
RecordTS Enterprise v7.0 for VMware Horizon

Installation Guide



<http://www.tsfactory.com>

Copyright Notice and Trademark

© 2024 TSFactory LLC. All Rights Reserved.

RecordTS and the TSFactory logo are registered trademarks or trademarks of TSFactory LLC, or its affiliated entities.

VMware, Horizon and the VMware logos are registered trademarks or trademarks of VMware, or its affiliated entities.

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.

Every effort has been made to ensure the accuracy of this manual. However, TSFactory LLC makes no warranties with respect to this documentation and disclaims any implied warranties of merchantability and fitness for a particular purpose. TSFactory LLC shall not be liable for any errors or for incidental or consequential damages in connection with the furnishing, performance, or use of this manual or the examples herein. The information in this document is subject to change without notice.

Version 1.2 – Updated February 6th, 2024

End User License Agreement

RecordTS by TSFactory LLC is protected by an End User License Agreement. To view the agreement, visit the company website at www.tsfactory.com, under RecordTS Documentation.

Contents

- Introduction 7**
 - What is RecordTS?7
 - Main Features.....7
 - Security/Audit compliance.....7
 - Developed for VMware Horizon7
 - Per user session recording7
 - How does RecordTS work?.....8

- Quick Overview 10**
 - Recorder10
 - Dashboard11
 - License Service11
 - Storage11

- Installing Base Modules 12**
 - Overview.....12
 - WARNINGS: Read This Before You Start...13
 - Prerequisites.....14
 - Step 1: Making a Place to Store Session Data15
 - RecordTS Storage Server.....15
 - How to Install the RecordTS Storage Server.....15
 - Step 2: Installing the RecordTS License Service19
 - How to install the RecordTS License Service.....19
 - Step 3: Installing the Dashboard Console service.....22
 - How to install the RecordTS Dashboard Console Service22
 - Step 4: Configuring Dashboard and the License Service25
 - Configuring Dashboard for RecordTS Storage Server25
 - Configuring Dashboard Security Access27
 - Configuring the RecordTS License Service.....28

- Installing Recorders 31**
 - Overview.....31
 - General process.....31
 - On-demand clones and instant clones:.....31
 - Recorder Types32
 - Prerequisites.....32
 - Installation Steps33
 - Pre-installation Requirements.....33
 - Installing the Recorder33
 - Configuring the Recorder.....37

- Playing Recorded Sessions 40**

- Optimizing RecordTS 42**
 - Dashboard Features42
 - Remote Dashboard Access42
 - Secure Web Access to Dashboard43
 - Enforce HTTPS only:45
 - Database Purging45
 - Retaining Sessions46

Session Playback Cache	46
Exporting the Session List	46
Setting up User Accounts	46
Adding Users.....	47
Editing Users.....	48
Deleting User Accounts	49
Importing User Accounts.....	49
Managing Imported User Accounts.....	51
Creating User Groups	52
Recorder Features.....	54
Buffer Settings.....	54
Remote Recorder Configuration Access.....	55
Secure Web Access to Recorder Config	55
Enforce HTTPS only:	58
RecordTS Storage Server Backup Tool	59
Help	59
Backup	60
Restore.....	60
Check	61
Info	62
Backup Tool Examples	63
Mapping a Network Drive.....	63
Examples	65
Support	67
How to get support	67
Dashboard Problems	67
Licensing Problems	68
Recorder Problems.....	68
List of Service Ports.....	68

This page intentionally left blank.

Introduction

What is RecordTS?

RecordTS is a remote desktop session recorder for Windows Terminal Services and VMware Horizon. What does it mean exactly? It means once installed on a server running VMware Horizon View Agent, administrators will be able to record everything users are doing during their sessions for later playback and/or archiving. It's pretty much the same as watching a video on your computer! Thanks to this product you can:

- Track who is connected to the server and see what they do.
- View selected recordings for a specific user, during a specific time period, etc.
- Track users actions that might have caused problems on a server.
- Save recorded sessions to the RecordTS Storage Server.

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. You can archive all recorded sessions for later playback, and in case of an audit it is just a matter of finding a particular session and watching!

Developed for VMware Horizon

Although other similar solutions do exist in the market, RecordTS is the first and only solution that integrates directly with VMware Horizon and up. This means increased performance and scalability, with much smaller recordings. RecordTS is NOT a screen capture program or screen scraper and is very difficult if not impossible to circumvent.

Per user session recording

Recorded sessions are saved individually on a per user basis. Recordings are stored in a database for later retrieval and replay.

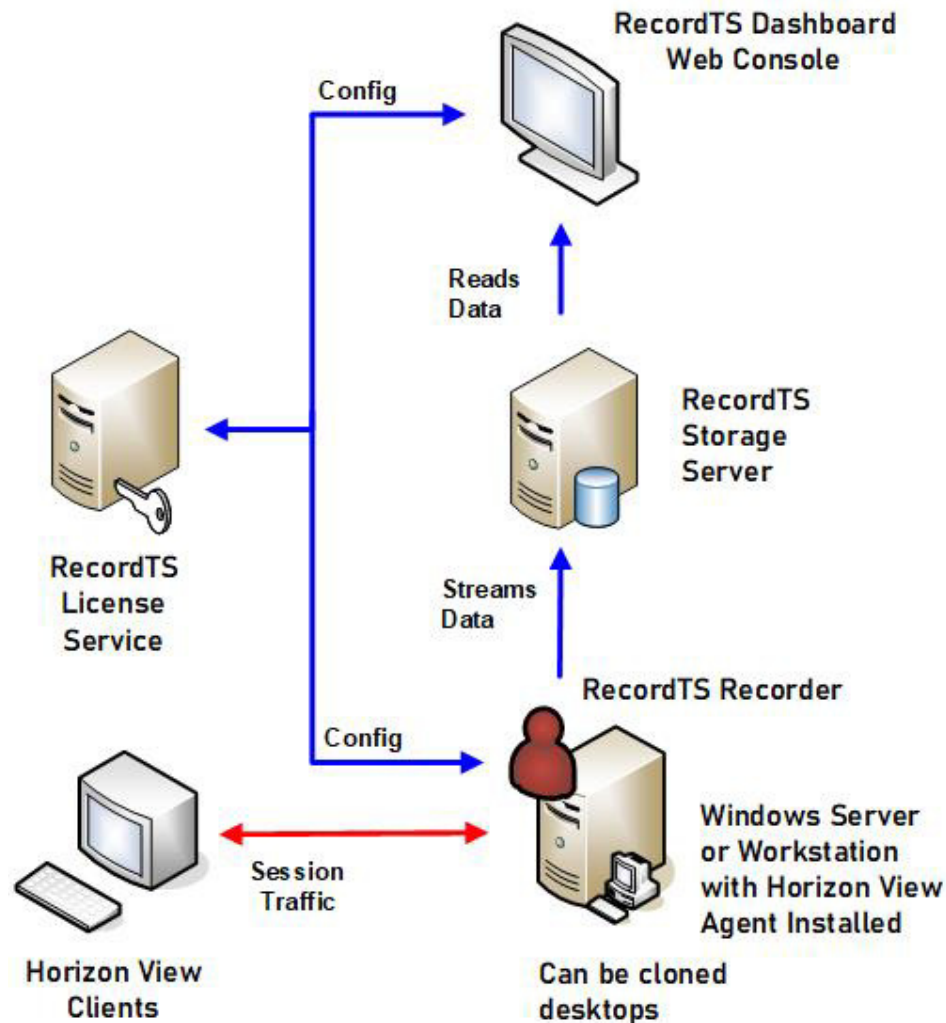
How does RecordTS work?

RecordTS integrates directly with VMware Horizon View Agent. Once a user connects remotely to a desktop or application, the session video is streamed to a central database. As RecordTS was developed from the ground up specifically for VMware Horizon, this process does not affect your server performance, scaling easily once more users and/or servers are added to the system.

Following are functional and network diagrams of typical network configurations of RecordTS v7 for VMware Horizon.

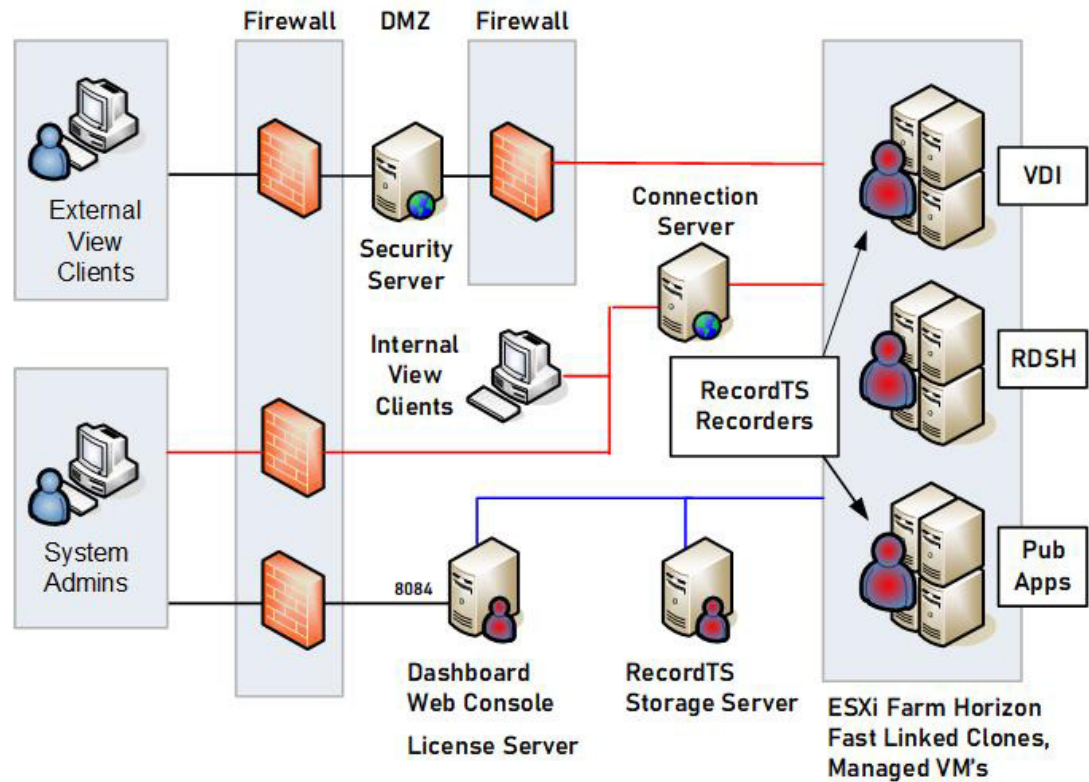
The next section will discuss the individual components in detail.

The diagram below shows only one Recorder, but there can be as many Recorders as needed. The upper limit on Recorders is dictated by database/storage server loading. Multiple database storages will be required to handle large server farms. Each recorder is installed on a Windows server or workstation with a Horizon View Agent.



**RecordTS v7 for VMware Horizon
Functional Diagram**

The following diagram shows a typical network layout of the RecordTS components integrated with the VMware Horizon architecture. Note that the Dashboard and License services are normally installed to the same machine and can be co-located with the database/storage server (however not recommended). For larger installations the database/storage server should be located on a separate machine to minimize loading when viewing sessions, enhance security and allow for larger drive space.



RecordTS v7 for VMWare Horizon View Network Configuration

Quick Overview

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

- **Recording Service (Recorder)**
- **Dashboard**
- **License Service**
- **Database / Storage Server**

Recorder

The basic component of RecordTS is the Recording Service or Recorder, installed on each of the target machines to be recorded. Its main job is to record remote user sessions and stream the video data to a central storage. From the time RecordTS Recorder is installed and properly configured on a Windows server or workstation with Horizon View Agent, each user session will be recorded and streamed to a database or storage server in a proprietary, very compressed video format. Recorded sessions will contain additional information about each session: computer name and IP address, user name, connection time and duration, etc. For each individual user, recorded sessions are stored separately.

The recorded sessions can be viewed or played as a video using the RecordTS Webplayer or exported to a common video format supported by most media players.

Dashboard

The RecordTS Dashboard is a web console app that allows the admin to centrally manage recorders, licensing and view recorded sessions. There is also statistics available for user and server usage. The Dashboard is where the admin can configure and manage the RecordTS License Service and authorize recorder installs on servers and other components such as additional dashboards and modules.

License Service

RecordTS implements a multi-mode based licensing scheme, where products can be purchased as a subscription, to use for a period of time (pay as you go). A software subscription must be purchased in order to authorize use of RecordTS software components.

During the trial period, the License server will allow as many servers and users that are needed for the trial period (usually 30 days). Once the trial expires, the system will stop recording until additional time is purchased.

NOTE: It is strongly suggested to purchase or renew subscriptions prior to expiration to avoid disruption of service.

Storage

RecordTS VMware Horizon Recorders stream session data to a central location for safe keeping and easy session playback. For high volume session recording, there is currently only one recommended option available for storing sessions:

- RecordTS Storage Server (included)

The RecordTS Storage Server must be setup and configured for use **prior** to installation of Dashboard and the Recorders. It is recommended to locate the storage system on a machine that has sufficient drive space available for storing session videos and network bandwidth to allow multiple session streams from the recorders to the storage server.

Session recording can be buffered in case the storage server becomes temporarily unavailable, slows down or the network becomes unstable, etc. Once connectivity to the database/storage is restored, buffered session data will be dumped to the storage server and normal operation will continue. If connectivity to the storage server is disrupted for extended periods of time, the buffers may fill completely and sessions will be suspended until connectivity to the storage server is restored.

Database session purging is available to automatically remove session videos past a specified number of days.

Installing Base Modules

Overview

RecordTS is made up of five major components: License service, Dashboard console, RecordTS Storage server, various Recorders and a session player. It is assumed a storage server is preinstalled and ready for remote connections and that the prerequisite software and configurations have been made prior to installing the RecordTS components.

The order of installation is as follows:

1. RecordTS Storage Server
2. License service
3. Dashboard console
4. Recorders

WARNINGS: Read This Before You Start...

Uninstall Older Versions

You cannot upgrade from older versions RecordTS (v5 or older) to RecordTS v7. You need to uninstall any older versions of RecordTS and reboot before installing v7. You can upgrade from v6 to v7.

Not on a RD or TS gateway

RecordTS is not intended to be installed on an RDGateway or TSGateway and may prevent either software from functioning properly.

Beware of AV, Endpoint Protection, Backup and Dictation Software

Some third-party software packages can interfere with the RecordTS recorder service installation and operation. Software such as antivirus, endpoint protection, backup and dictation software can prevent RecordTS from installing or recording properly.

- These packages must be completely disabled during installation.
- Some dictation software may need to be disabled or completely removed in order for RecordTS to operate properly.

Backup, Backup, Backup!

As with any new software, you should make a **complete backup** of the machines before installing RecordTS. This will enable you to quickly return the systems back to the way they were if you run into any problems.

Read This Manual

RecordTS is server-grade software, meaning it is intended for professionals that have a working knowledge of server and network management. There is a lot of useful and important information in this manual. Read it and save yourself some headaches and time. Get help if you have questions or need help installing and configuring RecordTS. There are some great trouble shooting tools towards the end of this manual.

Ask Questions

We are here to help you. If you are not sure about any aspect of how RecordTS works or is installed, then please contact our support department or one of our partners. You are probably not the first person to ask your question or be confused about this type of software. Servers are complicated and can be tricky to program. Contact us before installing or configuring so we can explain the process and help you have a great experience.

Prerequisites

VMware Horizon v7.5 or higher installed and properly configured and tested.

A functioning storage server, configured to accept remote connections.

For VMware Horizon, there is only one option:

RecordTS Storage Server	Installed anywhere that all components can access remotely
--------------------------------	--

At least 1 or 2 server grade machines:

1. Dashboard and license services installed with Windows Server 2016, 2019, 2022 or newer.
2. At least one Windows machine to log in remotely using the VMware Horizon View Client software.
3. A domain admin account (or equiv) that has access to all machines in the test.
4. **All machines must be part of the same domain under Active Directory IF you use Windows Authentication**
5. All machines must have their firewalls either turned off or properly configured with firewall rules to permit access for the RecordTS components to communicate with each other.
6. Certain programs such as antivirus and backup software can interfere with the proper installation and operation of RecordTS software, especially the recorders. It is strongly recommended to completely disable these programs on the recorded machines prior to installation. The antivirus and backup programs should be configured to ignore the RecordTS working folders and the RecordTS program processes if they are to be enabled after installation.

WARNING: RecordTS Single Server Edition cannot not be used for testing with VMware Horizon. The Single Server Edition will not work with VMware Horizon.

Upgrading: There is **no** upgrade path from older versions of RecordTS. All previous versions of RecordTS **must be removed** before installing v7!

Step 1: Making a Place to Store Session Data

The RecordTS for VMware Horizon Recorders will stream session data to a central storage area that must be setup and configured prior to installing any other components. You have only one option for storage:

- RecordTS Storage Server

RecordTS Storage Server

The RecordTS Storage Server may be installed on a machine by itself (preferred) or collocated with the RecordTS Dashboard/License services.

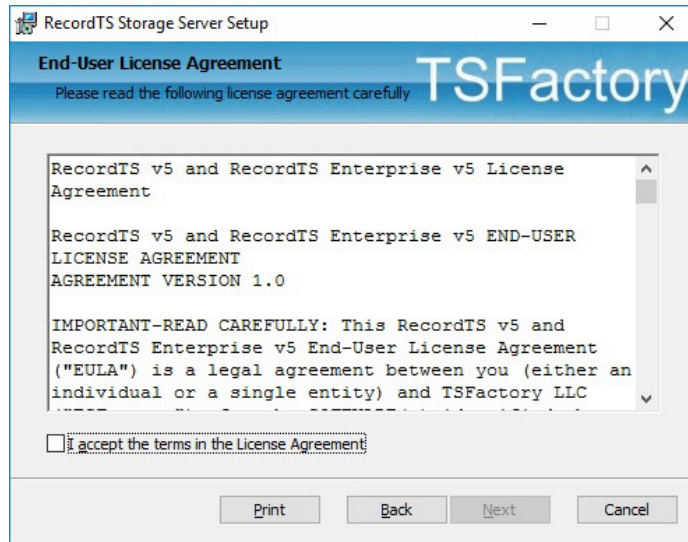
The server should be domain joined and have its firewall either disabled or configured to accept connections from the other RecordTS components. Also, plan for enough drive space to store the amount of sessions you would like to retain. Usually a terabyte or more is required.

How to Install the RecordTS Storage Server

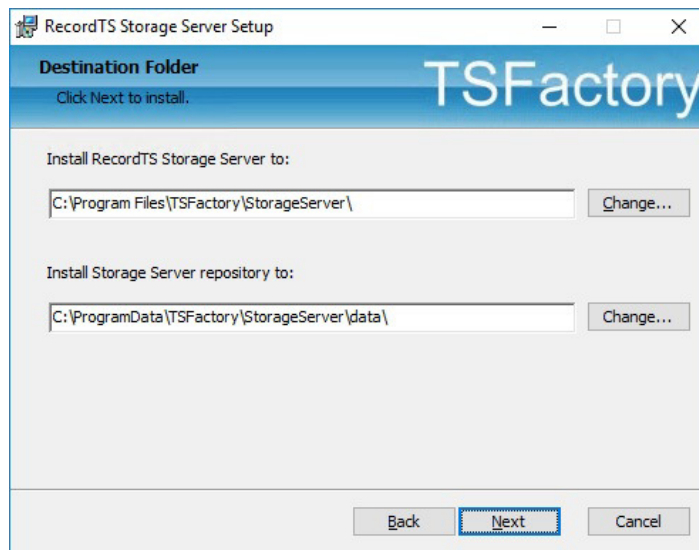
1. Download and run the RecordTS-Storage-Server-7.x.xxxx.msi installation file on the machine that the storage server is to reside. The installation wizard will appear. Close all other programs and then click Next.



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




2. Select the directory where the RecordTS storage server program files will be installed and where the data will be stored. Only local directories on the local machine can be used. If you do not want to use the default directory suggested by the installer, click Browse... to choose another directory. Then click Next.



3. Enter the credentials for a new admin account that will be created for you. This account will have sole access to the storage server and be required in the Dashboard and Recorder configurations.

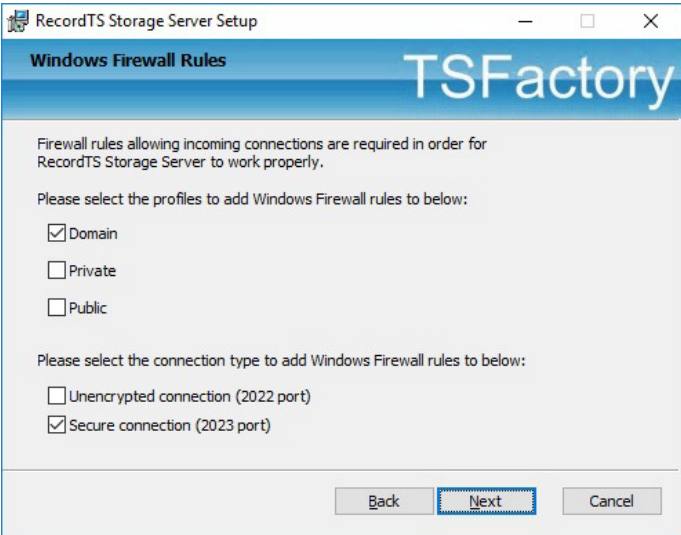
Important: Write down the admin credentials and keep in a safe place!



The screenshot shows a Windows-style window titled "RecordTS Storage Server Setup" with a blue header bar containing the "TSFactory" logo. Below the header, the text reads "Setup Storage Server Password" and "Please enter new storage server password". The main area contains three input fields: "Enter new login:" with the text "admin" entered, "Enter new password:", and "Confirm password:". At the bottom, there are three buttons: "Back", "Next" (which is highlighted with a blue border), and "Cancel".

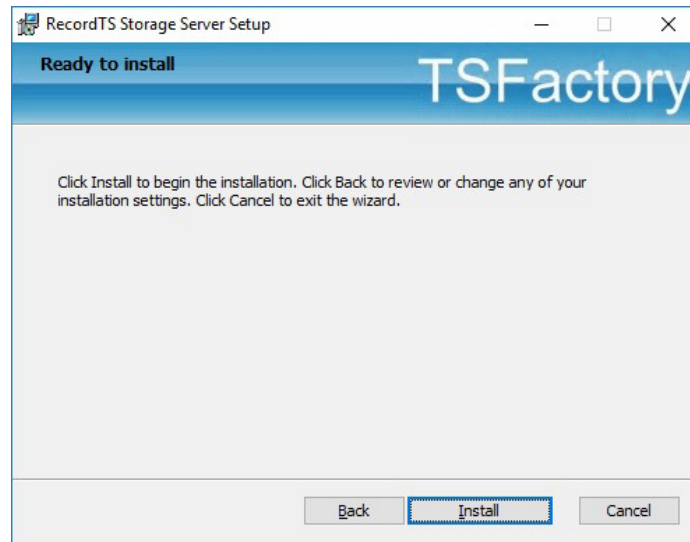
4. Configure firewall rules. Select the firewall profiles to add then select the connection type. Secure connection will allow encrypted traffic to the Storage Server from other components. This option must be configured on all components; otherwise unencrypted traffic will be used.

NOTE: You may check both connection types if you are unsure which type will be implemented, then later remove the unused firewall rule.



The screenshot shows a Windows-style window titled "RecordTS Storage Server Setup" with a blue header bar containing the "TSFactory" logo. Below the header, the text reads "Windows Firewall Rules". The main area contains the following text: "Firewall rules allowing incoming connections are required in order for RecordTS Storage Server to work properly." Below this, there are two sections. The first section is "Please select the profiles to add Windows Firewall rules to below:" with three checkboxes: "Domain" (checked), "Private" (unchecked), and "Public" (unchecked). The second section is "Please select the connection type to add Windows Firewall rules to below:" with two checkboxes: "Unencrypted connection (2022 port)" (unchecked) and "Secure connection (2023 port)" (checked). At the bottom, there are three buttons: "Back", "Next" (which is highlighted with a blue border), and "Cancel".

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 exit the installation wizard, click Finish.
7. The RecordTS Storage Server Service will appear in the Windows Services applet. Check to make sure the service is started.
You may now proceed to installing the License Service.

Step 2: Installing the RecordTS License Service

The RecordTS Dashboard may be installed on the same machine as the RecordTS license service. The box should be domain joined and have its firewall set, if enabled, to allow connections from Dashboard, the database server and recorders (other terminal servers and Windows machines being recorded).

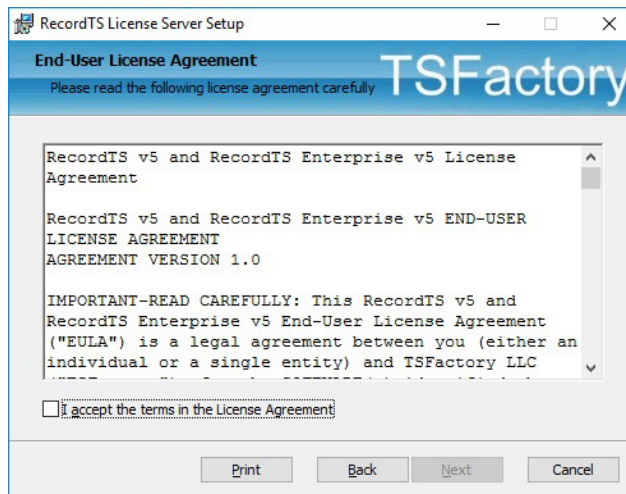
Note: after installing the RecordTS License Service, the service will appear in the Windows Services applet. It should be started.

How to install the RecordTS License Service

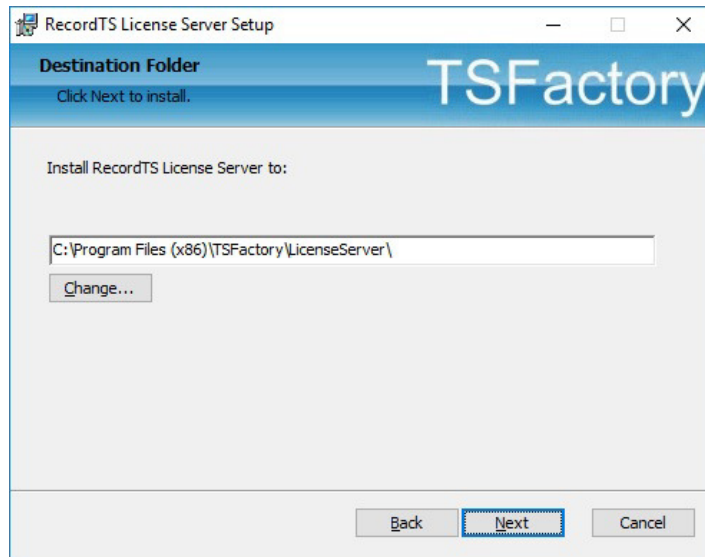
1. Download and run the RecordTS-LicenseServer-7.x.xxx.msi installation file on the machine that the license service is to reside. The installation wizard will appear. Close all other programs and then click Next.



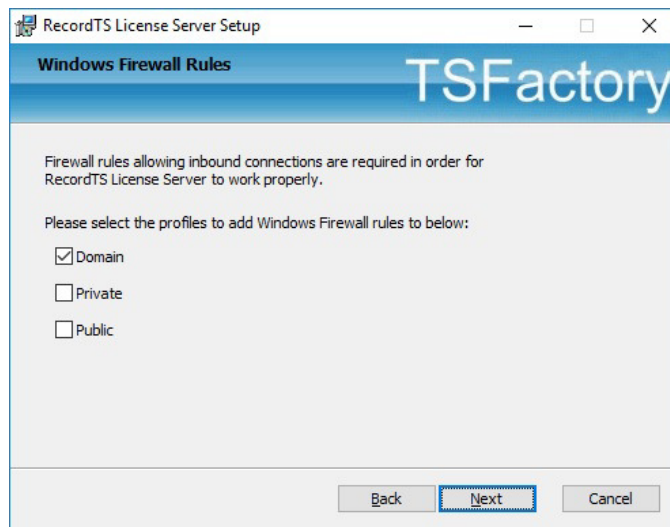
2. Carefully read the license agreement. If you agree to the terms, select the check box to confirm acceptance of the agreement. Click Next to continue installing. To exit Setup, click Cancel.



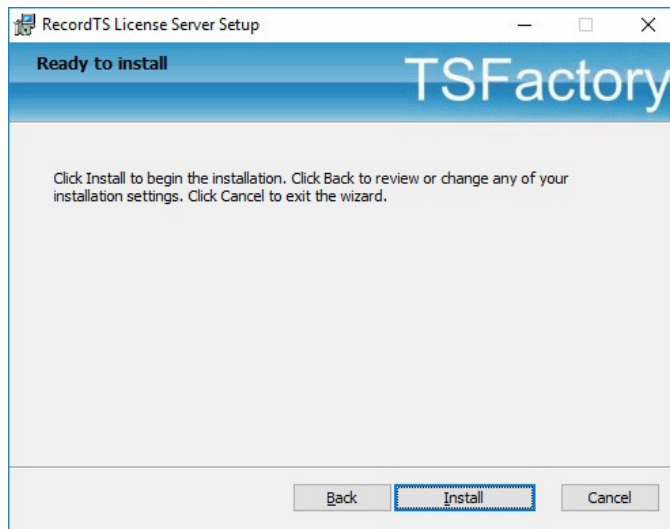
3. Select the directory where the RecordTS license service program files will be installed. Only local directories on the local machine can be used. If you do not want to use the default directory suggested by the installer, click Browse... to choose another directory. Then click Next.



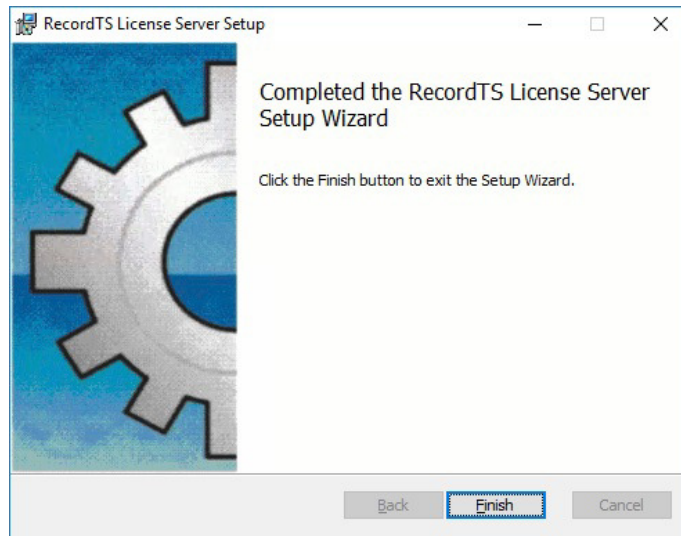
4. Select profiles to add firewall rules. This step will automatically add firewall rules to allow connections from other modules.



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 exit the installation wizard, click Finish.



7. The RecordTS License Service will appear in the Windows Services applet. Check to make sure the service is started. You may now proceed on to installing the Dashboard webconsole.

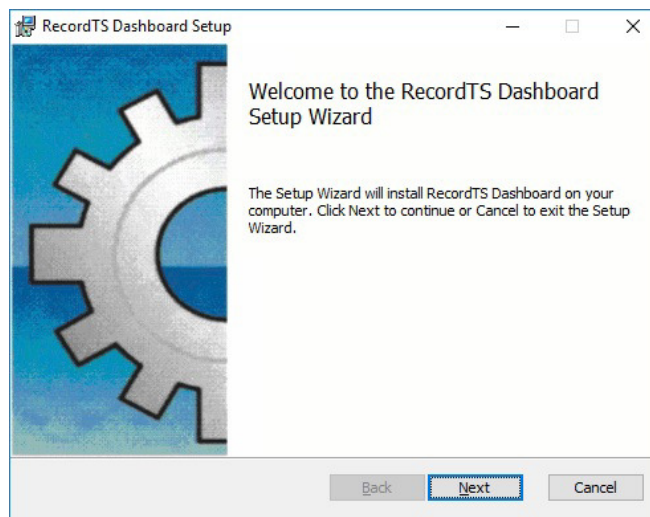
Step 3: Installing the Dashboard Console service

The RecordTS Dashboard Console Service must be installed on a Windows Server machine. RecordTS Dashboard may be installed on the same machine as the license service. The box should be domain joined and have its firewall configured (if enabled) to allow connections to the database server and from the recorders (other terminal servers and/or Windows machines being recorded).

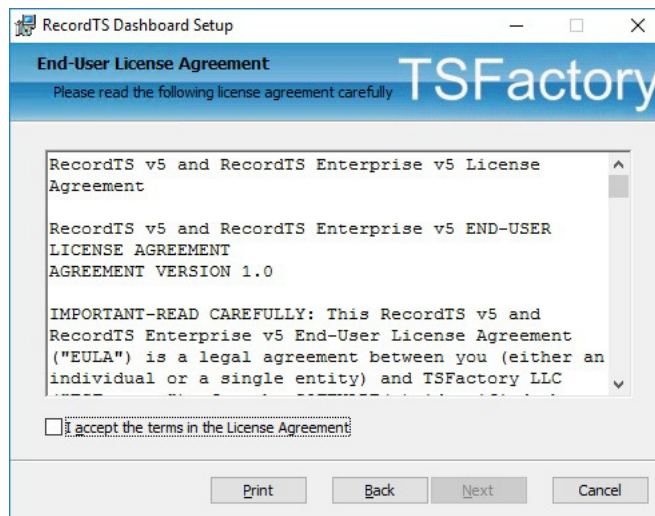
Note: after installing the RecordTS Dashboard Console Service, the service will appear in the Windows Services applet along with the RecordTS License Service, if installed, together on the same machine.

How to install the RecordTS Dashboard Console Service

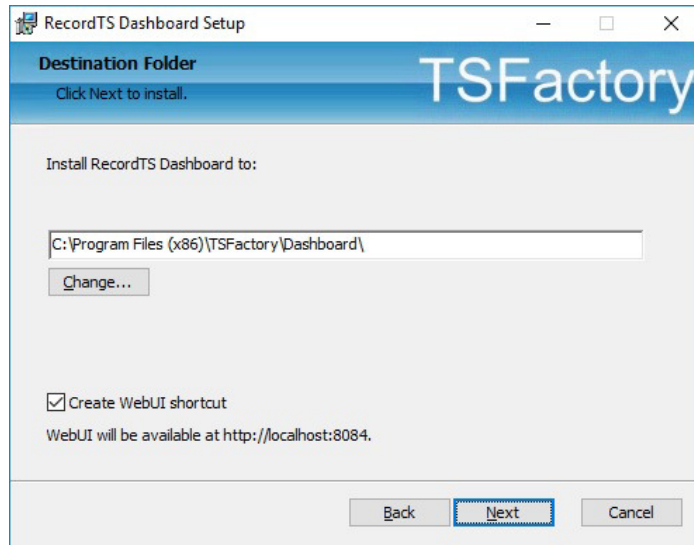
1. Download and run the RecordTS-Dashboard-7.x.xxx.msi installation file on the machine that the license service is to reside. The installation wizard will appear. Close all other programs and then click Next.



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.



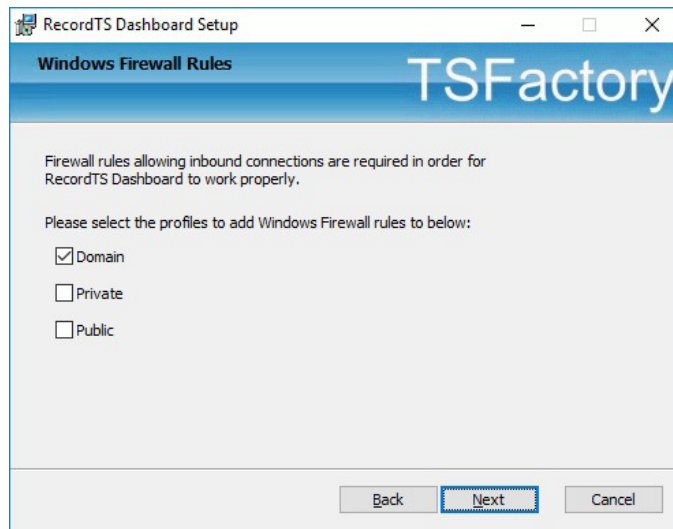
3. Select the directory where the RecordTS Dashboard service program files will be installed. Only local directories on the local machine can be used. If you do not want to use the default directory suggested by the installer, click Browse... to choose another directory.



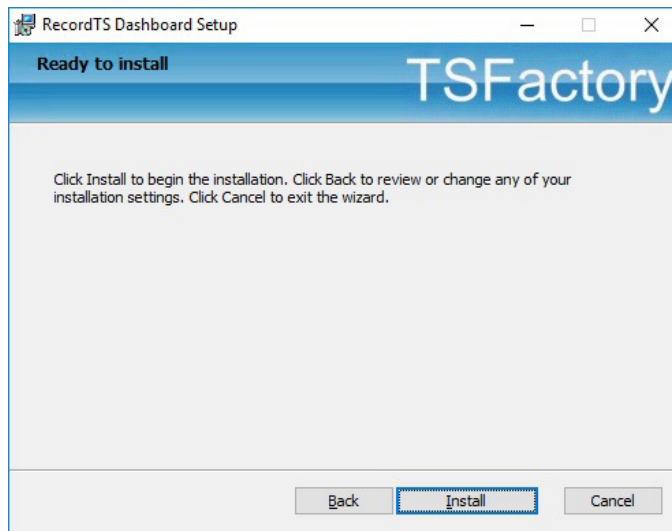
You may uncheck “Create WebUI Shortcut” to prevent installing shortcuts to each user’s application list. You can access the Dashboard webUI with this URL: <http://localhost:8084>.

Click Next to continue.

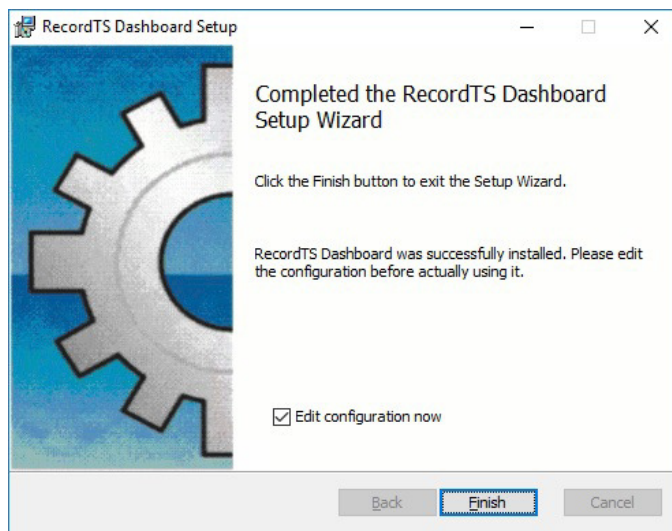
4. Select profiles to create firewall rules for. Click Next to continue.



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.



7. Uncheck the “Edit configuration now” checkbox.
8. To exit the installation wizard, click Finish.

You may now continue on with configuring the Dashboard and license services.

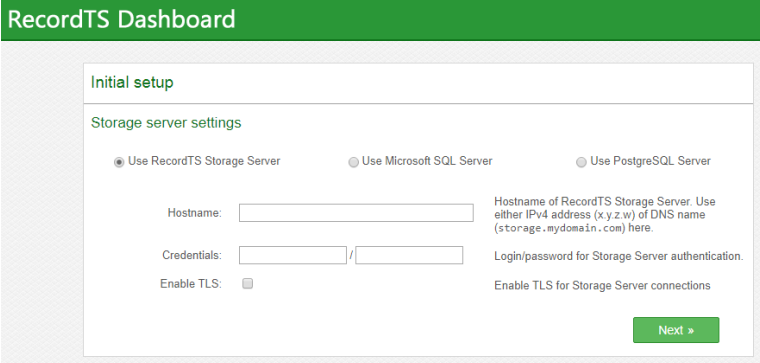
Step 4: Configuring Dashboard and the License Service

The RecordTS Dashboard Console is used to configure the RecordTS license service and various other components to do the following:

- ✓ Connect to the database/storage server to create a database (if none exists), and manage it.
- ✓ Authorize RecordTS software components for use, such as the recorders, remote user connections and all Dashboard instances, along with future RecordTS integrated products and components.
- ✓ Display a list of recorded sessions for the user to browse and play back.
- ✓ Setup user accounts to control access to Dashboard.
- ✓ Display licenses and usage information.

Configuring Dashboard for RecordTS Storage Server

1. Display the Dashboard console by locating the program shortcut in the programs list and selecting it.
2. The Dashboard Console should display in the default browser window. If it fails, then a possible problem could be that another program is using the assigned port 8084. This can be changed in the base configuration. Contact support for help with this.
3. First thing to configure is the storage server settings. RecordTS Storage Server should be selected. Change this if it is not. (see figure 3-1)

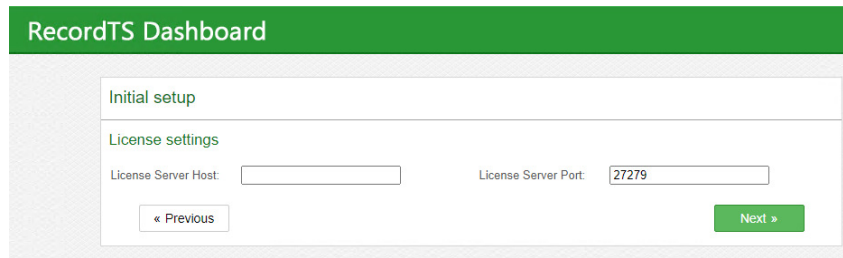


The screenshot shows the 'RecordTS Dashboard' interface with a green header. Below the header is a white box titled 'Initial setup'. Inside this box, there is a section for 'Storage server settings'. It features three radio buttons: 'Use RecordTS Storage Server' (selected), 'Use Microsoft SQL Server', and 'Use PostgreSQL Server'. Below these are three input fields: 'Hostname' (with a placeholder), 'Credentials' (split into two fields), and 'Enable TLS' (with a checkbox). To the right of the 'Hostname' field is a small text box explaining that the hostname can be an IPv4 address or a DNS name. To the right of the 'Credentials' fields is a text box indicating they are for login/password authentication. To the right of the 'Enable TLS' checkbox is a text box indicating it enables TLS for connections. A green 'Next >' button is located at the bottom right of the form.

Figure 3-1: Storage Server Settings

4. Enter the host server name where the Storage Server is installed, admin username and password that was used during install of the storage server. Click Next to continue.
5. The next thing to configure is the license server. Enter a hostname in the License Server Host field. You may use “localhost” as the value if the License Server is installed on this machine. Leave the License Server Port as the default value of 27279, unless it presents a port conflict, then change it and write down the new

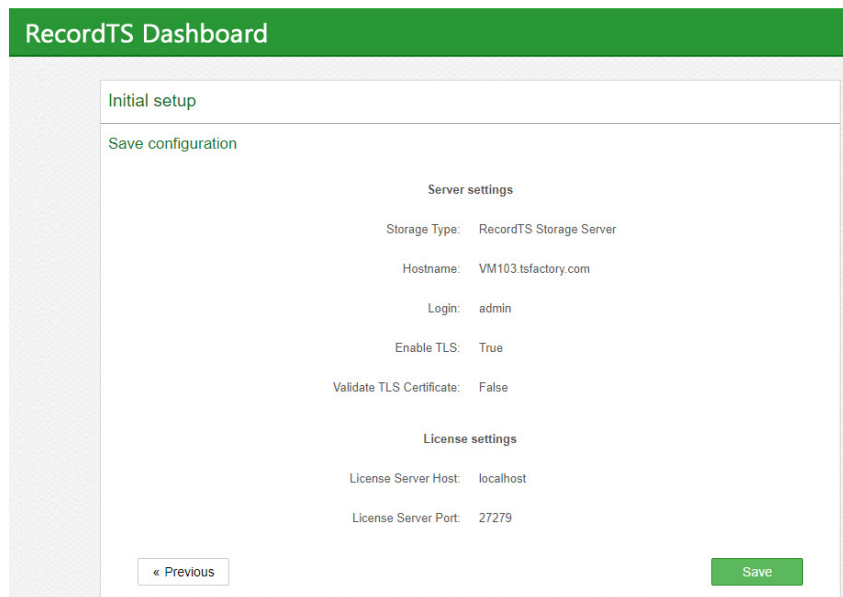
value and remember to update all other instances when asked (like in the Recorder setup).



The screenshot shows the 'RecordTS Dashboard' interface. At the top is a green header with the text 'RecordTS Dashboard'. Below the header is a white box containing the 'Initial setup' section. Underneath, there is a 'License settings' section with two input fields: 'License Server Host' (empty) and 'License Server Port' (containing '27279'). At the bottom of this section are two buttons: '« Previous' and 'Next »'.

Figure 3-2: License Server Settings

6. You should now be presented with a summary of the Storage Server database settings. Click Save if they are correct, otherwise click Previous to go back and change settings.



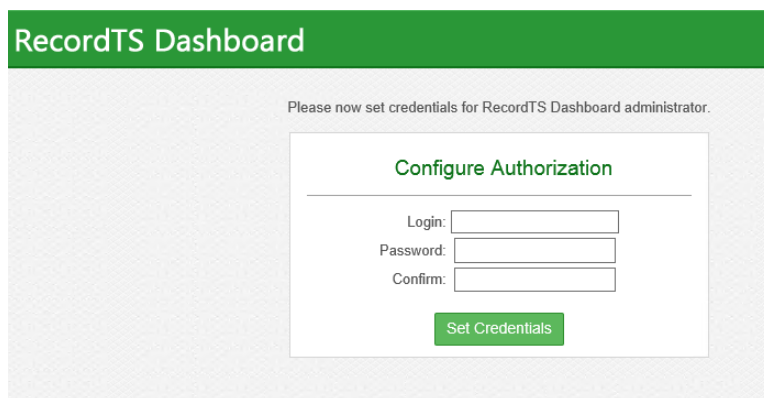
The screenshot shows the 'RecordTS Dashboard' interface. At the top is a green header with the text 'RecordTS Dashboard'. Below the header is a white box containing the 'Initial setup' section. Underneath, there is a 'Save configuration' section. This section is divided into two parts: 'Server settings' and 'License settings'. The 'Server settings' part includes: 'Storage Type: RecordTS Storage Server', 'Hostname: VM103.tsfactory.com', 'Login: admin', 'Enable TLS: True', and 'Validate TLS Certificate: False'. The 'License settings' part includes: 'License Server Host: localhost' and 'License Server Port: 27279'. At the bottom of this section are two buttons: '« Previous' and 'Save'.

Figure 3-3: Confirming Storage Server Settings

Move on to configuring Dashboard security access.

Configuring Dashboard Security Access

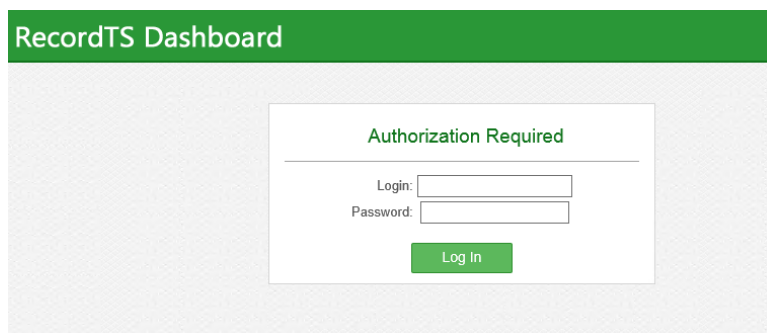
After saving the database settings, you will be required to enter administrative logon credentials for both Dashboard and License Server access. Enter a username and password for administrative access to the Dashboard webconsole (see figure 4-1).



The screenshot shows the RecordTS Dashboard interface. At the top, there is a green header with the text "RecordTS Dashboard". Below the header, a message reads "Please now set credentials for RecordTS Dashboard administrator." In the center, there is a white box titled "Configure Authorization". Inside this box, there are three input fields: "Login:", "Password:", and "Confirm:". Below these fields is a green button labeled "Set Credentials".

Figure 4-1: Creating Dashboard Administrator Credentials

Log into the Dashboard webconsole using the credentials entered in the previous step. Make sure you write down the username and password and store them in a secure place (see figure 4-2).



The screenshot shows the RecordTS Dashboard interface. At the top, there is a green header with the text "RecordTS Dashboard". Below the header, there is a white box titled "Authorization Required". Inside this box, there are two input fields: "Login:" and "Password:". Below these fields is a green button labeled "Log In".

Figure 4-2: Logging into the Dashboard Webconsole

After logging into the Dashboard webconsole, some warnings will be displayed. This is normal. Refer to figure 4.3.

NOTE: The warning messages will clear once the license service is configured properly.

1. Set the Security setting "Connections allowed" to "From any computer" to allow remote session playback from other computers.
2. Click Save Config

Continue on to configuring the License Server.

Figure 4-3: Saving the Dashboard Configuration.

Configuring the RecordTS License Service

1. If the License Service is located on a different server then enter that server name in the License Server Host field. You should leave the default port value unless it was changed.
2. Click on the Licensing tab and you should be presented with license service administrator logon credential fields (see figure 4-4).
3. Enter a username and password for the License Service administrator. This is NOT a Windows user account. You will need to enter the password a second time in the Confirm field.
4. HINT: Save these credentials in a safe place!
5. Click Set Credentials.

Figure 4-4: Creating Licensing Administrator Credentials

6. You will be presented with a logon screen (along with the same warning messages). Enter the administrator credentials from step #3 and hit the logon button to log into the License Server admin screen (see figure 4-5).

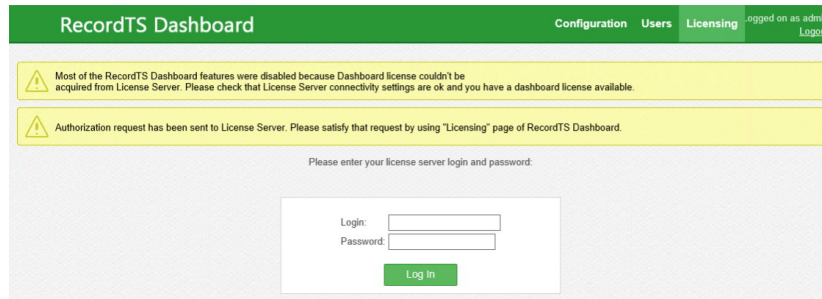


Figure 4-5: Logging into the Licensing Page

7. At this point the license service can run in Trial Mode for 30 days, unlicensed. After this it will require a license key OR subscription ID code. There are three license modes:
 - (a) Unlicensed, the license server goes into TRIAL MODE for 30 days, after which it will disable all modules if no license or subscription ID is entered.
 - (b) A subscription license.

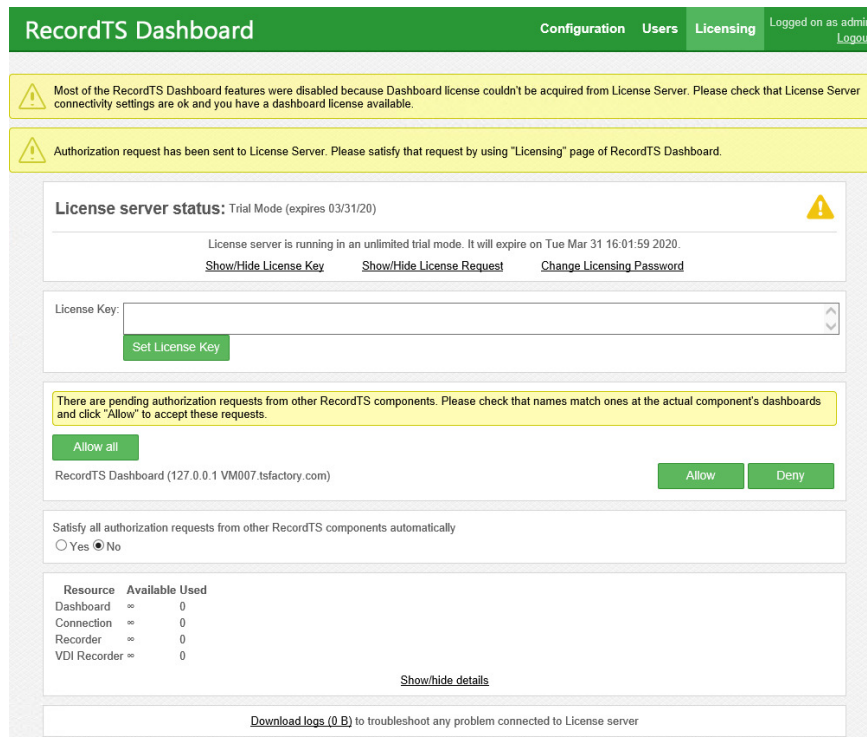


Figure 4-6: Authorizing the License Service

8. For convenience, you may select “Yes” to automatically authorize license requests from all modules for the “Satisfy all authorization requests” option.

Enabling Auto Authorization instructs the license server to automatically accept any authorization requests from all modules. This relieves you of having to manually authorize requests and is also good for on-demand instant clones where random repeated requests are expected.

9. If you are running the Trial, then move on to step 12.
10. If you have a license key, enter it into the License Key field and click on Set License Key.
11. The license service should report it has been authorized and is up and running.

NOTE: This process can take up to 5 mins.

12. The license service should now have an authorization request for Dashboard itself. Refer to figure 4-6. Click on the Allow button.

This process can take several minutes so refresh the window periodically until all the warning messages disappear.

13. Once the messages are gone, the Dashboard should be fully functional and the License Service should be ready to accept authorization requests from other components such as recorders (see figure 4-7).

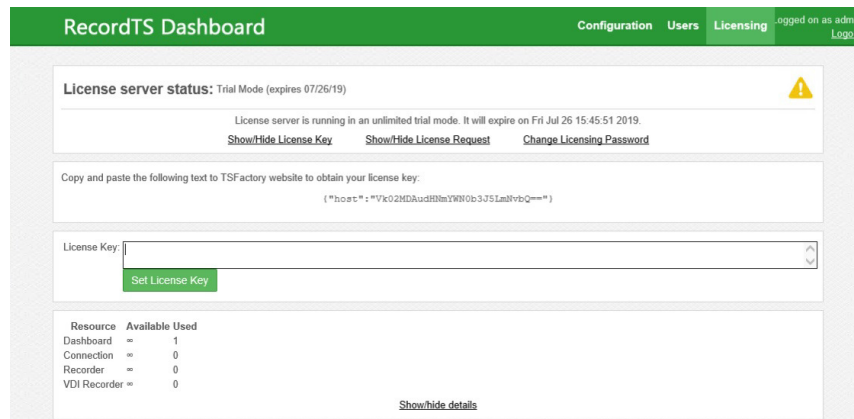


Figure 4-7: Fully Authorized Configuration in Trial Mode

It is now time to begin installing the recorders.

Installing Recorders

Overview

In order to record remote sessions on a Windows server or workstation, a RecordTS “recorder” must be installed on each machine you wish to record. Once a recorder is installed and properly configured, a recorder server license will be pulled from the general pool of recorder licenses held by the RecordTS license service.

For fast linked clones, the master VM should have a recorder installed and configured on it, then deployed to the Desktop group and pushed.

There will be brief interruptions in service while the recorders are being authorized by the license service and the overall configuration process is completed.

Please plan for down time while installing recorders in a production environment.

General process

1. Update firewall rules and disable antivirus software
2. Install recorder software *
3. Configure and test database/storage connectivity
4. Configure and test license server connectivity
5. Save the configuration (service will restart)
6. Authorize recorder in Licensing tab of Dashboard console **

IMPORTANT: The RecordTS license service can take up to several minutes to verify and authorize the recorder.

* remote connections will be lost during a system reboot

** sessions will not be recorded by the recorder until it is authorized

On-demand clones and instant clones:

Enable the Auto Authorization feature located on Dashboard / Licensing page. This will allow the license server to automatically authorize all requests from recorders.

Recorder Types

There is currently one type of recorder for RecordTS v7. This new recorder should be used for Horizon and any other desktop or published application. Only one recorder should be installed on each VM to be recorded.

NOTE: The RecordTS v7 recorder will work in any hosted environment and any version of Horizon, on a Windows server or workstation, cloned, etc.

Prerequisites

- ✓ RecordTS Dashboard and License Service installed and configured, ready to authorize and license recorders.
- ✓ A functioning RecordTS Storage Server, configured to accept remote connections (the same one used with Dashboard).
- ✓ A Windows server or workstation with properly configured firewall and VMware Horizon View Agent.
- ✓ Enable Auto Authorization feature of License Server

NOTE: Please refer to the TSFactory support website for up to date information or contact our support team with concerns or questions prior to installation.

Installation Steps

Pre-installation Requirements

FIREWALL: On the machine to be recorded, verify the firewall is either turned off or let the recorder installer create the necessary rules to allow the recorder service to operate (see support section at the end of this document).

ANTIVIRUS: Temporarily disable any antivirus programs that can interfere with the installation of the recorder service. Also, configure the antivirus program to ignore the recorder service and its working directories. Very important for Windows Server 2016!

ENDPOINT PROTECTION: Temporarily disable any endpoint protection programs that can interfere with the installation and operation of the recorder service. Also, configure the endpoint protection program to ignore the recorder service ports and its working directories.

Installing the Recorder

1. Download and run the RecordTS-Recorder-VMware-7.x.xxxx.msi installation file on the machine that is to be recorded, which should have the Horizon View Agent installed.

The installation wizard will appear. Close all other programs and then click Next.



Figure 5-1: Installing the Recorder

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.

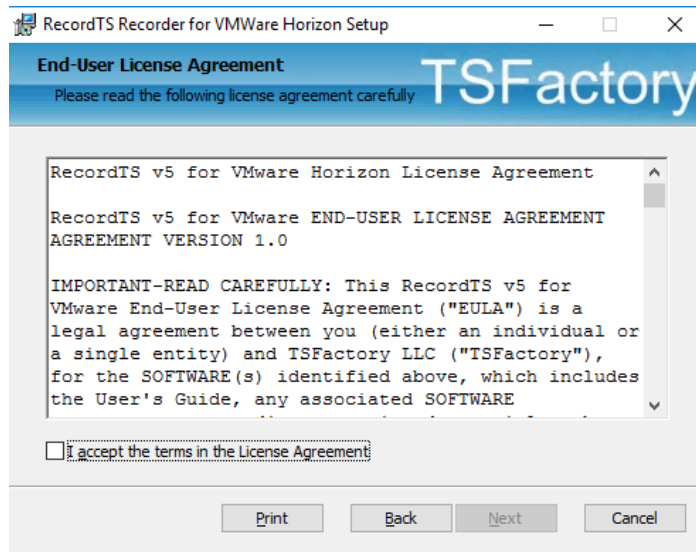


Figure 5-2: Accepting the License Agreement

3. Select the directory where the RecordTS recorder service program files will be installed. Only local directories on the local machine can be used. If you do not want to use the default directory suggested by the installer, click Browse... to choose another directory. You may uncheck "Create WebUI Shortcut" to prevent installing shortcuts to each user's application list. You can access the Dashboard webUI with this URL: <http://localhost:8086>.

Click Next to continue.

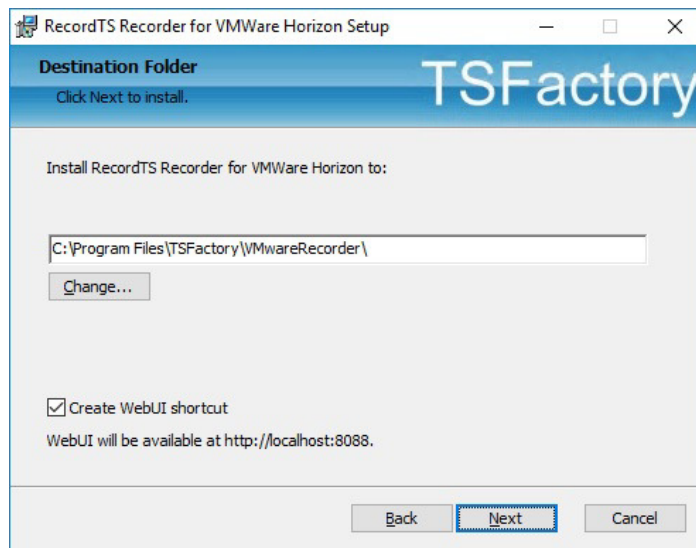


Figure 5-3: Selecting the Installation Directory

4. Select firewall rules to be created. Check the profiles to create firewall rules for this Recorder. The installer will automatically create the necessary rules to allow other components to communicate with the Recorder service.

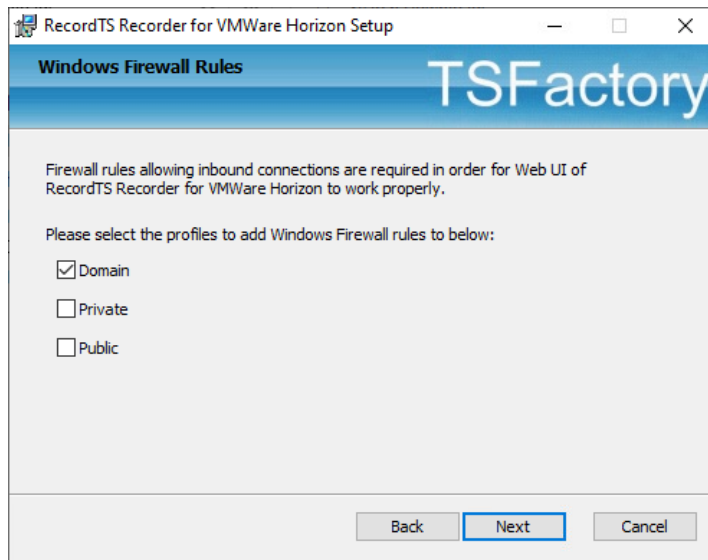


Figure 5-4: Creating firewall rules.

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.

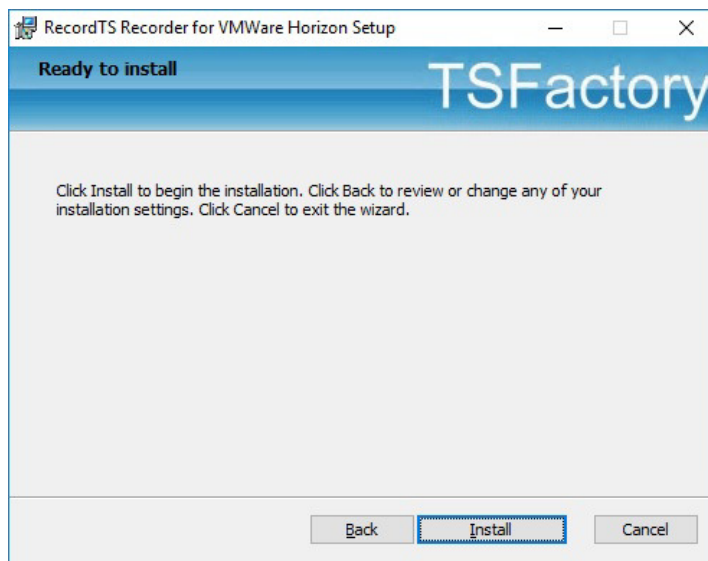


Figure 5-5: Beginning the Recorder Installation

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



Figure 5-6: Completing the Recorder Installation

7. Windows may ask you to restart the server. Select Yes to restart the server.

NOTE: Restarting the server while logged in remotely will terminate your session. Please use the local console for the following steps.

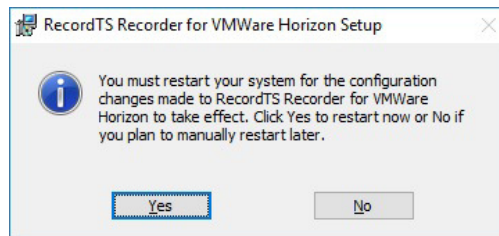


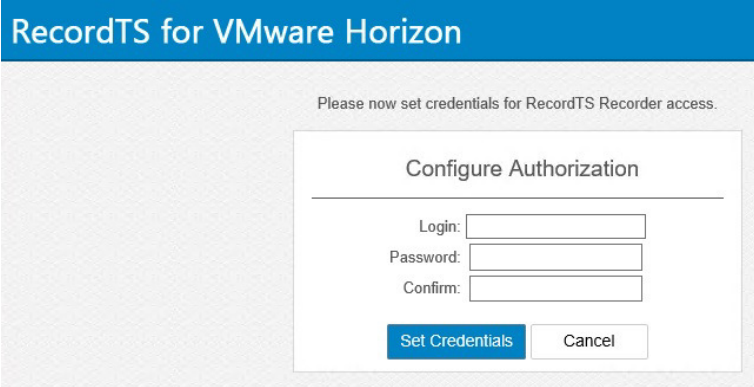
Figure 5-7: Restarting the System

Configuring the Recorder

- Find and open the Recorder Configuration shortcut in the RecordTS program group. If you elected not to install shortcuts, then you can open a browser and enter this URL:

http://localhost:8086

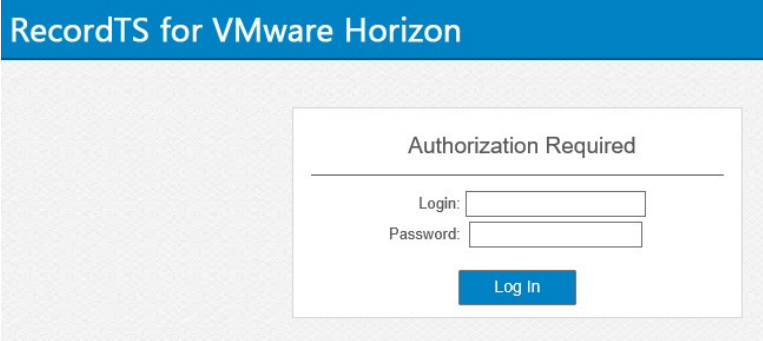
You will be requested to configure authorization access to the Recorder Configuration console. Enter a login and password (twice), then click on Set Credentials. Keep this information in a safe place for future reference.



The screenshot shows a web interface for 'RecordTS for VMware Horizon'. At the top, there is a blue header with the text 'RecordTS for VMware Horizon'. Below the header, a message reads 'Please now set credentials for RecordTS Recorder access.' The main content area contains a white box titled 'Configure Authorization'. Inside this box, there are three input fields: 'Login:', 'Password:', and 'Confirm:'. Below these fields are two buttons: 'Set Credentials' (highlighted in blue) and 'Cancel'.

Figure 5-8: Recorder Security Configuration

- You will be asked to enter the credentials from the previous step to gain access to the Recorder Configuration.



The screenshot shows a web interface for 'RecordTS for VMware Horizon'. At the top, there is a blue header with the text 'RecordTS for VMware Horizon'. Below the header, a message reads 'Authorization Required'. The main content area contains a white box with two input fields: 'Login:' and 'Password:'. Below these fields is a blue button labeled 'Log In'.

Figure 5-9: Accessing the Recorder Configuration

- Once you gain access to the Recorder Configuration, you should see the configuration console appear as seen in figure 5-10 below.

! Please provide database connection details.
Change the initial value of server and database to your real server and database name.

Database Settings

Storage Server: ?

Credentials: / ?

Enable TLS: ?

License Server

License Server Host: ? License Server Port: ?

Buffer Settings

Memory buffer size: MB ? File buffer: Enable: ?

Security

Connections allowed: From local computer only From any computer ?

Enable HTTPS: ?

Figure 5-10: Recorder Configuration Console

11. Enter the database/storage fields as they were entered in Dashboard and test for connectivity.
12. Enter the License Server hostname. You may leave “localhost” if the License Server is installed on this machine.
13. It is not recommended to change the License Server port address unless it was changed during configuration at the Dashboard.
14. Test for license server connectivity.
15. Set the Buffer Settings – enable if you intend to use this feature.
16. Now that all the settings have been entered and tested, click on Save Config. The service will restart.
17. The recorder configuration console should raise a warning that the recorder requires authorization from the license server. If it does not, refresh the window.

RecordTS for VMware Horizon Logged on as admin
[Change password](#) [Logout](#)

! Failed to allocate server lease for this recorder. Client connections won't be accepted. Please check that license server is up and running and there are enough concurrent server licenses available.

! Authorization request has been sent to License Server. Please satisfy that request by using "Licensing" page of RecordTS Dashboard.

Database Settings

Storage Server: ?

Credentials: / ?

Enable TLS: ?

License Server

License Server Host: ? License Server Port: ?

Buffer Settings

Memory buffer size: MB ? File buffer: Enable: ?

Security

Connections allowed: From local computer only From any computer ?

Enable HTTPS: ?

Figure 5-11: Recorder Configuration Console

On-Demand Clones and Instant Clones:

You will need to install the recorder on the master image and verify licensing authorization before publishing.

1. If you have enabled “Satisfy all authorizations requests” option in Dashboard / Licensing page, then the pending authorization warning should disappear in 1-2 minutes. You can advance to step 17 otherwise proceed with the next step.
2. Go to the Dashboard console and satisfy the recorder authorization request by clicking on the Allow button.

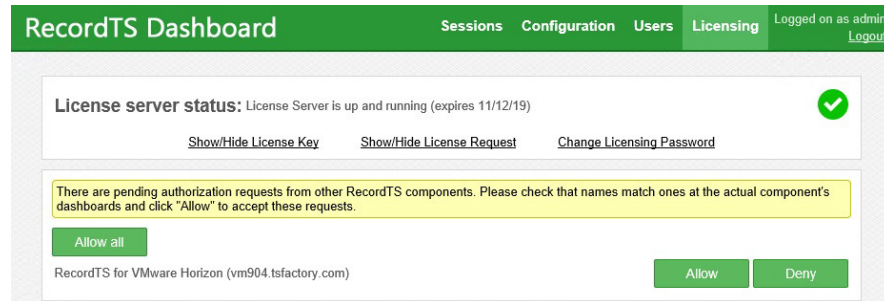


Figure 5-12: Recorder authorization request at Dashboard

18. Return to the recorder configuration console and refresh the window. You may need to log in again. **DO NOT CLICK SAVE.** When the error message clears, usually within 5 minutes, the recorder should be ready to accept connections and record.
19. Verify functionality by connecting remotely using the Horizon client and look for a session to appear in the Dashboard console Sessions tab.
20. The recorder should be up and running now. Continue for all remaining recorders.

Playing Recorded Sessions

The WebPlayer is a handy tool for playback of recording files. It does not require installation and only requires a browser on any Windows machine for convenient playback. User must have security access to the Dashboard to play back sessions.

How to view sessions locally:

1. Enter the Dashboard Console and navigate to the Sessions tab.

Id	Start date	Start time	End date	End time	User name	User domain	Session host	Client name	Data size	Don't purge	Protocol
1	07/16/19	00:21:05	07/16/19	00:22:45	user0	TSEFACTORY	MORTY		1.09 MB	<input type="checkbox"/>	MP4 Play Export

2. Locate a session to view.
3. Click on Play and your session will begin playback in a new browser tab.
4. Click on Export to export a session to disk in a standard video format (MP4) which can be played in most media players.
5. Close the tab when done viewing.

How to view sessions remotely:

1. Make sure the Dashboard Security setting "Connections allowed" is set to "From any computer" to allow remote session playback from other computers
2. From a remote browser, enter the following URL:

<http://Dashboard:8084>

Where Dashboard should be replaced with the actual Dashboard hostname or IP address.

3. Once the Dashboard Console appears, log in and navigate to the Sessions tab.
4. Click on Play and your session will begin playback in a new browser tab.

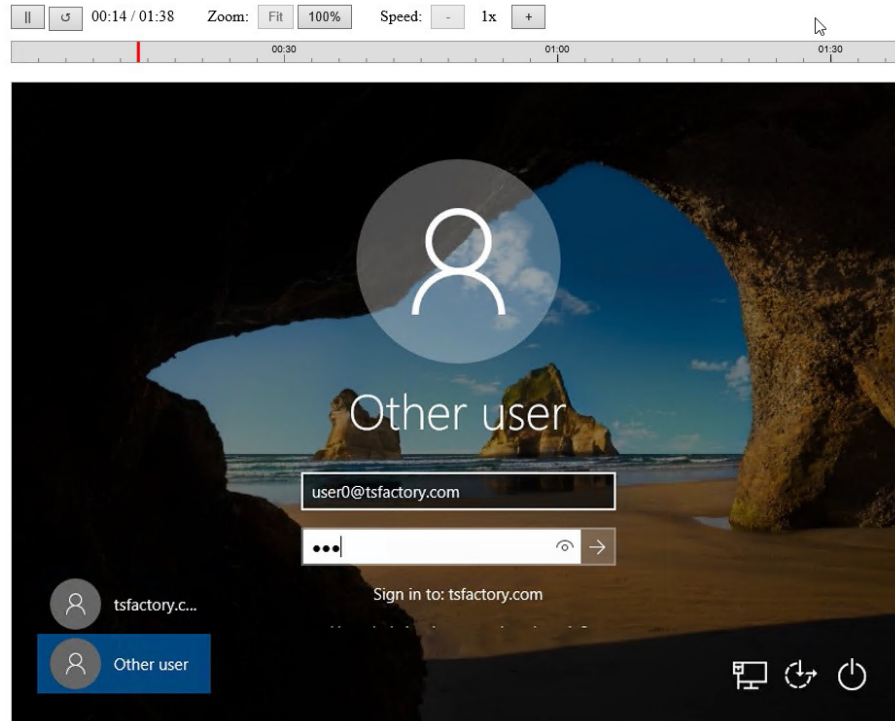


Figure 6-1: Viewing a Session in the WebPlayer

The video window can be resized to full screen for better viewing.

Most browsers offer exporting which is another way to save individual videos to disk in an MP4 video format. Below is an example of Internet Explorer v11 popup menu where you can save the video to disk.

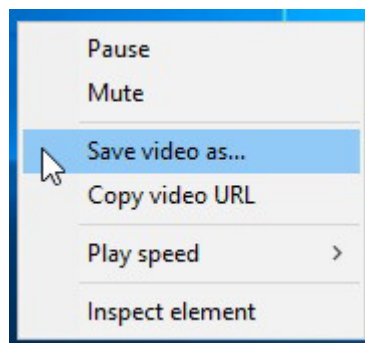
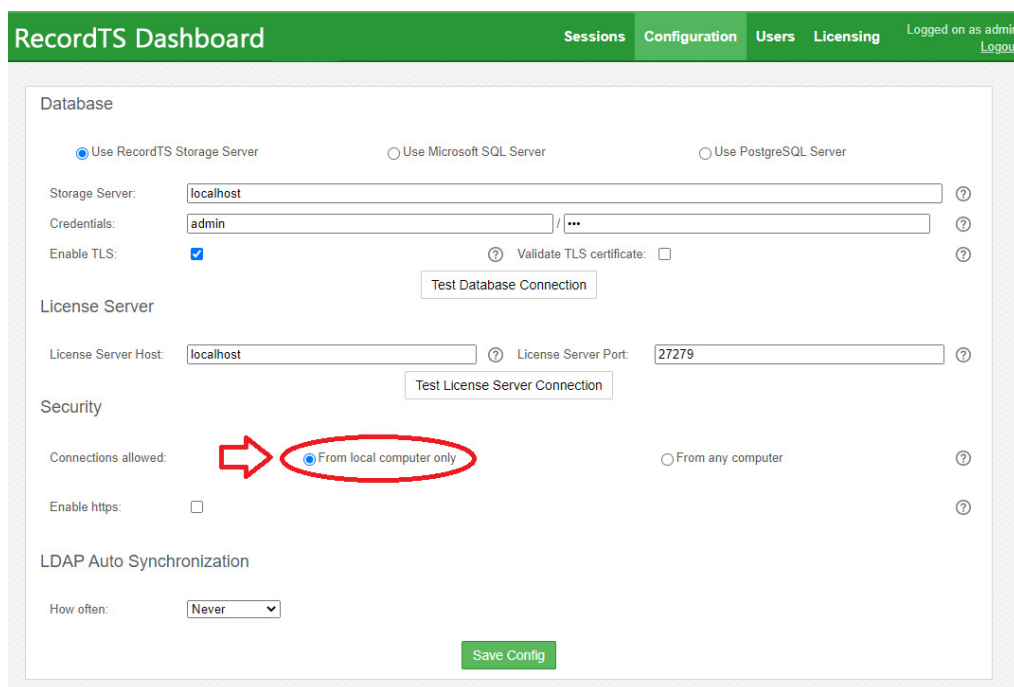


Figure 6-2: IE v11 Popup Menu

Optimizing RecordTS

Dashboard Features

There are many ways to optimize performance and take advantage of special features of RecordTS. Let's start by looking at the Dashboard webconsole Configuration page:



The screenshot shows the RecordTS Dashboard Configuration page. The top navigation bar includes 'Sessions', 'Configuration', 'Users', and 'Licensing', with a user logged in as 'admin'. The main configuration area is divided into sections: Database, License Server, Security, and LDAP Auto Synchronization. In the Security section, the 'Connections allowed' setting is currently set to 'From local computer only', which is highlighted with a red circle and a red arrow pointing to it. Other settings include 'Storage Server' (localhost), 'Credentials' (admin), 'Enable TLS' (checked), 'License Server Host' (localhost), and 'License Server Port' (27279). A 'Save Config' button is located at the bottom right of the configuration area.

Figure 7-1: Allowing remote access to Dashboard

Remote Dashboard Access

The “Connections allowed” feature lets you connect remotely to Dashboard from another computer using a browser. Select the “From any computer” to allow connections from other computers.

NOTE: Changing this feature will reduce security by allowing foreign computers to have access to the Dashboard configuration pages.

This feature is useful if you want to manage Dashboard remotely or allow others the ability to view recorded sessions from their desktop. To view sessions remotely, the user will need security access to the Dashboard prior to viewing any sessions.

To connect remotely, the user will need access permission to connect to the Dashboard machine. Refer to section “Setting up User Accounts further down this chapter. In a browser on the user’s desktop, enter this URL: <http://Dashboard:8084/config> where Dashboard should be replaced with the actual Dashboard hostname or IP address.

Secure Web Access to Dashboard

The “Enable https” option allows configuring Dashboard to accept secure browser connections using SSL/TLS (https).

Click on the Enable https checkbox to show the entire list of options for this feature:

Enable HTTPS:	<input checked="" type="checkbox"/>
Enforce HTTPS only:	<input type="checkbox"/> Visit this webconsole over HTTPS to make this option available
	<input checked="" type="radio"/> From file <input type="radio"/> Generate self-signed
Public certificate:	<input type="text"/> Browse ?
Certificate chain	<input type="text"/> Browse ?
Private key:	<input type="text"/> Browse ?

Figure 7-2: Enabling HTTPS access

There are three options to providing SSL certificates for secure web browsing:

1. Self-signed certificate
2. Customer generated certificate signed by hosted Certificate Authority such as Active Directory
3. Public certificate signed by a trusted Certificate Authority such as Godaddy, Thawte, etc.

The first item can be automatically generated by RecordTS Dashboard. The other two are provided by the customer.

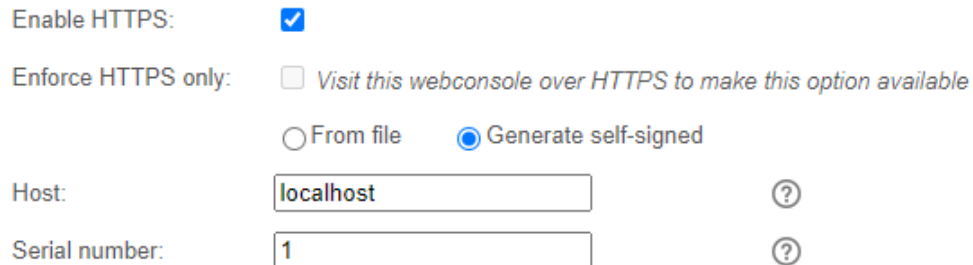
NOTE: Details for creating certificates for use with Dashboard https can be found in a separate document “Securing RecordTS Web Interfaces”. Contact our support staff for a copy of this document or visit our website.

Option #1 – Self-signed certificates

This is the simplest way to create certificates for https, but also the least secure as some browsers such as Firefox will not trust self-signed certificates.

There are a few steps to this process – generate the certificate, download the public certificate and copy it to any machines that will be accessing Dashboard remotely. The public certificate must be installed into the Windows Trusted Root CA store on each client machine.

Step 1: Click on Generate self-signed checkbox. You should see the screen change as depicted below:



The screenshot shows a configuration form for generating a self-signed certificate. It includes the following elements:

- Enable HTTPS:** A checkbox that is checked with a blue checkmark.
- Enforce HTTPS only:** A section with three options:
 - An unchecked checkbox followed by the text *Visit this webconsole over HTTPS to make this option available*.
 - A radio button labeled "From file".
 - A selected radio button labeled "Generate self-signed".
- Host:** A text input field containing the value "localhost" and a help icon (question mark) to its right.
- Serial number:** A text input field containing the value "1" and a help icon (question mark) to its right.

Figure 7-3: Generating a Self-signed Certificate

Step 2: Enter a fully qualified domain name (FQDN) of the Dashboard machine into the Host field, like vm603.tsfactory.com for example. Advance the serial number to any integer (for the browser's info).

Step 3: Save the configuration by clicking on the Save Config button. It will take a few moments to create the certificate and restart the Dashboard service. You can log back in afterwards.

Step 4: Download the public certificate by clicking on the "Download Certificate" link. You will be prompted to save it. You should install this certificate to the Trusted Root CA store on each machine that needs remote access to Dashboard. Alternatively, this can be done several ways including creating global policies and installing directly from a browser while connecting remotely.

To reset the certificate, simply click on the Reset certificate button and save configuration.

Option #2 – Hosted CA signed certificates

This method is useful for companies that host their own trusted certificate authority. The requirements for Dashboard are to provide Base64 encoded PEM file certificates. You will need three files: a public certificate, a private key file, and a certificate chain file containing the CA root and CA intermediate certificates combined into one file.

Step 1: Enter the filename (or browse) of the Public certificate.

Step 2: Enter the filename (or browse) of the Certificate chain file.

Step 3: Enter the filename (or browse) of the Private key file.

Step 4: Save the configuration by clicking on the Save Config button. It will take a few moments to save the configuration and restart the Dashboard service. You can log back in afterwards.

The CA root certificate and intermediate certificates should be installed on any machines that need access to Dashboard webconsole. The public certificate will be sent to browsers that connect to Dashboard during a normal https session.

Option #2 – Public CA signed certificates

The procedure for public CA signed certificates is the same as Option #2, only the CA root certificate and intermediate certificates will most likely be already installed on the client machines. This is because most browsers and Windows honor the public CA system by re-installing their root certificates.

NOTE: Firefox maintains its own trusted root CA certificates and requires special procedures for including the Windows certificate stores. Firefox does not inherently trust properly registered self-signed certificates.

After configuring the https security option, remotely connect a browser using https in the Dashboard URL. You should see a green lock or similar icon that indicates a secure connection has been made. Clicking into the icon should reveal Dashboard’s site certificate, which you should verify is correct.

Enforce HTTPS only:

This feature prevents a browser from connecting using non-secure protocols (http). The only way to enable this feature is to first configure the https option and then connect using https. Then the feature will allow you to enable it and force https only for browser connections.

Click the Save Config button after enabling this feature. The service will restart and require you to log back into Dashboard using https.

Database Purging

Located on the Sessions page in Dashboard, the database purging will automatically remove sessions older than three days (default) or whatever number of days you specify in the settings.

The screenshot shows the RecordTS Dashboard interface. At the top, there is a navigation bar with 'Sessions', 'Configuration', 'Users', and 'Licensing' tabs, and a user status 'Logged on as admin' with a 'Logout' link. Below the navigation bar is a search and filter section with fields for 'User Name', 'User Domain', 'Date Period' (From and To), 'Session Host', and 'Client Name'. There is also a checkbox for 'Enable wildcards for text filters' and 'Clear' and 'Apply' buttons. Below this is a table of sessions with columns: Id, Start date, Start time, End date, End time, User name, User domain, Session host, Client name, Data size, Don't purge, and Protocol. The table contains two rows of session data. Below the table, there is a summary of disk space usage: 'Total disk space used by RecordTS database is 3.23 MB. Dashboard uses 7.35 MB disk space for caching (clear cache)'. At the bottom, there is a checkbox labeled 'Enable database purging' which is circled in red.

Id	Start date	Start time	End date	End time	User name	User domain	Session host	Client name	Data size	Don't purge	Protocol
2	06/26/19	23:28:55	06/26/19	23:30:55	administrator	TSTFACTORY	VM601.tsfactory.com	MORTY.tsfactory	1.99 MB	<input type="checkbox"/>	RDP
1	06/26/19	23:23:56	06/26/19	23:27:18	administrator	TSTFACTORY	VM601.tsfactory.com	MORTY.tsfactory	1.24 MB	<input type="checkbox"/>	RDP

Figure 7-4: Database purge feature

Set the number of days to retain by adjusting the Purge period time. See figure 7-3 for an example of what the screen looks like.

The database will be scanned every 5 minutes for sessions that qualify for purging. The sessions that are older than the purge period will be marked for deletion. A second process will act separately to purge the marked sessions from the database. The two processes work together to manage purging the database continuously. Warning: large sessions can take extended periods of time to purge.

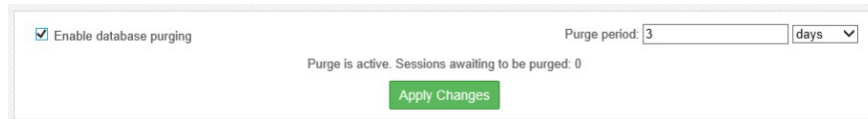
The screenshot shows a configuration panel for database purging. On the left, there is a checked checkbox labeled "Enable database purging". On the right, there is a "Purge period" field with the value "3" and a dropdown menu set to "days". Below these elements, a status message reads "Purge is active. Sessions awaiting to be purged: 0". At the bottom center of the panel is a green button labeled "Apply Changes".

Figure 7-5: Enabling database purging

Retaining Sessions

In order to keep certain sessions from being purged, simply check the “Don’t purge” box next to the session you wish to retain. Any checked sessions will be retained until the box is unchecked.

Session Playback Cache

The webplayer uses local disk cache to store temporary files created when converting and playing sessions. The cache may be cleared by clicking on the “clear cache” link.

Exporting the Session List

The complete session list can be exported to a comma separated values (CSV) file format that may be imported into a spreadsheet. To export the session list, click on the Export Session List link found on the Dashboard Sessions page. You will be prompted to open or save the file.

Setting up User Accounts

Users of Dashboard can be assigned accounts that will control which parts of Dashboard they can access. There are two types of accounts: administrator and viewer. Administrators have access to all areas of Dashboard, excluding Licensing, which is configured separately. Viewers only have access to the Sessions tab.

To setup a user account, click on the User tab. You should see the User accounts page as displayed below.

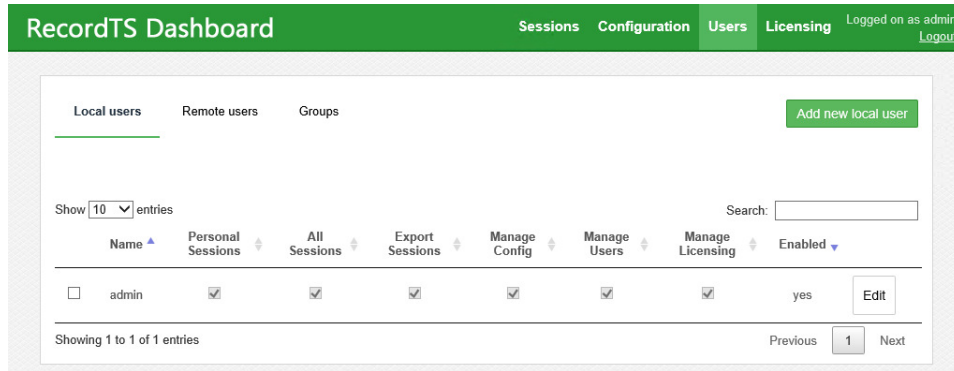


Figure 7-6: Setting up User accounts

There is one master administrator account setup during installation which cannot be deleted. More accounts may be added by importing or creating new users. You may setup as many user accounts as needed. Existing user accounts may be edited or deleted using the appropriate buttons as depicted below.

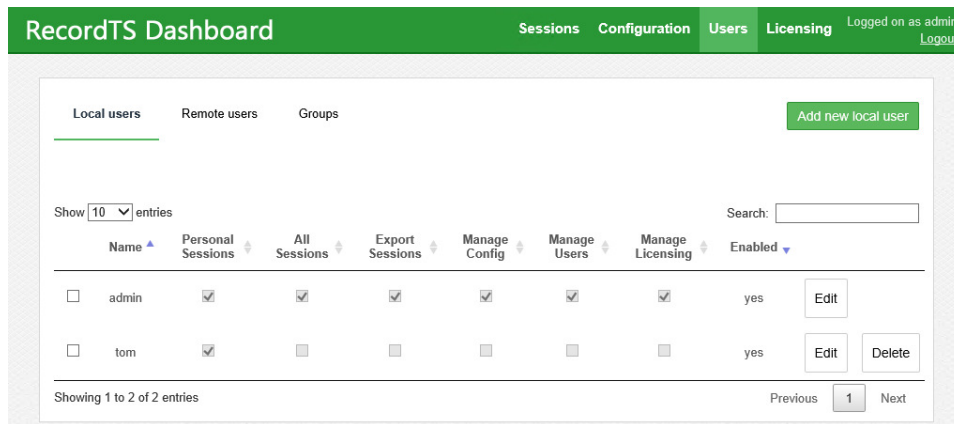
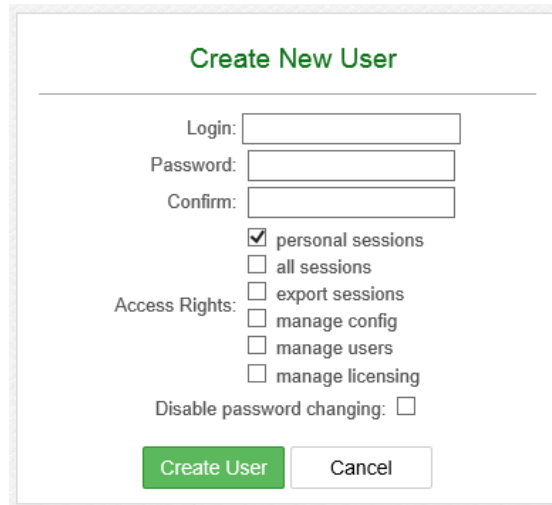


Figure 7-7: Managing User accounts

Adding Users

To add a new local user, click on “Add new user”. The Create New User dialog box will appear. Enter a login name for the new user along with a password. You will need to enter the same password twice to confirm.



The image shows a 'Create New User' dialog box. It has a title bar with the text 'Create New User' in green. Below the title bar, there are three input fields: 'Login:', 'Password:', and 'Confirm:'. Below these fields, there are five checkboxes under the heading 'Access Rights:'. The first checkbox, 'personal sessions', is checked. The other four checkboxes, 'all sessions', 'export sessions', 'manage config', and 'manage users', are unchecked. Below the checkboxes, there is a checkbox labeled 'Disable password changing:'. At the bottom of the dialog, there are two buttons: 'Create User' (highlighted in green) and 'Cancel'.

Figure 7-8: Create New User Dialog

Select access rights for the new user. Access to view the user's own personal sessions is selected by default. You may also grant a user access to view all other user's sessions, allow them to access the configuration and licensing pages, and allow them to manage users.

You may select Disable password changing to prevent the user from being able to change their password. This can be useful for viewer accounts assigned to a group of users, such as a team of doctors or emergency room personnel.

Click on the Create User button to commit the changes and create the new user account.

Editing Users

Click the Edit button next to a user you wish to change their account settings.

Profile Settings

Use the following form to change settings for user "tom"

New Login:

New Password:

New Password Confirm:

Access Rights:

- personal sessions
- all sessions
- export sessions
- manage config
- manage users
- manage licensing

Disable password changing:

Confirmation

Enter your password to save changes

Your Password:

Figure 7-9: Edit User Profile Dialog

You may change the user's login name, password or disable/enable them from changing their password. You will need to enter your admin password in order to save changes.

Click Save changes to commit the modifications made or Cancel to discard the changes and return to the previous screen.

Deleting User Accounts

To remove a user account, click on the Delete button next to their account login. You will be presented with a confirmation dialog box. Click on the Delete button to complete the process or Cancel to abort the mission and return to the previous screen.

Confirm User Delete

Please confirm that you want to delete user "joe".

Figure 7-10: Delete User Confirmation Dialog

Importing User Accounts

To import users from Active Directory or an LDAP server, first click on Remote users, then click on the "Import users" button. You should see the screen below appear:

The screenshot shows the RecordTS Dashboard with a green header containing 'RecordTS Dashboard', 'Sessions', 'Configuration', 'Users', 'Licensing', and 'Logged on as admin Logout'. Below the header, there are three tabs: 'Local users', 'Remote users' (which is selected), and 'Groups'. The 'Remote users' section contains the following fields and controls:

- Active Directory Server:** A text input field with the placeholder 'IP address or hostname' and a help icon.
- AD Server Port:** A text input field with the value '389' and a help icon.
- Base DN:** A text input field with the placeholder 'Base DN, e.g. "dc=example,dc=com"' and a 'Fetch DNs' button with a help icon.
- Group DN:** A text input field with the placeholder 'Group DN, e.g. "cn=Admins,dc=example,dc=com"' and a help icon.
- Credentials:** Two text input fields for 'Username' and 'Password', separated by a slash, with a help icon.
- Enable TLS:** A checkbox that is currently unchecked.
- Users Preferences:** A collapsed section indicated by a downward arrow.
- Advanced:** A collapsed section indicated by a downward arrow.

At the bottom of the form are two buttons: 'Test Connection' and 'Import'.

Figure 7-11: Import User Dialog

Enter the Active Directory Server IP address or FQDN hostname. You should not need to change the AD Server Port unless it has been changed from the default.

Enter the AD administrator username and password, then Test Connection to verify connectivity to the Active Directory server.

Click in the Base DN field and then click Fetch DNs. The Base DN field should populate with the base domain name data.

Click in the Group DN field if desired and enter group DN parameters such as “cn=Admins,dc=tsfactory,dc=com”.

Expand the Users Preferences and Advanced sections to view additional optional user import fields.

Under User Preferences, you may elect to enable all imported users by default and select specific areas to grant access.

Under Advanced, you may enter criterion to filter users by and specify which field will be used for each imported user’s login name.

Click on the Import button. If you have previously imported users, then you may click on the Sync button to update the imported user list against the Active Directory user list.

Click on “browse” when the item appears. This will display the imported users:

RecordTS Dashboard Sessions Configuration Users Licensing Logged on as admin Logout

License Server: pdc01.tsfactory.com:389
 TLS: Disabled
 Base: DC=tsfactory,DC=com
 Group: [none]
 Authorized user: administrator@tsfactory.com
 Filter: (&(objectCategory=Person)(sAMAccountName=*))
 Username attribute: userPrincipalName
 Status: Completed!

Show entries Search:

Name	Personal Sessions	All Sessions	Export Sessions	Manage Config	Manage Users	Manage Licensing	Enabled	
<input type="checkbox"/> TestUser1@tsfactory.com	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	no	Edit
<input type="checkbox"/> TestUser2@tsfactory.com	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	no	Edit
<input type="checkbox"/> tom@tsfactory.com	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	no	Edit
<input type="checkbox"/> user0@tsfactory.com	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	no	Edit
<input type="checkbox"/> user1@tsfactory.com	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	no	Edit
<input type="checkbox"/> user2@tsfactory.com	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	no	Edit
<input type="checkbox"/> user3@tsfactory.com	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	no	Edit

Showing 1 to 7 of 7 entries Previous Next

Figure 7-12: Imported Users

Managing Imported User Accounts

From this screen you may manage the imported user access rights. You may also disable users or delete them completely. Using the Edit button next to a user's line, you may edit their profile information.

RecordTS Dashboard Sessions Configuration Users Licensing Logged on as admin Logout

Edit User

Login: user3@tsfactory.com
 Full DN: CN=user3,OU=Domain Users,DC=tsfactory,DC=com

personal sessions
 all sessions
 May manage: export sessions
 manage config
 manage users
 manage licensing

Enabled: Yes No

Figure 7-13: Edit Imported User

Once you are done making changes to the user's profile, click Update User to commit the changes. These changes **are not posted** to Active Directory.

Creating User Groups

You can manage users via groups that you create. It is possible to create a group of employees that report to a manager and grant that manager rights to view their sessions. You may also prevent users within a group from viewing other user's sessions or even their own sessions, or lock them out of Dashboard completely.

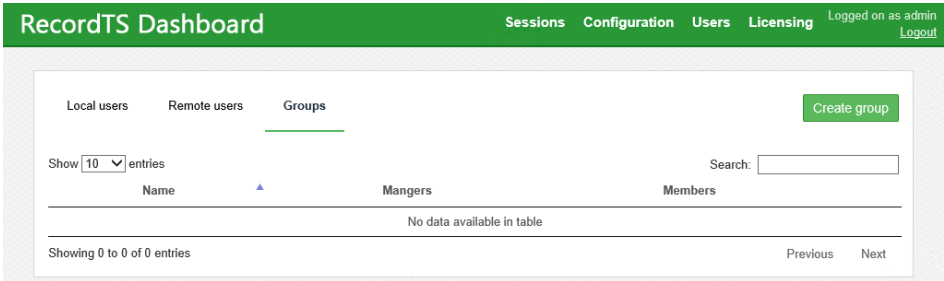


Figure 7-14: Creating User Groups

Click on the Create group button. The following screen will appear:

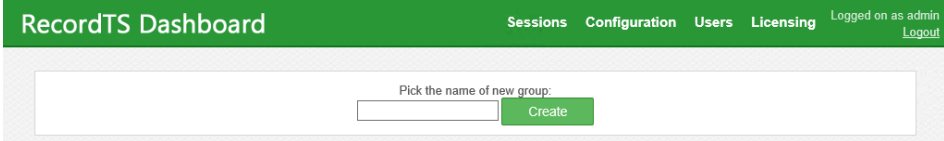


Figure 7-15: Create a Group

Enter the group name into the field and click Create. The following screen will appear:

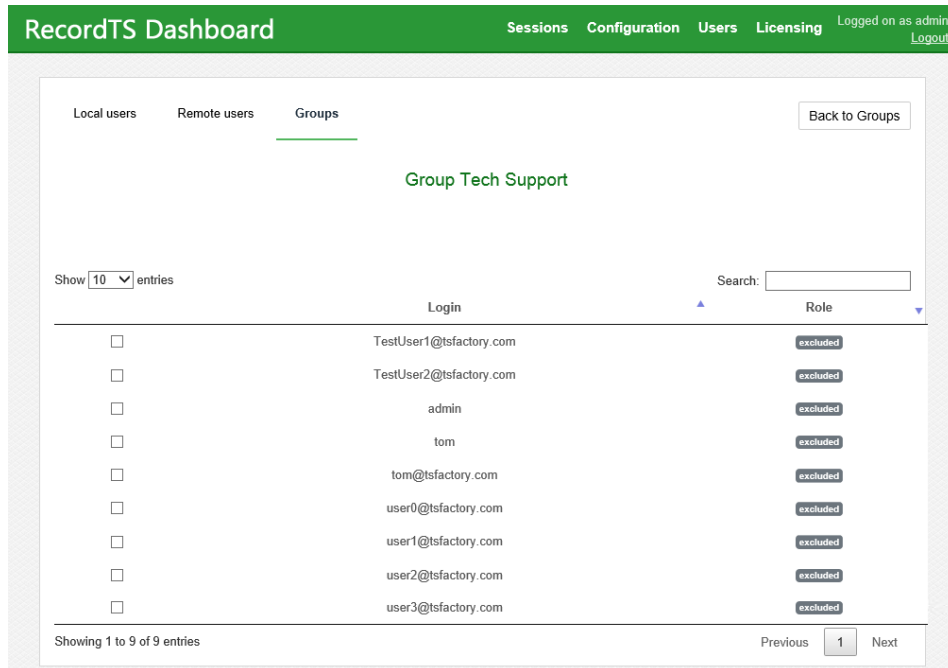


Figure 7-16: Select Users for New Group

Click on users to add to the group. As you click, you should see additional dialog fields appear like below. For each user, you may appoint the user as a member of the group, or a manager of the group, or they may be excluded from the group. You will be asked to save changes for each user you modify.

When you are done adding users to the new group, click on Back to Groups to save your changes and return to the Groups page.

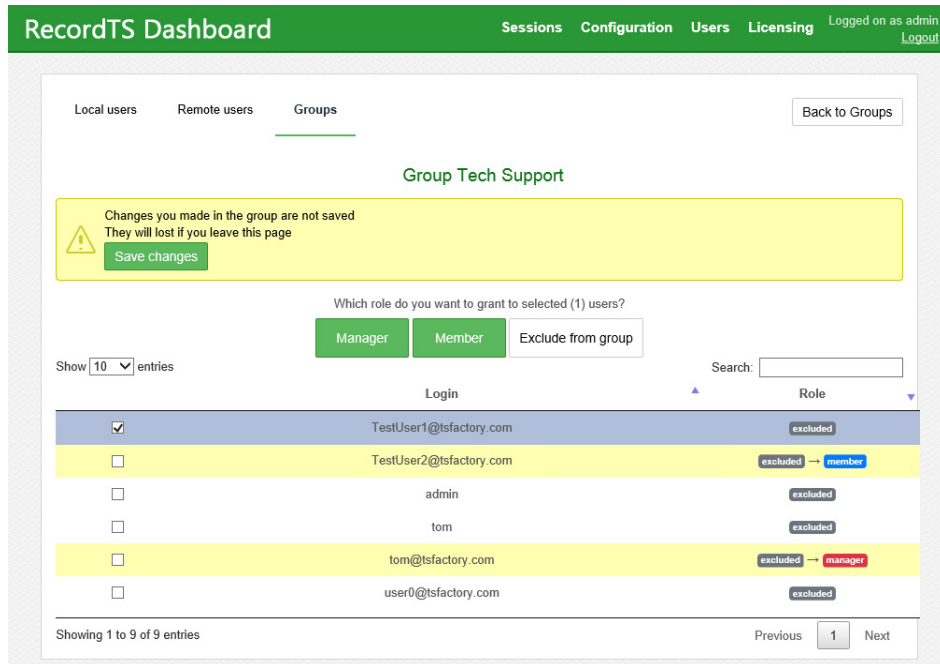


Figure 7-17: Select Users for New Group

Recorder Features

RecordTS recorder service has a number of built-in features that can enhance performance and data integrity. Let's take a look at the RecordTS for VMware Horizon Recorder Configuration:

The screenshot shows the 'RecordTS for VMware Horizon' configuration dialog. It is divided into several sections: Database Settings, License Server, Buffer Settings, and Security. The Database Settings section includes fields for Storage Server (vm103.tsfactory.com), Credentials (admin), and an Enable TLS checkbox (checked). The License Server section includes License Server Host (vm102.tsfactory.com) and License Server Port (27279). The Buffer Settings section includes Memory buffer size (256 MB) and File buffer (Enable: unchecked). The Security section includes Connections allowed (radio buttons for 'From local computer only' and 'From any computer', with 'From any computer' selected) and an Enable HTTPS checkbox (unchecked). A 'Save Config' button is at the bottom. Red circles and arrows highlight the 'Buffer Settings' section, the 'From any computer' radio button, and the 'Enable HTTPS' checkbox.

Figure 8-1: Recorder Configuration Dialog

Buffer Settings

This feature of the recorder is used to buffer session data during times of slow responsiveness or loss of connectivity to the database. In these instances, session data will continue to be streamed to local storages, depending on configuration settings. Once connectivity is restored, locally cached session data will be sent to the database and normal operation will continue.

The first place the recorder will store data is to local memory. The size of the buffer can be set in the Memory buffer size (MB) field. The default size is 256 MB. This option is always enabled allowing for brief moments of intermittent database connectivity.

The next place the recorder will store data is to a local file. This option is normally disabled and must be enabled for the recorder to take advantage of it. To enable, check the box labeled “Enable file buffer”.

This action will cause additional fields to be displayed as depicted in Figure 8-2 below.

Buffer Settings

Memory buffer size: MB File buffer: Enable: Size: MB

File buffer path:

Figure 8-2: Enabling the File Buffer Feature

The file buffer size can be adjusted by entering a number in the Size (MB) field. The default buffer size is 1024 MB. The file buffer file name and path can be set in the File buffer path field. It is ok to leave the default values as they are.

To summarize, when connectivity to the database becomes intermittent or lost, immediately the recorder will buffer session data into local memory until it fills. Then if file buffering is enabled, the recorder will store session data into a local file. When the file is completely filled (i.e. the file size is met), the recorder will cease storing data and automatically terminate the session. The user will lose their connection to prevent further unrecorded activity and also to act as a passive alarm system for the admins (users will complain).

Remote Recorder Configuration Access

The “Connections allowed” feature lets you connect remotely to the Recorder Configuration webconsole from another computer using a browser. Select the “From any computer” to allow connections from other computers.

This feature is useful if you want to manage Recorder configuration remotely.

NOTE: Changing this feature will reduce security by allowing foreign computers to have access to the Recorder configuration.

To connect remotely, the user will need administrator access to connect to the Recorder configuration webconsole. In a browser on the user’s desktop, enter this URL: <http://Recorder:8086> where Recorder should be replaced with the actual Recorder machine hostname, FQDN or IP address.

Secure Web Access to Recorder Config

The “Enable https” option allows configuring Recorder webconsole to accept secure browser connections using SSL/TLS (https).

Click on the Enable https checkbox to show the entire list of options for this feature:

Enable HTTPS:

Enforce HTTPS only: *Visit this webconsole over HTTPS to make this option available*

From file Generate self-signed

Public certificate: Browse

Certificate chain: Browse

Private key: Browse

There are three options to providing SSL certificates for secure web browsing:

1. Self-signed certificate
2. Customer generated certificate signed by hosted Certificate Authority such as Active Directory
3. Public certificate signed by a trusted Certificate Authority such as Godaddy, Thawte, etc.

The first item can be automatically generated by RecordTS Recorder webconsole. The other two are provided by the customer.

NOTE: Details for creating certificates for use with Recorder webconsole https can be found in a separate document “Securing RecordTS Web Interfaces”. Contact our support staff for a copy of this document or visit our website.

Option #1 – Self-signed certificates

This is the simplest way to create certificates for https, but also the least secure as some browsers such as Firefox will not trust self-signed certificates.

There are a few steps to this process – generate the certificate, download the public certificate and copy it to any machines that will be accessing Recorder webconsole remotely. The public certificate must be installed into the Windows Trusted Root CA store on each client machine.

Step 1: Click on Generate self-signed checkbox. You should see the screen change as depicted below:

Enable HTTPS:

Enforce HTTPS only: *Visit this webconsole over HTTPS to make this option available*

From file Generate self-signed

Host:

Serial number:

Step 2: Enter a fully qualified domain name (FQDN) of the Recorder machine into the Host field, like vm602.tsfactory.com for example. Advance the serial number to any integer (for the browser's info).

Step 3: Save the configuration by clicking on the Save Config button. It will take a few moments to create the certificate and restart the Recorder webconsole service. You can log back in afterwards.

Step 4: Download the public certificate by clicking on the "Download Certificate" link. You will be prompted to save it. You should install this certificate to the Trusted Root CA store on each machine that needs remote access to the Recorder webconsole. Alternatively, this can be done several ways including creating global policies and installing directly from a browser while connecting remotely.

To reset the certificate, simply click on the Reset certificate button and save configuration.

Option #2 – Hosted CA signed certificates

This method is useful for companies that host their own trusted certificate authority. The requirements for Dashboard are to provide Base64 encoded PEM file certificates. You will need three files: a public certificate, a private key file, and a certificate chain file containing the CA root and CA intermediate certificates combined into one file.

Step 1: Enter the filename (or browse) of the Public certificate.

Step 2: Enter the filename (or browse) of the Certificate chain file.

Step 3: Enter the filename (or browse) of the Private key file.

Step 4: Save the configuration by clicking on the Save Config button. It will take a few moments to save the configuration and restart the Recorder webconsole service. You can log back in afterwards.

The CA root certificate and intermediate certificates should be installed on any machines that need access to the Recorder webconsole. The public certificate will be sent to browsers that connect to the Recorder webconsole during a normal https session.

Option #2 – Public CA signed certificates

The procedure for public CA signed certificates is the same as Option #2, only the CA root certificate and intermediate certificates will most likely be already installed on the client machines. This is because most browsers and Windows honor the public CA system by re-installing their root certificates.

NOTE: Firefox maintains its own trusted root CA certificates and requires special procedures for including the Windows certificate stores. Firefox does not inherently trust properly registered self-signed certificates.

After configuring the https security option, remotely connect a browser using https in the Recorder webconsole URL. You should see a green lock or similar icon that indicates a secure connection has been made. Clicking into the icon should reveal Dashboard's site certificate, which you should verify is correct.

Enforce HTTPS only:

This feature prevents a browser from connecting using non-secure protocols (http). The only way to enable this feature is to first configure the https option and then connect using https. Then the feature will allow you to enable it and force https only for browser connections.

Click the Save Config button after enabling this feature. The service will restart and require you to log back into Recorder webconsole using https.

RecordTS Storage Server Backup Tool

The RecordTS Storage Server comes with scripts that allow you to back up and restore the database files. There are also options to check the integrity and display information on an existing archive.

WARNING: The RecordTS Storage Server service **must be stopped** before creating a backup of the database. This means all users must be logged off and no session recording is happening. Plan ahead for system to be offline while the backup or restore takes place.

Here are the basic modes for performing a backup of the storage database along with restoring it and operations to verify the integrity of an archive.

Help

This mode will display instructions on how to use the tool.

To display tool help:

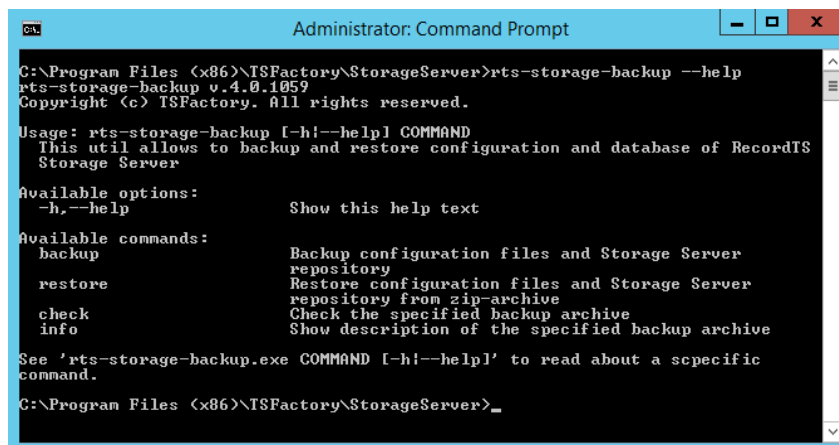
On the machine that RecordTS Storage Server is installed, open a DOS command or Powershell window and navigate to the RecordTS Storage Server program files folder here:

```
C:\Program Files\TSFactory\StorageServer
```

Execute the following command:

```
> rts-storage-backup --help
```

Here is the output:



```
Administrator: Command Prompt
C:\Program Files (x86)\TSFactory\StorageServer>rts-storage-backup --help
rts-storage-backup v.4.0.1059
Copyright (c) TSFactory. All rights reserved.

Usage: rts-storage-backup [-h|--help] COMMAND
This util allows to backup and restore configuration and database of RecordTS
Storage Server

Available options:
-h,--help          Show this help text

Available commands:
backup             Backup configuration files and Storage Server
                  repository
restore            Restore configuration files and Storage Server
                  repository from zip-archive
check              Check the specified backup archive
info              Show description of the specified backup archive

See 'rts-storage-backup.exe COMMAND [-h|--help]' to read about a specific
command.
C:\Program Files (x86)\TSFactory\StorageServer>_
```

Backup

This mode will copy the database files to a specified location using various command line switches to tailor the archive.

Simple backup procedures:

On the machine that RecordTS Storage Server is installed, first stop the storage server service, then open a DOS command or Powershell window and navigate to the RecordTS Storage Server program files folder here:

```
C:\Program Files\TSFactory\StorageServer
```

Execute the following command:

```
> rts-storage-backup backup -d backupfolder
```

where: *backupfolder* is the directory to store the backup.

The backup process will take time to copy the database files so expect some down time while the process completes.

Command line switches include:

- d, --directory Directory to save an archive with backup data
- n, --name ARG Specify name of backup archive.
- c, --comment Include a comment with backup archive.
- compress Compress files in an archive.
- no-compression Store files without compression.
- bzip Pack data with BZip2 algorithm.
- f, --force Suppress user input requests.
- h, --help Display help.

If a custom name is not specified, the tool will generate a name for you with the format: RTS_Storage_ServerYYYYMMDD-XXXXXX.zip

The .zip file extension will automatically added if no extension was specified.

Where: YYYY = year, MM = month, DD = day, XXXXXX = internally generated timestamp suffix.

Restore

This mode restores data from an archive.

Simple restore procedures:

On the machine that RecordTS Storage Server is installed on, first stop the storage server service, open a DOS command or Powershell window and navigate to the RecordTS Storage Server program files folder here:

```
C:\Program Files\TSFactory\StorageServer
```

Execute the following command:

```
> rts-storage-backup restore -a archive
```

where: *archive* is the path\filename of the archive.

The tool will warn you the existing configuration files will be removed. This is normal. Press Enter to continue restoring or type 'n' to quit.

The restore process will take time to extract and copy the database files from the archive so expect some down time while the process completes.

Command line switches include:

- a, --archive ARG Specify name of the archive file to restore.
- f, --force Suppress user input requests.
- h, --help Display help.

Check

This mode verifies archive integrity.

On the machine that RecordTS Storage Server is installed, open a DOS command or Powershell window and navigate to the RecordTS Storage Server program files folder here:

```
C:\Program Files\TSFactory\StorageServer
```

Execute the following command:

```
> rts-storage-backup check -a archive
```

where: *archive* is the name and location of the archive file.

The integrity checking process may take time so plan accordingly.

Command line switches include:

- a, --archive ARG Specify name of the archive file to restore.
- h, --help Display help.

Info

This mode reports information about an archive.

On the machine that RecordTS Storage Server is installed, open a DOS command or Powershell window and navigate to the RecordTS Storage Server program files folder here:

```
C:\Program Files\TSFactory\StorageServer
```

Execute the following command:

```
> rts-storage-backup info -a archive
```

where: *archive* is the name and location of the archive file.

The information reporting process may take time so plan accordingly.

Command line switches include:

- a, --archive ARG Specify name of the archive file to restore.
- h, --help Display help.

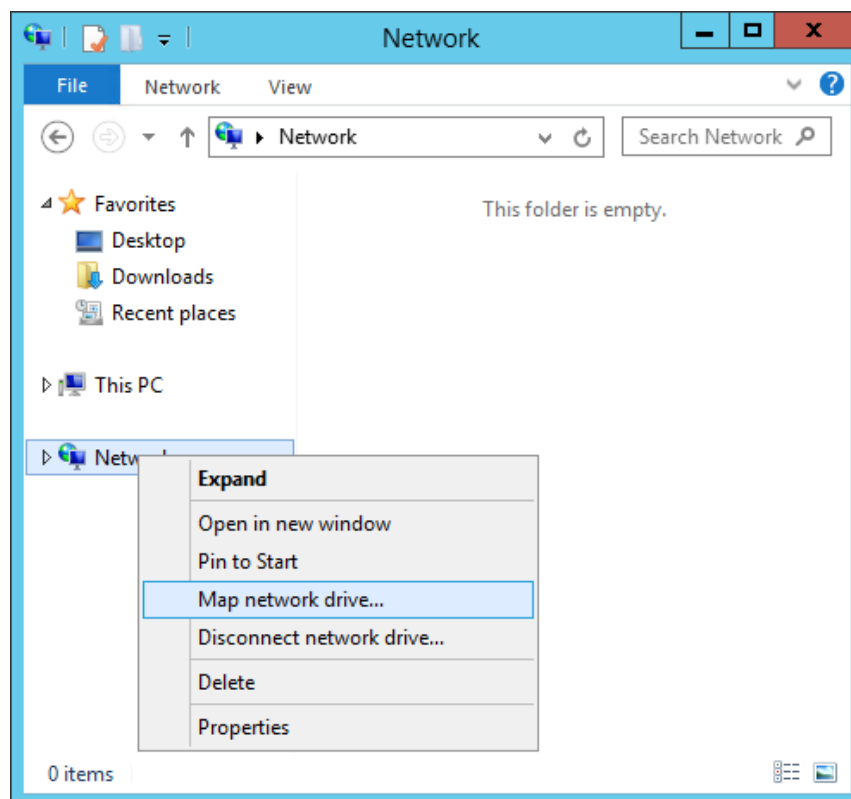
Backup Tool Examples

For the following examples, you should stop the storage server service before performing a backup or restore operation. All commands are executed from the RecordTS program files folder in a DOS command or Powershell window. See previous section for more information on this process.

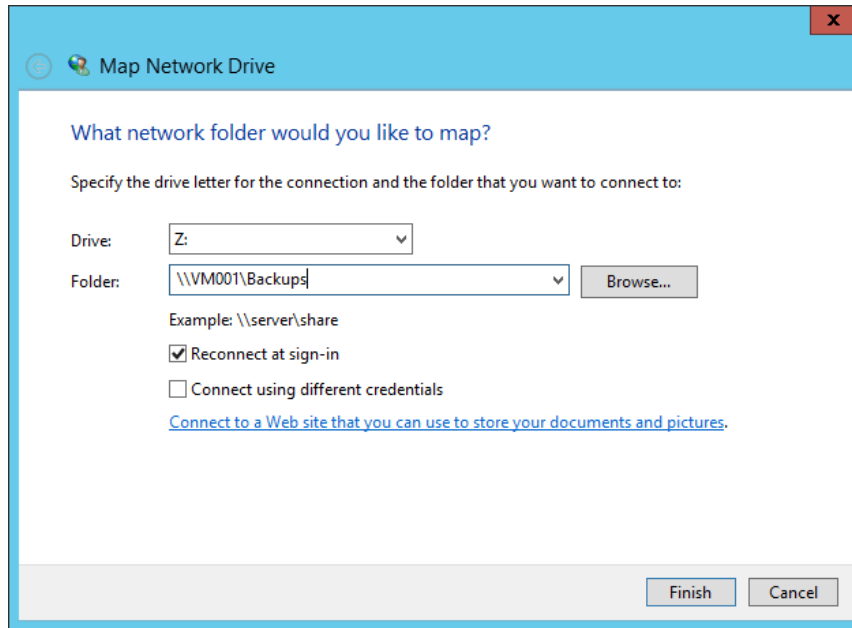
To backup the database to another machine (network share) on your network, you will first need to map a local network drive to that machine.

Mapping a Network Drive

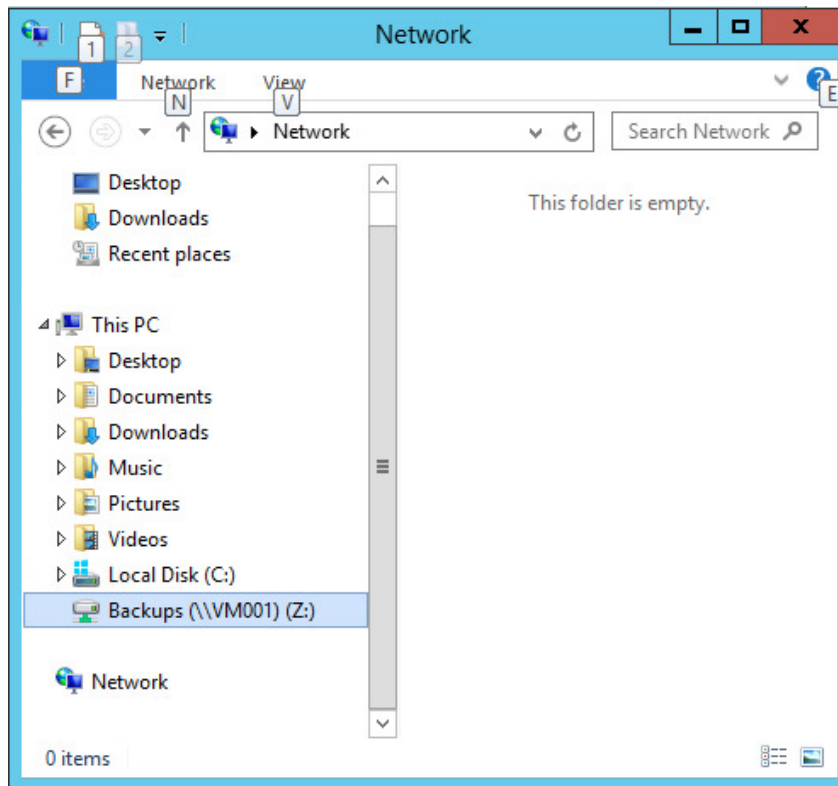
On the RecordTS Storage Server, open File Explorer and right mouse click over the Network icon.



Click on “Map network drive...” and enter the network share name in the Folder field or click Browse to locate the folder. Modify the other settings and click on Finish to map the share to a local drive.



The mapped drive should appear in the drive list. You are now ready to use it for backups. See below.




Examples

Example #1:

Backup the database to mapped network drive Z: using archive name “rtsbackup2018.zip” and add a comment to the archive.

```
> rts-storage-backup backup -d Z: -n rtsbackup2018.zip -c  
“weekly video backup”
```

Here is a screen shot of the backup procedure:



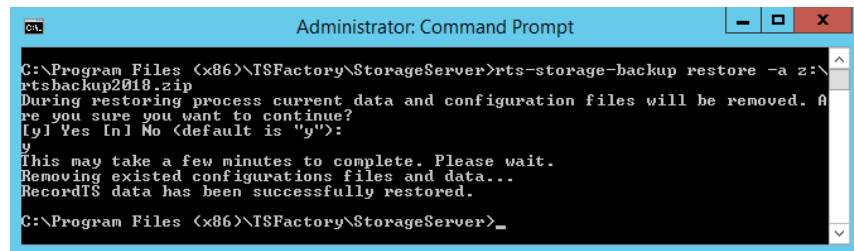
```
Administrator: Command Prompt  
C:\Program Files (x86)\TSFactory\StorageServer>rts-storage-backup backup -d Z: -n rtsbackup2018.zip -c "weekly video backup"  
This may take a few minutes to complete. Please wait.  
RecordIS data has been saved to Z:\rtsbackup2018.zip  
C:\Program Files (x86)\TSFactory\StorageServer>_
```

Example #2:

Restore the database from an archive file located on a locally mapped network drive Z: with the archive file name “rtsbackup2018.zip”.

```
> rts-storage-backup restore -a z:\rtsbackup2018.zip
```

Here is a screen shot of the restore procedure:



```
Administrator: Command Prompt  
C:\Program Files (x86)\TSFactory\StorageServer>rts-storage-backup restore -a z:\rtsbackup2018.zip  
During restoring process current data and configuration files will be removed. Are you sure you want to continue?  
[y] Yes [n] No (default is "y"):  
y  
This may take a few minutes to complete. Please wait.  
Removing existed configurations files and data...  
RecordIS data has been successfully restored.  
C:\Program Files (x86)\TSFactory\StorageServer>_
```

Example #3:

Check the integrity of an archive file located on a locally mapped network drive Z: with the archive file name “rtsbackup2018.zip”.

```
> rts-storage-backup check -a z:\rtsbackup2018.zip
```

Here is a screen shot of the archive integrity check procedure:



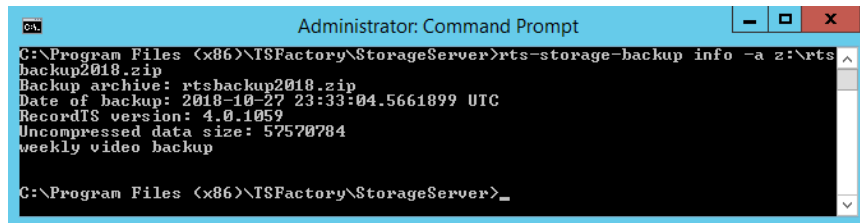
```
Administrator: Command Prompt
C:\Program Files (x86)\TSFactory\StorageServer>rts-storage-backup check -a z:\rts
sbackup2018.zip
Checking for: Z:\rtsbackup2018.zip
The backup archive has been checked. OK
C:\Program Files (x86)\TSFactory\StorageServer>_
```

Example #4:

Display the information from an archive file located on a locally mapped network drive Z: with the archive file name “rtsbackup2018.zip”.

```
> rts-storage-backup info -a z:\rtsbackup2018.zip
```

Here is a screen shot of the archive information dump:



```
Administrator: Command Prompt
C:\Program Files (x86)\TSFactory\StorageServer>rts-storage-backup info -a z:\rts
backup2018.zip
Backup archive: rtsbackup2018.zip
Date of backup: 2018-10-27 23:33:04.5661899 UTC
RecordTS version: 4.0.1059
Uncompressed data size: 57570784
weekly video backup
C:\Program Files (x86)\TSFactory\StorageServer>_
```

Note the last line will be the comment if one was specified during backup.

Support

How to get support

Below are some solutions to the more common problems encountered during product installation and configuration. The TSFactory website is another excellent resource for solutions to commonly found problems.

If you cannot resolve your problem using these solutions, please contact our technical support team at support@tsfactory.com.

Support Disclaimer:

Assistance is limited to providing suggestions for problem resolution and in some extreme cases, remote debug. The customer is expected to try any suggestions and use whatever resources they have to resolve their problems. Customers are encouraged to work with local resellers and partners that are listed on our website to assist in problem resolution.

Dashboard Problems

Database connection errors:

Make sure you have selected RecordTS Storage Server for the storage database. The RecordTS recorder will only work with the native RecordTS database storage.

Verify connectivity to the database server using the Test Connectivity button. Make sure you have entered the proper username and password you selected when setting up the RecordTS Storage Server.

Check the Enable TLS checkbox if you intend to use this option. You may uncheck this box to test connectivity without TLS enabled.

Make sure the machine Dashboard is installed on has access to the storage server machine and verify firewall rules are updated and correct. Try turning off firewalls for testing only.

License Server connection errors:

If you have installed the license service on the same machine as Dashboard, then you can leave the default settings for license server name as "localhost". Otherwise you will need to enter the hostname or IP address of the server where the license server was installed. Make sure you have configured the firewall to allow connections to the license server, especially if it is in a DMZ.

Dashboard console will not display:

Usually this is due to another program using port 8084. Either change the other program to use another port or contact support for instructions on changing the Dashboard port.

Licensing Problems

License server warnings are not clearing after configuration:

Usually they will disappear within 4-5 minutes. Please be patient and wait. Refresh the screen often. If they still are not clearing then contact support for assistance.

Recorder Problems

Database connection errors:

Verify connectivity to the database server by clicking on the Test Connectivity button.

Check firewall rules on both machines for incoming and outgoing connections. You can disable the firewalls temporarily for testing purposes only.

Make sure the storage server service is started. Look for any related warnings or errors in the Windows event logs.

Users can connect to their desktops, but no recordings are being made:

Verify the correct recorder is installed on the target machine to be recorded and that the users are using the Horizon View Client to access their desktops.

Make sure recording for Horizon View Agent has been enabled via the Windows registry entry. Contact TSFactory support for more information on this.

List of Service Ports

License Service: 27279
Dashboard Config: 8084
Recorder Config: 8086
Storage Server: 2022 (unencrypted)
2023 (Secure TLS)