				
SRAppGV1 Rule	2S ···			
Search (Ctrl+/) Access control (IAM)	« + Request routing rule			
Tags				
Diagnose and solve problems	Name	Туре	Listener	
ttings	SRHttpRule80	Basic	SRListener80	
Configuration	SRHttpRule443	Basic	SRListener443	
	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 a the application gateway will apply this r	nd IP address for traffic that uses a specified protocol. If the listener criteria are met, outing 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 r 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 * 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 SRHttpRule443 * 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 * (i)	AGbackendpool
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 least one backend target.
Rule name	SRHttpRule22334
	arote
* Listener * Backend t	argeo
A listener "listens" on a	specified port and IP address for traffic that uses a specified protocol. If the listener criteria are met, y will apply this routing rule.

SRHttpRule22334 SRAppGV1		
Configure a routing rule to send traffic f contain a listener and at least one backe	rom a given frontend IP address to one or more backend targets. A routing rule must end target.	
Rule name	SRHttpRule22334	
define the behavior of the routing rule		
Target type	Backend pool Redirection	
Backend target * 🕡	AGbackendpool ~	/
HTTP settings * 🛈	SRHttpSetting22334	/
-		

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

Troubleshoot

June 22, 2022

The troubleshooting information contains solutions to some issues you might encounter during or after installing the Session Recording components.

Warning:

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

Installation of server components fails

June 22, 2022

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 22, 2022

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 22, 2022

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**.

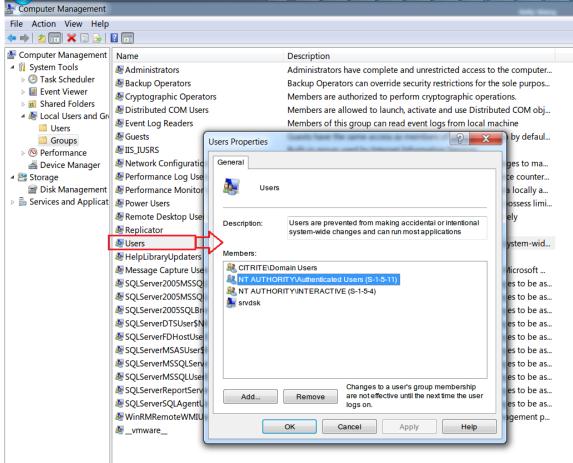
• The Session Recording Broker returned an unknown error while evaluating a record policy query. Error code 5 (Access Denied). For more information, see the Event log on the Session Recording server. This error occurs when sessions are started and a request for a record policy evaluation is made. The 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 22, 2022

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.

Sessions are not recording

January 10, 2024

If sessions are not recording successfully, check the application event log in the Event Viewer on the Session Recording agent and Session Recording server. Doing so can provide valuable diagnostic information.

If sessions are not recording, the possible cause might be:

- Component connectivity and certificates. If the Session Recording components cannot communicate with each other, session recording can fail. To troubleshoot recording issues, verify that all components are configured correctly to point to the correct machines and that all certificates are valid and correctly installed.
- Non-Active Directory domain environments. Session Recording is designed to run in a Microsoft Active Directory domain environment. If you are not running in an Active Directory environment, you might experience recording issues. Ensure that all Session Recording components are running on machines that are members of an Active Directory domain.
- Session sharing conflicts with the active policy. Session Recording matches the active policy with the first published application that a user opens. Subsequent applications opened during the same session continue to follow the policy that is in force for the first application. To prevent session sharing from conflicting with the active policy, publish the conflicting applications on separate multi-session OS VDAs.
- **Recording is not enabled.** By default, installing the Session Recording Agent on a multi-session OS VDA enables recording for the VDA. Recording does not occur until an active recording policy is configured to allow it.
- **The active recording policy does not permit recording.** A session can be recorded only when the session meets the rules of the active recording policy.
- Session Recording services are not running. For sessions to be recorded, the Session Recording Agent service must be running on a multi-session OS VDA and the Session Recording Storage Manager service must be running on the machine hosting the Session Recording Server.
- **MSMQ is not configured.** If MSMQ is not correctly configured on the server running the Session Recording Agent and the machine hosting the Session Recording Server, recording problems might occur.
- Windows performance counters are missing, disabled, or corrupted for the Session **Recording agent.** You might see the following errors in the application log on the Session Recording agent:

Event Viewer (Local)	Application Number of	events: 140.773				
Custom Views	Level	Date and Time	Source	Event ID	Task Category	
Application	Error	03/11/2023 10:45:44	Citrix Session Recording Agent	1006	None	
Security	Error	03/11/2023 10:45:44	Citrix Session Recording Agent	1007	None	
Setup	(i) Information	03/11/2023 10:45:43	Citrix Session Recording Agent	3001	None	
System	(i) Information	03/11/2023 10:45:43	Citrix Session Recording Agent	0	None	
Forwarded Events	(1) Information	03/11/2023 10:44:42	Citrix Profile Management	1002	None	
Applications and Services Lo	(i) Information	03/11/2023 10:44:41	Citrix Profile Management	1000	None	
C Subscriptions	(i) Information	03/11/2023 10:44:41	Citrix Profile Management	1001	None	
	(1) Information	03/11/2023 10:44:40	Citrix Profile Management	2001	None	
	(i) Information	03/11/2023 10:44:40	Citrix Profile Management	2000	None	
	(i) Information	03/11/2023 10:44:40	CitrixCseEngine	9	None	
	(i) Information	03/11/2023 10:44:39	CitrixCseEngine	8	None	
	(i) Information	03/11/2023 10:44:17	CitrixCseEngine	9	None	
	General Details					
	Exception Caught while starting service. Exception Details Type: System.InvalidOperationException Mpssage Category does not exist. Stack trace at System.Diagnostics.PerformanceCounter.Initializemp[I] at System.Diagnostics.PerformanceCounter.com(String categoryName, String counterName, String instanceName, Boolean readOnly) at System.Diagnostics.PerformanceCounter.com(String categoryName, String counterName) at System.Diagnostics.PerformanceCounter.com(String categoryName, String counterName) at System.Diagnostics.PerformanceCounter.com(String categoryName, String counterName) at SmAudAgent.PerformanceDataCollector.com() at SmAudAgent.LogQueue9roducer.ctm() at SmAudAgent.ThrStrinceLicenseTimerCallback(Object state)					

To resolve the issue, rebuild all performance counters by completing the following steps:

- 1. Open the Command Prompt (CMD) as an administrator.
- 2. Navigate to windows\system32 by typing cd c:\windows\system32\.
- 3. Type lodctr /R, and then press **Enter**. The lodctr /R command rebuilds performance counters.
- 4. After the lodctr /R command is executed, some rebuilt counters might be disabled. To check the counter status, run the lodctr /Q command. If you see that a counter is disabled, you can enable it by running the lodctr /E: [counter name] command.

Unable to view live session playback

June 22, 2022

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 22, 2022

• When you view corrupted or incomplete recordings in the player, you might also see warnings in the Event logs on the Session Recording agent.

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 22, 2022

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.

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.

Verify that the Session Recording database is connected

- 1. Using a SQL Management tool, open your SQL instance that contains the Session Recording database you installed.
- 2. Open the Security permissions of the Session Recording database.
- 3. Verify that the Session Recording Computer Account has access to the database. For example, if the machine hosting the Session Recording server is named **SsRecSrv** in the MIS domain, the computer account in your database must be configured as **MIS\SsRecSrv\$**. This value is configured during the Session Recording database installation.

Test IIS connectivity

You can test connections to the Session Recording server IIS site by using a Web browser to access the Session Recording Broker webpage. It can help you determine whether problems with communication between Session Recording components stem from misconfigured protocol configuration, certification issues, or problems starting Session Recording Broker. To verify IIS connectivity for the Session Recording agent:

- 1. Log on to the server where the Session Recording Agent is installed.
- 2. Open a Web browser and type the following address:
 - For HTTPS: https://servername/SessionRecordingBroker/RecordPolicy .rem?wsdl, where servername is the name of the machine hosting the Session Recording server.
 - For HTTP: http://servername/SessionRecordingBroker/RecordPolicy. rem?wsdl, where servername is the name of the machine hosting the Session Recording server.
- 3. If you are prompted for NT LAN Manager (NTLM) authentication, log on with a domain administrator account.

To verify IIS connectivity for the Session Recording player:

- 1. Log on to the workstation where the Session Recording player is installed.
- 2. Open a Web browser and type the following address:
 - For HTTPS: https://servername/SessionRecordingBroker/Player.rem? wsdl, where servername is the name of the machine hosting the Session Recording server.
 - For HTTP: http://servername/SessionRecordingBroker/Player.rem? wsdl, where servername is the name of the machine hosting the Session Recording server.
- 3. If you are prompted for NT LAN Manager (NTLM) authentication, log on with a domain administrator account.

To verify IIS connectivity for the Session Recording policy console:

- 1. Log on to the server where the Session Recording policy console is installed.
- 2. Open a Web browser and type the following address:
 - For HTTPS: https://servername/SessionRecordingBroker/PolicyAdministration .rem?wsdl, where servername is the name of the machine hosting the Session Recording server.
 - For HTTP: http://servername/SessionRecordingBroker/PolicyAdministration .rem?wsdl, where servername is the name of the machine hosting the Session Recording server.
- 3. If you are prompted for NT LAN Manager (NTLM) authentication, log on with a domain administrator account.

If you see an XML document within your browser, it verifies that the Session Recording policy console is connected to the Session Recording server using the configured protocol.

Troubleshoot certificate issues

If you are using HTTPS as your communication protocol, the machine hosting the Session Recording server must be configured with a server certificate. All component connections to the Session Recording server must have root certificate authority (CA). Otherwise, attempted connections between the components fail.

You can test your certificates by accessing the Session Recording Broker webpage as you would when testing IIS connectivity. If you are able to access the XML page for each component, the certificates are configured correctly.

Here are some common ways certificate issues cause connections to fail:

- **Invalid or missing certificates.** If the server running the Session Recording agent does not have a root certificate to trust the server certificate and cannot trust and connect to the Session Recording server over HTTPS, causing connectivity to fail, verify that all components trust the server certificate on the Session Recording server.
- **Inconsistent naming.** If the server certificate assigned to the machine hosting the Session Recording server is created using an FQDN, all connecting components must use the FQDN when connecting to the Session Recording server. If a NetBIOS name is used, configure the components with a NetBIOS name for the Session Recording server.
- **Expired certificates.** If a server certificate expired, connectivity to the Session Recording server through HTTPS fails. Verify the server certificate assigned to the machine hosting the Session Recording server is valid and has not expired. If the same certificate is used for the digital signing of session recordings, the event log of the Session Recording server provides error messages that the certificate expired or warning messages when it is about to expire.

Search for recordings using the player fails

June 22, 2022

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 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.



© 2024 Cloud Software Group, Inc. All rights reserved. Cloud Software Group, the Cloud Software Group logo, and other marks appearing herein are property of Cloud Software Group, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).

© 1999–2024 Cloud Software Group, Inc. All rights reserved.