Configuring Security Features of Session Recording

Summary
This article provides information about the security features of Citrix Session Recording and outlines the process of configuring Session Recording security features. Session Recording is designed to be deployed within a secure network and accessed only by authorized personnel. As Session Recording is a security product, it is important to restrict access to Session Recording data from unauthorized users. It is imperative that Session Recording data does not fall into the wrong hands. The centralized architecture of Session Recording provides the ability to secure access to Session Recording resources and data using several different methods. Session Recording security features are enabled through built-in configuration tools and configuration of several Windows components.

Session Recording Communication Security
Communication between Session Recording components is achieved through Internet Information Services (IIS) and Microsoft Message Queueing (MSMQ). IIS provides the web services communication link between each Session Recording component, while MSMQ provides a reliable data transport mechanism for sending recorded session data from the Session Recording Agent to the Session Recording Server. This section describes methods for securing both IIS and MSMQ for use with Session Recording. IIS topics include certificates, SSL, Integrated Windows authentication, and configuring IIS ports. This article describes MSMQ and methods available to secure MSMQ communication through the MSMQ hardened mode.

Internet Information Services (IIS)
Internet Information Services (IIS) hosts the Session Recording Broker, a web application that handles the search queries and file download requests from the Session Recording Player, policy administration requests from the Session Recording Policy Console and evaluates recording polices from the Session Recording Agent for each XenApp session. IIS also hosts the Microsoft Message Queueing (MSMQ) virtual directory when MSMQ HTTP support is enabled, allowing recorded session data to be sent via HTTP or HTTPS.

IIS supports several methods for securing access to IIS web applications and services:

- Certificates in IIS for Using SSL
- Integrated Windows Authentication
- Configuring IIS Ports
**Certificates in IIS**

The Session Recording Broker is configured by default to require secure channel (SSL) using 128-bit encryption. IIS supports SSL security through a valid server certificate installed on the IIS web site where SSL security is to be applied. As the Broker is installed as a virtual directory named `SessionRecordingBroker` under Default Web Site of IIS, a server certificate is required for the Default Web Site before SSL connections are accepted by the Session Recording Broker. To establish an SSL connection, you need a server certificate at one end of the connection and the certificate of the certificate authority (CA) that issued the server certificate at the other end.

- **Server certificate** - A server certificate certifies the identity of a server. The type of digital certificate that is required by the Session Recording Broker is called a server certificate.
- **Issuing CA certificate** - A certificate that identifies the CA that signed the server certificate. The issuing CA certificate belongs to the CA. This type of digital certificate is required by the Agent, Player, and Policy Console to verify the server certificate.

When establishing an SSL connection from the Agent, Player, or Policy Console, the IIS web server sends its server certificate to the client. When receiving a server certificate, the Agent, Player, or Policy Console checks to see which CA issued the certificate and if the CA is trusted by the client. If the CA is not trusted, the certificate is declined and an error is logged in the Application Event log for the Agent or an error message is displayed to the user in the Player or Policy Console.

A server certificate is installed by gathering information about the server and requesting a CA to issue a certificate for that server. It is important to specify the correct information when requesting a server certificate and ensuring the server name is specified correctly, such that if the Fully Qualified Domain Name (FQDN) is used for connecting clients (Agent, Player, and Policy Console) the certificate information specified to the CA must use the FQDN of the server rather than the NetBIOS name. Likewise, if NetBIOS names are used, do not specify the FQDN when requesting a server certificate. Install the server certificate into the local machine's certificate store and the issuing CA certificate on each connecting client.

Your organization might have a private CA that issues server certificates and this can be used with Session Recording. For a private CA, ensure each client machine has the issuing CA certificate installed. Refer to Microsoft documentation about using certificates and certificate authorities. Alternatively, a number of companies and organizations currently act as CA's, including VeriSign, Baltimore, Entrust, and their respective affiliates.

All certificates have an expiration date, which is defined when issued by the CA. The expiration date can be found by checking the properties of the certificate. The
Administrator must ensure certificates are renewed before the expiration date to prevent any errors occurring in Session Recording.

To install a server certificate in IIS
The Session Recording installation is configured to use HTTPS, and requires the Default Web Site to be configured with a server certificate issued from a CA. These steps provide an outline on how to install a server certificate in IIS.

1. As an administrator, log on to the server that hosts the Session Recording Server.
2. From the Start menu, select Start > Control Panel > Administrative Tools > Internet Information Services (IIS) Manager.
3. In the left pane, click the servername node (where servername is the name of the server where you are enabling HTTPS).
4. In Features View tab, double-click Server Certificate and follow the onscreen instructions of the Web Server Certificate Wizard to request a server certificate.
5. Send the certificate request file to your CA.
6. Once you have received a server certificate from your CA repeat steps 1-4 to install the server certificate. The Web Server Certificate Wizard guides you through installing the certificate.

To use HTTPS as the communication protocol (if HTTPS has been disabled)
The Session Recording installation is configured to use HTTPS, however if this has been changed to HTTP and you want to change Session Recording back to HTTPS, you must change several settings.

It’s recommended to disable SSLv2, SSLv3, and TLS 1.0 on the Session Recording Server. For more information, see the Microsoft articles How to disable PCT 1.0, SSL 2.0, SSL 3.0, or TLS 1.0 in Internet Information Services and How to restrict the use of certain cryptographic algorithms and protocols in Schannel.dll.

1. Enable secure connections for the Session Recording Broker in IIS on the Session Recording Server:
   a) As an administrator, log on to the server that hosts the Session Recording Server.
   b) From the Start menu, select Start > Control Panel > Administrative Tools > Internet Information Services (IIS) Manager.
   c) In the left pane, expand the servername node (where servername is the name of the server where you are enabling HTTPS) by choosing servername > Sites > Default Web Site > SessionRecordingBroker.
   d) Click SessionRecordingBroker and double-click SSL Settings in Features view tab.
   e) In the SSL Settings page, enable the Require SSL check box.
   f) Click Apply to save the setting and exit the dialog boxes.

2. Change the protocol setting from HTTP to HTTPS for the Session Recording Agent service installed on each computer hosting XenApp Server OS VDA.
a) As an administrator, log on to each server where the **Session Recording Agent** is installed.

b) From the Start menu, select **Start > All Programs > Citrix > Session Recording > Session Recording Agent Properties**. The Session Recording Agent Properties dialog box appears.

c) Select the **Connections** tab.

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

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

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

   b) From the Start menu, select **Start > All Programs > Citrix > Session Recording > Session Recording Player**. The Session Recording Player launches.

   c) Select **Tools > Options > Connections**, select the server, and select **Modify**.

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

4. Change the protocol setting from HTTP to HTTPS in the Session Recording Policy Console:

   a) Log on to the server where the Session Recording Policy Console is installed.

   b) From the Start menu, select **Start > All Programs > Citrix > Session Recording > Session Recording Policy Console**. The Connect to Session Recording Server dialog box appears.

   c) Select **HTTPS** from the **Protocol** drop-down list and select **OK** to connect. If the connection is successful, this setting is remembered the next time you launch the Session Recording Policy Console.

**Integrated Windows Authentication**

The Session Recording Broker virtual directory, **SessionRecordingBroker** is configured to support authentication only through Integrated Windows authentication. This requirement ensures that only Windows authenticated users and computers are able to access the Broker services. Integrated Windows authentication is based on the Kerberos v5 authentication algorithm as implemented by Active Directory. As the Session Recording Broker is never accessed from the Internet, the other IIS authentication options available are not required and must never be turned on. By using Integrated Windows Authentication, the role based security of the Broker is maintained and access to session recording policy and session recording data by anonymous users is strictly prohibited. The Session Recording Agent, Policy Console, and Player authenticate using the connecting user's current Windows credentials. For the Policy Console and Player this is the currently logged on user. As the Agent service runs as a service under the local system account, the credentials presented to the server are those of the computer itself. In all cases, the principal (user or computer account) of the connecting client must belong to the same or trusted domain as the server.
connection request made from a local non-domain user, workgroup or an untrusted domain always fails.

**Configuring IIS Ports**

Session Recording components that connect to the Session Recording Broker are capable of connecting using non-default communication ports. Secure connections to the Broker by default use port 443 for HTTPS traffic; however it is possible to change this port in IIS to another unused port between 1 and 65535. Changing the HTTPS port can act as an obfuscation measure and conceal the Broker web application. Before changing the HTTPS port in IIS, it is important that the new port is not already in use by the server for another application or service. The *services* file in the `SystemRoot\System32\Drivers\Etc` directory lists TCP and UDP port numbers used by Windows Server or use the `netstat -a` command, checking the port is not already in use or listening. Ensure that any firewalls between Session Recording components also allow access to the Session Recording Server using this port. Note that obfuscation of port numbers should never be used as an alternative to SSL or IPSec.

**To change the default HTTPS Port**

1. Change the default HTTPS port in IIS on the Session Recording Server:
   a) As an administrator, log on to the server that hosts the Session Recording Server.
   b) From the Start menu, select Start > Control Panel > Administrative Tools > Internet Information Services (IIS) Manager.
   c) In the left pane, expand the `servername` node (where `servername` is the name of the server where you are changing the HTTPS port) by choosing `servername` > Sites > Default Web Site.
   d) Click Default Web Site. In the Actions panel, under Edit Site, click Bindings.
   e) In the Site Bindings dialog box, click the https entry, and then click Edit.
   f) In the Edit Site Binding dialog box, change the port number in the Port field.
      (e.g. Change from 443 to 8081)
   g) Click OK to save the setting and exit the dialog box.

2. Change the port setting for HTTPS for the Session Recording Agent service installed on each computer hosting XenApp Server OS VDA:
   a) Log on to each server where the Session Recording Agent is installed.
   b) From the Start menu, select Start > All Programs > Citrix > Session Recording > Session Recording Agent Properties. The Session Recording Agent Properties dialog box appears.
   c) Select the Connections tab.
   d) If using HTTPS for MSMQ, then in the Session Recording Storage Manager message queue area, clear the Use default check box and change the port number in the HTTP/HTTPS port field to the new port number.
   e) In the Session Recording Broker area, clear the Use default check box and change the port number in the HTTP/HTTPS port field to the new port number.
f) Select OK to accept the change. If you are prompted to restart the service, select Yes.

3. Change the port setting for HTTPS in the Session Recording Player settings:
   a) Log on to the workstation where the Session Recording Player is installed.
   b) From the Start menu, select Start > All Programs > Citrix > Session Recording > Session Recording Player. The Session Recording Player launches.
   c) Select Tools > Options > Connections, select the server, and select Modify.
   d) Clear the Use default check box and change the port number in the Port field to the new port number.
   e) Select OK (twice) to accept the change and exit the dialog box.

4. Change the port setting for HTTPS in the Session Recording Policy Console:
   a) Log on to the server where the Session Recording Policy Console is installed.
   b) From the Start menu, select Start > All Programs > Citrix > Session Recording > Session Recording Policy Console. The Connect to Session Recording Server dialog box appears.
   c) Clear the Use default check box and change the port number in the Port field to the new port number.
   d) Select OK to connect. If the connection is successful, this setting is remembered the next time you launch the Session Recording Policy Console.

Internet Protocol Security (IPSec)
You can implement Internet Protocol Security (IPSec) as an alternative to using SSL to secure data between Session Recording components. IPSec is an Internet standard for secure communications that is part of the TCP/IP stack, providing authenticated and encrypted communication. IPSec must be enabled and configured on each computer hosting a Session Recording component. Configure IPSec using the Local Security Settings (IP Security Policies) for each server and workstation. Refer to the Microsoft Documentation for further information on IPSec.

Microsoft Message Queuing (MSMQ)
Microsoft Message Queuing (MSMQ) provides reliable transport of data from the Session Recording Agent to the Session Recording Server using an MSMQ private message queue named CitrixSmAudData. Session Recording supports three types of MSMQ message transport protocols; TCP, HTTP and HTTPS. You maintain configuration of the MSMQ transport protocol for Session Recording through the Connections tab in the Session Recording Agent Properties application, with the default setting of TCP. Typically, MSMQ messages are sent and received through the TCP transport protocol using remote procedure calls (RPC). If IPSec is not used, data is sent as plaintext. The preferred approach is for communication to be secured with SSL by using the HTTP/S mode provided by MSMQ. When MSMQ HTTP support is enabled, messages may also be received through IIS using either HTTP or HTTPS. By default, the MSMQ service opens the following ports to send and receive messages:
The Session Recording Agent installation configures the Agent to send MSMQ messages using TCP. Secure MSMQ by enabling **MSMQ HTTP Support** on the Session Recording Server machine and setting the transport protocol in the **Session Recording Agent Properties** application to HTTPS. Furthermore, when MSMQ is set to HTTP hardened mode on the server, the MSMQ service does not listen on any of the above ports and only HTTP messages received by the IIS virtual directory for MSMQ are accepted and processed. As no TCP or UDP ports are open, the client can send MSMQ messages using only HTTP or HTTPS. MSMQ hardened mode using HTTPS also provides the ability for the Session Recording Server to be secured using firewalls, and allowing only HTTPS port (443) access to be granted. Citrix recommends that you always set up production Session Recording systems in this way.

**To Enable MSMQ HTTP Support**
1. As an administrator, log on to the Session Recording Server.
2. From the **Start** menu, select **Start > Control Panel > Add or Remove Programs**.
3. From the Add or Remove Programs dialog select, **Add or Remove Windows Components**.
4. From the Windows Components Wizard select, **Application Server > Details > Message Queuing > Details**, enable the check box for **MSMQ HTTP Support** and clear the check box for **Active Directory Integration** (if enabled).
5. Click **OK** to the **Message Queuing Setup** dialog and **OK** to the **Message Queuing** and **Application Server** dialogs.
6. Click **Next** to install.

**To configure the Session Recording Agent to Send MSMQ messages using HTTPS**
1. As an administrator, log on to the computer hosting the Session Recording Agent service.
2. From the **Start** menu, select **Start > All Programs > Citrix > Session Recording > Session Recording Agent Properties**.
3. In the Session Recording Agent Properties dialog box, click **Connections** tab.
4. In the **Session Recording Storage Manager message queue** section, select **HTTPS** from the **Protocol** field and select **OK** to accept the change. If you are prompted to restart the service, select **Yes**.

**To enable MSMQ Hardened Mode**
1. As an administrator, log on to the Session Recording Server.
2. From the **Start** menu, select **Start > Control Panel > Administrative Tools > Computer Management**.
3. Expand **Services and Applications**, then right click on **Message Queuing** and select **Properties**.
4. From the Message Queuing Properties dialog box select, **Server Security** tab and enable the **Enable hardened MSMQ mode to secure this computer on the Internet** check box.

5. Click **OK** to save the setting and click **Yes** to restart the **Message Queuing Service** and **Citrix Session Recording Storage Manager**.

6. Click **Restart Now** to the **Message Queuing – Restart System** dialog box for the changes to take effect. The server will now restart.

**Agent Security**
The Session Recording Agent is a Windows service that records XenApp sessions, sending session recording data to the Session Recording Server using MSMQ. The Session Recording Driver acquires session data, which is read by the Agent. The Agent collects information about the session and sends this to the Session Recording Broker using its web services interface to determine if the session should be recorded. The Broker then returns a policy decision and the Agent either continues recording or discontinues recording. If the Agent discontinues recording, the session data already recorded is deleted. Periodically, the Agent communicates with the Broker to determine the current Session Recording rollover parameters and a list of live session recordings currently being played. A key security feature of the Session Recording system is that no additional listener ports are ever opened on computers running XenApp Server OS VDA with Session Recording enabled. The only accessible interface into the Session Recording Agent is the optional Event API.

**Event API**
You can enable or disable the Session Recording Event API on a per-server basis. The default setting for each Session Recording Agent installation is for the COM interface to be disabled. With the Event API turned off, the Agent has no accessible interfaces. Any attempts to connect to the interface fail until you enable it. The Event API is secured to allow local access and activation permissions only to users of the following built-in groups:

- Terminal Server User
- Interactive
- System

The Event API requires a session ID to insert events into sessions currently recording; however, if the supplied session ID is not a current Terminal Services session or the supplied session is not being recorded by the Session Recording Agent, the function call to the Event API is ignored and no error is returned to the caller. This is to prevent the Event API being used as a means for detecting whether a particular session is actually being recorded. This does not prevent a user from one session adding events into the recorded session of another user.
Session Recording Security Roles
Session Recording provides role-based security for authorizing user access to Session Recording Broker data and resources. The role-based security is based on three Session Recording Broker functions:

- **Player** – Search for and view session recording files from the Session Recording Player
- **PolicyQuery** – Query Session Recording Server for policy evaluations from the Session Recording Agent
- **PolicyAdministrator** – View and change record policies on the Session Recording Server from the Session Recording Policy Console

Roles are configured using the Session Recording Authorization Console installed on the Session Recording Server machine. All requests made by users that require Player or PolicyAdministrator role membership are audited by the Broker and logged in the Windows Application Event log. This also includes attempts where the request failed because the user was not a member of the required role.

Authorization Console
The Session Recording Authorization Console is built on the Windows Server Authorization Manager snap-in for the Microsoft Management Console (MMC). It is configured to load the Session Recording Broker authorization store XML file that contains the Broker security roles. The authorization store XML file is named SessionRecordingAzManStore.xml, protected with a strong Access Control List (ACL) and is stored in the directory ProgramFiles/Citrix/Session Recording/Server/App_Data.

Members of Session Recording security roles may be domain or local users, groups, and computer accounts. The default members for each security role are:

<table>
<thead>
<tr>
<th>Security Role</th>
<th>Default Member</th>
</tr>
</thead>
<tbody>
<tr>
<td>Player</td>
<td>None</td>
</tr>
<tr>
<td>PolicyQuery</td>
<td>Authenticated Users</td>
</tr>
<tr>
<td>PolicyAdministrator</td>
<td>Local Administrators</td>
</tr>
</tbody>
</table>

The Player role by default has no members to restrict unauthorized users from playing recorded sessions. Only users who need access to a Session Recording role should be granted access to that specific role. For example, do not grant access to the PolicyQuery or PolicyAdministrator roles for a Player user who only reviews session recordings, but grant access to the Player role only. Furthermore, ensure that users who no longer require access to a role are removed from that particular role.

The PolicyQuery role by default is quite broad in which users and computers are able to access this role. The PolicyQuery role for example, could be accessed by any user or machine that is an authenticated user.

To improve the security of this role, remove the Authenticated Users group from the PolicyQuery roles respectively. Then, add only the necessary computers to the PolicyQuery security role, such that the PolicyQuery role contains only the computer
accounts of the machines hosting XenApp Server OS VDA that have the Session Recording Agent installed and enabled. Any changes to security roles are not immediate as the Session Recording Broker updates its internal cache of the security roles once every minute from the Session Recording Broker authorization store XML file. To force an immediate update of the security roles for the Broker, recycle the `SessionRecordingAppPool` application pool in the IIS Applications Pools, after changing security roles.

**To Remove Users from Session Recording Roles**
1. As an administrator, log on to the server where Session Recording Server is installed.
2. From the Start menu, select Start > All Programs > Citrix > Session Recording > Session Recording Authorization Console. The Session Recording Authorization Console appears.
3. From the left pane of the Session Recording Authorization Console, select one of the three Session Recording security roles.
4. From the right pane of the Session Recording Authorization Console, select a user to remove and from the main menu, select Action > Delete. Any changes to the security roles take effect in the Session Recording Broker during the update (that occurs once every minute).

**To Assign User or Computers to Session Recording Roles**
1. As an administrator, log on to the server where Session Recording Server is installed.
2. From the Start menu, select Start > All Programs > Citrix > Session Recording > Session Recording Authorization Console. The Session Recording Authorization Console appears.
3. From the left pane of the Session Recording Authorization Console select, one of the three Session Recording security roles.
4. From the main menu, select Action > Assign Windows Users and Groups.
5. Add the necessary users, groups, or computers to the security role and click OK when finished. When adding computers, in the Select Users, Computers, or Groups dialog box, click Object Types... and select Computers from the Object Types dialog box and click OK. Any changes to the security roles take effect in the Session Recording Broker during the update (that occurs once every minute).

**To recycle the Session Recording Broker**
1. As an administrator, log on to the server where Session Recording Server is installed.
2. From the Start menu, select Start > Control Panel > Administrative Tools > Internet Information Services (IIS) Manager.
3. In the left pane, expand the `servername` node (where `servername` is the name of the server where you are recycling the Session Recording Broker) by choosing `servername` > Application Pools > `SessionRecordingAppPool`.
4. Right-click `SessionRecordingAppPool` and select Recycle.
Auditing of Security Roles
The Session Recording Broker audits all access to the Player and PolicyAdministrator roles by logging success and failure audits to the Windows Application Event log. This includes access to:

- Searching for session recordings
- Downloading session recordings
- Loading policies
- Changing the active policy
- Creating new policies
- Deleting policies
- Saving policies

When access is granted for a role, a Success Audit event log entry is created stating the user who was granted access and the particular file or action granted. When access is denied, a Failure Audit event log entry is created stating the user request was rejected, the user who was denied access, and the requested role that was denied. Users are denied access when they are not a member of a role.

Storage Directories
Session Recordings are stored in the SystemDrive:\SessionRecordings directory by default. You can change the directory where they are stored, or add additional storage directories to load balance storage across multiple volumes. Storage directories can be specified to a local drive, SAN volume, or UNC network path. Network mapped drive letters are not supported. The Storage Manager stores Session Recording files using a directory structure of <StorageDirectory>\year\month\day, where <StorageDirectory> is the storage directory specified in the Session Recording Server Properties application. When a new session recording file is created, subdirectories are created based upon the current date (for example, if the date is 31 January, 2007 the session recording would reside in <StorageDirectory>/2007/01/31).

For local drive and SAN volume storage directories, the existence of the storage directory is not required when specified in the Session Recording Server Properties application. The directory is created automatically and a strong Access Control List (ACL) is applied when the Storage Manager Service is restarted. If the directory already exists and is empty, the Storage Manager deletes the directory and recreates the directory with the strong ACL. If however the directory exists and contains one or more files, changes to the ACL for the existing directory are not made. It is the responsibility of the Administrator to ensure strong ACLs are applied to this directory.

The ACL that is applied to a new directory is not inherited from the parent directory, but any subdirectories of the storage directory inherit the ACL applied by the Storage Manager. The list of Access Control Entries (ACE) forming the storage directory ACL is:

<table>
<thead>
<tr>
<th>Account</th>
<th>Access Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local Administrators</td>
<td>Full Control</td>
</tr>
</tbody>
</table>
Although UNC network paths are supported as a storage directory these cannot be secured by the Storage Manager. It is the responsibility of the Administrator to secure UNC network paths by applying the ACLs listed above, substituting Local Service and Network Service accounts with the Active Directory machine account (domainname\machinename$) of the Session Recording Server. For performance and security reasons, Citrix does not recommend using UNC network paths for storing recording files.

It is important to protect and secure storage directories as much as possible. Do not enable Windows shares to allow users direct access to Session Recording files for Storage directories. Use the Broker where the download of files is highly restricted, encrypted and audited for all access to storage directories. Consider the physical security of disks when securing the storage directories. Ensure servers running Session Recording components are physically secure. If possible, lock these machines in a secure room to which only authorized personnel can gain direct access.

The Storage Manager supports the use of several storage directories to load balance Session Recording files across multiple volumes. The load balancing operates using a round robin method, by cycling through the storage directories and storing each new Session Recording file in the next storage directory. It is possible to add the same storage directory more than once, to improve load balancing across several directories.

**To Add storage directories to the Session Recording Server**
1. As an administrator, log on to the Session Recording Server.
2. From the Start menu, select Start > All Programs > Citrix > Session Recording > Session Recording Server Properties.
3. In the Session Recording Server Properties dialog box, click Storage tab. The current storage directory appears in the File storage directories list.
4. Click Add, type the path for the new storage directory or browse to locate the directory, and then click OK. If the directory does not exist, Session Recording creates the new directory and assigns ACLs to the directory.
5. Click OK to accept the change. If you are prompted to restart the service, select Yes.

**Playback Protection**
Session Recording Playback Protection is a feature of the Broker that encrypts session recording files before they are downloaded from the Broker for viewing in the Player. By default, playback protection is enabled and requires no configuration of certificates, on either the Broker or Player computers. Since Playback Protection is a server side setting, once it is enabled all Player requests for downloading Session Recording files are encrypted. This prevents unauthorized access and tampering of Session Recording files.
Recordings while they reside on the Player computer. Playback Protection is implemented using 2048-bit RSA key pairs from the Player computer (generated on first use of the Player), a 128-bit TripleDES (3DES) symmetric key generated on the Broker computer, and using an SHA-1 hash algorithm to verify the decrypted data. The algorithm implementations of RSA, TripleDES and SHA-1 are all FIPS compliant. The diagram below illustrates the process of playing a file with Playback Protection.

When a user of the Player requests a session recording to download from the Session Recording Server (Broker), the Player sends to the Broker, the RSA public key from the User’s Crypto Store and the requested session recording file ID. If first-time use of the Player, a 2048-bit RSA key pair is generated using the Microsoft Cryptographic API for the Player user and stored in the User’s Crypto Store on the local machine.

When the Broker begins encrypting a session recording file, it generates a TripleDES (3DES) 128-bit symmetric key. The symmetric key is then used to encrypt the contents of the requested plaintext session recording file (.ICL) retrieved from the master file storage location, to create an .ICLE file. The encrypted session recording file (.ICLE) is stored temporarily in the Windows temporary files directory.

The RSA public key from the Player is then used to encrypt the symmetric key and the SHA-1 hash of the .ICLE file, to create an .ICLK file that is also stored temporarily in the Windows temporary files directory. The Broker then proceeds to stream the encrypted session recording file (.ICLE) and key file (.ICLK) to the Player. Once the Player receives both files, the Broker deletes the files from the Windows temporary files directory.

The Player stores the downloaded encrypted files on the local disk in the Player cache directory. The encrypted files can safely reside on the local disk of the Player computer as the private keys required for decryption are held safely within the User’s Crypto Store, which only the original user can access.
To decrypt the recording file, the Player reads the RSA private key from the User’s Crypto Store and decrypts the key file (.ICLK) to retrieve the symmetric key and the SHA-1 hash, which is then used for verifying the encrypted session recording file is correct. The symmetric key is then used to decrypt the encrypted Session Recording file (.ICLE) back to a plaintext session recording file (.ICL). The decrypted file (.ICL) is secured with access to the file locked to the Player process, it only exists while the Session Recording is playing in the Player and is deleted when the file is closed by the Player.

Playback Protection is not applied to live session playback as live sessions are constantly changing. However, live session recording files are only cached temporarily on the Player computer while a live session recording is playing and is deleted when the session recording file is closed by the Player, either when a user stops playing the Session Recording or the Player is closed. It is possible to disable live session playback from the Session Recording Server and prevent live sessions from being played.

**To enable Playback Protection (if disabled)**
1. As an administrator, log on to the Session Recording Server.
2. From the Start menu, select Start > All Programs > Citrix > Session Recording > Session Recording Server Properties.
3. In the Session Recording Server Properties dialog box, click Playback tab.
4. In the Playback Protection section, enable the Encrypt session recording files downloaded for playback check box and select OK to accept the change.

**To disable Live Session Playback**
1. Log on to the Session Recording Server
2. From the Start menu, select Start > All Programs > Citrix > Session Recording > Session Recording Server Properties.
3. In the Session Recording Server Properties dialog box, click Playback tab.
4. In the Live Session Playback section, clear the Allow live session playback check box and select OK to accept the change.