Session Recording allows you to record the on-screen activity of any user session hosted from a VDA for Server OS or Desktop OS, over any type of connection, subject to corporate policy and regulatory compliance. Session Recording records, catalogs, and archives sessions for retrieval and playback.

Session Recording uses flexible policies to trigger recordings of application sessions automatically. This enables IT to monitor and examine user activity of applications - such as financial operations and healthcare patient information systems - supporting internal controls for regulatory compliance and security monitoring. Similarly, Session Recording also aids in technical support by speeding problem identification and time-to-resolution.

**Enhanced security through logging and monitoring.** Session Recording allows organizations to record on-screen user activity for applications that deal with sensitive information. This is especially critical in regulated industries such as healthcare and finance. Where personal information that must not be recorded is involved, policy controls allow selective recording.

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

Session Recording is not designed or intended to contribute to the collection of evidence for legal proceedings. Citrix recommends that organizations using Session Recording use 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. When 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

Feb 26, 2018

The insertion of USB mass storage devices can be logged. As of the 7.17 release, Session Recording can log the insertion of a Client Drive Mapping (CDM) mapped or generic redirected USB mass storage device in a client device where Citrix Receiver for Windows or for Mac is installed, and can tag the event in the recording. For more information, see Log insertion of USB mass storage devices.
Fixed issues

Feb 26, 2018
This release does not address any customer-reported issues.
Known issues

Feb 26, 2018
When Machine Creation Services (MCS) or Provisioning Services (PVS) creates multiple VDAs with the configured master image and 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 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

Feb 26, 2018  Session Recording Version 7.17
This release of Session Recording can include third party software licensed under the terms defined in this document.
System requirements

Feb 26, 2018

Session Recording Administration components

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.

Supported operating systems:
- Windows Server 2016
- Windows Server 2012 R2

Supported Microsoft SQL Server versions:
- Microsoft SQL Server 2017 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

Requirement: .NET Framework 4.7.1, 4.6.2

Supported operating systems:
- Windows Server 2016
- Windows Server 2012 R2

Other requirements:
- Internet Information Services (IIS) 10, 8.5, 8.0, or 7.5
- .NET Framework Version 4.7.1, 4.6.2
- 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

Supported operating systems:
- Windows Server 2016
- Windows Server 2012 R2

Requirement: .NET Framework 4.7.1, 4.6.2
Session Recording Agent

Install the Session Recording Agent on every XenApp and XenDesktop server on which you want to record sessions.

Supported operating systems:

- Windows Server 2016
- Windows Server 2012 R2
- Windows 10 Version 1803, 1709, 1703, 1607

Requirements:

- XenApp and XenDesktop 7.17 with Platinum license
- XenApp and XenDesktop 7.15 LTSR CU1 with Platinum license
- XenApp and XenDesktop 7.6 LTSR CU5 with Platinum license (VDA for Windows Server OS only, VDA for Windows Desktop OS not supported)
- .NET Framework 4.7.1, 4.6.2
- Microsoft Message Queuing (MSMQ), with Active Directory integration disabled and MSMQ HTTP support enabled

Session Recording Player

Supported operating systems:

- Windows 10 Version 1803, 1709, 1703, 1607

Requirement: .NET Framework 4.7.1, 4.6.2

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

Feb 26, 2018

Session Recording consists of five components:

- **Session Recording Agent.** A component installed on each VDA for Server OS or Desktop 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 handles the search queries and file download requests from the Session Recording Player, handles policy administration requests from the Session Recording Policy Console, and evaluates recording policies for each XenApp and XenDesktop session.
  - The Storage Manager. A Windows service that manages the recorded session files received from each Session Recording-enabled computer running XenApp and XenDesktop.
  - 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 XenApp and XenDesktop 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.

This illustration shows the Session Recording components and their relationship with each other:

In the deployment example illustrated here, the Session Recording Agent, Session Recording Server, Session Recording Database, Session Recording Policy Console, and Session Recording Player all reside behind a security firewall. The Session Recording Agent is installed on a VDA for Server OS or Desktop 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 for Server OS on which the Session Recording Agent is installed. Inside the firewall, the Session Recording Agent, Session Recording Policy Console, Session Recording Player, and Session Recording Database all communicate with the Session Recording Server.
Plan your deployment

Feb 26, 2018

Session Recording does not support Desktop Composition Redirection (DCR) display mode. By default, Session Recording disables DCR in a session if the session is to be recorded by recording policy. You can configure this behavior in Session Recording Agent properties.

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.

Alternatively, if you have a large site with many agents and plan to record many graphically intense applications (for example, AutoCAD applications), or you have many sessions to record, a Session Recording Server can experience a high performance demand. To alleviate performance issues, you can install multiple Session Recording Servers and enable the load balancing feature to make the Session Recording Servers work as a load balancing pool and to share the work load from different VDAs.

Use this type of deployment for recording sessions for one or more sites. The Session Recording Agent is installed on each VDA for Server OS in a site. The site resides in a data center behind a security firewall. The Session Recording Administration components (Session Recording Database, Session Recording Server, and Session Recording Policy Console) are installed on other servers and the Session Recording Player is installed on a workstation, all behind the firewall but not in the data center. Outside the firewall, in an unsecured network environment, are XenApp clients, such as a workstation, mobile devices, and a laptop computer.
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, Citrix does not recommend installing the Session Recording Player as a published application.

The Session Recording installation is configured for TLS/HTTPS communication. Ensure that you install a certificate on the Session Recording Server and that the root certificate authority (CA) is trusted on the Session Recording components.

If you install the Session Recording Database on a standalone server running SQL Server 2017 Express Edition, SQL Server 2016 Express Edition, SQL Server 2014 Express Edition, SQL Server 2012 Express Edition, or SQL Server 2008 R2 Express Edition, the server must have TCP/IP protocol enabled and SQL Server Browser service running. These settings are disabled by default, but they must be enabled for the Session Recording Server to communicate with the database. For information about enabling these settings, 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 that only Microsoft Outlook should be recorded, the recording commences when the user opens Outlook. However, if the user opens a published Microsoft Word second (while Outlook is running), Word also is recorded. Conversely, if the active policy does not specify that Word should be recorded, and the user launches Word before Outlook (which should be recorded, according to the policy), Outlook is not recorded.

Though you can install the Session Recording Server on a Delivery Controller, Citrix does not recommend that you do so 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 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.
Security recommendations

Feb 26, 2018

Session Recording is designed to be deployed within a secure network and accessed by administrators, and as such, is secure. Out-of-the-box deployment is designed to be 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 for sending 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:

- 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. Citrix recommends 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.
- XenApp and XenDesktop administrators 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.
- Citrix recommends that you 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 as the Player role, do not grant that user local administrator role for any player machine. Disable anonymous access.
- Citrix recommends 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 click Properties.
  2. Click the Advanced tab, and then under Startup and Recovery, click Settings.
  3. 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
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.
- Citrix recommends 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.
- Citrix recommends using a third-party security solution or Windows mechanism to protect Session Recording components. Session Recording components include:
  - On Session Recording Server
    - Processes: SsRecStoragemanager.exe and SsRecAnalyticsService.exe
    - Services: CitrixSsRecStorageManager and CitrixSsRecAnalyticsService
    - All files in Session Recording Server installation folder
    - Registry keys at HOTKEY_LOCAL_MACHINE\Software\Citrix\SmartAuditor\Server
  - On Session Recording Agent
    - Process: SsRecAgent.exe
    - Service: CitrixSmAudAgent
    - All files in Session Recording Agent installation folder
    - Registry keys at HOTKEY_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.
2. From the Windows Start menu on each Session Recording Server, open Administrative Tools > Computer Management.
4. Click the private queue citrixsmauddata to open the Properties page and select the Security tab.
5. Add the computers or security groups of the VDAs that send MSMQ data to this server and grant them the **Send Message** permission.
- Properly protect the event log for the Session Record Server and Session Recording Agents. We recommend using a Windows or third-party remote logging solution to protect the event log or redirect the event log to the remote server.
- Ensure that servers running the Session Recording components are physically secure. If possible, lock these computers in a secure room to which only authorized personnel can gain direct access.
- Isolate servers running the Session Recording components on a separate subnet or domain.
- Protect the recorded session data from users accessing other servers by installing a firewall between the Session Recording Server and other servers.
- Keep the Session Recording Administration Server and SQL database up-to-date with the latest security updates from Microsoft.
- Restrict non-administrators from logging on to the administration machine.
- Strictly limit who is authorized to make recording policy changes and view recorded sessions.
- Install digital certificates, use the Session Recording file signing feature, and set up TLS communications in IIS.
- Set up MSMQ to use HTTPS as its transport. The way is to set the MSMQ protocol listed in Session Recording Agent Properties to HTTPS. For more information, see Troubleshoot MSMQ.
- Use TLS 1.1 or TLS 1.2 (recommended) and disable SSLv2, SSLv3, TLS 1.0 on the Session Recording Server and Session Recording Database. For more information, see the Microsoft article at http://support.microsoft.com/default.aspx?scid=kb/en-us:187498.

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 > Administrative 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.
  - Citrix recommends 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:**

  1. Log on to the computer 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](https://support.microsoft.com/en-us/kb/3135244).
     d. Add a DWORD value SchUseStrongCrypto = 1 under `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NetFramework\v4.0.30319` and `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NetFramework\v4.0.30319`.
     e. Restart the computer.

  2. Log on to the computer 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 same as substeps 1-d and 1-e. 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](https://support.microsoft.com/en-us/kb/3135244). To use TLS 1.2, configure HTTPS as the communication protocol for the Session Recording components.

For information about configuring the Session Recording security features, see Knowledge Center article [CTX200868](https://docs.citrix.com).
Scalability considerations

Feb 26, 2018

Installing and running Session Recording requires few extra resources beyond what is necessary to run XenApp. However, if you plan to use Session Recording to record a large number of sessions or if the sessions you plan to record can result in large session files (for example, graphically intense applications), consider the performance of your system when planning your Session Recording deployment.

For more information about building a highly scalable Session Recording system, see Citrix article CTX200869.

Consider how much data you will be sending to each Session Recording Server and how quickly the servers can process and store this 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, multiply the number of sessions recorded by the average size of each recorded session and divide 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.)

You can improve performance by optimizing the performance of a single Session Recording Server or by installing multiple Session Recording Servers on different machines.

Disk and storage hardware are the most important factors to consider when planning a Session Recording deployment. The write performance of your storage solution is especially important. The faster data can be written to disk, the higher the performance of the system overall.

Storage solutions suitable for use with Session Recording include a set of local disks controlled as RAID arrays by a local disk controller or by an attached SAN.

**Note:** Do not use Session Recording with NAS. Performance and security problems can occur when recording data is written to a network drive.

For a local drive setup, a disk controller with built-in cache memory enhances performance. A caching disk controller must have a battery backup facility to ensure data integrity in a power failure.

A 100Mbps 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 100Mbps link.

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.

Consider the following specifications for the computer on which a Session Recording Server is installed:

- A dual CPU or dual-core CPU is recommended
- 4 GB of RAM is recommended
Exceeding these specifications does not significantly improve performance.

If a single Session Recording Server does not meet your performance needs, 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.

The Session Recording Database requires Microsoft SQL Server 2017, Microsoft SQL Server 2016, Microsoft SQL Server 2014, Microsoft SQL Server 2012, or Microsoft SQL Server 2008 R2. The volume of data sent to the database is very 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 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 four million 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 XenApp or XenDesktop 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

Feb 26, 2018
This chapter details how to install Session Recording by using the XenApp and XenDesktop installer and how to upgrade and uninstall Session Recording. It contains the following sections:

Installation checklist

Install Session Recording

Upgrade Session Recording

Uninstall Session Recording

Installation checklist

You can install the Session Recording components by using the XenApp and XenDesktop installer.

Before you start the installation, complete this list:

<table>
<thead>
<tr>
<th>✓</th>
<th>Step</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Select the machines on which you want to install each Session Recording component. Ensure that each computer meets the hardware and software requirements for the component or components to be installed on it.</td>
</tr>
<tr>
<td></td>
<td>Use your Citrix account credentials to access the XenApp and XenDesktop download page and download the product ISO file. Unzip the ISO file or burn a DVD of it.</td>
</tr>
<tr>
<td></td>
<td>To use the TLS protocol for communication between the Session Recording components, install the correct certificates in your environment.</td>
</tr>
<tr>
<td></td>
<td>Install any hotfixes required for the Session Recording components. The hotfixes are available from the Citrix Support.</td>
</tr>
<tr>
<td></td>
<td>Configure Director to create and activate the Session Recording policies. For more information, see Configure Director to use the Session Recording Server.</td>
</tr>
</tbody>
</table>

Note:

- Citrix recommends that you divide the published applications into separate Delivery Groups based on your recording policies. Session sharing for published applications can conflict with active policies if they are in the same Delivery Group. Session Recording matches the active policy with the first published application that a user opens.
- If you are planning to use Machine Creation Services (MCS) or Provisioning Services, prepare a unique QMId. Failure to comply can cause recording data losses.
- SQL Server requires that TCP/IP is enabled, the SQL Server Browser service is running, and Windows Authentication is used.
- To use HTTPS, configure server certificates for TLS/HTTPS.
- Ensure that users under Local Users and Groups > Groups > Users have write permission to the C:\windows\Temp folder.

Install Session Recording

Citrix recommends that you install the Session Recording Administration, Session Recording Agent, and Session Recording Player components on separate servers. The following procedures detail how to install these components:

Install the Session Recording Administration components
Install the Session Recording Agent
Install the Session Recording Player

The Session Recording Administration components include the Session Recording Database, Session Recording Server, and Session Recording Policy Console. You can choose the component to install on a server.

Step 1: Download the product software and launch the wizard

1. If you have not downloaded the XenApp and XenDesktop ISO yet, use your Citrix account credentials to access the XenApp and XenDesktop download page and download the product ISO file. Unzip the ISO file or burn a DVD of it.
2. Use a local administrator account to log on to the machine where you are installing the Session Recording Administration components. Insert the DVD in the drive or mount the ISO file. If the installer does not launch automatically, double-click the AutoSelect application or the mounted drive.
   The installation wizard launches.

Step 2: Choose which product to install
Deliver applications and desktops to any user, anywhere, on any device.

- Hybrid cloud, cloud and enterprise provisioning
- Centralized and flexible management

Manage your delivery according to your needs:

- **XenApp** Deliver applications: 
  - Start
- **XenDesktop** Deliver applications and desktops:
  - Start
  - Cancel

Click **Start** next to the product to install **XenApp** or **XenDesktop**.

**Step 3: Select Session Recording**
Select the **Session Recording** entry.

**Step 4: Read and accept the license agreement**
On the **Software License Agreement** page, read the license agreement, accept it, and then click **Next**.

**Step 5: Select the components to install and the installation location**
On the Core Components page:

- **Location**: By default, components are installed in C:\Program Files\Citrix. The default location works for most deployments. You can specify a custom installation location.
- **Component**: By default, all the check boxes next to the components that can be installed are selected. The installer knows whether it is running on a Desktop OS or a Server OS. It allows the Session Recording Administration components to be installed on a Server OS only. It does not allow the Session Recording Agent to be installed on a machine that has no VDA installed in advance. If you install the Session Recording Agent on a machine that has no VDA installed in advance, the **Session Recording Agent** option is unavailable.

Select **Session Recording Administration** and click **Next**.
Step 6: Select the features to install

Session Recording Administration
The Session Recording Administration components are the Session Recording Database, the Session Recording Server, and the Session Recording Policy Console. You can choose which of these components to install on a server.

Session Recording Agent
This component cannot be installed on this machine.

Session Recording Player
Install the Session Recording Player on the Session Recording Server or one or more workstations in the domain for users who view session recordings.
On the Features page:

- By default, all the check boxes next to the features that can be installed are selected. Installing all these features on a single server is fine for a proof of concept. However, for a large production environment, Citrix recommends 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. 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.

- To add another feature on the same server after you select and install a feature or features on it, you can only run the msi package but cannot run the installer again.

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

**Note:** The Session Recording Database is not an actual database. It is a component responsible for creating and configuring the required databases in the Microsoft SQL Server instance during installation. Session Recording supports three solutions for database high availability based on Microsoft SQL Server. For more information, see Database high availability.

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

- Deployment 1: Install the Session Recording Server and Session Recording Database on the same machine and the
Microsoft SQL Server on a remote machine. *(Recommended)*

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

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

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

- **Instance name**: If the database instance is not a named instance as you configured when you set up the instance, you can use only the computer name of the SQL Server. If you have named the instance, use `computer-name\instance-name` as the database instance name. To determine the server instance name you are using, run `select @@servername` on the SQL Server. The return value is the exact database instance name.

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

**Important**

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

- You must have the **securityadmin** and **dbcreator** server role permissions of the database. If you do not have the permissions, you can:
  - Ask the database administrator to assign the permissions for the installation. After the installation completes, the **securityadmin** and **dbcreator** server role permissions are no longer necessary and can be safely removed.
  - Or, use the SessionRecordingAdministrationx64.msi package (unzip the ISO file, and you can find this msi package under …\x64\Session Recording). 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 computer 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.

Click **Next**.

3. Review the prerequisites and confirm the installation.

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

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

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

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

- The Session Recording Administrator Logging is an optional subfeature of the Session Recording Server. Select the Session Recording Server before you can select the Session Recording Administrator Logging.
- Citrix recommends that you install the Session Recording Administrator Logging together with the Session Recording Server at the same time. If you don't want the Administrator Logging feature to be enabled, you can disable it on a later page. However, if you choose not to install this feature at the beginning but want to add it later, you can only manually add it by using the SessionRecordingAdministrationx64.msi package.

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

- **Instance name**: Type the name of your SQL Server in the **Instance name** text box. If you are using a named instance, type `computer-name\instance-name`; otherwise, type `computer-name` only.
- **Database name**: Type a custom database name in the **Database name** text box or use the default database name `CitrixSessionRecording` that is preset in the text box.
- You must have the **securityadmin** and **dbcreator** server role permissions of the database. If you do not have the permissions, you can:
  - Ask the database administrator to assign the permissions for the installation. After the installation completes, the **securityadmin** and **dbcreator** server role permissions are no longer necessary and can be safely removed.
  - Or, use the `SessionRecordingAdministrationx64.msi` package to install the Session Recording Server. During the msi installation, a dialog box prompts for the credentials of a database administrator with the **securityadmin** and **dbcreator** server role permissions. Type the correct credentials and then click **OK** to continue the installation.
  - After typing the correct instance name and database name, click **Test connection** to test the connectivity to the Session Recording Database.
  - Type the Session Recording Server computer account, and then click **Next**.

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

- **The Administration Logging database is installed on the SQL Server instance:** This text box is not editable. The SQL Server instance name of the Administration Logging database is automatically grabbed from the instance name that you typed on the Database and Server Configuration page.

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

  **Note:** The Administrator Logging database name must be different from the Session Recording Database name that is set in the Database name text box on the previous, Database and Server Configuration page.

- After typing the Administrator Logging database name, click **Test connection** to test the connectivity to the Administrator Logging database.

- **Enable Administration Logging:** By default, the Administration Logging feature is enabled. You can disable it by clearing the check box.

- **Enable mandatory blocking:** By default, mandatory blocking is enabled. The normal features might be blocked if logging fails. You can disable mandatory blocking by clearing the check box.

Click **Next** to continue the installation.

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

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

Click Finish to complete the installation of the Session Recording Server.

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

1. On the Features page, select Session Recording Policy Console and click Next.
2. Review the prerequisites and confirm the installation.
The **Summary** page shows your installation choices. You can click **Back** to return to the earlier wizard pages and make changes. Or, click **Install** to start the installation.

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

Click Finish to complete your installation of the Session Recording Policy Console.

Step 7: Install Broker_PowerShellSnapIn_x64.msi

Important: To use the Session Recording Policy Console, you must have the Broker PowerShell Snap-in (Broker_PowerShellSnapIn_x64.msi) installed. The snap-in cannot be automatically installed by the installer. Locate the snap-in on the XenApp and XenDesktop ISO (layout\image-full\x64\Citrix Desktop Delivery Controller) and follow the instructions for installing it manually. Failure to comply can cause an error.

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

Step 1: Download the product software and launch the wizard

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

The installation wizard launches.
Step 2: Choose which product to install

Deliver applications and desktops to any user, anywhere, on any device.

- Hybrid cloud, cloud and enterprise provisioning
- Centralized and flexible management

Manage your delivery according to your needs:

- **XenApp** Deliver applications
  - Start

- **XenDesktop** Deliver applications and desktops
  - Start

Click **Start** next to the product to install: **XenApp** or **XenDesktop**.

Step 3: Select Session Recording
Select the Session Recording entry.

Step 4: Read and accept the license agreement
On the **Software License Agreement** page, read the license agreement, accept it, and then click **Next**

**Step 5: Select the component to install and the installation location**
Select **Session Recording Agent** and click **Next**.

**Step 6: Specify the Agent configuration**
On the **Agent Configuration** page:

- If you have installed the Session Recording Server in advance, type the name of the computer where you installed the Session Recording Server and the protocol and port information for the connection to the Session Recording Server. If you have not installed Session Recording yet, you can change such information later in **Session Recording Agent Properties**.

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

**Step 7**: Review the prerequisites and confirm the installation
The Summary page shows your installation choices. You can click Back to return to the earlier wizard pages and make changes. Or, click Install to start the installation.

Step 8: Complete the installation
The **Finish Installation** page shows green check marks for all the prerequisites and components that have been installed and initialized successfully.

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

**Note:** When Machine Creation Services (MCS) or Provisioning Services (PVS) creates multiple VDAs with the configured master image and 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 be able to receive session logoff signals and therefore, sessions might always be in Live status.

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

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

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

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

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

   ```powershell
   Set-ExecutionPolicy RemoteSigned
   ```

2. Create a scheduled task, set the trigger as on system startup, and run with the SYSTEM account on the PVS or MCS master image machine.

3. Add the command as a startup task.

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

**Summary of the GenRandomQMID.ps1 script:**

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

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

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

# Get dependent services

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

# Restart MSMQ to get a new QMId

Restart-Service -force MSMQ

# Start dependent services

if ($depServices -ne $null) {
    foreach ($depService in $depServices) {
        $startMode = Get-WmiObject win32_service -filter "NAME = '$($depService.Name)''' | Select -Property StartMode

        if ($startMode.StartMode -eq "Auto") {
            Start-Service $depService.Name
        }
    }
}

Automate installations

To install the Session Recording Agent on multiple servers, write a script that uses silent installation.

The following command line installs the Session Recording Agent and creates a log file to capture the installation information.
For 64-bit systems:

msiexec /i SessionRecordingAgentx64.msi /q /l*v yourinstallationlog SESSIONRECORDINGSERVERNAME=yourservename SESSIONRECORDINGBROKERPROTOCOL=yourbrokerprotocol SESSIONRECORDINGBROKERPORT=yourbrokerport

Note: The SessionRecordingAgentx64.msi file in the XenApp and XenDesktop ISO is under \layout\image-full\x64\Session Recording.

For 32-bit systems:

msiexec /i SessionRecordingAgent.msi /q /l*v yourinstallationlog SESSIONRECORDINGSERVERNAME=yourservename SESSIONRECORDINGBROKERPROTOCOL=yourbrokerprotocol SESSIONRECORDINGBROKERPORT=yourbrokerport

Note: The SessionRecordingAgent.msi file in the XenApp and XenDesktop ISO is under \layout\image-full\x86\Session Recording.

Where:

yourservename is the NetBIOS name or FQDN of the computer hosting the Session Recording Server. If not specified, this value defaults to localhost.

yourbrokerprotocol is HTTP or HTTPS that Session Recording Agent uses to communicate with Session Recording Broker. If not specified, this value defaults to HTTPS.

yourbrokerport is the port number that Session Recording Agent uses to communicate with Session Recording Broker. If not specified, this value defaults to zero, which directs Session Recording Agent to use the default port number for your selected protocol: 80 for HTTP or 443 for HTTPS.

/l*v specifies verbose logging.

yourinstallationlog is the location of your installation log file.

/q specifies the quiet mode.

Install the Session Recording Player on the Session Recording Server or on workstations in the domain.

Step 1: Download the product software and launch the wizard

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

The installation wizard launches.

Step 2: Choose which product to install
Deliver applications and desktops to any user, anywhere, on any device.

- Hybrid cloud, cloud and enterprise provisioning
- Centralized and flexible management

Manage your delivery according to your needs:

- **XenApp** Deliver applications
  - Start
- **XenDesktop** Deliver applications and desktops
  - Start

Click **Start** next to the product to install **XenApp** or **XenDesktop**.

**Step 3: Select Session Recording**
Select the **Session Recording** entry.

**Step 4: Read and accept the license agreement**
On the **Software License Agreement** page, read the license agreement, accept it, and then click **Next**

**Step 5: Select the component to install and the installation location**
Select Session Recording Player and click Next.

Step 6: Review the prerequisites and confirm the installation
The Summary page shows your installation choices. You can click Back to return to the earlier wizard pages and make changes. Or, click Install to start the installation.

Step 7: Complete the installation
The Finish Installation page shows green check marks for all the prerequisites and components that have been installed and initialized successfully.

Click Finish to complete the installation of the Session Recording Player.

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 Session Recording 7.6 (or later) to the latest release of Session Recording.

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

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

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, ensure 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.

Uninstall Session Recording

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

For security reasons, the Administrator Logging Database is not removed after the components are uninstalled.
Yikes! 404 ... We feel your pain.
The page you are trying to view is not here. The link might be misspelled or outdated.

Some things to try:
- Go to Docs.citrix.com and search or navigate for the content
- Clear your browser cache and retry the link
- Report the problem and we’ll investigate
- Copy the address & use the Feedback link at the bottom of Docs.citrix.com to tell us about it
Configure

Feb 26, 2018

After installing the Session Recording components, you can perform the following steps to configure Session Recording to record XenApp or XenDesktop sessions and allow users to view them:

- Configure the connection to the Session Recording Server
- Authorize users
- Create and activate recording policies
- Specify where recordings are stored
- Specify file size for recordings
- Customize notification messages
- Enable or disable recording
- Log insertion of USB mass storage devices
- Enable or disable digital signing
- Administrator Logging
- Database high availability
- Load balancing
- Change your communication protocol
- Configure CEIP
Configure the connection to the Session Recording Server

Before a Session Recording Player can play sessions, you must configure it to connect to the Session Recording Server that stores the recorded sessions. Each Session Recording 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 the Player is configured with the ability to connect to multiple Session Recording Servers, users can change which Session Recording Server the Player connects to by selecting a check box on the Connections tab at Tools > Options.

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 computer 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 for the Session Recording Server you want to connect to.

The connection between the Session Recording Agent and the Session Recording Server 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 server name or its IP address.
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.
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.
Authorize users

Feb 26, 2018

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

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

- **PolicyAdministrator**: Grants the right to view, create, edit, delete, and enable recording policies. By default, administrators of the computer 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 XenApp and XenDesktop sessions. There is no default membership in this role.

When you install Session Recording, no user has the right to play recorded sessions. You must assign the right to each user, including the administrator. A user without the permission to play recorded sessions receives the following error message when trying to play a recorded session:

![Search Failed](https://docs.citrix.com)

To assign users to a role, do the following:

1. Log on as an administrator to the computer 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 Active Directory.

Any changes made to the console take effect during the update that occurs once every minute.
Create and activate recording policies

Feb 26, 2018

Use the Session Recording Policy Console to create and activate policies that determine which sessions are recorded.

**Important:** To use the Session Recording Policy Console, you must have the Broker PowerShell Snap-in (Broker_PowerShellSnapIn_x64.msi) installed. The snap-in cannot be automatically installed by the installer. Locate the snap-in on the XenApp and XenDesktop ISO (layout\image-full\x64\Citrix Desktop Delivery Controller) and follow the instructions for installing it manually. Failure to comply can cause an error.

You can activate system policies available when Session Recording is installed or create and activate your own custom policies. Session Recording system policies apply a single rule to all users, published applications, and servers. Custom policies specifying which users, published applications, and servers are recorded.

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

**System policies**

Session Recording provides the following system policies:

- **Do not record.** The default policy. If you do not specify another policy, no sessions are recorded.
- **Record everyone with notification.** If you choose this policy, all sessions are recorded. A pop-up window appears to notify recording occurrence.
- **Record everyone without notification.** If you choose this policy, all sessions are recorded. No pop-up window appears to notify recording occurrence.

System policies cannot be modified or deleted.

**Create a custom policy**

When you create your own policy, you make rules to specify which users and groups, published applications, and servers have their sessions recorded. A wizard within the Session Recording Policy Console helps you create rules. To obtain the list of published applications and servers, you must have the site administrator read permission. Configure that on this site's Delivery Controller.

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:

- **Do not record.** (Choose Disable session recording in the Rules wizard.) This recording action specifies that sessions meeting the rule criteria are not recorded.
- **Record with notification.** (Choose Enable session recording with notification in the Rules wizard.) This recording action specifies that sessions meeting the rule criteria are recorded. A pop-up window appears to notify recording occurrence.
- **Record without notification.** (Choose Enable session recording without notification in the Rules wizard.) This
recording action specifies that sessions meeting the rule criteria are recorded. Users are unaware that they are being recorded.

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

- **Users or Groups.** Creates a list of users or groups to which the recording action of the rule applies. Session Recording allows you to use Active Directory groups and white list users.
- **Published Resources.** Creates a list of published applications or desktops to which the recording action of the rule applies. In the Rules wizard, choose the XenApp and XenDesktop site or sites on which the applications or desktops are available.
- **Delivery Groups or Machines.** Creates a list of Delivery Groups or machines to which the recording 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 recording 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.

**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 next highest priority
- Rules with the **Record without notification** action have the lowest priority

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

To create a custom policy, do the following:

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 **Action > Add New Policy**.
3. Right-click the **New policy** and select **Add Rule**.
4. Select a recording option - In the Rules wizard, select **Disable session recording**, **Enable Session Recording with notification** (or **without notification**), and then click **Next**.
5. Select the rule criteria - You can choose one or any combination of the options:
   - Users or Groups
   - Published resources
   - Delivery Groups or Machines
   - IP Address or IP Range
6. Edit the rule criteria - To edit, click the underlined values. The values are underlined based on the criteria you chose in the previous step.
   **Note:** If you choose the **Published Resources** 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.

7. Follow the wizard to finish the configuration.

Note: Limitation regarding prelaunched application sessions:

- If the active policy tries to match an application name, the applications launched in the prelaunched session are not matched, which results in the session not being recorded.
- If the active policy records every application, when a user logs on to Citrix Receiver for Windows (at the same time that a prelaunched session is established), a recording notification appears and 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 ensures that prelaunched sessions can be recorded. However, notifications still appear.

Session Recording allows you to use Active Directory groups when creating policies. Using Active Directory groups instead of individual users simplifies 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 members of this group by selecting the Finance group in the Rules wizard when creating the rule.

You can create Session Recording policies ensuring that the sessions of some users in your organization are never recorded. This case is called white listing these users. White listing is useful for users who handle privacy-related information or when your organization does not want to record the sessions of a certain class of employees. For example, if all managers in your company are members of an Active Directory group named Executive, you can ensure that these users' sessions 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.

Activate a policy

1. Log on to the server where the Session Recording Policy Console is installed.
2. Start the Session Recording Policy Console.
3. If you are prompted by a Connect to Session Recording Server pop-up window, ensure that the name of the Session Recording Server, protocol, and port are correct. Click OK.
4. In the Session Recording Policy Console, expand Recording Policies.
5. Select the policy you want to make the active policy.
6. From the menu bar, choose Action > Activate Policy.

Modify a policy

1. Log on to the server where the Session Recording Policy Console is installed.
2. Start the Session Recording Policy Console.
3. If you are prompted by a Connect to Session Recording Server pop-up window, ensure that the name of the Session Recording Server, protocol, and port are correct. Click OK.
4. In the Session Recording Policy Console, expand Recording Policies.
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 Action > 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 policy or a policy that is active.
1. Log on to the server where the Session Recording Policy Console is installed.
2. Start the Session Recording Policy Console.
3. If you are prompted by a Connect to Session Recording Server pop-up window, ensure that the name of the Session Recording Server, protocol, and port are correct. Click OK.
4. In the Session Recording Policy Console, expand Recording Policies.
5. In the left pane, select the policy you want to delete. If the policy is active, you must activate another policy.
6. From the menu bar, choose Action > Delete Policy.
7. Select Yes to confirm the action.

Understand rollover behavior

When you activate a policy, the previously active policy remains in effect until the user's session ends. However, sometimes the new policy takes effect when the 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 policy while a session is being recorded and a rollover occurs:

<table>
<thead>
<tr>
<th>If the previous policy was:</th>
<th>And the new policy is:</th>
<th>After a rollover, the policy will be:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do not record</td>
<td>Any other policy</td>
<td>No change. The new policy takes effect only when the user logs on to a new session.</td>
</tr>
<tr>
<td>Record without notification</td>
<td>Do not record</td>
<td>Recording stops.</td>
</tr>
<tr>
<td>Record with notification</td>
<td>Record with notification</td>
<td>Recording continues and a notification message appears.</td>
</tr>
<tr>
<td>Record with notification</td>
<td>Do not record</td>
<td>Recording stops.</td>
</tr>
<tr>
<td>Record without notification</td>
<td>Record without notification</td>
<td>Recording continues. No message appears the next time a user logs on.</td>
</tr>
</tbody>
</table>
Configure Director to use the Session Recording Server

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

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

Feb 26, 2018

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

**Note:** To archive files or restore deleted files, use the ICLDB command. For more information, see [how to archive and restore recordings](https://docs.citrix.com). 

By default, recordings are stored in the drive:`SessionRecordings` directory of the computer hosting the Session Recording Server. You can change the directory where the recordings are stored, add extra directories to load-balance across multiple volumes, or make use of additional space. Multiple directories in the list indicate that recordings are load-balanced across the directories. You can add a directory multiple times. Load balancing cycles through the directories.

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 **Storage** tab.
4. Use the **File storage directories** list to manage the directories where recordings are stored.

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

You can create file storage directories on the local drive, the SAN volume, or a location specified by a UNC network path. Network mapped drive letters are not supported. Do not use Session Recording with NAS. Serious performance and security problems can occur when recording data is written to a network drive.

By default, archived recordings are restored in the drive:`SessionRecordingsRestore` directory of the computer hosting the Session Recording Server. You can change the directory.

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 **Storage** tab.
4. In the **Restore directory for archived files** field, type your directory for restoring archived recordings.
Specify file size for recordings

Feb 26, 2018

As recordings grow in size, the files can take longer to download and react 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 opens a new one to continue recording. This action is called a rollover.

You can specify two thresholds for a rollover:

- **File size.** When the file reaches the specified number of MB, Session Recording closes the file and opens a new one. By default, files roll over after reaching 50 MB. You can specify a limit from 10 MB to 1 GB.
- **Duration.** After the session records for the specified number of hours, the file is closed and a new file is opened. By default, files roll over after recording for 12 hours. You can specify a limit from one to 24 hours.

Session Recording checks both fields to determine which event occurs first to determine when to roll over. For example, if you specify 17MB for the file size and six hours for the duration and the recording reaches 17MB in three hours, Session Recording reacts to the 17MB file size to close the file and open a new one.

To prevent the creation of many small files, Session Recording does not roll over until at least one hour elapses (this is the minimum number that you can type) regardless of the value specified for the file size. The exception to this rule is if the file size surpasses 1 GB.

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 **Rollover** tab.
4. Type an integer between 10 and 1,024 to specify the maximum file size in MB.
5. Type an integer between 1 and 24 to specify the maximum recording duration in hours.
Customize notification messages

Feb 26, 2018

If the active recording policy specifies that users are notified when their sessions are recorded, a pop-up window appears displaying a notification message after the users type their credentials. The default notification message is “Your activity with one or more of the programs you recently started is being recorded. If you object to this condition, close the programs.” The users can click **OK** to dismiss the window and continue their sessions.

The default notification message appears in the language of the operating system of the computers hosting the Session Recording Server.

You can create custom notifications in 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.

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 **Notifications** tab.
4. Click **Add**.
5. Choose the language for the message and type the new message. You can create only one message for each language.

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

Feb 26, 2018

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

When you install the Session Recording Agent, recording is enabled. Citrix recommends that you disable Session Recording on servers that are not recorded because they experience a small impact on performance, even if no recording takes place.

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 Server OS VDA check box to specify whether or not sessions can be recorded for this server.
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.

Session Recording allows you to use third-party applications to insert custom data, known as events, to recorded sessions. These events appear when the session is viewed using the Session Recording Player. They are part of the recorded session file and cannot 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 that is being recorded, the text is inserted to the recording at that point. When the session is played using the Session Recording Player, the viewer can locate and count the times that the user opened a browser by noting the number of markers that appear in the Events and Bookmarks list in the Session Recording Player.

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. You must enable each server separately. You cannot globally enable all servers in a site.
- Write applications built on the Event API that runs within each user's XenApp 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 Citrix article CTX226844. The Session Recording Event API .dll is installed as part of the Session Recording installation. You can find it at C:\Program 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 option.
server check box.
Log insertion of USB mass storage devices

Feb 26, 2018

As of the 7.17 release, Session Recording can log the insertion of a Client Drive Mapping (CDM) mapped or generic redirected USB mass storage device in a client device where Citrix Receiver for Windows or for Mac is installed, and can tag the event in the recording. With this feature, you can easily search for events of interest from large amounts of recordings and can locate the events during playback in the Session Recording Player.

Note

Currently, only the insertion of USB mass storage devices (USB Class 08) can be logged. To make the feature work as expected, upgrade both Session Recording and the VDA to Version 7.17 or later.

Enable or disable the logging feature

On the Session Recording Agent, three registry keys are added for enabling or disabling the feature. The keys are set to 0 by default, which means the feature is disabled by default.

To enable or disable the feature, do the following:

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\SessionEvents.
4. Set the value of EnableSessionEvents to 1 or use the default value, 0.
   1: enable event logging globally
   0: disable event logging globally
5. Set the value of EnableCDMUSBDriveEvents to 1 or use the default value, 0.
   1: enable logging the insertion of CDM mapped USB mass storage devices
   0: disable logging the insertion of CDM mapped USB mass storage devices
6. Set the value of EnableGenericUSBDriveEvents to 1 or use the default value, 0.
   1: enable logging the insertion of generic redirected USB mass storage devices
   0: disable logging the insertion of generic redirected USB mass storage devices
7. Restart the Session Recording Agent to make your settings take effect.
8. (Optional) In Citrix Studio, configure the CDM mapping policy (enabled by default) and the USB redirection policy (disabled by default) as required.

The following table describes the usage scenarios and the corresponding registry key settings.

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Registry Key Setting</th>
</tr>
</thead>
</table>
| To log the insertion of both CDM mapped and generic redirected USB mass storage devices | EnableSessionEvents = 1  
EnableCDMUSBDriveEvents = 1 |
**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 Registry Editor can be solved. Use Registry Editor at your own risk. Be sure to back up the registry before you edit it.

---

**Play back recordings with tagged events**

When you play back a recording with events tagged for the insertion of mass storage devices, the events are present in the *Events and Bookmarks* panel and show as yellow dots in the lower part of the Session Recording Player as follows:
You can use events to navigate through a recorded session, or skip to the points where the events are tagged.

Search for recordings with tagged events

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

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

2. Define your search criteria in the Advanced Search dialog box. The Events tab allows you to search, by Event type, for tagged events in sessions. You can use the Common, Date/Time, and Event type filters in combination to search for recordings that meet your criteria. For example, you can search for recordings with the insertion events of CDM mapped USB mass storage devices within 24 hours.
The **Event type** drop-down list itemizes all event types that have been logged by Citrix Session Recording. You can select any one of the event types to search. Selecting **Any Citrix-defined event** means to search for all recordings with any type of events logged by Citrix Session Recording.
Enable or disable digital signing

If you install certificates on the computers on which the Session Recording components are installed, you can enhance the security of your Session Recording 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.

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 Signing tab.
4. Browse to the certificate that enables secure communication among the computers on which the Session Recording components are installed.

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 Signing tab.
4. Click Clear.
Administrator Logging

Feb 26, 2018

Session Recording Administrator Logging logs the following activities:

- Changes to recording policies on the Session Recording Policy Console or Citrix Director.
- Changes in Session Recording Server Properties.
- Downloads of recordings in the Session Recording Player.
- Recording a session by Session Recording after policy query.
- Unauthorized attempts to access the Administrator Logging service.

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.

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 server 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 recording of sessions is not impacted by the mandatory blocking setting.

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 computer hosting the Session Recording Server.
2. In IIS Manager, click Application Pools.
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 Microsoft SQL Server.
6. Grant the read permission to the account for the registry key at HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server.

By default, Administrator Logging logs every recording action after the policy query completes. This case might generate a large amount of loggings. To improve the performance and save the storage, disable this kind of logging in Registry.

1. As an administrator, log on to the computer 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 action logging
   - 1 enable the recording action logging

Session Recording provides a web-based UI to query all Administrator Logging data.

On the computer hosting the Session Recording Server:

1. From the Start menu, choose Session Recording Administrator Logging.
2. Type the credentials of a LoggingReader user.

On other computers:

1. Open a web browser and visit the webpage for Administrator Logging.  
   For HTTPS: https://servername/SessionRecordingLoggingWebApplication/, where servername is the name of the computer hosting the Session Recording Server.
   For HTTP: http://servername/SessionRecordingLoggingWebApplication/, where servername is the name of the computer hosting the Session Recording Server.
2. Type the credentials of a LoggingReader user.
Database high availability

Feb 26, 2018

Session Recording supports the following solutions for database high availability based on Microsoft SQL Server. The databases can automatically fail over when the hardware or software of a principal or primary SQL Server fails, which ensures that Session Recording continues to work as expected.

- **Always On Availability Groups**
  

- **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 [https://msdn.microsoft.com/en-us/library/ms189134.aspx](https://msdn.microsoft.com/en-us/library/ms189134.aspx).

- **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 [https://msdn.microsoft.com/en-us/library/ms189852.aspx](https://msdn.microsoft.com/en-us/library/ms189852.aspx).

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, you must manually change the SQL Server instance name to the name of the availability group listener or SQL Server network in HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server\SmAudDatabaseInstance.**

- **For database mirroring, you must manually add the failover partners for databases in 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.
Load balancing

Feb 26, 2018

This feature is to support load balancing across the Session Recording Servers. To use this feature, configure load balancing on Citrix NetScaler so that the Session Recording Servers can achieve load balancing and automatic failover.

An enhancement has been achieved that some load balancing configurations can be synchronized among all Session Recording Servers.

Note

This feature requires Version 7.16 or later of the Session Recording Server and Session Recording Agent.

- All Session Recording Servers share the same folder to store recording files.
- All Session Recording Servers share the same Session Recording Database.
- (Recommended) Install only one Session Recording Policy Console component and all Session Recording Servers share this Console.

Configure load balancing

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

Configure load balancing (Citrix NetScaler part)

Add the Session Recording Servers to the load balancing servers in Citrix NetScaler.

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.

1. Create virtual servers with the same NetScaler 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)
1. (Recommended) Type the same Session Recording Database name during the Session Recording Server installation.

2. If you choose the Administrator Logging feature, Citrix recommends that you type the same Administrator Logging Database name when you install each Session Recording Server.

3. After sharing the Read/Write permission of the file storage folder with all Session Recording Server machine accounts, 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 key in the Session Recording Server registry (HKEY_LOCAL_MACHINE\Software\Citrix\SmartAuditor\Server).
   - Key name: EnableLB;
   - Key value: 1 (D_WORD, meaning enable)

5. If you choose the HTTP or the HTTPS protocol for the Session Recording Storage Manager message queue, create a Host for the NetScaler VIP address, add redirection in C:\Windows\System32\msmq\Mapping\sample_map, and restart the Message Queuing service.

   The redirection is similar to:

   ```xml
   <redirections xmlns="msmq-queue-redirections.xml">
   <redirection>
       <from>http://<NetScalerHost>*/msmq/private$/CitrixSmAudData</from>
       <to>http://<LocalFqdn>/msmq/private$/CitrixSmAudData</to>
   </redirection>
   <redirection>
       <from>https://<NetScalerHost>*/msmq/private$/CitrixSmAudData</from>
       <to>https://<LocalFqdn>/msmq/private$/CitrixSmAudData</to>
   </redirection>
   </redirections>
   ```

   Where `<NetScalerHost>` is the created FQDN of the NetScaler VIP address, and `<LocalFqdn>` is the FQDN of the local host.

6. (Recommended) After configuring one Session Recording Server registry, you can use the following script to export configurations from this Server registry and import the registry to the other Session Recording Server registries. Also, you can use the script to add redirection mapping for message queue.

   ```sh
   # Copyright (c) Citrix Systems, Inc. All rights reserved.
   
   <#
   
   .SYNOPSIS
   
   This script is used to sync configurations between Session Recording Servers for load balancing deployment.
   ```
.DESCRIPTION

Will do below kinds of actions:

1. Export values from the registry key: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server to SrServerConfig.reg;

2. Import from SrServerConfig.reg and overwrite values in registry key: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server;

3. Add redirection mapping sr_lb_map.xml in %windir%\System32\msmq\mapping\;

   3.1 sr_lb_map.xml will consist redirection rule for both http and https, and not port specific.

.PARAMETER Action

   Export - to export the registry configurations of Session Recording Server to a registry file

   Import - to import the registry configurations of Session Recording Server from a registry file

   AddRedirection - to add HTTP/HTTPS redirection for MSMQ

.PARAMETER NetScalerHost

   The host name or FQDN of NetScaler.

.OUTPUTS

   Exported configuration file (SrServerConfig.reg) or backup configuration file (SrServerConfig.reg.bk)
.EXAMPLE

SrServerConfigurationSync.ps1 -Action Export

.EXAMPLE

SrServerConfigurationSync.ps1 -Action Import

.EXAMPLE

SrServerConfigurationSync.ps1 -Action AddRedirection -NetScalerHost netscaler.xd.local

.EXAMPLE

SrServerConfigurationSync.ps1 -Action Import,AddRedirection -NetScalerHost netscaler.xd.local

.EXAMPLE

SrServerConfigurationSync.ps1 -Action Import,Export,AddRedirection -NetScalerHost netscaler.xd.local

#>

###########################################################################

# Parameters section #
###

Param(

[Parameter(Mandatory = $true)]

[ValidateSet("Export", "Import", "AddRedirection")]

[string[]]$Action,

[Parameter(Mandatory = $false)]

[string]$NetScalerHost

)

###

# Default variables section #

###

$SR_SERVER_REG_PATH = "HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server"

$REG_FILE_PATH = "SrServerConfig.reg"

$REG_BACKUP_FILE_PATH = "SrServerConfig.reg.bk"

$TEMP_REDIRECT_XML = "sr_lb_map.xml"
$REDIRECT_XML_PATH = "$env:windir\System32\msmq\mapping"

############# MAIN #############

Try
{

If ($Action -Contains "export") {

Write-Host "Exporting current Session Recording Server Configuration to registry file: $REG_FILE_PATH ..." -ForegroundColor Green

& REG EXPORT $SR_SERVER_REG_PATH $REG_FILE_PATH /Y

Write-Host "Finish exporting." -ForegroundColor Green

}

If ($Action -Contains "import")
{

If (!(Test-Path $REG_FILE_PATH))
{

Write-Host "No $REG_FILE_PATH founded. Aborted." -ForegroundColor Yellow

}
Write-Host "No $REG_FILE_PATH founded. Aborted." -ForegroundColor Yellow

Exit 0

}

# Back up previous registry key

Write-Host "Back up Session Recording Server Configuration to Registry file: $REG_BACKUP_FILE_PATH ..." -ForegroundColor Green

& REG EXPORT $SR_SERVER_REG_PATH $REG_BACKUP_FILE_PATH /Y

Write-Host "Importing Session Recording Server Configuration from Registry file: $REG_FILE_PATH ..." -ForegroundColor Green

& REG IMPORT $REG_FILE_PATH 2>$null

Write-Host "Finish importing." -ForegroundColor Green

}

If ($Action -Contains "addredirection")

{

    # Check if netscaler host is given; If not, exit normally with warning.

    If(([[String]::IsNullOrEmpty($NetScalerHost)))

    {

    

```
Write-Host "No NetScaler host name is specified. Finish adding redirection." -ForegroundColor Yellow

Exit 0

}

If (!(Test-Path $TEMP_REDIRECT_XML))
{
    New-Item $TEMP_REDIRECT_XML -Type file
}

$SysInfo = Get-WmiObject -Class Win32_ComputerSystem

$LocalFqdn = "(@(SysInfo.Name).@(SysInfo.Domain)"

$RedirectXmlContent =

@*

<redirections xmlns="msmq-queue-redirections.xml">
  <redirection>
    <from>http://$NetScalerHost*/msmq/private$/CitrixSmAudData</from>
    <to>http://$LocalFqdn/msmq/private$/CitrixSmAudData</to>
  </redirection>
</redirections>
</redirection>

<redirection>

<from>https://$NetScalerHost*/msmq/private$/CitrixSmAudData</from>

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

</redirection>

</redirections>

"@

# Don't take care of encoding

$RedirectXmlContent | Out-File -FilePath $TEMP_REDIRECT_XML

Write-Host "Copying $TEMP_REDIRECT_XML to $REDIRECT_XML_PATH ..." -ForegroundColor Green

Copy-Item $TEMP_REDIRECT_XML -Destination $REDIRECT_XML_PATH

Write-Host "Restarting MSMQ service ..." -ForegroundColor Green

Restart-Service msmq -Force

Write-Host "Finish adding HTTP/HTTPS Redirection for MSMQ." -ForegroundColor Green
Exit 0

}

Catch

{

    Write-Host "$_.Exception.Message" -ForegroundColor Red

    Exit 1

}

Finally

{

    # Nothing to do

}
6b. On one Session Recording Server, after configuring the EnableLB registry key, start a command prompt as an administrator and run the `powershell.exe -file SrServerConfigurationSync.ps1 –Action Export,AddRedirection –NetScalerHost <NetScalerHost>` command, where `<NetScalerHost>` is the created FQDN of the NetScaler VIP address.

6c. After the script executes, 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.

6d. 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 –NetScalerHost <NetScalerHost>` command, where `<NetScalerHost>` is the created FQDN of the NetScaler VIP address.

6e. After the script executes, the EnableLB key is added to the other Session Recording Server registries and an `sr_lb_map.xml` file is added to the C:\Windows\System32\msmq\Mapping path.

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

Add the NetScaler VIP address or its FQDN as the connected Session Recording Server.

Add all the Session Recording Server machine accounts to the shared Session Recording Database and assign them with the db_owner permission.
Change your communication protocol

Feb 26, 2018

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.

1. Log on to the computer 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:
   1. Log on to each server where the Session Recording Agent is installed.
   2. From the Start menu, choose Session Recording Agent Properties.
   3. In Session Recording Agent Properties, choose the Connections tab.
   4. 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:
   1. Log on to each 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, select the server, and choose Modify.
   4. 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:
   1. Log on to the server where the Session Recording Policy Console is installed.
   2. From the Start menu, choose Session Recording Policy Console.
   3. 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.

1. Log on to the computer 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:
   1. Log on to each server where the Session Recording Agent is installed.
   2. From the Start menu, choose Session Recording Agent Properties.
   3. In Session Recording Agent Properties, choose the Connections tab.
   4. 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:
   1. Log on to each 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, select the server, and choose Modify.
   4. 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:
1. Log on to the server where the Session Recording Policy Console is installed.
2. From the **Start** menu, choose **Session Recording Policy Console**.
3. 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 CEIP

Mar 01, 2018

When you participate in the Citrix Customer Experience Improvement Program (CEIP), anonymous configuration and usage data is collected and sent to Citrix to help improve the product quality and performance. For more information on CEIP, see About the Citrix Customer Improvement Program (CEIP) and Citrix Insight Services.

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 computer 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.
View recordings

Feb 26, 2018

Use the Session Recording Player to view, search, and bookmark recorded XenApp or XenDesktop 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, and sessions that are completed.

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

**Note**: A Session Recording administrator must grant users the right to access the recorded sessions of VDAs for Server OS. If you are denied access to viewing sessions, contact your Session Recording administrator.

When the Session Recording Player is installed, the Session Recording administrator typically sets up a connection between the Session Recording Player and a Session Recording Server. If this connection is not set up, the first time you perform a search for files, you are prompted to set it up. Contact your Session Recording administrator for setup information.
Launch the Session Recording Player

Feb 26, 2018

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

This illustration shows the Session Recording Player with callouts indicating its major elements. The functions of these elements are described throughout the following articles.

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.

If the Session Recording administrator sets up your Session Recording Player with the ability to connect to multiple Session Recording Servers, you can select the Session Recording Server that your Session Recording Player 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 and playback protection

Feb 26, 2018

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 XenApp or XenDesktop server.

Some functionality is not available when you view sessions that are not recorded completely:

- A digital signature cannot be assigned until recording is complete. If digital signing is enabled, you can view live playback sessions, but they are not digitally signed and you cannot view certificates until the session is completed.
- Playback protection cannot 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 cannot cache a file until recording is complete.

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.

As a security precaution, Session Recording automatically encrypts recorded files before they are downloaded for viewing in the Session Recording Player. This playback protection prevents recorded files from being copied and viewed by anyone other than the user who downloaded the file. The files cannot be played back 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 the cache on the workstation where the Session Recording Player is installed until they are opened by an authorized user.

Citrix recommends that you use HTTPS to protect the transfer of data.

By default, playback protection 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 Encrypt session recording files downloaded for playback check box.
Open and play recordings

Feb 26, 2018

Open recordings

You can open session recordings in 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 telling you 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.

**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](https://docs.citrix.com).

1. Log on to the workstation where 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**

The name of a recorded session file begins with `i_`, which is followed by a unique alphanumeric file ID and then the `.icl` or `.icle` extension. The `.icl` extension denotes the recordings without playback protection applied. The `.icle` extension denotes the recordings with playback protection applied. Recorded session files are saved in a folder that incorporates the date the sessions were recorded. For example, the file for a session recorded on December 22, 2014, is saved in folder path `2014\12\22`.

1. Log on to the workstation where 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
Creating the Favorites folders allows you to quickly access recordings that you view frequently. These Favorites folders reference recorded session files that are stored on your workstation or on a network drive. You can import and export these files to other workstations and share these folders with other Session Recording Player users.

**Note:** Only users with access rights to the Session Recording Player can download the recorded session files associated with the Favorites folders. Contact your Session Recording administrator for the access rights.

To create a Favorites subfolder:

1. Log on to the workstation where the Session Recording Player is installed.
2. From the **Start** menu, choose **Session Recording Player**.
3. In the **Session Recording Player** window, select the **Favorites** folder in your Workspace pane.
4. From the menu bar, choose **File > Folder > New Folder**. A new folder appears under the **Favorites** folder.
5. Type the folder name, then press **Enter** or click anywhere to accept the new name.

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

### Play recordings

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

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

If you have inserted markers to the recording or if the recorded session contains custom events, you can also navigate through the recorded session by going to those markers and 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 does not support SpeedScreen Multimedia Acceleration for XenApp or the Flash quality adjustment policy setting for XenApp. When this option is enabled, playback displays a black square.
- Session Recording cannot record the Lync webcam video when using the HDX RealTime Optimization Pack.
- When you record a session with a resolution higher than or equal to 4096 x 4096, there might be fragments in the recording appearance.
- 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.

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. Use Player controls to:
Play the selected session file.

Pause playback.

Stop playback. If you click **Stop**, then **Play**, the recording restarts at the beginning of the file.

Halve the current playback speed down to a minimum of one-quarter normal speed.

Double the current playback speed up to a maximum of 32 times normal speed.

Use the seek slider in the lower part of the Player window to jump to a different position within the recorded session. You can drag the seek slider to the point in the recording you want to view or click anywhere on the slider bar to move to that location.

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

<table>
<thead>
<tr>
<th>Key:</th>
<th>Seek action:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Home</td>
<td>Seek to the beginning.</td>
</tr>
<tr>
<td>End</td>
<td>Seek to the end.</td>
</tr>
<tr>
<td>Right Arrow</td>
<td>Seek forward five seconds.</td>
</tr>
<tr>
<td>Left Arrow</td>
<td>Seek backward five seconds.</td>
</tr>
<tr>
<td>Move mouse wheel one notch down</td>
<td>Seek forward 15 seconds.</td>
</tr>
<tr>
<td>Move mouse wheel one notch up</td>
<td>Seek backward 15 seconds.</td>
</tr>
<tr>
<td>Ctrl + Right Arrow</td>
<td>Seek forward 30 seconds.</td>
</tr>
<tr>
<td>Ctrl + Left Arrow</td>
<td>Seek backward 30 seconds.</td>
</tr>
<tr>
<td>Page Down</td>
<td>Seek forward one minute.</td>
</tr>
<tr>
<td>Page Up</td>
<td>Seek backward one minute.</td>
</tr>
<tr>
<td>Ctrl + Move mouse wheel one notch up</td>
<td>Seek forward 90 seconds.</td>
</tr>
<tr>
<td>Key:</td>
<td>Seek action:</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>Ctrl + Move mouse wheel one notch up</td>
<td>Seek backward 90 seconds.</td>
</tr>
<tr>
<td>Ctrl + Page Down</td>
<td>Seek forward six minutes.</td>
</tr>
<tr>
<td>Ctrl + Page Up</td>
<td>Seek backward six minutes.</td>
</tr>
</tbody>
</table>

**Note:** 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.

You can set the Session Recording Player to play recorded sessions 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.

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.

Fast review mode allows you to set Session Recording Player to skip the portions of recorded sessions in which no action takes place. This setting saves time for playback viewing. However, it does not skip animated sequences such as animated mouse pointers, flashing cursors, or displayed clocks with second hand movements.

1. Log on to the workstation where 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.

Options allow you to change how recorded sessions appear in the Player window. You can pan and scale the image, show the playback in full screen, display the Player window in a separate window, and 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.
   - **Tip**: 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.
Highlight idle periods

Feb 26, 2018

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.
Cache recordings

Each time you open a recorded session file, the Session Recording Player downloads the file from the location where the recordings are stored. If you download the same files frequently, you can save download time by caching the files on your workstation. Cached files are stored on your workstation in this folder:

```
userprofile\AppData\Local\Citrix\SessionRecording\Player\Cache
```

You can specify how much disk space is used for the cache. When the recordings fill the specified disk space, Session Recording deletes the oldest, least used recordings to make room for new recordings. You can empty the cache at any time to free up disk space.

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.

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.
Use events and bookmarks

Feb 26, 2018
You can use events and bookmarks to help you navigate through recorded sessions.

Events are inserted to sessions while they are recorded, using the Event API and a third-party application. 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 to the recorded sessions using the Session Recording Player. Bookmarks are associated with the recorded session until you delete them, but they are not saved as part of the session file. 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 and bookmarks appear as dots in the lower part of the Player window. Events appear as yellow dots; bookmarks appear as blue dots. Moving the mouse over these dots 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.

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.

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**.

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**.

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 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**.
Troubleshoot

Feb 26, 2018
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 Registry Editor can be solved. Use Registry Editor at your own risk. Be sure to back up the registry before you edit it.
Installation of Server components fails

Feb 26, 2018
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

Feb 26, 2018

When you install the Session Recording Database or 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

Feb 26, 2018

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, followed by the 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 on which the Session Recording Agent resides does not trust or have a CA certificate for. Alternatively, the certificate might have expired or been revoked.
  
  Resolution: Verify that the correct CA certificate is installed on the server hosting the Session Recording Agent or use a CA that is trusted.

- **The remote server returned an error: (403) forbidden.** This is a standard HTTPS error displayed when you attempt to connect using HTTP (nonsecure protocol). The computer hosting the Session Recording Server rejects the connection because it accepts only secure connections.
  
  Resolution: 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 (this is the default member) being removed from the Policy Query role of the Session Recording Authorization Console.
  
  Resolution: 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.
  
  Resolution: Verify that the Session Recording Server is started, IIS is running on the server, and the server is connected to the network.
When the Session Recording Server cannot 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 in the Event Viewer of the computer hosting 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 computer hosting 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:**

- The Express Edition of Microsoft SQL Server 2008 R2, Microsoft SQL Server 2012, Microsoft SQL Server 2014, or Microsoft SQL Server 2016 is installed on a stand-alone server and does not have the correct services or settings configured for Session Recording. The server must have TCP/IP protocol enabled and SQL Server Browser service running. See the Microsoft documentation for information about enabling these settings.
- During the Session Recording installation (administration portion), incorrect server and 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 computer hosting the Session Recording Server or the computer 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://msdn.microsoft.com/en-us/library/cc646023.aspx](https://msdn.microsoft.com/en-us/library/cc646023.aspx).

**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

Feb 26, 2018

If your application sessions are not being recorded successfully, start by checking the application event log in the Event Viewer on the VDA for Server OS that runs the Session Recording Agent and Session Recording Server. Doing so can provide valuable diagnostic information.

If sessions are not being recorded, 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 computers 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 computers 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 VDAs for Server OS.

- **Recording is not enabled.** By default, installing the Session Recording Agent on a VDA for Server OS enables the server for recording. 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 VDA for Server OS and the Session Recording Storage Manager service must be running on the computer 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 computer hosting the Session Recording Server, recording problems might occur.
Unable to view live session playback

Feb 26, 2018
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

Feb 26, 2018

- If recordings are corrupted or incomplete when you view them using the Session Recording 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>`

  This issue happens 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.

  This issue is caused by insufficient Session Recording Agent buffer size when recording graphic intensive sessions.

  As a workaround, change the registry value of
  `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\SmAudBufferSizeMB` to a higher one in the Session Recording Agent, and then restart the machine.
Verify component connections

During the setup of Session Recording, the components might not connect to other components. All the components communicate with the Session Recording Server (Broker). By default, the Broker (an IIS component) is secured using the IIS default website certificate. If one component cannot connect to the Session Recording Server, the other components might also fail when attempting to connect.

The Session Recording Agent and Session Recording Server (Storage Manager and Broker) log connection errors in the applications event log in the Event Viewer of the computer hosting the Session Recording Server, while the Session Recording Policy Console and 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 value for Session Recording Server is the correct server name of the computer hosting the Session Recording Server.
5. Verify that the server given as the value for Session Recording Server can be contacted by your VDA for Server OS.

Note: Check the application event log for errors and warnings.

Verify that the Session Recording Server is connected

Caution: Using 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 Registry Editor can be solved. Use Registry Editor at your own risk.

1. Log on to the computer hosting the Session Recording Server.
2. Open the Registry Editor.
3. Browse to HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server.
4. Verify that the value of SmAudDatabaseInstance 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 computer 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

Testing connections to the Session Recording Server IIS site by using a Web browser to access the Session Recording Broker webpage 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 computer hosting the Session Recording Server
   - For HTTP: http://servername/SessionRecordingBroker/RecordPolicy.rem?wsdl, where servername is the name of the computer 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 computer hosting the Session Recording Server
   - For HTTP: http://servername/SessionRecordingBroker/Player.rem?wsdl, where servername is the name of the computer 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 computer hosting the Session Recording Server
   - For HTTP: http://servername/SessionRecordingBroker/PolicyAdministration.rem?wsdl, where servername is the name of the computer 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 computer running the Session Recording Policy Console is connected to the computer hosting the Session Recording Server using the configured protocol.

Troubleshoot certificate issues

If you are using HTTPS as your communication protocol, the computer 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 computer 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 computer 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 computer hosting the Session Recording Server provides error messages that the certificate expired or warning messages when it is about to expire.
Reference: Manage your database records

Feb 26, 2018

The ICA Log database (ICLDB) utility is a database command-line utility used to manipulate the session recording database records. This utility is installed during the Session Recording installation in the drive:\Program Files\Citrix\SessionRecording\Server\Bin directory at the server hosting the Session Recording Server software.

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:


Note: More extensive instructions are available in the help associated with the utility. To access the help, from a command prompt, type drive:\Program Files\Citrix\SessionRecording\Server\Bin directory, type iclb /?. To access help for specific commands, type iclb command /?.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>archive</td>
<td>Archives the session recording files older than the retention period specified.</td>
</tr>
<tr>
<td></td>
<td>Use this command to archive files.</td>
</tr>
<tr>
<td>dormant</td>
<td>Displays or counts the session recording files that are considered dormant.</td>
</tr>
<tr>
<td></td>
<td>Dormant files are session recordings that were not completed due to data loss.</td>
</tr>
<tr>
<td></td>
<td>Use this command to verify if you suspect that you are losing data. You can check whether the session recording files are becoming dormant for the entire database, or only recordings made within the specified number of days, hours, or minutes.</td>
</tr>
<tr>
<td>import</td>
<td>Imports session recording files to the Session Recording database.</td>
</tr>
<tr>
<td></td>
<td>Use this command to rebuild the database if you lose database records.</td>
</tr>
<tr>
<td></td>
<td>Also, use this command to merge databases (if you have two databases, you can import the files from one of the databases).</td>
</tr>
<tr>
<td>locate</td>
<td>Locates and displays the full path to a session recording file using the file ID as the criteria.</td>
</tr>
<tr>
<td></td>
<td>Use this command when you are looking for the storage location of a session recording file.</td>
</tr>
<tr>
<td></td>
<td>It is also one way to verify if the database is up-to-date with a specific file.</td>
</tr>
<tr>
<td>remove</td>
<td>Removes the references to session recording files from the database.</td>
</tr>
<tr>
<td></td>
<td>Use this command (with caution) to clean up the database. Specify the retention period to</td>
</tr>
</tbody>
</table>
be used as the criteria.

You can also remove the associated physical file.

<table>
<thead>
<tr>
<th>command</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>removeall</td>
<td>Removes all of the 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.</td>
</tr>
<tr>
<td>version</td>
<td>Displays the Session Recording Database schema version.</td>
</tr>
<tr>
<td>/l</td>
<td>Logs the results and errors to the Windows event log.</td>
</tr>
<tr>
<td>/f</td>
<td>Forces the command to run without prompts.</td>
</tr>
<tr>
<td>/s</td>
<td>Suppresses the copyright message.</td>
</tr>
<tr>
<td>/?</td>
<td>Displays help for the commands.</td>
</tr>
</tbody>
</table>