
RecordTS

Installation Guide



<http://www.tsfactory.com>

Information in this document is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of TSFactory LLC.

RecordTS and the TSFactory logo are copyright of TSFactory LLC. © 2005-2010 TSFactory LLC. All rights reserved.

Version 2.0 – Updated May 1st, 2010

Contents

- Introduction** **5**
- What is RecordTS? 5
- Main Features..... 5
 - Security/Audit compliance..... 5
 - Developed for Terminal Services 5
 - Per user session recording 5
 - File conversion capabilities 6
- How does RecordTS work? 6
- Quick Overview: 6
 - Recording Agent 6
 - Repository Manager..... 6
 - Web Console..... 7

- Installing RecordTS** **8**
- Step 1: Installing the RecordTS Recorder 8
- Step 2: Installing the Repository Manager service 9
- Step 3: Installing the Player 10
- Step 4: Configuring RecordTS..... 11
- Step 5: Configuring the Database 12
- Step 6: Configuring Repository Manager 16
- Step 7: Configuring Web Console 20

This page intentionally left blank.

Introduction

What is RecordTS?

RecordTS is a session recorder for Windows Terminal Services. What does it mean exactly? It means once installed on a server running Terminal Services (with or without the Citrix add-on) or simply a Windows server or workstation with Remote Desktop/Remote Administration enabled, administrators will be able to record everything users are doing during their sessions for later playback and/or archiving. Pretty much the same as watching a video on your computer! Thanks to this product you can:

- Track who is connected to the computer and what they do on it
- View selected recordings for a specific user, during a specific time period, etc.
- Track users actions that might have caused problems on a computer
- Save recording files in a specific native format (RecordTS), as well as other popular video formats

Main Features

Security/Audit compliance

Instead of looking at hundreds of entries in log files, RecordTS allows you to actually see everything that was done as it happened. As you can archive all recorded sessions (to tape or an offsite location for example) for later playback, in case of an audit it is just a matter of restoring a file and watching!

Developed for Terminal Services

Although other similar solutions do exist in the market, RecordTS is the first and only solution that works directly at the protocol level (RDP – ICA to be supported at Q1, 2007). This means increased performance and scalability, with much smaller recordings.

Per user session recording

Recorded sessions are saved individually on a per user basis. RecordTS can also be configured to record only certain users.

File conversion capabilities

By default RecordTS saves all sessions in its own, proprietary format. These files can be easily exported to major standard formats like Macromedia Flash and Microsoft AVI.

How does RecordTS work?

RecordTS works directly at the Terminal Server intercepting all requests made to the RDP port. Once intercepted, the RDP stream is recorded to a file (one per user per session) on the local server or at any other network location. As RecordTS was developed from the ground up specifically for Terminal Services, this process does not affect your Terminal Server performance, scaling easily once more users are added to the system.

Quick Overview:

Below is the list of basic components of RecordTS. Each component will be discussed more in depth further into the manual.

- **Recording Agent**
- **Repository Manager**
- **Web Console**

Recording Agent

The basic component of RecordTS is the Recording Agent, installed on each of the target machines to be recorded. Its main job is to record user sessions and store the recording files locally. From the time RecordTS Recording Agent is installed on a server or workstation, each user session will be recorded and saved as a file in the native RecordTS format in a specific folder. Recording files will contain additional information about the session: computer name and IP address, user name, connection time and duration, etc. For each individual user, recording files can be stored in separate directories on the local machine.

The recording files can be viewed or played as a video using the RecordTS Player. Recordings may be converted from the RecordTS format to AVI or SWF for viewing in other media players such as MS Windows Media Player.

Repository Manager

The Repository Manager schedules and moves recording files stored locally on the machines where the recording is taking place to one or more file servers (backup storage). While it is moving them, it scans the

recording files for meta data (user info, text, etc) and stores the data into an SQL database. This information is used for quicker searching and reporting. It also possible to purge unwanted or older recording files from storage to free up disk space.

Web Console

Web Console provides a way to manage the whole system centrally from a web browser. It lets you search for specific recordings based on date, user info, etc and then play the videos on demand. You can also generate reports from the Web Console as well.

Thus, RecordTS provides all the tools necessary for creating recordings of user sessions and then manipulating and viewing them.

Installing RecordTS

Step 1: Installing the RecordTS Recorder

The RecordTS Recording Agent must be installed on each machine where you wish to record remote user sessions. Note: after installing the RecordTS Recording Agent, the Recording Agent service will appear on the server under the list of services. From this point on, the Recording Agent service will commence recording user sessions. You can control which users are recorded using the configuration screen.

How to install the RecordTS Recording Agent:

1. Run the RecordTS.msi installation file on the server. The installation wizard will appear. Close all other programs and then click Next.
2. Carefully read the license agreement. If you agree to the terms, select the check box to confirm acceptance of the agreement. Click Next to continue installing. To exit Setup, click Cancel.
3. Choose the RecordTS installation mode that meets your requirements. Click Next.
4. Select the directory in which recording files will be saved. Only local directories on the local machine can be used as temporary storage. If you do not want to use the default directory suggested by the installer, click Browse... to choose another directory. Then click Next.
5. To start the installation program, click Install. To modify the installation options that are mentioned in the previous steps, click Back. To exit Setup, click Cancel.
6. Once the installation program finishes copying the necessary files to the system, the installation process has successfully completed. To run the Recording Agent Configuration Tool, select Run Configuration Tool. To exit the installation wizard, click Finish.
7. After installation has completed a dialog box will appear offering to restart the computer. This is necessary to activate the Recording Agent recording service. Click OK to reboot immediately.

After restarting the Recording Agent, the recording service should be installed and running on the server. All user sessions will be recorded and stored in the specified directory on the machine.

Step 2: Installing the Repository Manager service

Repository Manager runs as a Windows service helps manage the Recording Agent recording files. It will collect, scan & database and store the recording files to central file storage units. Repository Manager can be installed on any computer that has access to all recording file local storages, and to the central SQL database.

How to install the Repository Manager

Run the setup file RecordTS-Repository.msi. The installation wizard will appear. Close all other programs and then click Next.

Carefully read the license agreement. If you agree to the terms, select the check box to confirm acceptance of the agreement. To continue, click Next. To exit Setup, click Cancel.

To start the installation of the Repository Manager, click Install. If you would like to go back and change any settings, click Back. To exit Setup, click Cancel.

Once the installer finishes copying the necessary files to the system, the installation process has completed successfully. To exit the installation wizard, click Finish.

To work with Repository Manager after installation, it must be configured. First it's necessary to configure the database, which is detailed in Step 5 – Configuring the Database.

Step 3: Installing the Player

The Player is a handy tool for playback of recording files. It can be installed independently of RecordTS onto any Windows machine for convenient playback.

How to install the Player:

1. Run the setup file RecordTS-Player.msi. The installation wizard will start. Close all other programs and click Next.
2. Carefully read the license agreement. If you agree to the terms, select the check box to confirm acceptance of the agreement. To continue, click Next. To exit Setup, click Cancel.
3. To start the installation program, click Install Now. If you would like to go back and change any settings, click Back. To exit Setup, click Cancel. To go back and change any of the prior settings, click Back. To exit Setup, press Cancel.
4. Once the installer finishes copying the necessary files to the system, installation of the player has successfully completed. To exit the installation wizard, click Finish.

To start Player, on the Start menu, select All Programs, RecordTS, and then click RecordTS Player. It can now be used to open recording files to view, and convert them into other formats such as AVI or SWF.

Step 4: Configuring RecordTS

After you have installed the RecordTS Agents, you can now launch the RecordTS MMC snap-in and further configure the RecordTS Recorders.

How to configure the RecordTS Agent:

1. To open RecordTS MMC snap-in, from the Start menu click All programs, RecordTS, and then RecordTS Configuration. To open the configuration manager, from the Action menu select Properties.
2. To change the folder where all recorded sessions will be stored, on the Storage tab enter a valid path into the Default Storage Folder textbox. This can be only a local path.
3. To change the path template used for the subfolders that will be created under the local storage root folder, on the Storage tab enter a template in the textbox. The default template is: `{Domain}\{User}\{ConnectedDate:yyyy.MMMMMM}\{ConnectedDate:dddddd}\{ConnectedTime:HH-mm-ss}`
4. You can select an action that you want RecordTS to take in case the storage folder is out of disk space. By default RecordTS prevents new connections to the system and disconnects all users on the system. If you prefer, you can choose to disable session recording (not recommended).
5. To prevent tampering of the recording files, from the Security tab you can determine if RecordTS should digitally sign all recorded files. You must have a valid certificate stored on your Terminal Server in order to perform this action.
6. To enable digital signing of recording files you should:
7. check Digitally sign all recordings from the Security tab;
8. click Select to indicate the security certificate to be used.

By default RecordTS records all sessions established to the machine. If you want to specify only certain users to be recorded, from the Users tab, make sure you select Only for users listed below. After this you can add users you want record to the list by clicking Add.

If you want to specify only certain computers to be recorded, from the IP Filter tab, make sure you select Only for IP addresses listed below. After this you can add the IP-addresses of the machines you only want to record to the list by clicking Add.

Step 5: Configuring the Database

Once installed, the RecordTS service will appear on the server. The RecordTS service monitors all connections to this server and records the sessions and saves the recording files in a special directory. In order to manage repositories located on different computers, or to manipulate recordings and view them, you will need to set up and initialize the RecordTS database. Without the use of the database, the supervisor will only be able to view files from storages by using the RecordTS Player.

How to configure the database:

1. To open the Database Configuration Tool in the Start menu, select All programs, RecordTS, and then click the Repository Configuration Tool.
2. In the dialog, the system will offer you two options settings: Create a New Database, and Specify an Existing One. If you select an existing database, it can be located on a remote SQL server. Click the appropriate link.

How to create a new database:

1. To create a new database, you need to install Microsoft SQL Server 2005 (or equiv.) and administrator rights to it. If these conditions are satisfied, click Next. If SQL Server is not installed, you must download it and install it. For installation instructions, click How to install SQL Server in the setup wizard.
2. In the drop-down list, select the SQL server on which you want to create a database. To make the server appear in the list of available SQL servers after its installation, you must manually start the SQL Server. To do this, do the following:
 - a) Click Start, All Programs, Microsoft SQL Server 2005, Configuration Tools, and click the Configuration Manager SQL Server.
 - b) In SQL Server Configuration Manager, expand the Services and in the details pane, locate the named instance of SQL Server. Right-mouse-click over the named instance and select Properties.
 - c) In the Properties dialog box, SQL Server on the Service tab, you must change the startup mode of service. To do this, set the startup mode to Automatic - this service needs to start automatically at system startup. To save changes, click Apply.
 - d) To start the service, open the Log On tab, click Start. The green arrow icon next to the name of the server and on the toolbar indicates that the server startup was successful.
 - e) Click OK to close the Configuration Manager SQL Server.

3. After starting the SQL Server service, click the button right of the name of the server to update the server list. Wait until the list is updated, and then select SQL Server.
4. Select the necessary authentication mode used to connect to an instance of SQL Server.

During setup, you must select an authentication mode for the Database Engine. There are two possible modes: Windows Authentication mode and mixed mode. Windows Authentication mode enables Windows Authentication and disables SQL Server Authentication. Mixed mode enables both Windows Authentication and SQL Server Authentication. Windows Authentication is always available and cannot be disabled.

If you select Mixed Mode Authentication during setup, you must provide and then confirm a strong password for the built-in SQL Server system administrator account named sa. The sa account connects by using SQL Server Authentication.

If you select Windows Authentication during setup, Setup creates the sa account for SQL Server Authentication but it is disabled. If you later change to Mixed Mode Authentication and you want to use the sa account, you must enable the account. Any Windows or SQL Server account can be configured as a system administrator. Because the sa account is well known and often targeted by malicious users, do not enable the sa account unless your application requires it. Never set a blank or weak password for the sa account.

When a user connects through a Windows user account, SQL Server validates the account name and password using the Windows principal token in the operating system. This means that the user identity is confirmed by Windows. SQL Server does not ask for the password, and does not perform the identity validation. Windows Authentication is the default authentication mode, and is much more secure than SQL Server Authentication. Windows Authentication uses Kerberos security protocol, provides password policy enforcement with regard to complexity validation for strong passwords, provides support for account lockout, and supports password expiration. A connection made using Windows Authentication is sometimes called a trusted connection, because SQL Server trusts the credentials provided by Windows.

When using SQL Server Authentication, logins are created in SQL Server that are not based on Windows user accounts. Both the user name and the password are created by using SQL Server and stored in SQL Server. Users connecting using SQL Server Authentication must provide their credentials (login and password) every time that they connect. When using SQL Server Authentication, you must set strong passwords for all SQL Server accounts.

5. Click Test Connection to try to connect to SQL server using the chosen authentication mode and check the user rights for creating new database. In the dialog box the system will report the result. If the connection is successful, click Next. If the connection could not be established, check your SQL server.
6. In the field New Database type the name of the new database. Click Next.
7. Check the name of the database and SQL server name. If everything is correct, then click Next to create the database.
8. Wait until the process of creating a database completed. The installation process can be viewed in the consolidated journal wizard. If the process of creating a database completed successfully, click Next.
9. To close the wizard database, click Finish. After configuring the database you can proceed to configure the Repository Manager and Web Console.

Note

If the wizard has a green sign next to the component, configuration completed successfully. If there is a red sign, it means that the component still needs to be configured.

How to use an existing database:

1. In the drop-down list, select the SQL server that contains the desired database.
2. Click the button near the Database field to update the list of databases that exist on the selected server. Select a database.
3. Select the necessary authentication mode used to connect to an instance of SQL Server.

During setup, you must select an authentication mode for the Database Engine. There are two possible modes: Windows Authentication mode and mixed mode. Windows Authentication mode enables Windows Authentication and disables SQL Server Authentication. Mixed mode enables both Windows Authentication and SQL Server Authentication. Windows Authentication is always available and cannot be disabled.

If you select Mixed Mode Authentication during setup, you must provide and then confirm a strong password for the built-in SQL Server system administrator account named sa. The sa account connects by using SQL Server Authentication.

If you select Windows Authentication during setup, Setup creates the sa account for SQL Server Authentication but it is disabled. If you later change to Mixed Mode Authentication and you want to use the sa account, you must enable the account. Any Windows

or SQL Server account can be configured as a system administrator. Because the sa account is well known and often targeted by malicious users, do not enable the sa account unless your application requires it. Never set a blank or weak password for the sa account.

When a user connects through a Windows user account, SQL Server validates the account name and password using the Windows principal token in the operating system. This means that the user identity is confirmed by Windows. SQL Server does not ask for the password, and does not perform the identity validation. Windows Authentication is the default authentication mode, and is much more secure than SQL Server Authentication. Windows Authentication uses Kerberos security protocol, provides password policy enforcement with regard to complexity validation for strong passwords, provides support for account lockout, and supports password expiration. A connection made using Windows Authentication is sometimes called a trusted connection, because SQL Server trusts the credentials provided by Windows.

When using SQL Server Authentication, logins are created in SQL Server that are not based on Windows user accounts. Both the user name and the password are created by using SQL Server and stored in SQL Server. Users connecting using SQL Server Authentication must provide their credentials (login and password) every time that they connect. When using SQL Server Authentication, you must set strong passwords for all SQL Server accounts.

4. Click Test Connection to try to connect to SQL server taking into account the chosen mode of authentication. In the dialog box the system will report the result. If the connection is successful, click OK to close the wizard. If the connection could not be established, check your SQL server.

Step 6: Configuring Repository Manager

Repository Manager's main function is to move recording files from the computers they are created on to other storage devices for long term storage, back up archival and protection. If you choose not to install Repository Manager then you will need to manage the recording files manually. Recording files are created on each of the computers that RecordTS is installed, and will eventually fill the resident local hard drive. Repository Manager can automatically handle the task of periodically moving existing recording files from their local storages to other storage devices.

How to configure Repository Manager

1. To run Repository Configuration Tool, on the Start menu, click All programs, RecordTS, and then click the Repository Configuration Tool.
2. If the database is already configured (noted in the wizard), click Run Repository Manager Configuration Tool, to start the Configuration Tool. If not then you must first set up the database.
3. Click Next.
4. Make sure that all necessary conditions for configuring Repository Manager are made, that is, marked by a green sign, and in the Status field should indicate successful. If any condition is not fulfilled, it will be marked in red and in the Status field will be error, and in the field, Error Report, will contain a link which can help determine the cause of the error. If you have problems, contact technical support. If all conditions are satisfied, click Next.
5. Select the user from whose account Repository Manager will run. It is necessary to ensure safe access to the database, as the rights required will be assigned only to the user. Select "Use an existing account" or "Create a new one".

Select an existing user:

- a) Select the Use an existing account.
- b) Click Select to select an account.
- c) In the dialog box, select the desired account. If the computer is in the domain, it is advisable to choose a domain account so that the Repository Manager can have all the rights to work with other computers in the domain. If your computer is not joined to a domain, you must select a local account. Click OK.
- d) Provide a password for the selected account.
- e) Click Next.

Create a new user

- a) Select Create a new user

- b) Enter User's full name and the name of his account.
- c) Choose the type of account. If the computer is in the domain, it is advisable to create an domain account so that the Repository Manager can have all the rights necessary to work with other computers on the domain. If your computer is not in a domain, you must create a local account.
- d) Enter a password for the new account. See Guidelines for creating strong passwords. Remember this password.
- e) Enter the password again to confirm.
- f) Click Next.

If all the required fields are filled and the passwords match, the configuration process continues.

6. Select the type of service start up for the Repository Manager. To set the service to start automatically at startup, select Automatic. To run it manually, select Manual. Click Next.
7. Verify that the specified parameters are correct, select Set permissions to assign the necessary rights to the selected account to allow the SQL server to access the database. Click Test Connection to test the connection to SQL server. If the connection is successful, click Next. If the connection fails, click Back to change the current settings.
8. Check the consolidated list of changes to be made in the system. To continue, click Next.
9. Wait until the configuration process has completed. If there are problems encountered during configuration then causes can be found in the consolidated log. If the configuration process completed successfully, click Next.
10. Configuration of Repository Manager has completed. Select Open the Repository Manager Configuration, if you want to start the Repository Manager Configuration after you complete the wizard. To close the wizard, click Finish.

Immediately after configuration, Repository Manager it is not yet ready to use. You still need to register all existing Recorders and setup tasks to move recording files, etc.

How to register a Recorder

1. Start the Repository Manager Configuration. To do this, on the Start menu, select All Programs, RecordTS, and then click Repository Manager Configuration.
2. In the console tree, expand the RecordTS Repository Management and then click Recorders.
3. In the action pane, click Add Recorder.

OR

On the Action menu click Add Recorder.

4. In the dialog box, click Next to begin the registration of a Recorder.
5. Select the computer where the Recorder is running (RecordTS has been installed). Specify the directory where the recording files are being stored. Click Next.
6. Enter the name of a share folder where the files will be stored , and its description. Click Next.
7. To assure the Repository Manager has access to a specific repository, you must assign access rights.
8. Specify the name of the Recorder and the name of its stores, or leave the default settings. These names will appear in the list of Recorders and storage list respectively. Click Next.
9. Registering of a Recorder is complete. Click Finish to close the dialog.

To view all registered Recorders in the console tree, expand RecordTS Repository Management and click Recorders. In the details pane the Recorder list will appear.

To see all the storages in the console tree, expand RecordTS Repository Management and click Storages. In the details pane all active and archive storages will appear.

After the above actions, all new files that appear in storages of registered Recorders will be added to the database. This is the only task of the Repository Manager, the current default. To change the set of operations with the store, you must create a new task for the Repository Manager.

How to create a task for the Repository Manager

1. Start the Repository Manager Configuration.
2. In the console tree, expand the RecordTS Repository Management and click Jobs.
3. In the action pane, click Create Job.

OR

In the Action menu, click New Job.

4. In the dialog box on the Basic Properties tab, specify the title of the job, its type and all fields needed to be filled in accordance with the selected type. If necessary, you can write a detailed comment on the task of describing what it does.
5. On the Schedule tab, select the necessary option. Fill in additional fields if necessary. In the Description box, check the result.
6. Select Delete when finished and Retry a failed execution, if necessary. Click OK. New task in an active mode should appear in the details pane.

When you create a job to move or delete files, it is required to specify a filter on which files will be selected for these operations. By default, the Repository Manager contains the only filter: All files.

How to create a filter

1. Start the Repository Manager Configuration.
2. In the console tree, expand the RecordTS Repository Management and click Filters.
3. In the action pane, click Create Filter.

OR

In the Action menu click Create Filter.

4. In the dialog box on the General Properties tab, specify the filter name and a detailed comment describing what this filter is designed to do.
5. Click on the Criteria. You can use it to manage the list of criteria for the filter: add new, edit or delete existing one. To create a new criterion, click Add.
6. In the presented list, select the necessary type of criteria for filtering files. Click Select. In accordance with the selected type in the box, fill in the fields you want to set the filter parameters.
7. Specify the necessary parameters and the comparison operation on the basis of which will be filtered. Click OK.
8. If necessary, edit the created filter.
9. To complete the creation of a filter, click OK. After closing the dialogue, the new filter should appear in the left column of panels of detailed actions.

Step 7: Configuring Web Console

Web Console provides a convenient way to view recording files and specific details about them using a web browser. It also allows searching for recordings filtered by various parameters, such as file size, start time, end time, duration, etc.

System Requirements

Before you configure Web Console, make sure that IIS Server v5.5 or later is installed along with RecordTS Repository Manager.

How to configure Web Console

1. To open Web Console Configuration Tool, on the Start menu, select All programs, RecordTS, and then click the Repository Configuration Tool.
2. If the database is already configured (marked by a sign in the configuration wizard), click Run WebConsole Configuration Tool, to start the Web Console Configuration Tool. If not, then you must first set up the database.
3. Click Next.
4. Make sure that all necessary conditions for Web Console configuration are met, that is, marked by a green sign, and the Status field should indicate successful. If any condition is not fulfilled, it will be marked in red and in the Status field will be an error. The field Error Report will contain a link which can help you determine the cause of the error. If you have problems, contact technical support. If all conditions are satisfied, click Next.
5. Specify the settings for the Web site. You can leave the default IP address. If the Web server has more than one web site configured, then enter the host name to contact the Web Console. Otherwise, if you only specify an IP Address, the Web server will not be able to determine which application should be run. Click Next.
6. Select the user to run Web Console, making sure they will be given sufficient rights to access data and display them. For security purposes, it is desirable to specify a user other than the one that was selected for the archive services, as Web Console requires far fewer privileges. Select, Use an existing account or Create a new one.

Select an existing user

- a. Select Use an existing account.
- b. Click Select to choose a specific account.
- c. In the dialog box, select the desired account. If the database is located on the local computer, you can choose a local account. If the database is located on another

computer in the domain, you must specify a domain account to access it. Click OK.

- d. Provide a password for the selected account.
- e. Click Next.

Create a new user

- a) Select Create a new user
 - b) Enter Users's full name and the name of his account.
 - c) Choose the type of account. If the database is located on the local computer, you can choose a local account. If the database is located on another computer in the domain, you must specify a domain account to access it.
 - d) Enter a password for the new account. Remember this password.
 - e) Enter the password again to confirm.
 - f) Click Next.
 - g) If all the required fields are filled and the passwords match, the configuration process will continue.
- 7) Select the location of the group "RTSAdmins". Members of this group will have the right to access to the Web Console. Therefore, if the computer is in the domain, and you want to have access to the Web Console from any computer in that domain, but also have the right to create a domain group, then enter the Domain group. In any other case, specify the Local Group. Click Next.
- 8) See a list of changes that will be made in the system during the configuring process. To continue, click Next.
- 9) Wait until the configuration process completed. If any problems occurred causes can be found in the consolidated log. If the configuration process completed successfully, click Next.
- 10) The process of Web Console configuration is completed. Select Start Web Console now to start the Web Console immediately after the completion of the wizard. Select Create a shortcut on the desktop to create a shortcut to the Web Console on the desktop. To close the wizard, click Finish.