RecordTS Enterprise v7.0 for Citrix Virtual Apps & Desktops

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.

Citrix and the Citrix logo are registered trademarks or trademarks of Citrix, 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 6

What is RecordTS? 6
Main Features 6
Security/Audit compliance 6
Developed for Citrix Apps and Desktops 6
Per user session recording 6
How does RecordTS work? 7

Quick Overview 9

Recorder 9
Dashboard 9
License Service 9
Database 10

Installing Base Modules 11

Overview 11
WARNINGS: Read This Before You Start… 12
Prerequisites 13
Step 1: Making a Place to Store Session Data 15
RecordTS Storage Server 15
How to Install the RecordTS Storage Server 15
Installing Microsoft SQL Server 18
Installing PostgreSQL Server 18
Step 2: Installing the RecordTS License Service 19
How to install the RecordTS License Service 19
Step 3: Installing the Dashboard Console service 22
How to install the RecordTS Dashboard Console Service 22
Step 4: Configuring Dashboard and the License Service 25
Configuring Dashboard for MS SQL Server 25
Configuring Dashboard for PostgreSQL Server 27
Configuring Dashboard for RecordTS Storage Server 29
Configuring Dashboard Security Access 31
Configuring the RecordTS License Service 32

Installing Recorders 36

Overview 36
General process 36
On-demand clones and instant clones: 36
Recorder Types 37
Prerequisites 37
RecordTS Recorder 38
Pre-installation Requirements 38
Installing the Recorder 38
Configuring the Recorder 44

Playing Recorded Sessions 48

Optimizing RecordTS 50

Dashboard Features 50
Remote Dashboard Access 50
Secure Web Access to Dashboard 51

Enforce HTTPS only: 53
Database Purging 53
Retaining Sessions 54
Session Playback Cache 54
Exporting the Session List 54
Setting up User Accounts 54
Adding Users 55
Editing Users 56
Deleting User Accounts 57
Importing User Accounts 57
Managing Imported User Accounts 59
Creating User Groups 60
Recorder Features 62
Buffer Settings 63
Remote Recorder Configuration Access 63
Secure Web Access to Recorder Config 64
Enforce HTTPS only: 66
Drain Mode 66
RecordTS Storage Server Backup Tool 68
Help 68
Backup 69
Restore 69
Check 70
Info 71
Backup Tool Examples 72
Mapping a Network Drive 72
Examples 74

Support **76**

How to get support 76
Dashboard Problems 76
Licensing Problems 77
Recorder Problems 77
Database Problems 78
Downloading Log Files 79
List of Service Ports 80

This page intentionally left blank.

Introduction

What is RecordTS?

RecordTS is a remote desktop session recorder for Windows Terminal Services and Citrix Virtual Apps & Desktops, formerly XenApp and XenDesktop. What does it mean exactly? It means once installed on a server running Citrix Virtual Citrix Apps & Desktops, 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 a Microsoft SQL Server database or PostgreSQL Server database or 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 Citrix Apps and Desktops

Although other similar solutions do exist in the market, RecordTS is the first solution to be totally protocol agnostic, meaning RecordTS does not rely upon any particular hosting environment or integrating with other product's software or agents. RecordTS is NOT a screen capture program or screen scraper and is very difficult if not impossible to circumvent.

Per user session recording

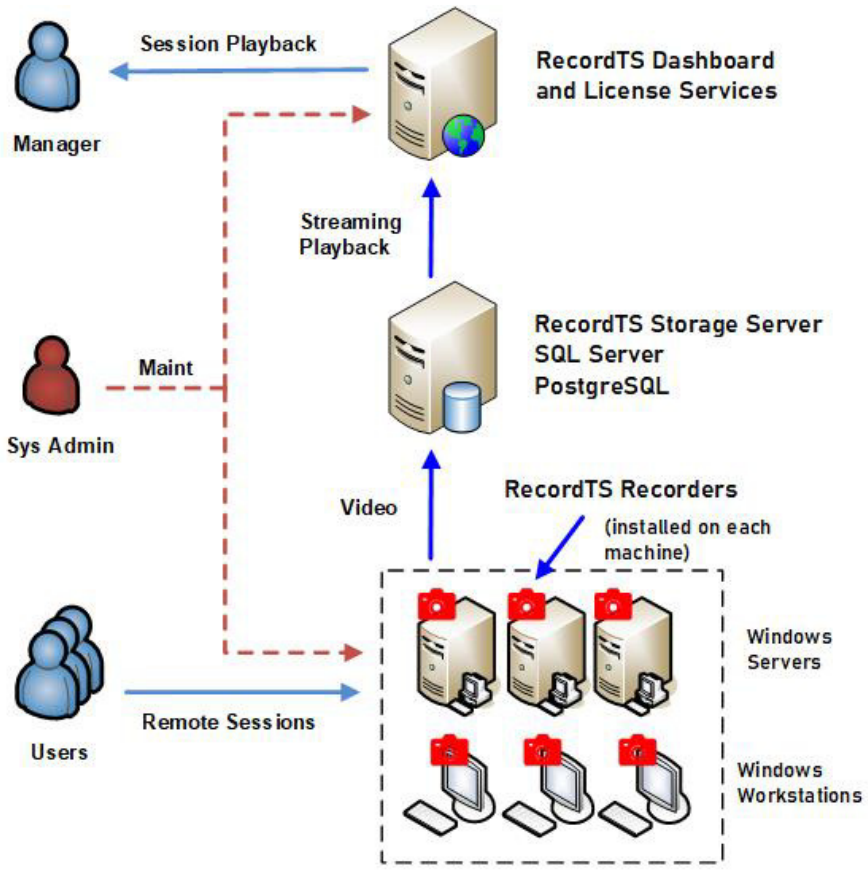
Recorded sessions are saved individually on a per user basis. Recordings are stored in a database for later retrieval and replay.

How does RecordTS work?

RecordTS recording service runs directly on a machine with the Citrix Virtual Delivery Agent (VDA) installed, captuing video of desktop activity. Session video is streamed directly to a central database for playback and safekeeping. As RecordTS was developed from the ground up specifically for Citrix products, this process does not affect server performance, scaling easily once more users and/or servers are added to the system.

Below are several functional and network diagrams of typical network configurations for RecordTS v7.

The next section will discuss the individual components in detail.

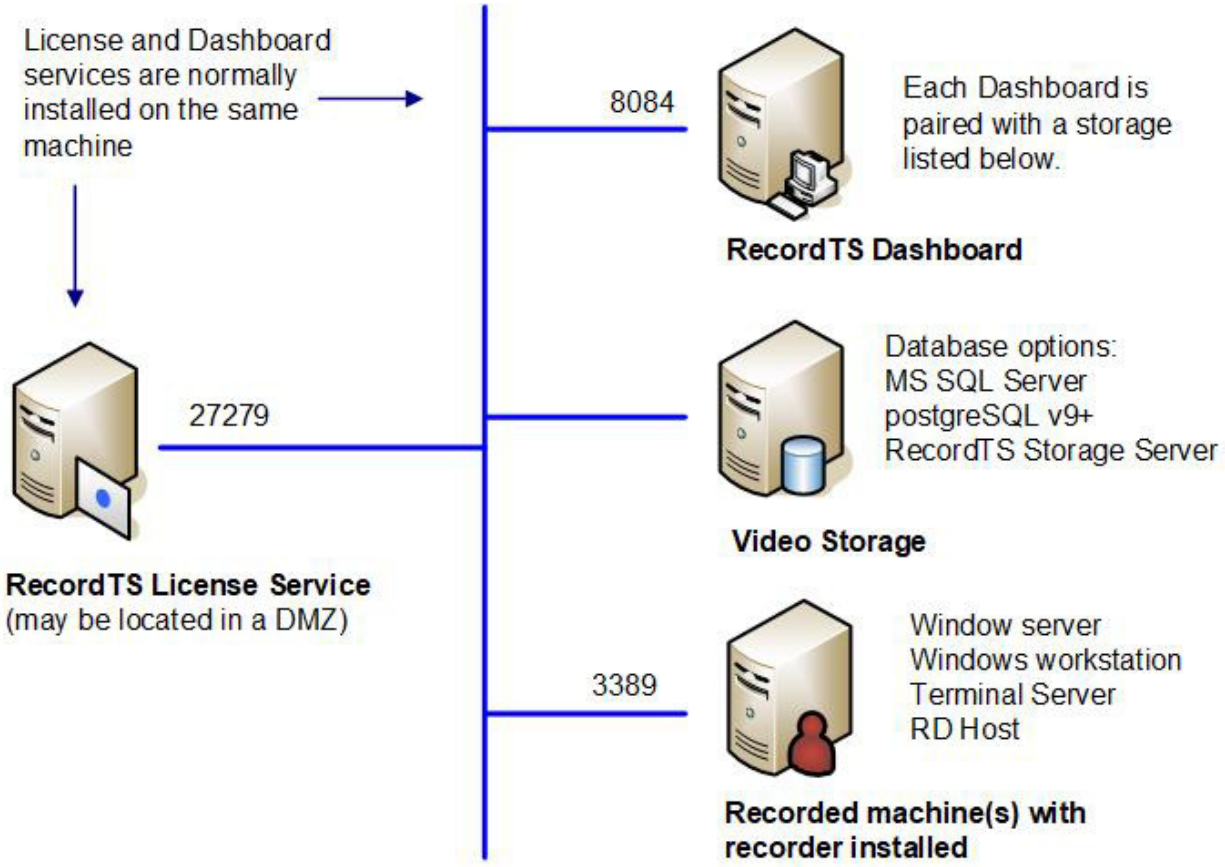


RecordTS v7 Enterprise Edition
Functional Diagram

The following diagram shows a typical network layout of the RecordTS components. Note that the Dashboard and License services are normally installed to the same machine and can be co-located with the database server. For larger installations the database should be located on a

separate machine to minimize loading when viewing sessions and enhance security.

The diagram below shows only one Recorder, but there can be as many Recorders as needed. The upper limit on Recorders is mainly dictated by database/storage loading. Multiple databases or storages will be required to handle large server farms.



RecordTS v7 Enterprise 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)**
- **DC Proxy Service**
- **Dashboard**
- **License Service**
- **Database / Storage Server**

Recorder

The basic component of RecordTS is the Recording Service or Recorder, installed on each of the target recorded machines. Its main job is to record user sessions and store the video files to a central database. From the time RecordTS Recorder is installed and properly configured on a Citrix enabled server or workstation, each user session will be recorded and saved to a database in the native RecordTS 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 in the database.

The recorded sessions can be viewed or played as a video using the RecordTS Webplayer or exported and played in any standard video player. .

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 recorders and other components such as additional dashboards and modules.

License Service

RecordTS implements a subscription licensing scheme, where products will be licensed for use for a period of time. A software subscription must

be purchased in order to authorize use of RecordTS software components.

The RecordTS License Service must be installed to authorize and license RecordTS components for use. The License Service can be installed anywhere (but usually with Dashboard) and then configured from the Dashboard console. Once the License Service is properly configured, the customer will be directed to obtain a ***license key*** to authenticate the License service. Without the license key, the license service will not enable any RecordTS components.

Database

RecordTS Recorders stream session data to a central location for safe keeping and easy session playback. There are three options available for storing sessions:

- RecordTS Storage Server (included)
- PostgreSQL v9 or higher
- Microsoft SQL Server 2014, 2016 or higher

One of these storage systems 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.

If you prefer to use a commercial database server, then Microsoft SQL Server 2014, 2016 or newer (full version) can be used, or alternatively PostgreSQL v9 or newer with appropriate ODBC database drivers installed on Dashboard and Recorder machines (not on database server itself unless it is on one of those machines). The PostgreSQL ODBC drivers are supplied with the RecordTS software. Installation instructions are posted later in this manual.

Session recording can be buffered in case the SQL/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 SQL database/storage and normal operation will continue. If connectivity to the SQL database/storage is disrupted for extended periods of time, the buffers may fill completely and sessions will be suspended until connectivity to the SQL database is restored. There is now an option called Bypass Mode to allow sessions to continue recording even though licensing has been exceeded or the database/storage server has become inaccessible.

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

Installing Base Modules

Overview

RecordTS for Citrix Virtual Apps & Desktops is made up of five major components: License service, Dashboard console with session player, a Database or storage server, session Recorders, and a DC Proxy. It is assumed a database/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 or SQL Database Server
2. License service
3. Dashboard console
4. Recorders
5. DC Proxy

WARNINGS: Read This Before You Start…

Uninstall Older Versions

You cannot upgrade from older versions RecordTS (v1, v2 or v3) to RecordTS v6. You need to uninstall any older versions of RecordTS and reboot before installing v6.

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

A functioning database or storage server, configured to accept remote connections.

Choose from one of the following options:

MS SQL Server	(v2014 or higher) Full Version (not Express) configured for Windows Authentication (preferred) and allowing remote connectivity
- OR -	
PostgreSQL	(v9.022 or later), configured for Windows Authentication (preferrred) and allowing remote connectivity
- OR -	
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 or higher.
2. Windows servers 2016 running Citrix Virtual Apps environment
3. PostGreSQL ODBC 32-bit drivers for Windows, v9.3.4 (to be installed on any box that accesses the PostgreSQL database server). The ODBC drivers are included in the download package.

   NOTE: *it is not necessary to configure a data source; only install the drivers*.
4. At least one Windows machine to log in remotely from (act as a client).
5. A domain admin account (or equiv) that has access to all machines in the test, especially the SQL database server and SQL server itself.
6. **All machines must be part of the same domain under Active Directory IF you use Windows Authentication**
7. 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.
8. 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.

NOTE: (*for testing only)* you can install all of the components onto a Citrix VDA machine and have a single server install for your test environment. This is not a recommended configuration for production, especially if you intend on recording more than one machine. In this case it makes more sense to install the license service, Dashboard console and database/storage server on a separate machine during initial testing phases to verify operation and connectivity.

Upgrading: There is **no** upgrade path from very old versions of RecordTS (v1 to v5). All previous versions *less than* v5 of RecordTS ***must be removed*** before installing v7!

Step 1: Making a Place to Store Session Data

RecordTS Recorders will stream session data to a central storage area that must be setup and configured prior to installing any other components. You have several options for storage:

- RecordTS Storage Server
- Microsoft SQL Server
- PostgreSQL Server

Installing and configuring each of these systems will be described in the following sections.

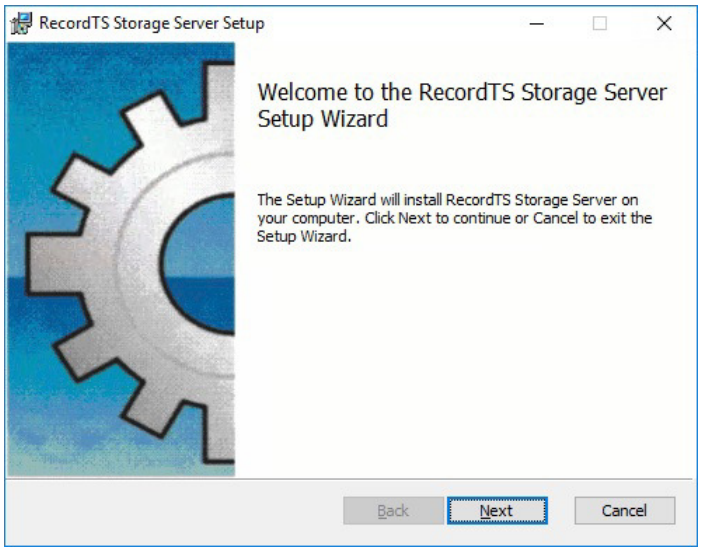
RecordTS Storage Server

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

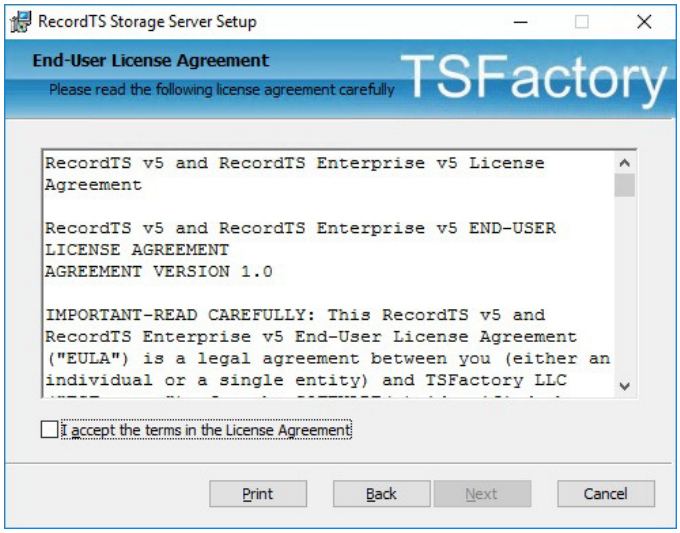
The server should be domain joined and have its firewall either disabled or configured to accept connections from the other RecordTS components. Also, plan for enough drive space to store the amount of sessions you would like to retain. Usually a terabyte or more is required.

How to Install the RecordTS Storage Server

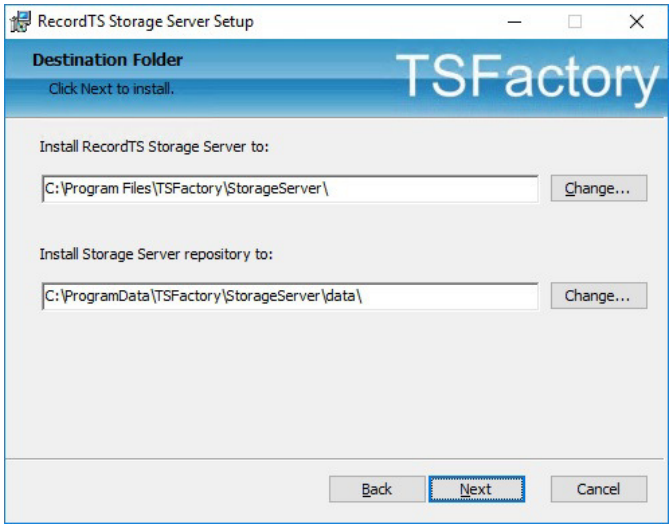
1. Download and run the RecordTS-Storage-Server-7.x.xxxx.msi installation file on the machine that the storage server is to reside. The installation wizard will appear. Close all other programs and then click Next.



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.

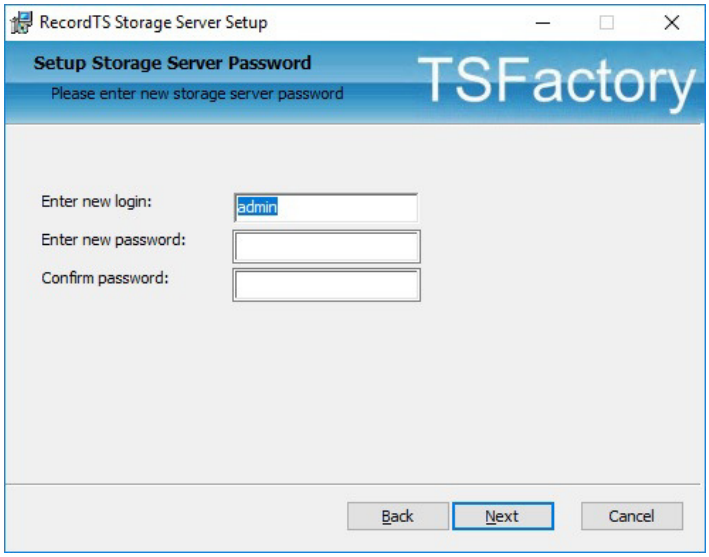


2. Select the directory where the RecordTS storage server program files will be installed and where the data will be stored. Only local directories on the local machine can be used. If you do not want to use the default directory suggested by the installer, click Browse... to choose another directory.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



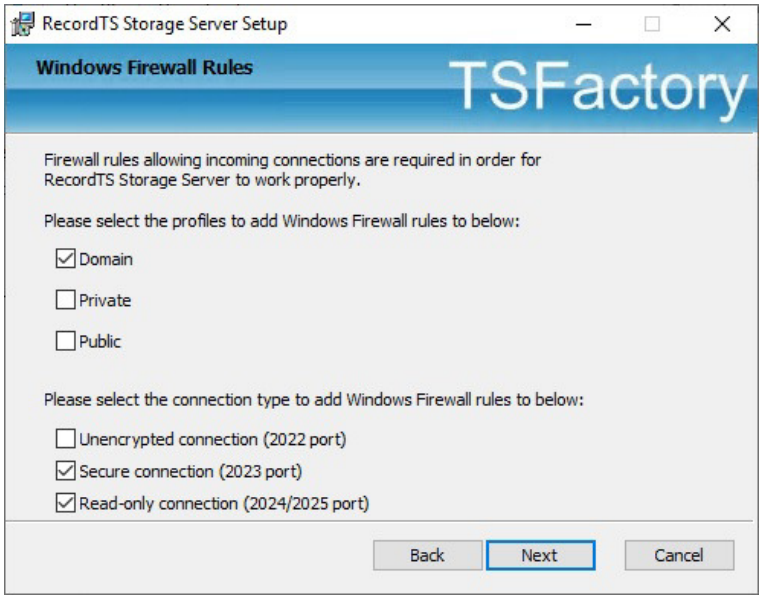
3. Enter the credentials for a new admin account that will be created for you. This account will have sole access to the storage server and be required in the Dashboard and Recorder configurations.

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

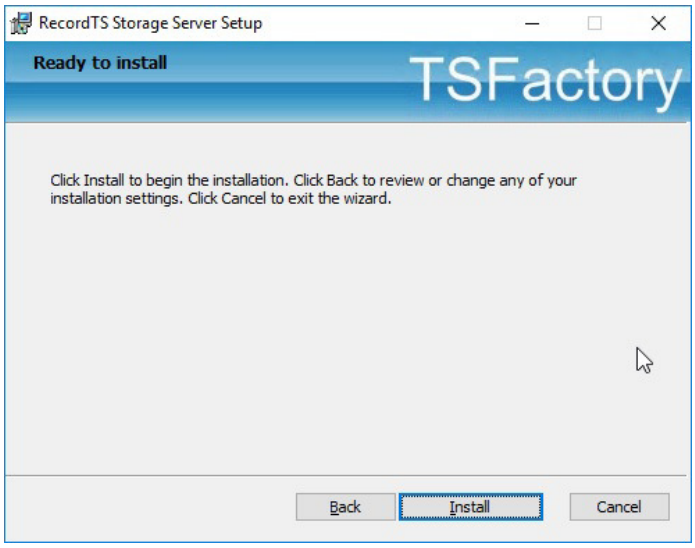


4. Configure firewall rules. Select the firewall profiles to add then select the connection type. Secure connection will allow encrypted traffic to the Storage Server from other components. This option must be configured on all components; otherwise unencrypted traffic will be used. You may check both types if you are unsure which type will be implemented then later remove the unused firewall rule.

   NOTE: Read-only connection is a new option and intended for high capacity scenarios for improved session playback. You may leave it enabled until you decide it will not be used.



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.

Installing Microsoft SQL Server

Follow the manufacturer's instructions and recommendations for installing their database server. Please note the usage of "instance" means you may choose to create multiple SQL servers (instances) running on one machine. During installation, you will be allowed to rename the default instance (along with setting logon credentials), and create additional instances. Please write down this information as it will be required to configure Dashboard and the Recorders.

Note: By default, MS SQL Server will need to be manually configured for remote access. Instructions for doing this can be found at the end of this manual.

Installing PostgreSQL Server

Follow the manufacturer's instructions and recommendations for installing their database server. Please note during installation you will be allowed to rename the default maintenance database and create admin credentials. Please write down this information as it will be required to configure Dashboard and the Recorders.

You do not need to install posgres ODBC drivers on the database server. The ODBC drivers should be installed on the Dashboard and Recorder machines, not the database server unless it is co-located with one of these components.

Note: By default, the postgreSQL database server will need to be manually configured for remote access. Instructions for doing this can be found at the end of this manual.

Step 2: Installing the RecordTS License Service

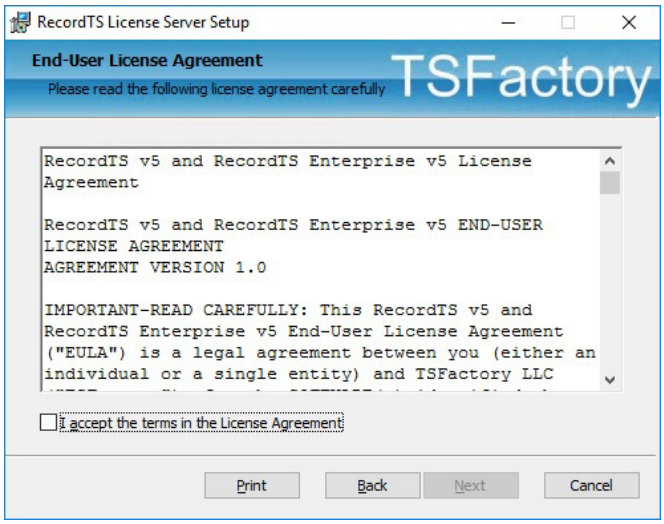
The RecordTS Dashboard may be installed on the same machine as the RecordTS license service. The box should be domain joined and have its firewall set, if enabled, to allow connections from Dashboard, the database server and recorders (other terminal servers and Windows machines being recorded).

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

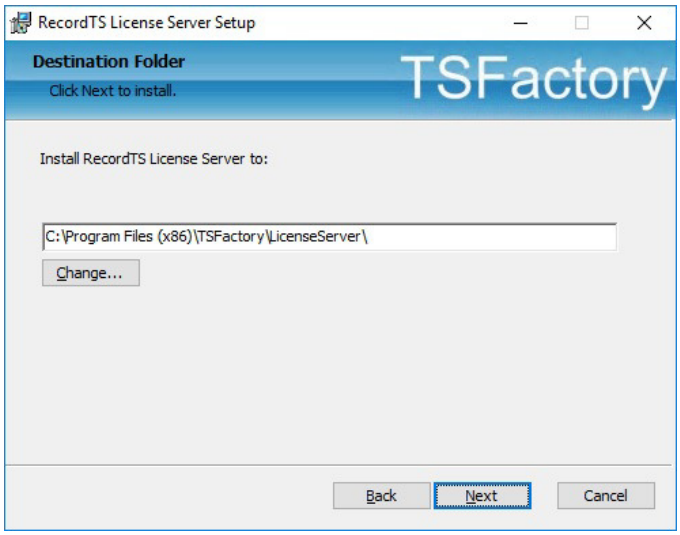
How to install the RecordTS License Service

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.

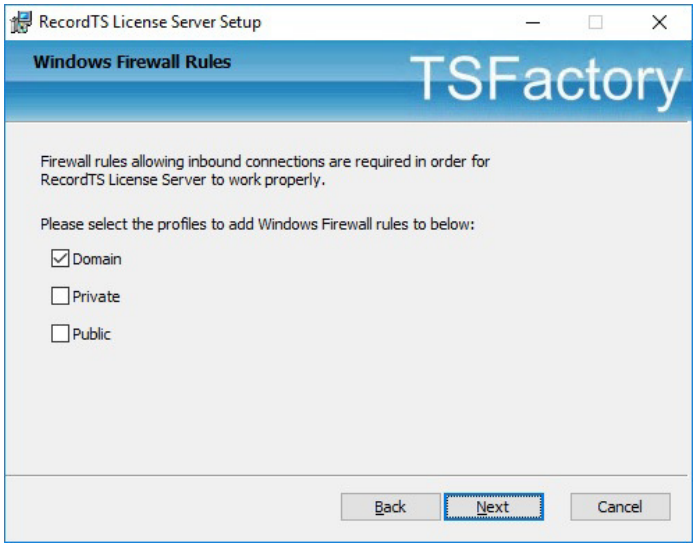
2. Carefully read the license agreement. If you agree to the terms, select the check box to confirm acceptance of the agreement. Click Next to continue installing. To exit Setup, click Cancel.



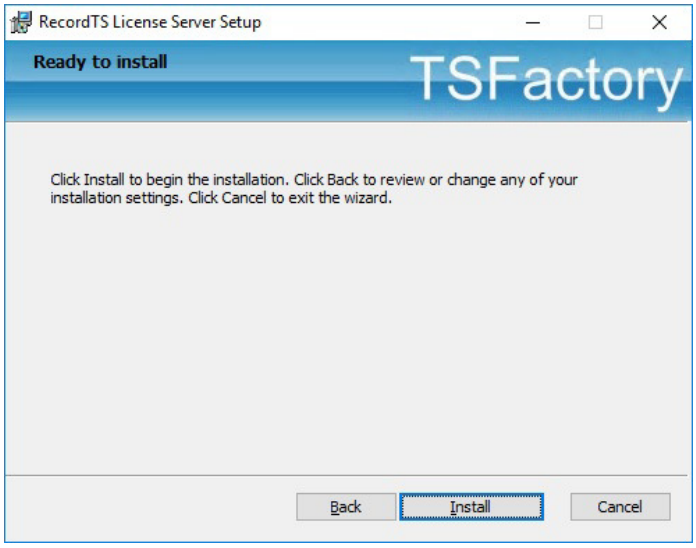
3. Select the directory where the RecordTS license service program files will be installed. Only local directories on the local machine can be used. If you do not want to use the default directory suggested by the installer, click Browse... to choose another directory. Then click Next.



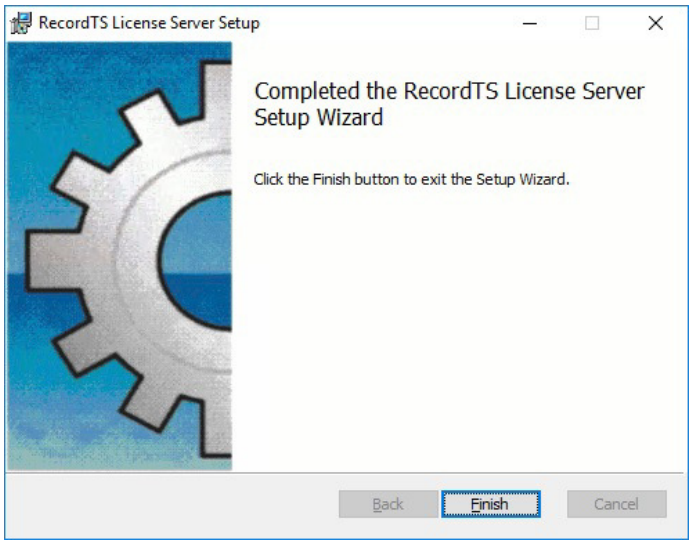
4. Select profiles to add firewall rules. This step will automatically add firewall rules to allow connections from other modules.



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.

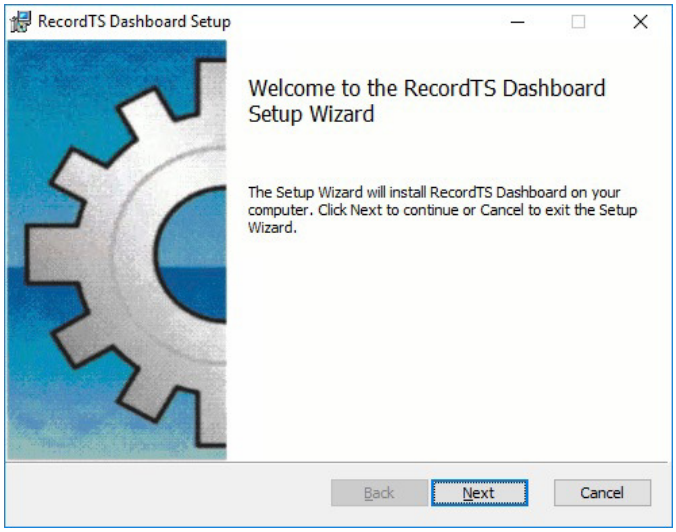
Step 3: Installing the Dashboard Console service

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).

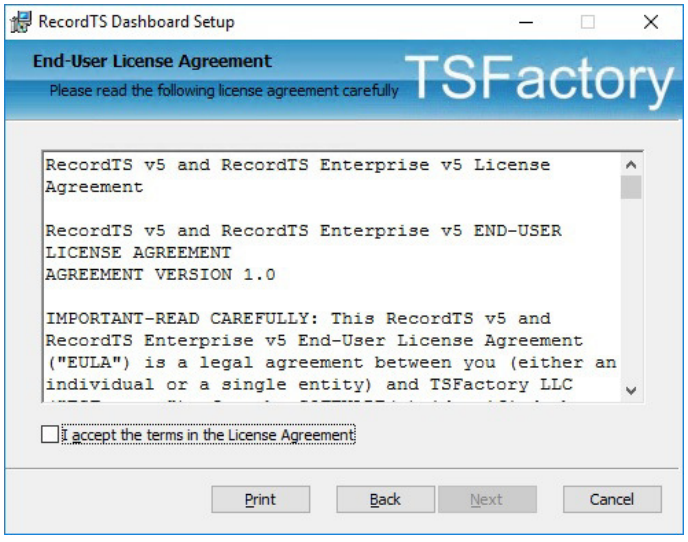
Note: after installing the RecordTS Dashboard Console Service, the service will appear in the Windows Services applet along with the RecordTS License Service, if installed, together on the same machine.

How to install the RecordTS Dashboard Console Service

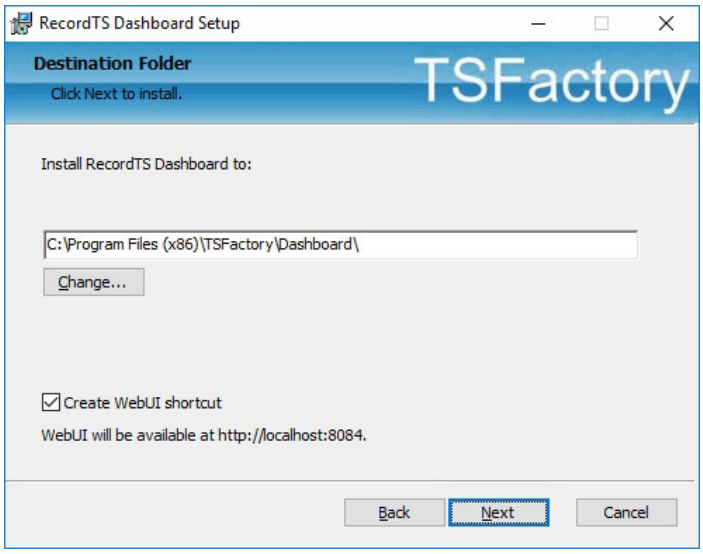
1. Download and run the RecordTS-Dashboard-7.x.xxx.msi installation file on the machine that the license service is to reside. The installation wizard will appear. Close all other programs and then click Next.



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.



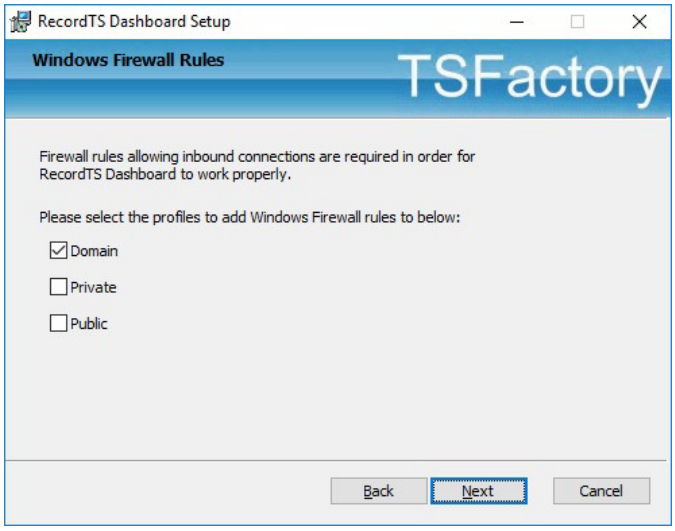
3. Select the directory where the RecordTS Dashboard service program files will be installed. Only local directories on the local machine can be used. If you do not want to use the default directory suggested by the installer, click Browse... to choose another directory.



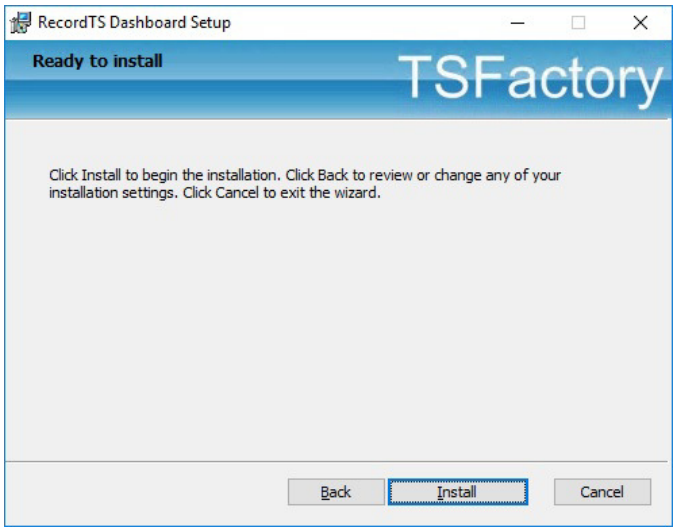
You may uncheck “Create WebUI Shortcut” to prevent installing shortcuts to each user’s application list. You can access the Dashboard webUI with this URL: http://localhost:8084.

Click Next to continue.

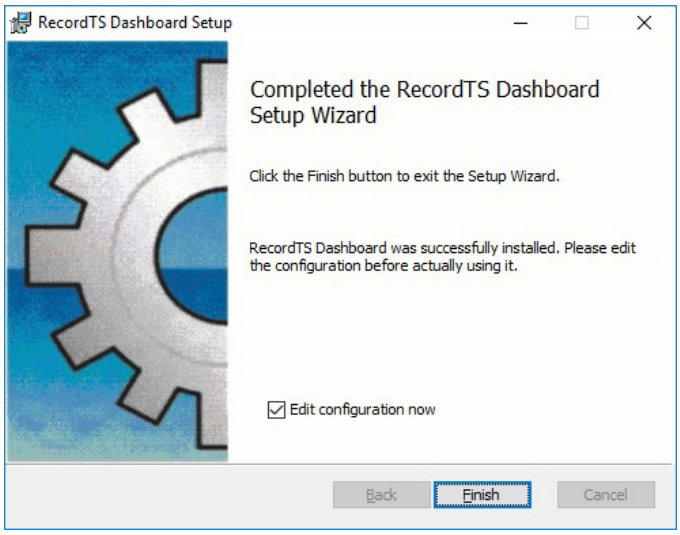
4. Select profiles to create firewall rules for. Click Next to continue.



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.
9. The RecordTS Dashboard Service will appear in the Windows Services applet.

IMPORTANT: Set the service to “log on as” a domain admin user account (or equiv) that has access to the SQL server database. This user account needs administrative rights, specifically database creation and admin.

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

    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:

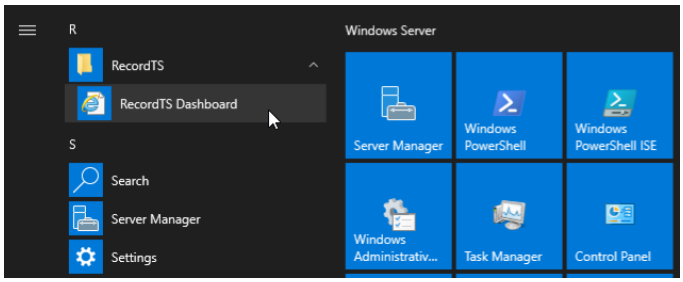
- ✓ Connect to the database server to create a database (if none exists), and manage it.
- ✓ Authorize RecordTS software components for use, such as the recorders, remote user connections and all Dashboard instances, along with future RecordTS integrated products and components.
- ✓ Display a list of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

For Subscription Customers only:

- ✓ Connect to the TSFactory website servers to obtain subscription license information using a subscription ID supplied from the online customer account (you need to create one).

Configuring Dashboard for MS SQL 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 if you need help with this.

IMPORTANT: Set the Dashboard service to “log on as” a domain admin user account (or equiv) that has access to the SQL server database. This user account needs administrative rights, specifically database creation and admin.

3. The first thing to configure is the Database server settings. Microsoft SQL Server should be selected by default. (see figure 1-1).

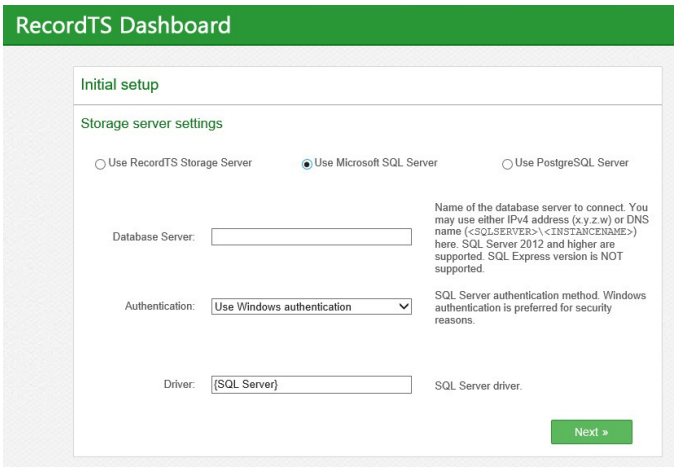


Figure 1-1: Database Server Settings – MS SQL Server

4. Enter the database server name and instance like this: <sqlserver>\<instancename> substituting your SQL server names, such as <SQLSERVER2012\MSSQLSERVER> where the first name is the actual hostname of the server itself and the second name is the SQL server instance (there can be serveral SQL database server instances co-located on the same server). This is NOT the actual database file name - that will come later. Normally you can leave the *instancename* blank to use the default instance.

NOTE: Only SQL Server 2014, 2016 or 2019 FULL VERSION is supported (not the Express version due to 10 gig space limitations)

5. Select the type of authentication to the SQL server: either Windows Authentication (preferred method) or SQL Server Authentication. The latter will require entering a username and password with rights to create and manage a database.
6. Click Next
7. Enter a name for the database (no filename extension is necessary).

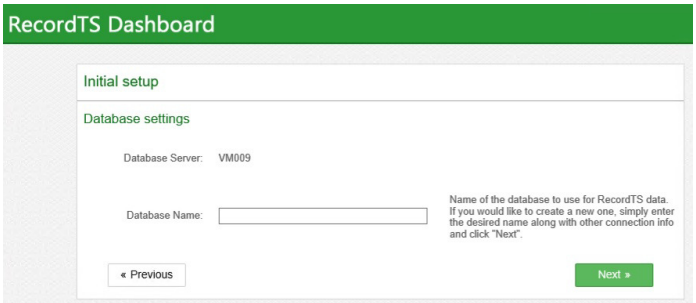


Figure 1-2: Database Settings – MS SQL Server

8. Click Next
9. You may be prompted to create the database if it does not exist. Click the “Create database” button to proceed.

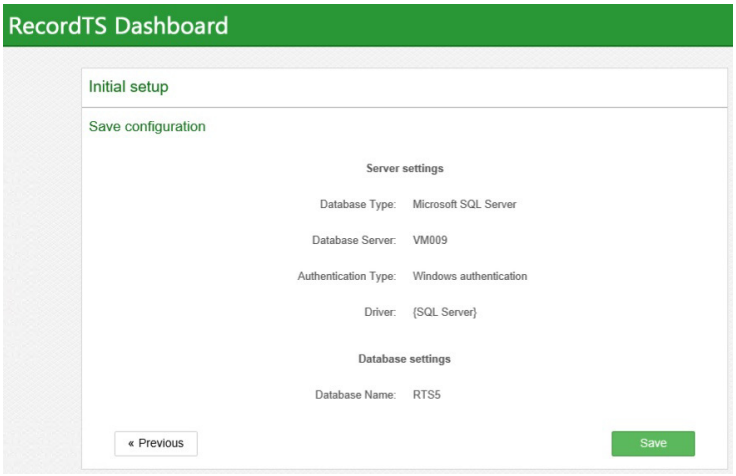


Figure 1-3: Confirming Database Settings – MS SQL Server

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

11. Move on to configuring Dashboard security access.

Configuring Dashboard for PostgreSQL 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 Database server settings. Microsoft SQL Server should be selected. Change this to PostgreSQL Server by selecting the far-right radio button (see figure 2-1).

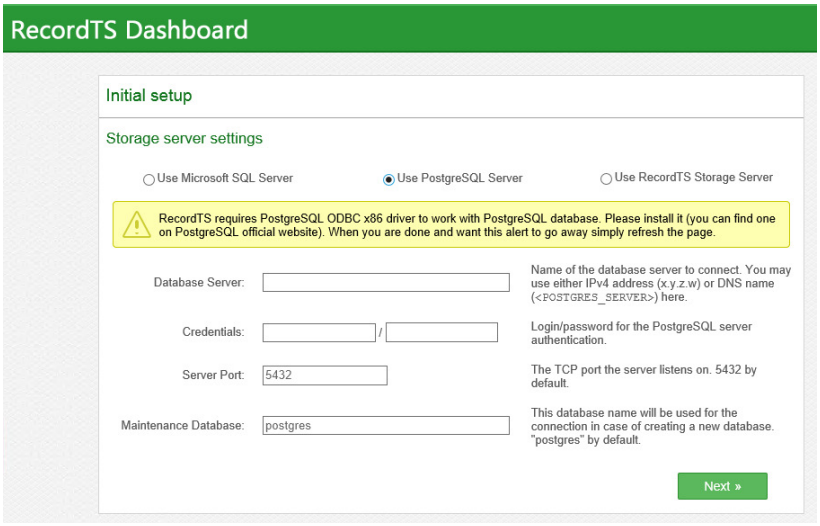


Figure 2-1: Database Server Settings – PostgreSQL Server

4. Enter the database server name, admin username and password (usually “postgres” and the password for this account). You can safely use the default values for the server port and maintenance database fields. If they are different then enter them now.

NOTE: You will need to have installed the 64-bit Postgres ODBC database drivers (provided in the download zip) in order for Dashboard to communicate with the PostgreSQL database. If this is not completed, then an error will be raised when Dashboard attempts to communicate with the database server. Stop now and install the ODBC drivers if needed (do not configure a data source). You may also need to edit the Postgres config files to allow remote access from other machines to the Postgres database.

5. Click Next to continue.

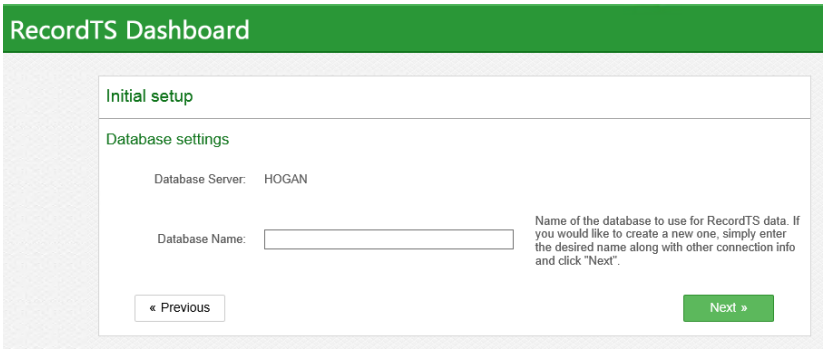


Figure 2-2: Database Settings – PostgreSQL Server

6. Enter a name for the database you wish to use. It will be created for you if it does not exist.
7. Click Next
8. You may be prompted to create the database if it does not exist. Click the “Create database” button to proceed.

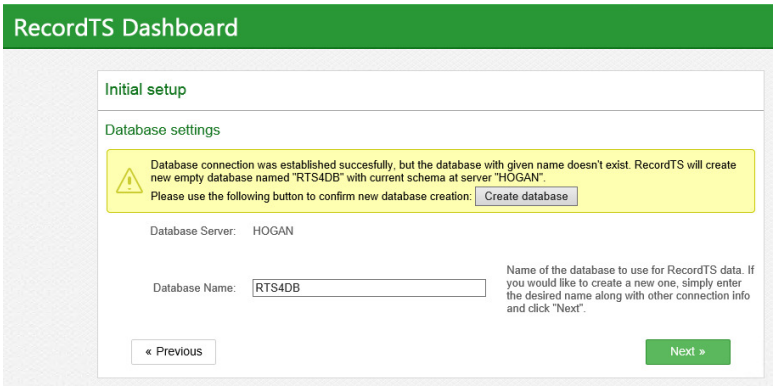


Figure 2-3: Creating the Database – PostgreSQL Server

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

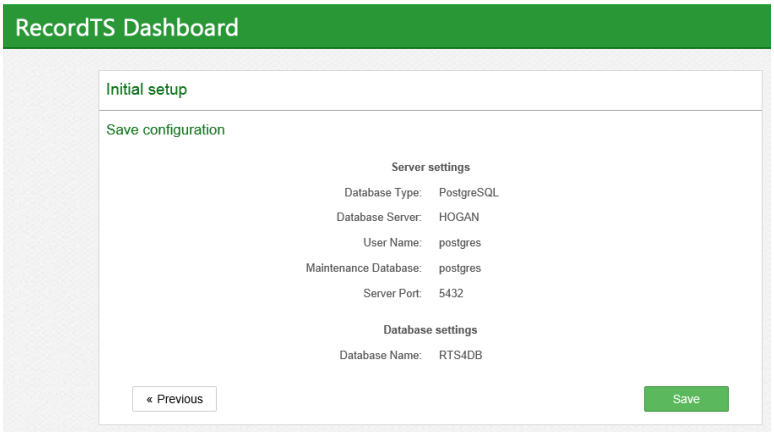


Figure 2-4: Confirming Database Settings – PostgreSQL Server

10. Move on to configuring Dashboard security access.

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. Microsoft SQL Server may be selected. Change this to TSFactory Storage Server by selecting the far-right radio button. (see figure 3-1)

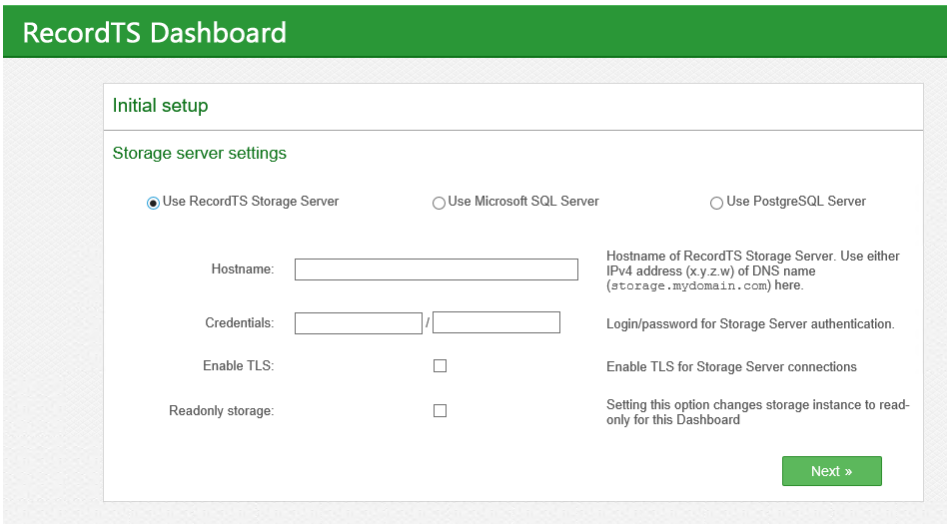


Figure 3-1: Storage Server Settings

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. Check the Enable TLS box to enable secure communications with other modules. Click Next to continue. Leave Readonly storage unchecked for now.

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).

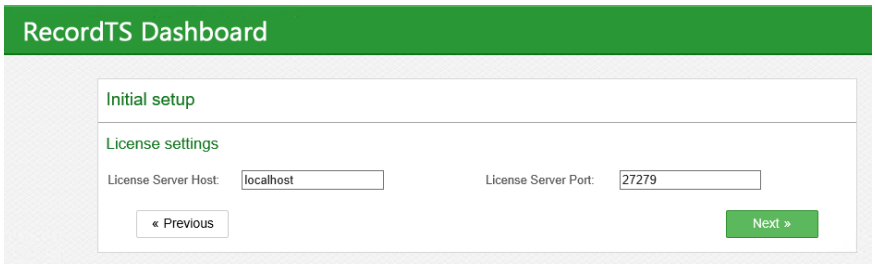


Figure 3-2: License Server Settings

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.

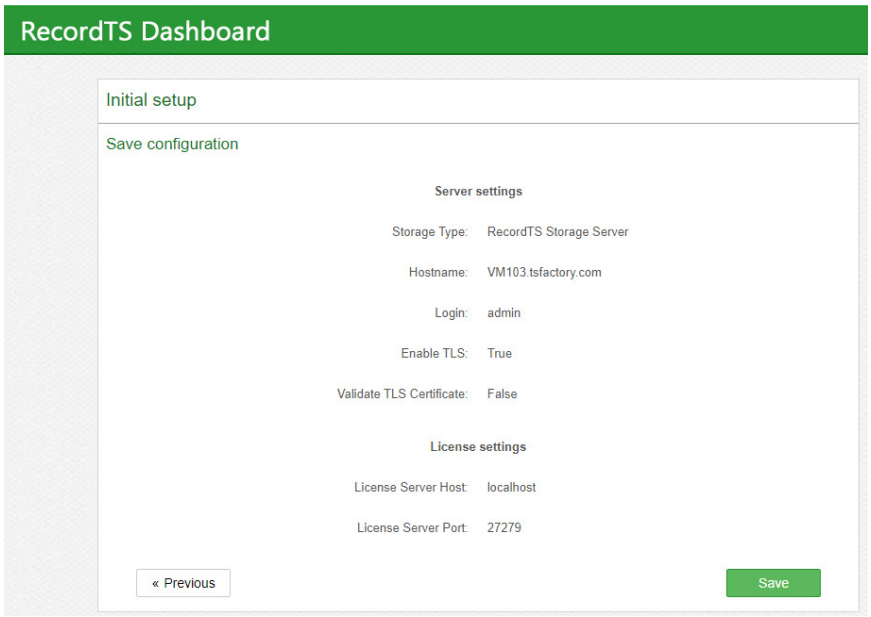


Figure 3-3: Confirming Storage Server Settings

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).

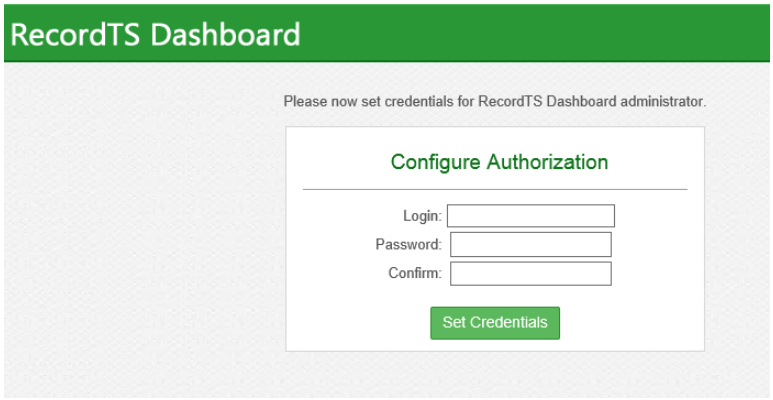


Figure 4-1: Creating Dashboard Administrator Credentials

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).

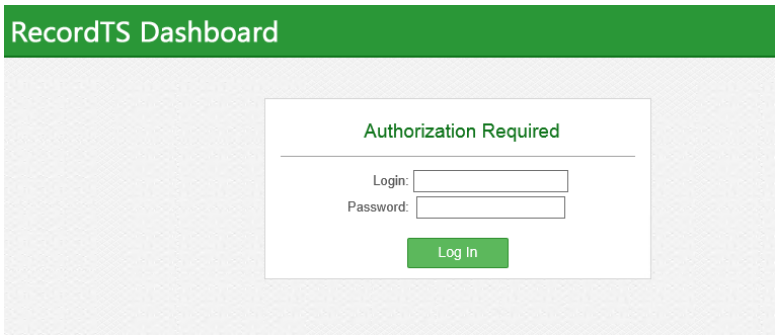


Figure 4-2: Logging into the Dashboard Webconsole

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.

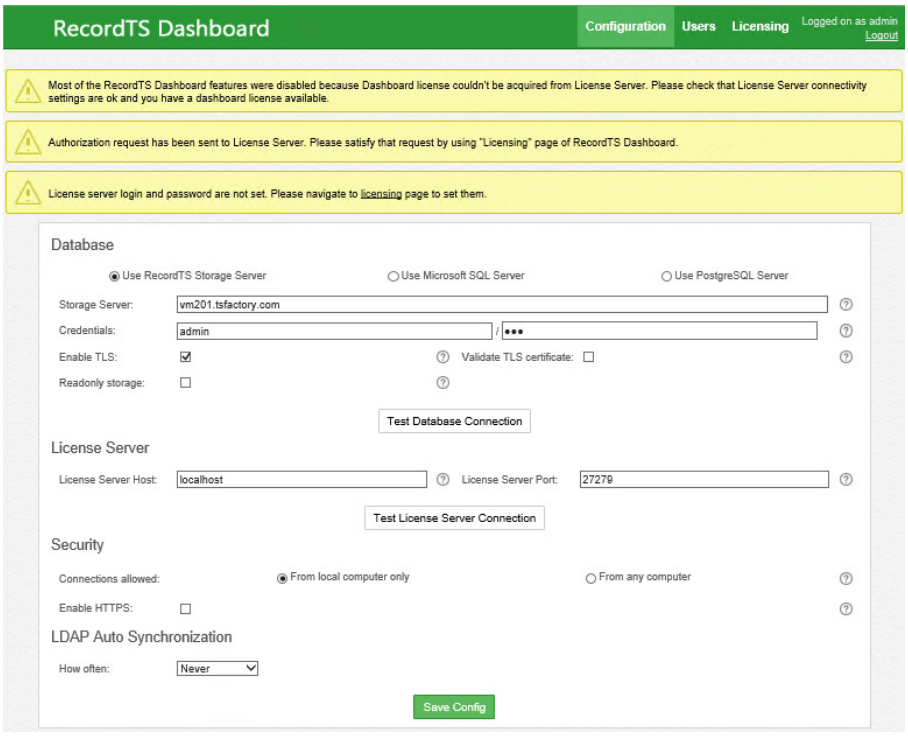


Figure 4-3: Saving the Dashboard Configuration.

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.

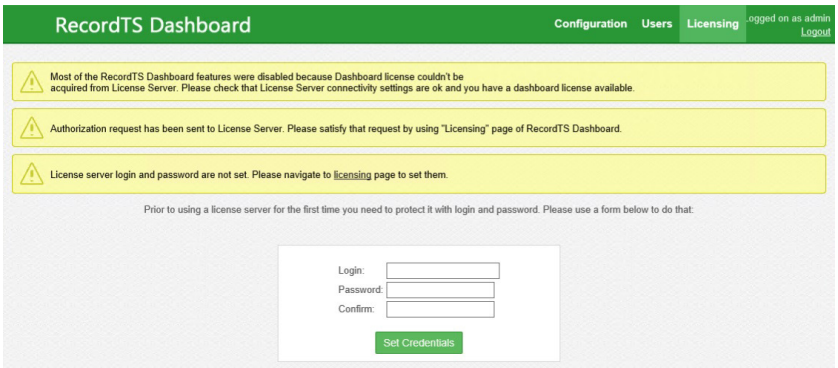


Figure 4-4: Creating Licensing Administrator Credentials

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).

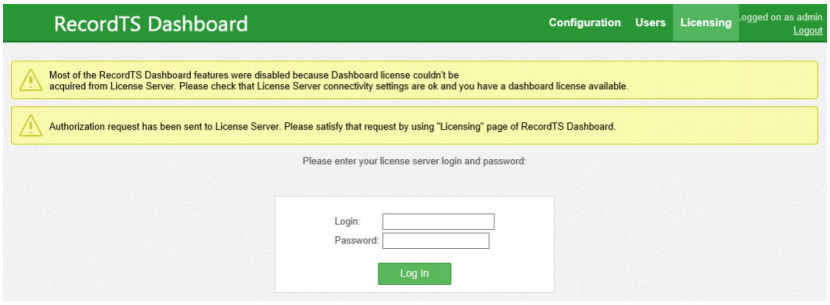


Figure 4-5: Logging into the Licensing Page

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 license key permanently enables the license server.

   (c) A subscription ID effectively links this license server to your customer account. (requires internet connection)

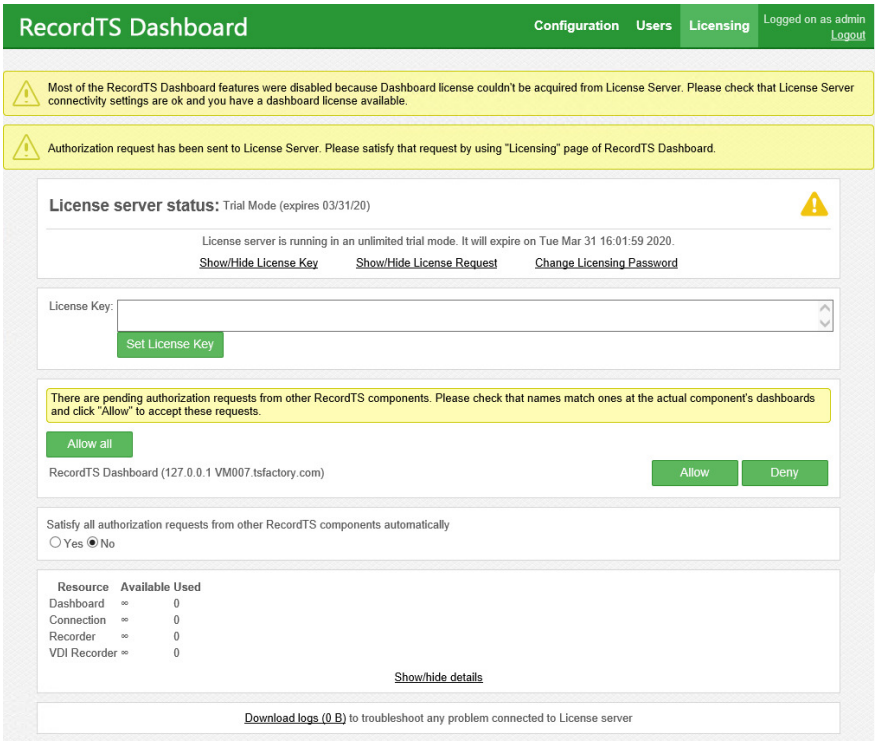


Figure 4-6: Authorizing the License Service

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. If you are using a subscription, log in to your customer account and locate your subscription ID or find the one issued by a TSFactory rep. Copy and paste it into the License Key field (no spaces or new lines after the last character which should be an equal '=' sign) and click on Set License Key.

12. The license service should report it has been authorized and is up and running.

    For subscriptions - if the license server reports authorization required then you may need to return to your customer account and manually authorize this license server. If you look at your subscription in your customer account, there should now be an "Authorize" button. Click on it to authorize your license server.

    Refreshing the Dashboard window should clear the messages after manual authorization.

NOTE: This process can take **up to 5 mins.**

13. 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.

14. 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).

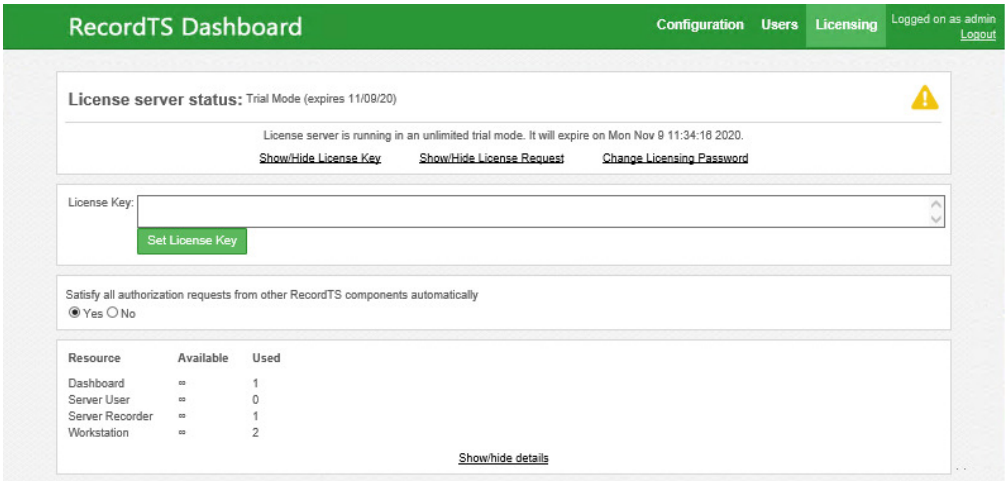


Figure 4-7: Fully Authorized Configuration in Trial Mode

It is now time to begin installing the recorders.

Installing Recorders

Overview

In order to record remote sessions on a Citrix Apps and Desktops server, 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. In the case of workstations, a workstation license will be pulled.

NOTE: Workstation licenses do not require corresponding user licenses. Only server licenses require user licenses for each remote session.

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 **
7. Configure additional options such as https access

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

* remote connections may be lost during these steps
** connections will not be accepted 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 only one type of Recorder in v7 named WVD Recorder. The WVD recorder replaces the previous recorders targeted toward specific protocols. Only one WVD Recorder should be installed on each machine to be recorded.

Supported Windows operating systems:

Windows Server: 2016 and up

Windows Workstation: v10 and up

Prerequisites

- ✓ RecordTS Dashboard and License Service installed and configured, ready to authorize and license recorders.
- ✓ A functioning database server, configured to accept remote connections (the same one used with Dashboard).
- ✓ A Windows machine with Citrix VDA installed in a properly configured, fully tested Citrix Virtual Apps & Desktops environment with Storefront and Delivery Controller.
- ✓ A domain admin or equivalent account to use as Recorder service logon as user account that has admin rights to access the SQL server database if this storage option was enabled.
- ✓ Appropriate postgreSQL database 64-bit ODBC drivers installed (do NOT configure a data source) if this storage option was enabled.
- ✓ 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.

Pre-installation Requirements

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

Warning: you may lock yourself out of the machine remotely after the first restart if you don't fix this beforehand.

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 and newer!

ENDPOINT PROTECTION: Temporarily disable and endpoint protection that may interfere with the installation of the recorder service and its listening ports. Check with your network admins to find out if they are running endpoint protection on the network.

Installing the Recorder

1. Download and run the RecordTS-Recorder-7.x.xxxx.msi installation file on the machine that is to be recorded. 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.

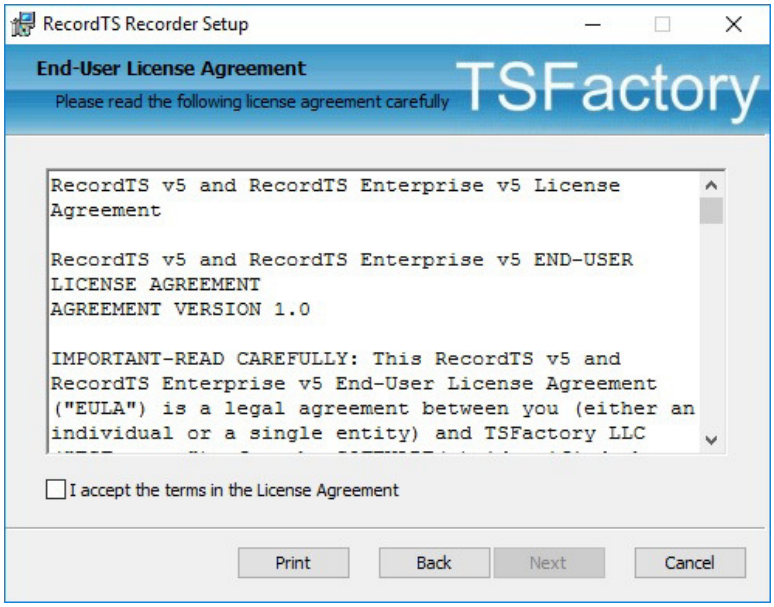


Figure 5-2: Accepting the License Agreement

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:8087.

   Click Next to continue.

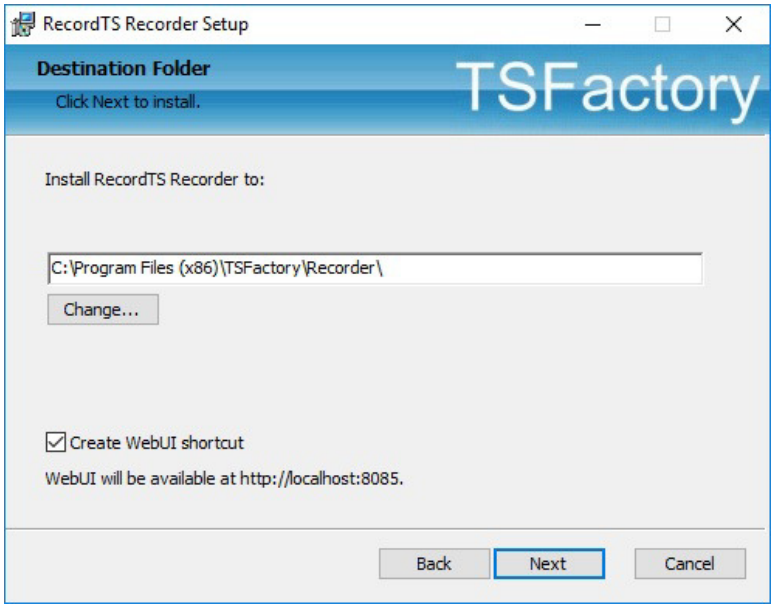


Figure 5-3: Selecting the Installation Directory

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.

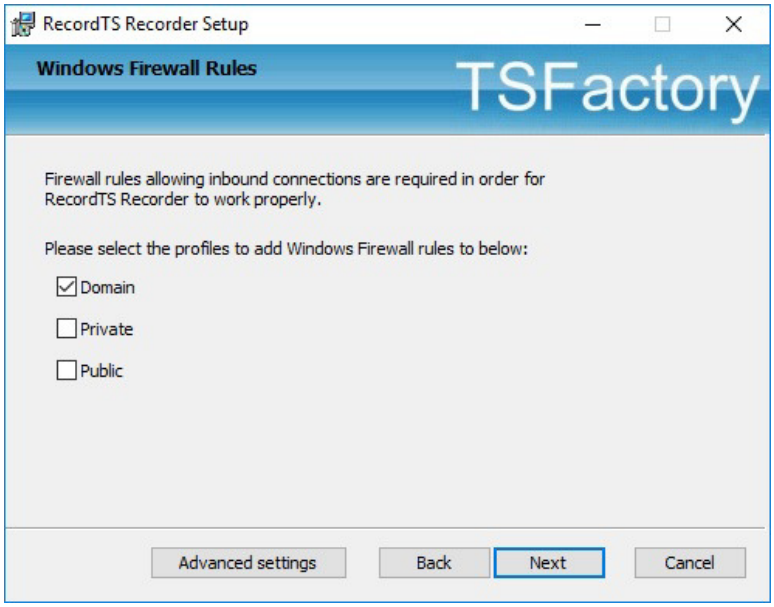


Figure 5-4: Creating firewall rules.

5. In this step, you can choose to enable Licensing Bypass Mode, which allows users to connect remotely without being recorded when RecordTS user licenses are not available. By default, users are not allowed to connect remotely if RecordTS user license are not available. This ensures that all sessions are recorded. Enabling bypass mode should be considered carefully and only used when user connectivity is more important than recording sessions.

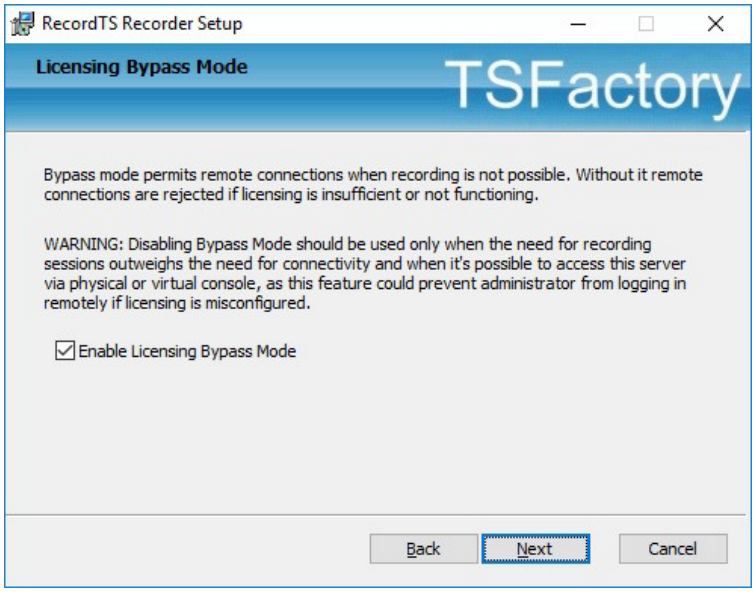


Figure 5-6: Enabling Licensing Bypass Mode

6. In this step, you can choose to enable Database Bypass Mode, which allows users to connect remotely without being recorded when RecordTS cannot connect to the database server to store session data. By default, users are not allowed to connect remotely if the RecordTS recorder loses connection to the

database server. This ensures that all sessions are recorded. Enabling bypass mode should be considered carefully and only used when user connectivity is more important than recording sessions.

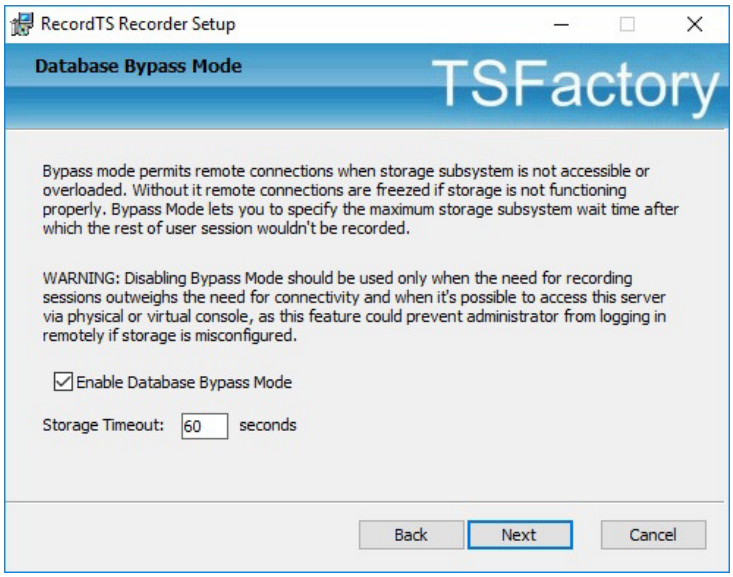


Figure 5-7: Enabling Database Bypass Mode

7. 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.

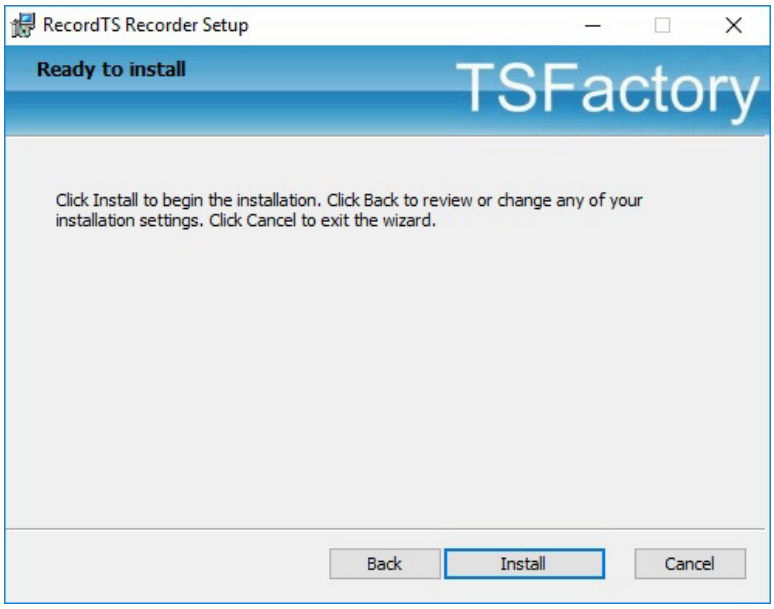


Figure 5-9: Beginning the Recorder Installation

8. 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 5-10: Completing the Recorder Installation

9. 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.

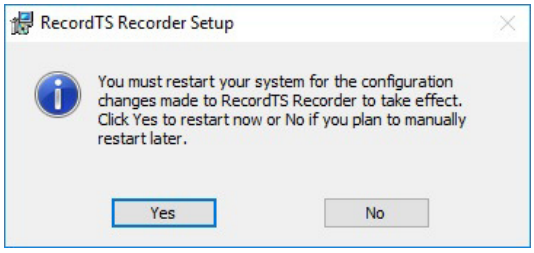


Figure 5-11: Restarting the System

10. Once the system reboots, open the Windows Services applet. The RecordTS Recorder Service and Helper Service should be listed in the Windows Services applet. Check to make sure the Recorder Service is started. The Helper Service does not need to be started.

IMPORTANT: If you are using SQL Server or PostgreSQL Server, then do the following step (do not do this step if you are using RecordTS Storage Server):

Find the RecordTS Recorder Service again. View the properties window and **modify the service to "log on as" a domain admin** or equivalent user account that has full access to the database server (not necessary for the RecordTS Storage Server). Save your changes. The service may warn that a restart is required. Restart the service.

WARNING Restarting the Recorder service may terminate any remote sessions *including yours if you are connected remotely*.

Configuring the Recorder

1. 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.

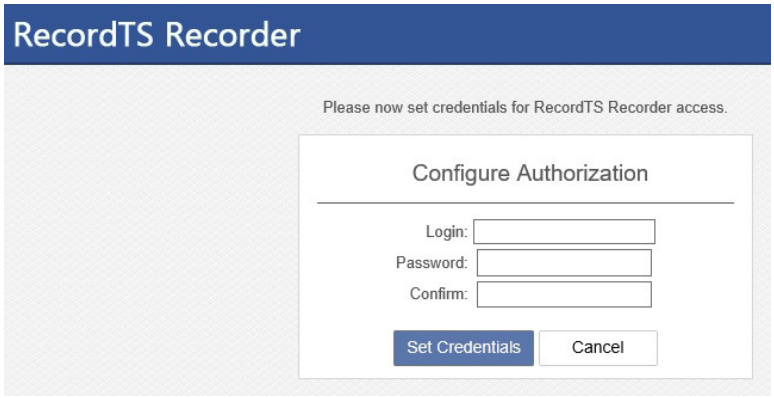


Figure 5-12: Recorder Configuration Console

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

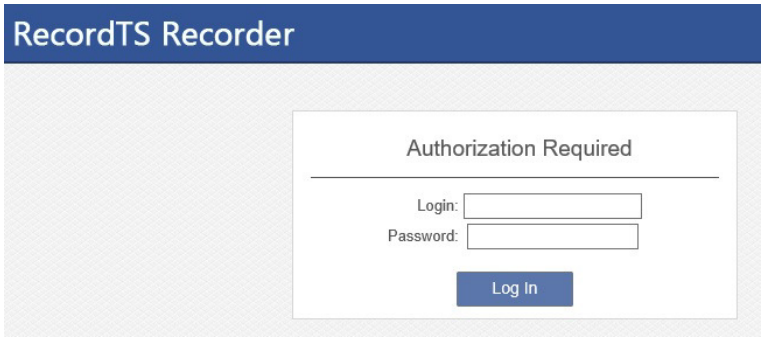


Figure 5-13: Accessing the Recorder Configuration

3. Once you gain access to the Recorder Configuration, you should see the configuration console appear as seen in figure 5-11 below.

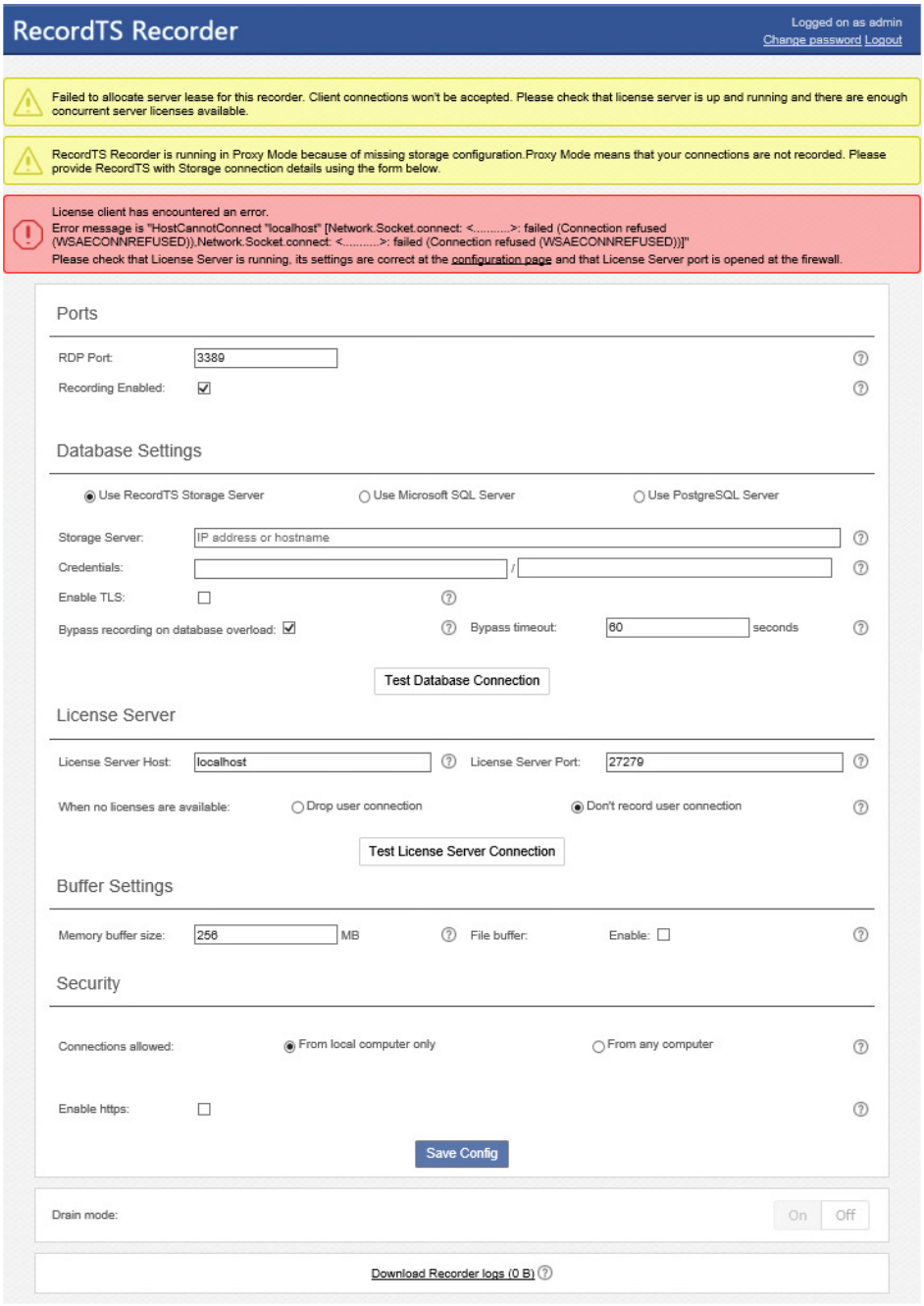


Figure 5-14: Recorder Configuration Console

4. It is recommended to leave the Ports settings as they are unless the terminal server port has been changed. RDP recording may be disabled for this server by unchecking the Recording Enabled check box.
5. Enter the database/storage fields as they were entered in Dashboard and test for connectivity.
6. Enable the Database Bypass mode if so desired. Enabling this feature will allow remote connections and not record them if the system cannot access the database to store session data.

7. Enter the License Server hostname. You may leave “localhost” if the License Server is installed on this machine (not a recommended configuration).
8. It is not recommended to change the License Server port address unless it was changed during configuration at the Dashboard. Test for connectivity.
9. Enable License Bypass mode if so desired. Enabling this feature will allow unrecorded remote connections when licenses cannot be aquired from the RecordTS License Service.
10. Set the Buffer Settings – enable if you intend to use this feature.
11. Enable Security settings such as allowing connections to this webconsole from other computers and https options.
12. Turn on Drain Mode if you intend to use this feature. Enabling this feature will allow graceful session log off while waiting for a system reboot. Once all sessions are logged off (no new connections will be allowed) the system will be allowed to reboot.
13. Now that all the settings have been entered and tested, click on Save Config. The service will restart and request authorization again. Enter the credentials from step 10 and click Log in.
14. The recorder configuration console should raise a warning that the recorder requires authorization from the license server. If it does not, refresh the window.

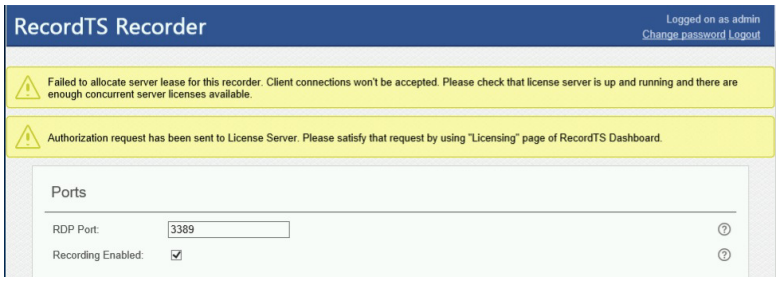


Figure 5-15: Recorder Configuration Console

On-Demand Clones and Instant Clones:

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

15. 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.
16. Go to the Dashboard console and satisfy the recorder authorization request by clicking on the Allow button.

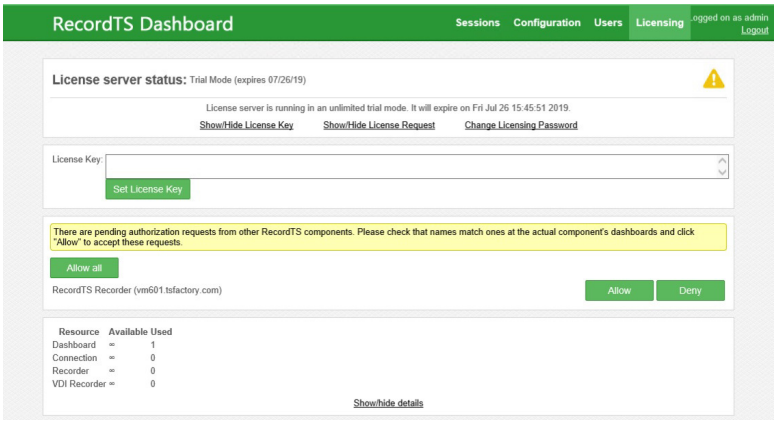


Figure 5-16: Recorder authorization request at Dashboard

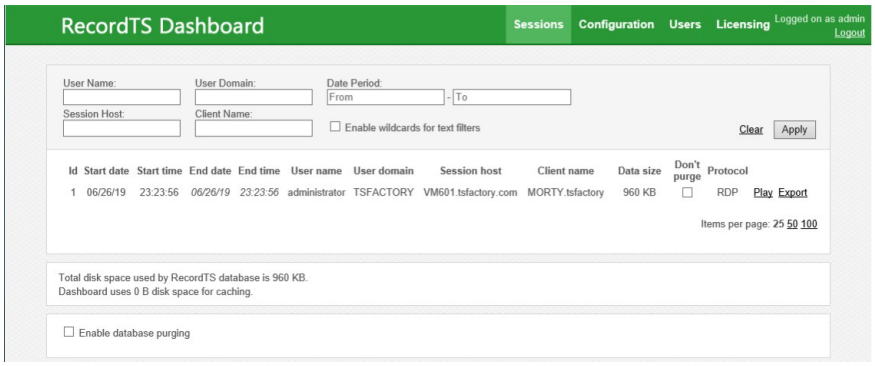
17. Return to the recorder configuration console and refresh the window. You may need to log in again. **DO NOT CLICK SAVE**. When the error message clears, usually within 5 minutes, the recorder should be ready to accept connections and record.
18. Verify functionality by connecting remotely and look for a session to appear in the Dashboard webconsole Sessions tab.

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.



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 (.m2ts) [Blu-ray Disc Audio-Video (BDAV) MPEG-2 Transport Stream] 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.
5. Close the tab when done viewing.

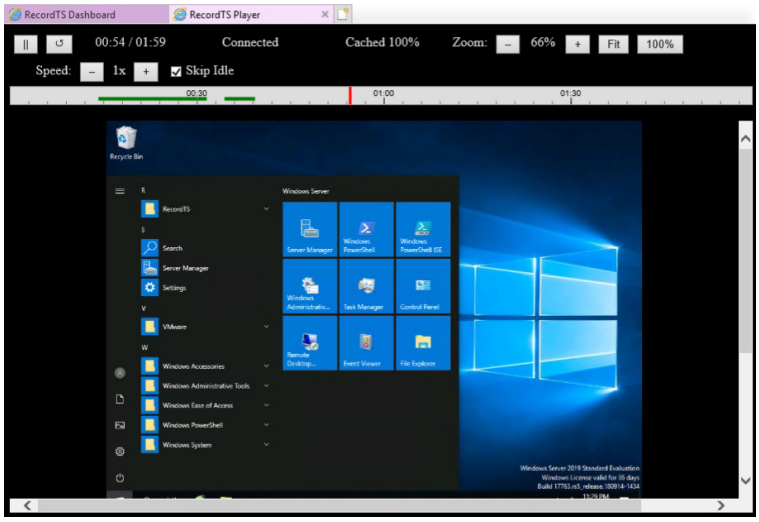


Figure 6-1: Viewing a Session in the WebPlayer

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:

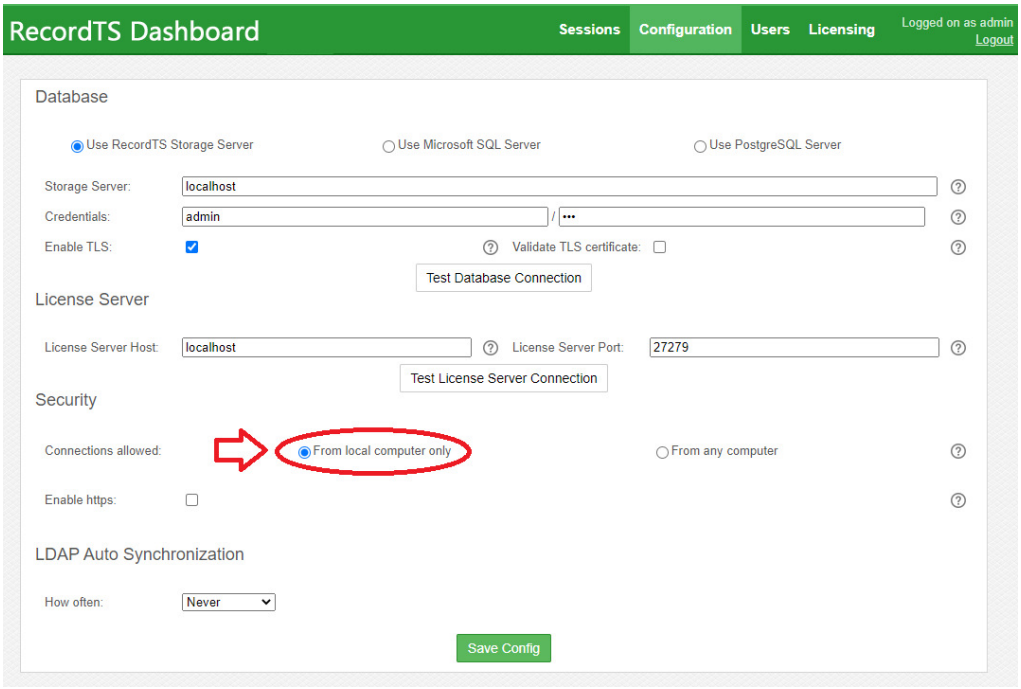


Figure 7-1: Allowing remote access to Dashboard

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:

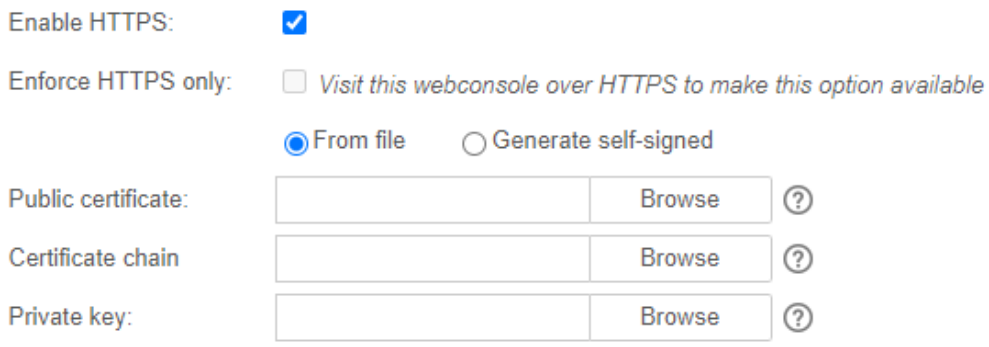


Figure 7-2: Enabling HTTPS access

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:

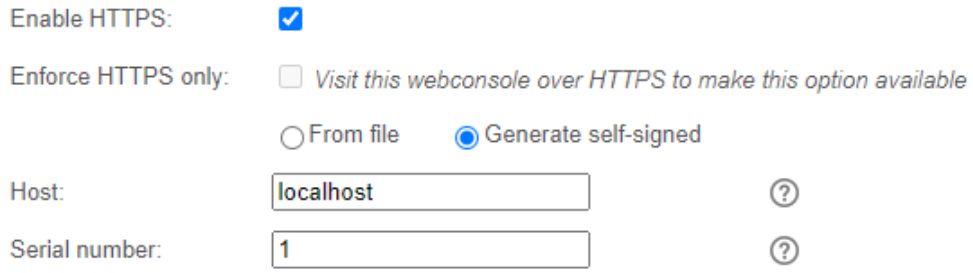


Figure 7-3: Generating a Self-signed Certificate

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 is 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.

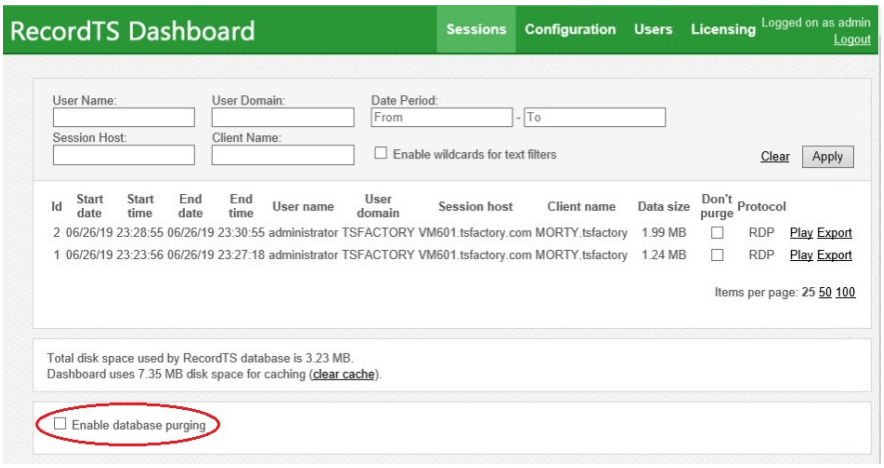


Figure 7-4: Database purge feature

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.

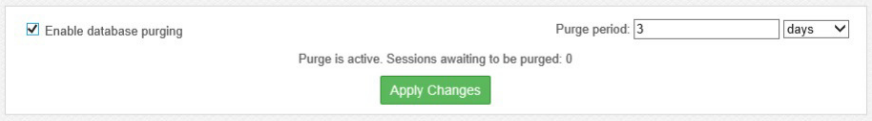


Figure 7-5: Enabling database purging

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.

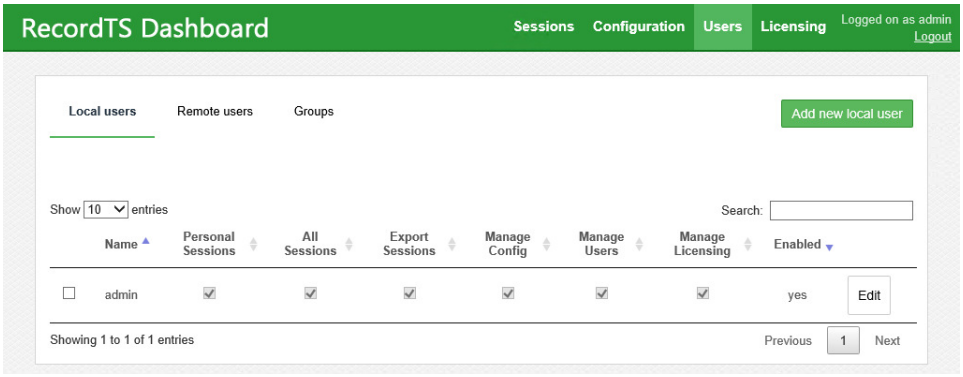


Figure 7-6: Setting up User accounts

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.

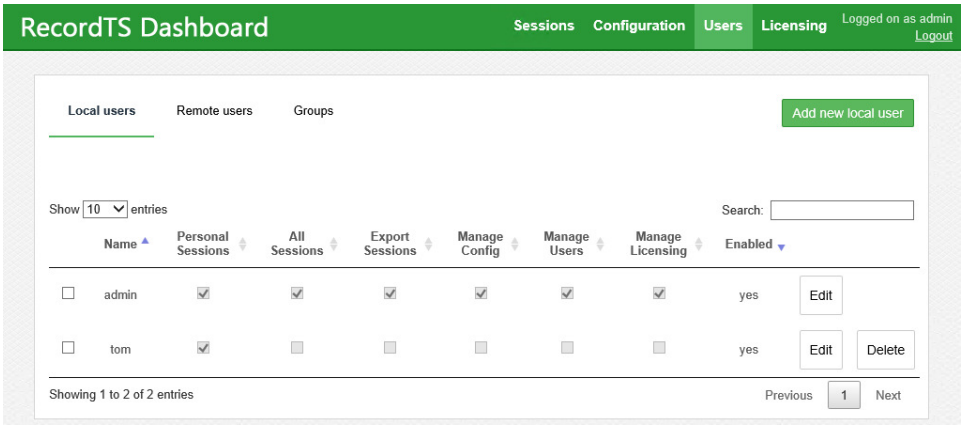


Figure 7-7: Managing User accounts

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.

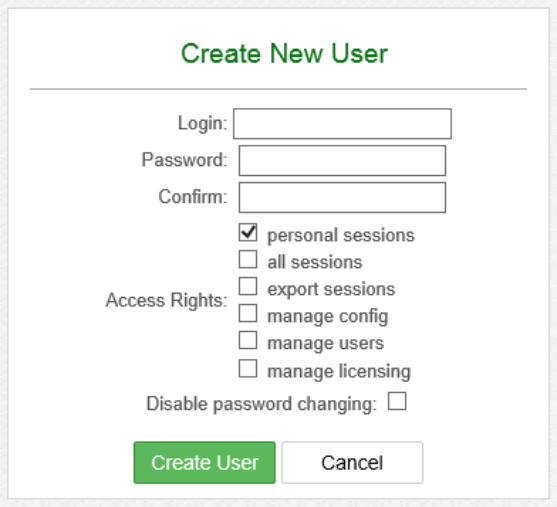


Figure 7-8: Create New User Dialog

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.

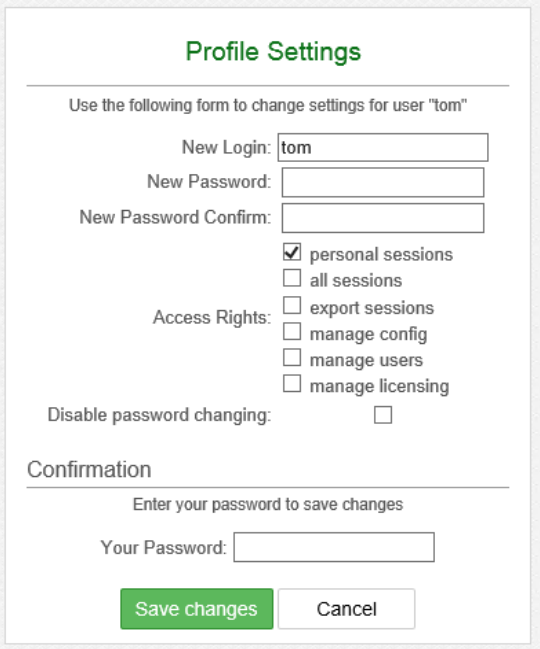


Figure 7-9: Edit User Profile Dialog

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.

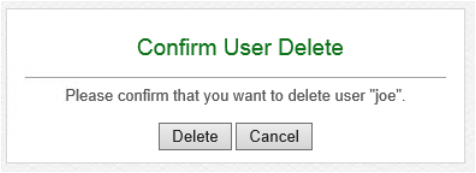


Figure 7-10: Delete User Confirmation Dialog

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:

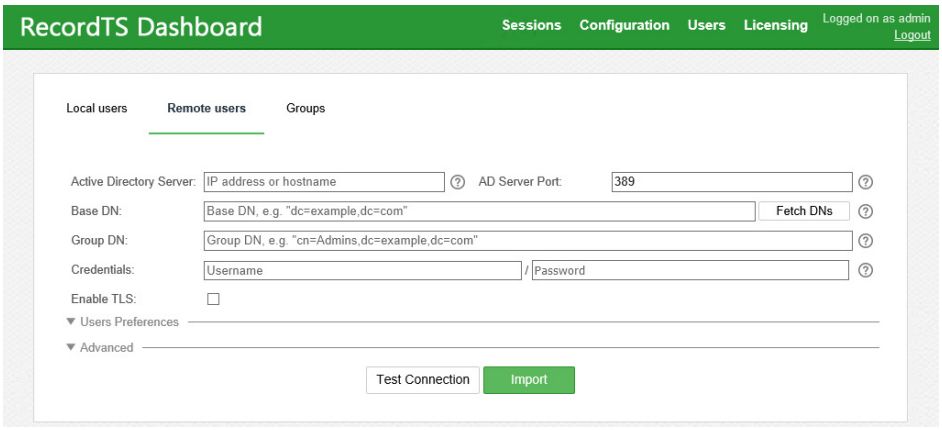


Figure 7-11: Import User Dialog

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:

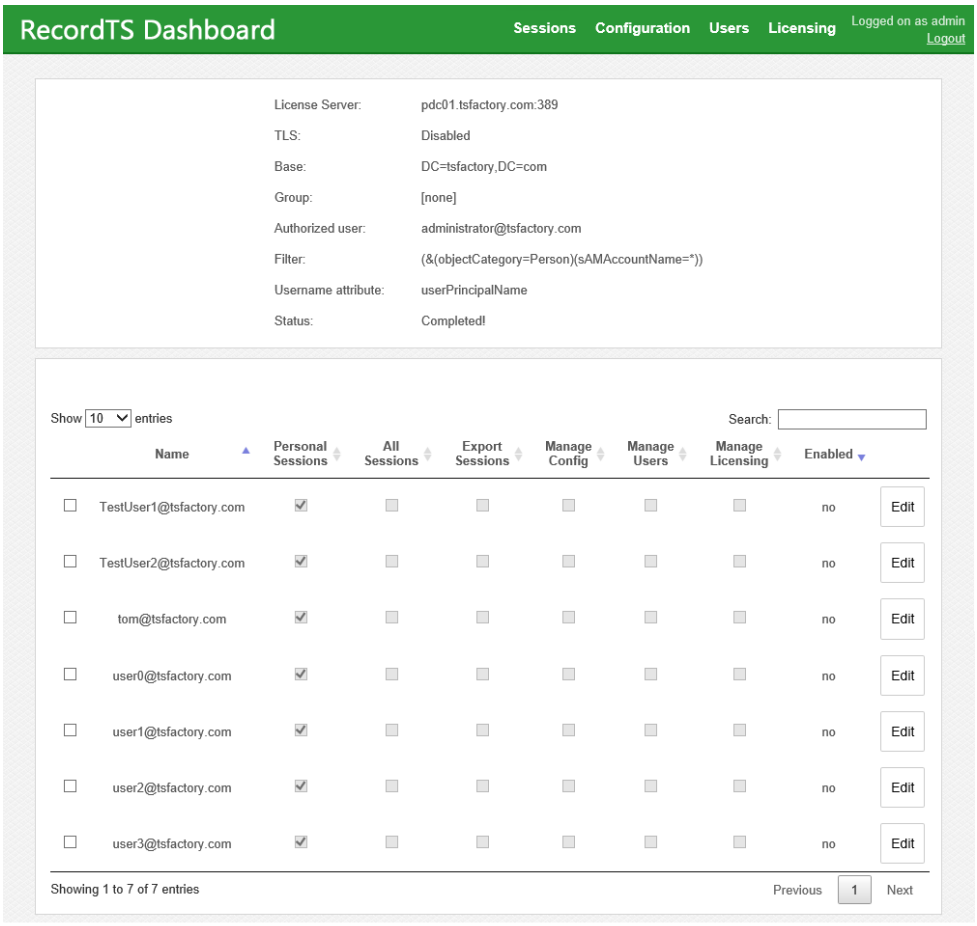


Figure 7-12: Imported Users

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.

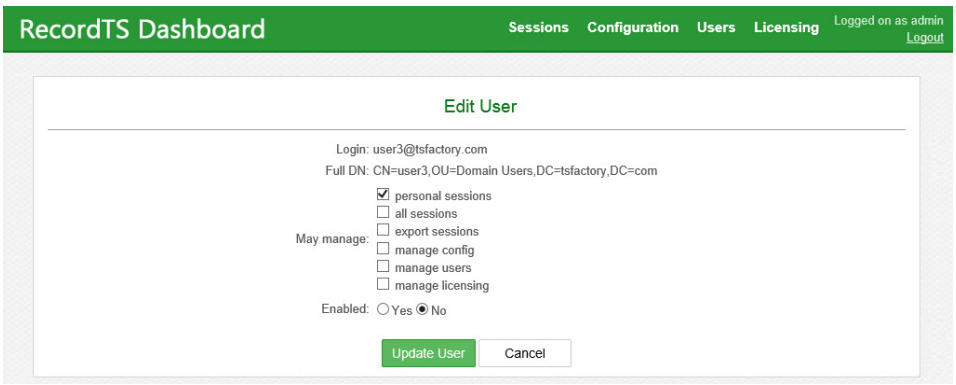


Figure 7-13: Edit Imported User

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.

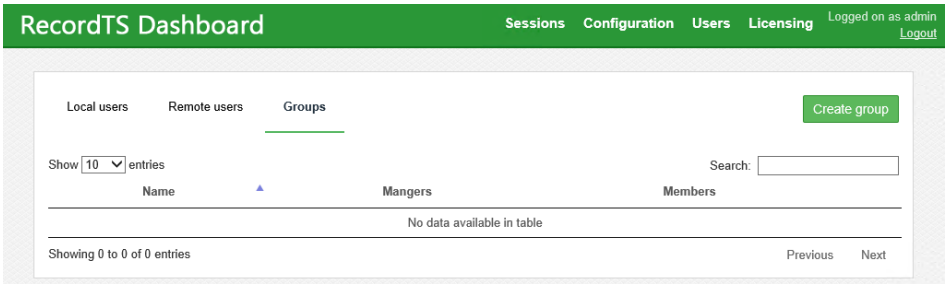


Figure 7-14: Creating User Groups

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

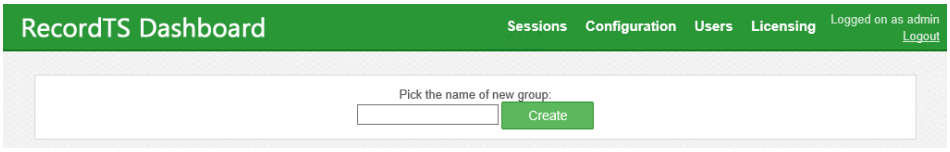


Figure 7-15: Create a Group

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

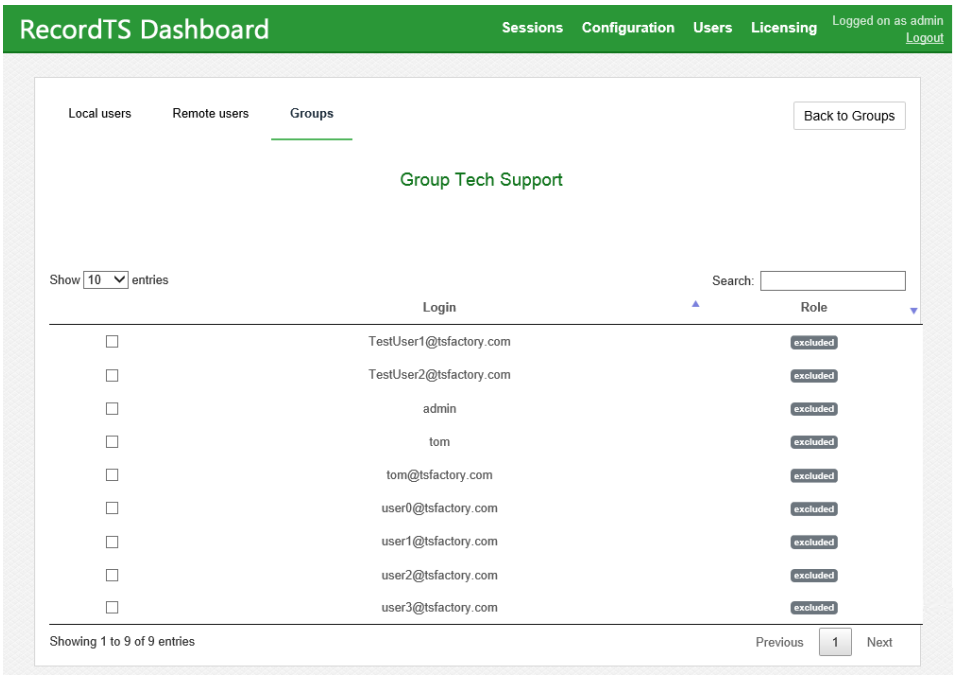


Figure 7-16: Select Users for New Group

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.

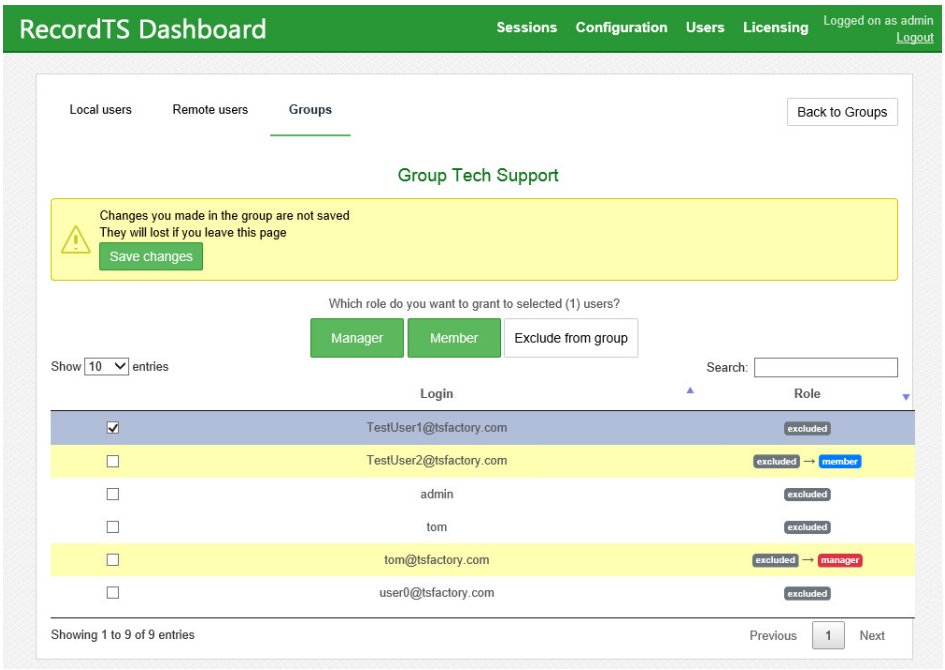


Figure 7-17: Select Users for New Group

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 Recorder for Terminal Services Configuration:

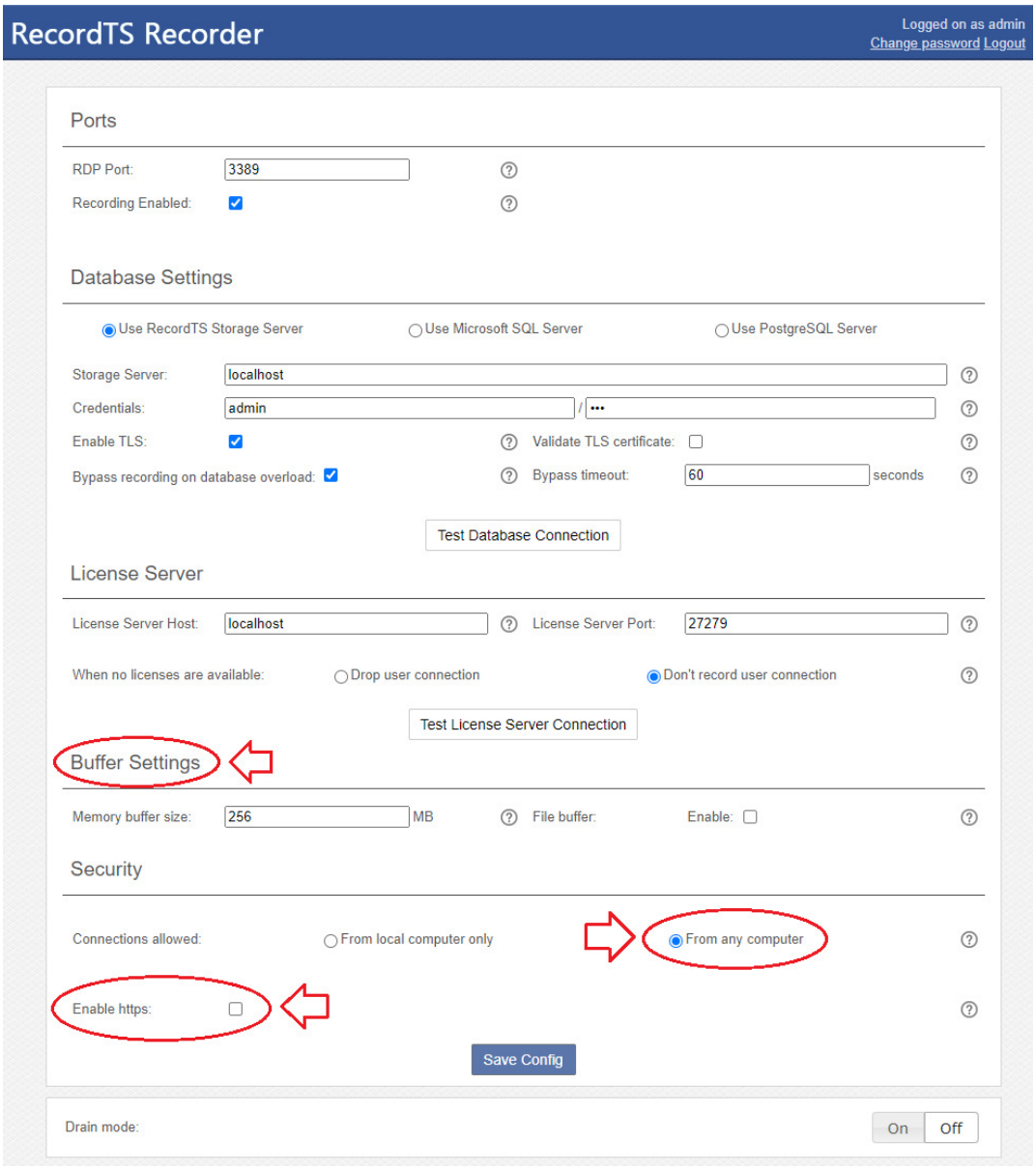


Figure 8-1: Recorder Configuration Dialog

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.

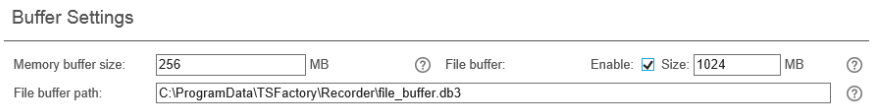


Figure 8-2: Enabling the File Buffer Feature

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).

NOTE: There is a non-documented feature that can change the default behavior of the recorder when buffers are completely exhausted to allow sessions to continue without being recorded. Please contact support for instructions on how to set this option via registry edits.

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.

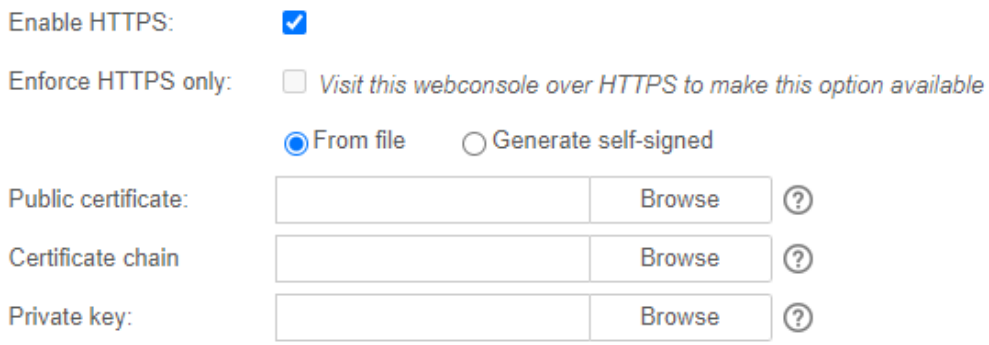
NOTE: Changing this feature will reduce security by allowing foreign computers to have access to the Recorder configuration.

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:8085 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:



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.

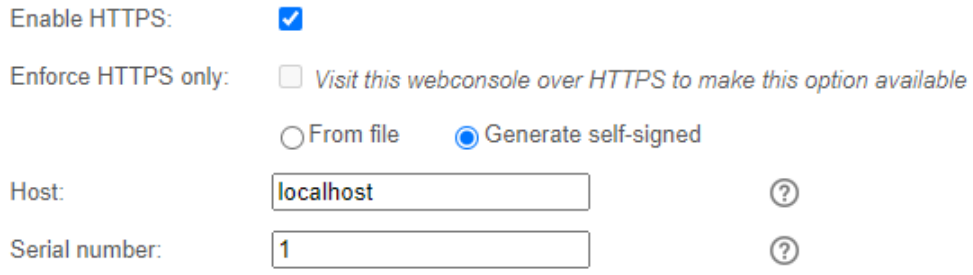
NOTE: Details for creating certificates for use with Recorder webconsole https can be found in a separate document "Securing RecordTS Web Interfaces". Contact our support staff for a copy of this document or visit our website.

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:



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 is 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.

Drain Mode

The drain mode feature allows users to continue working when a server reboot is initiated by Windows. The recorder will hold off the reboot until the last remaining user has logged off their session. Then the system reboot will commence and new RDP connections will be ignored until the recorder service has determined that Windows terminal services is ready to accept new connections. Normal operations will continue once the recorder is listening on port 3389 and ready to accept remote desktop connection requests.

To enable Drain Mode, click on the On button labeled Drain mode as shown in figure 8-3 below.

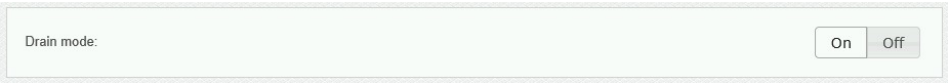


Figure 8-3: Drain Mode Option

Once Drain Mode has been enabled, a warning message will be displayed, indicating the number of users currently logged into the system and any actions that will be taken. Refer to figure 8-4 below.

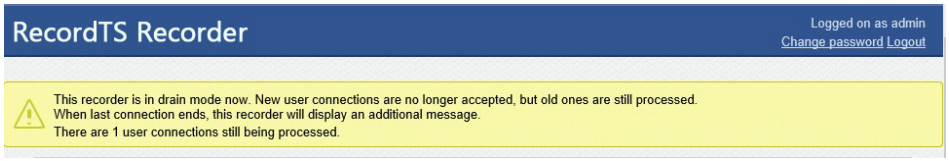


Figure 8-4: Drain Mode Example Warning Message

Disabling Drain Mode will dispense with the warning message and return operation back to normal. Once all remote sessions have disconnected, a message will be displayed informing that Drain Mode may be turned off.

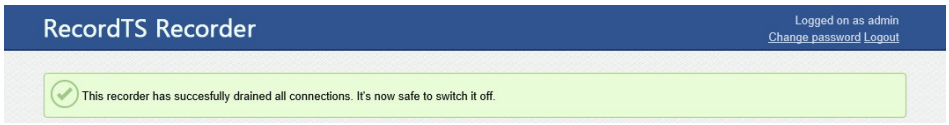


Figure 8-5: Drain Mode "All Clear" Message

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:

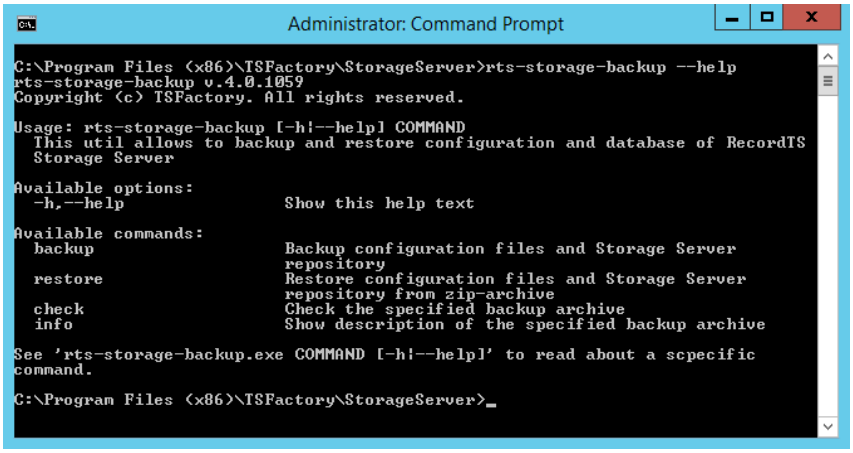
On the machine that RecordTS Storage Server is installed, open a DOS command or Powershell window and navigate to the RecordTS Storage Server program files folder here:

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

Execute the following command:

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

Here is the output:



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.

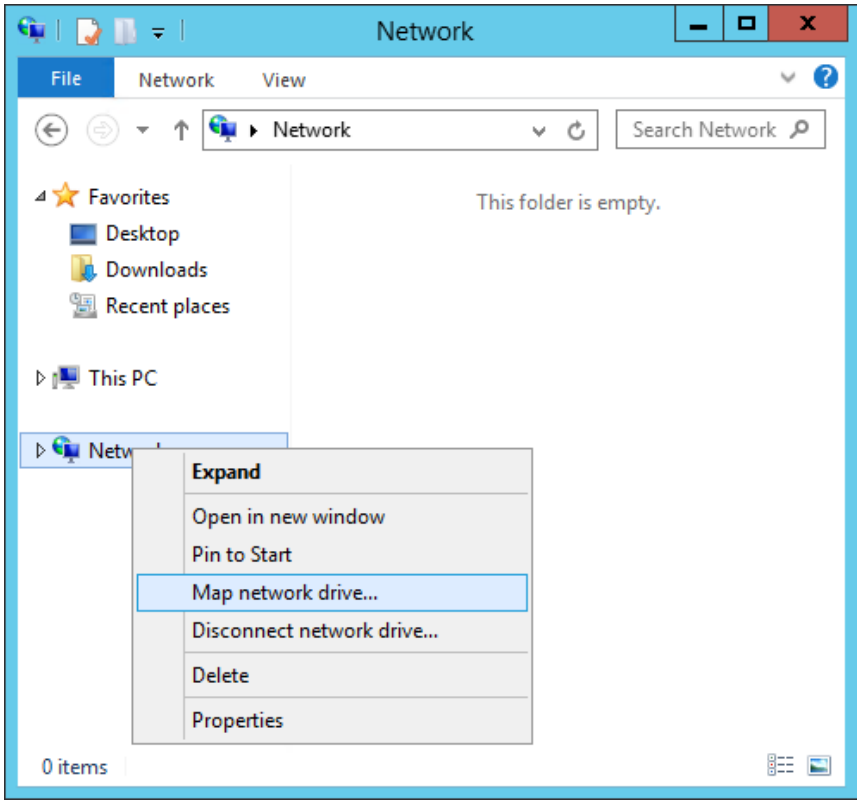
Backup Tool Examples

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.

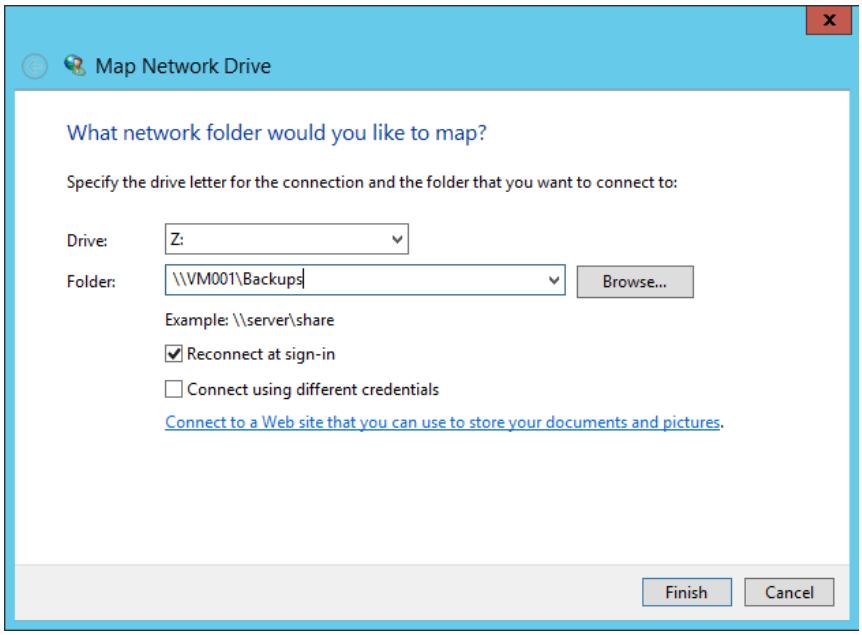
To backup the database to another machine (network share) on your network, you will first need to map a local network drive to that machine.

Mapping a Network Drive

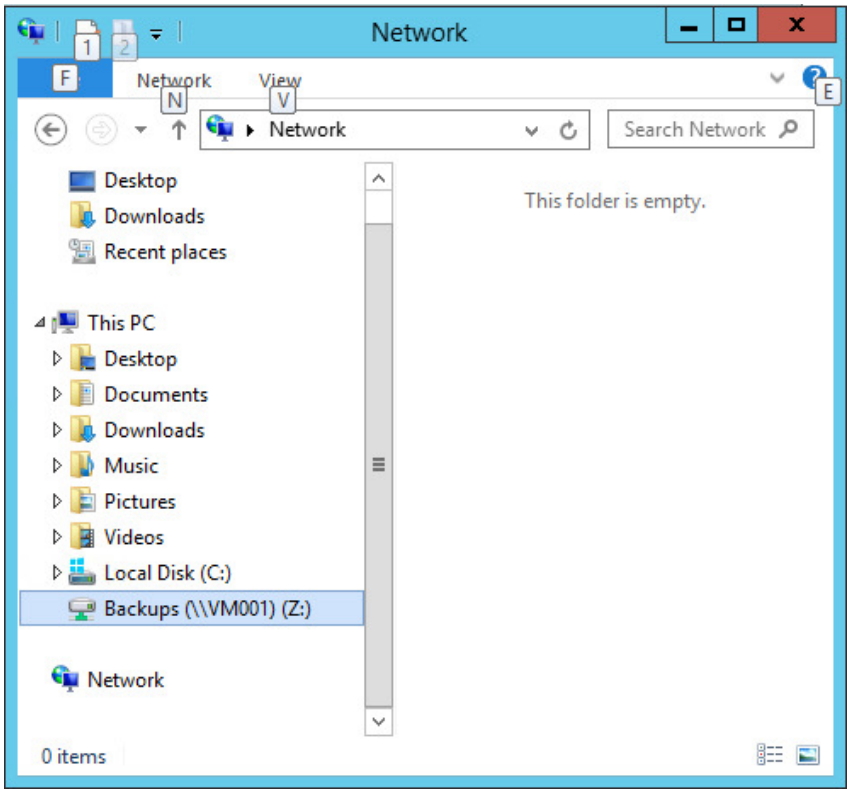
On the RecordTS Storage Server, open File Explorer and right mouse click over the Network icon.



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”
```

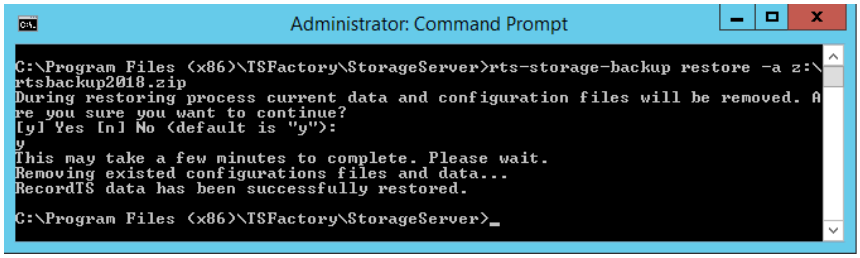
Here is a screen shot of the backup procedure:

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:



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
```

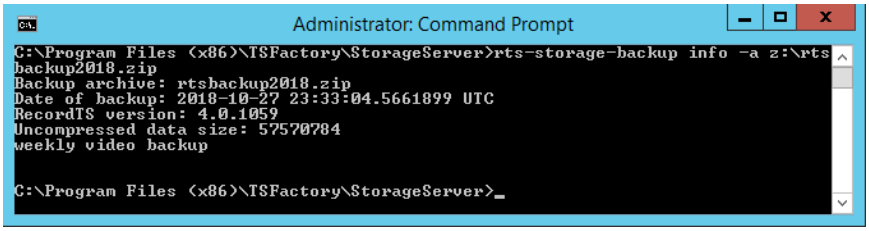
Here is a screen shot of the archive integrity check procedure:

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:



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 resourses 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:

Check that the Dashboard service is set to “log on as” a user account such as a domain admin or equivalent that has permissions to access and manage the database server. Rights should include database creation. The service will need restarting once the user account has been assigned.

Verify connectivity to the database server using a database admin tool. Sometimes SQL Server and postgreSQL need to be configured to accept remote connections. Refer to the Database Problems section below for more info on how to configure the databases to allow remote connections.

If you are using postgreSQL, make sure the postgres ODBC 32-bit drivers are installed. You do not need to create a data source, just install the drivers. The 64-bit drivers will not work so please use the drivers that are included in the download zip file.

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:

Check that the Recorder service is set to “log on as” a user account such as a domain admin or equivalent that has permissions to access and manage the database server. Rights should include database creation. The service will need restarting once the user account has been assigned.

Verify connectivity to the database server using a database admin tool. Sometimes SQL Server and postgreSQL need to be configured to accept remote connections. Refer to the Database Problems section below for more info on how to configure the databases to allow remote connections.

If you are using postgreSQL, make sure the postgres ODBC 32-bit drivers are installed. You do not need to create a data source, just install the drivers. The 64-bit drivers will not work so please use the drivers that are included in the download zip file.

Users cannot connect remotely after installation and rebooting:

There are several reasons why this can happen. First verify that the Recorder service has installed itself properly. Check the recorder service is running and then look for any errors in the Windows event logs. Make sure you are not logged in locally and have Record Local Admin Sessions disabled.

Please make sure you completely disable all anti-virus software as it will see this port movement as an assault on the system and prevent RecordTS from installing properly.

Database Problems

Before we get into listing common problems, one of the first things to note is that by default, both MS SQL Server and PostgreSQL require additional configuration to allow remote access to the databases. Each product is different in its configuration and if you suspect this is the problem, then please refer to the sections below on how to configure the database to allow remote connections.

Database connection errors:

Check that the Recorder and Dashboard services are set to “log on as” a user account such as a domain admin or equivalent that has permissions to access and manage the database server. Rights should include database creation. The service will need restarting once the user account has been assigned.

Verify connectivity to the database server using a database admin tool. By default, SQL Server and postgreSQL need to be configured to accept remote connections. Refer to the sections below that describe how to configure the databases to allow remote connections.

If you are using postgreSQL, make sure the postgres ODBC 32-bit drivers are installed. You do not need to create a data source, just install the drivers. The 64-bit drivers will not work so please use the drivers that are included in the download zip file.

Database cannot be created or accessed:

This is usually because someone tried to create the database themselves. Please let the software create the database for you as it will create the necessary schema and tables that are required by RecordTS.

Verify that the user account that the Dashboard or Recorder service is set to “log on as” has the required permissions to create and manage a database.

Database schema needs to be updated:

Simply click on the upgrade button and RecordTS will make the current database format compatible with the new database schema.

Configuring PostgreSQL to Allow Remote Connections:

PostgreSQL needs to be configured to allow connections from other machines on the network. By default it blocks all remote connections. You will need to edit the postgres configuration file “pg_hba.conf” to allow remote connections. This **cannot** be done from the database admin utility PGAdmin. You must edit the configuration

file manually as shown below. The path to the file will look something like this:

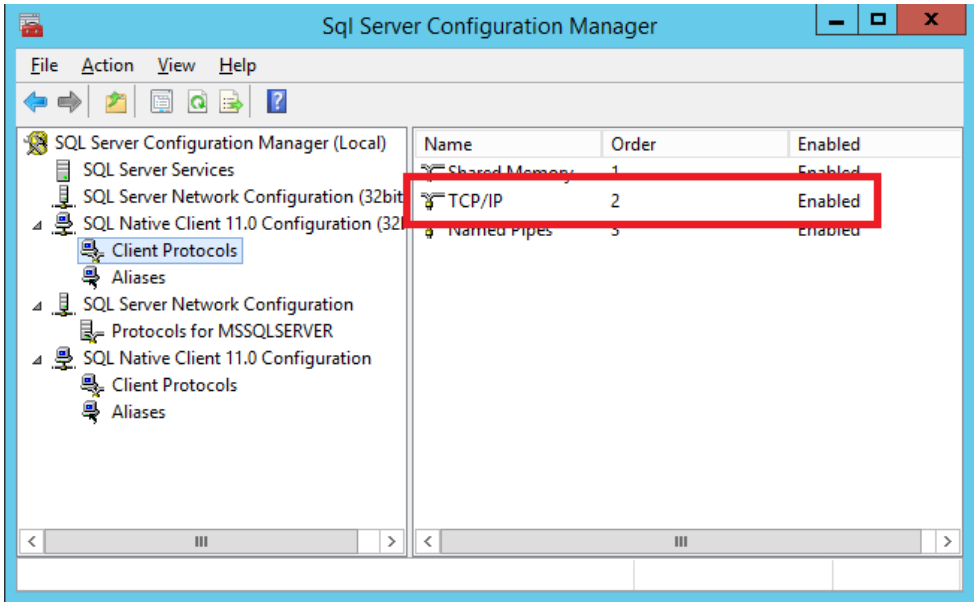
```
C:\Program Files\PostgreSQL\9.6\data
```

Here is an example to allow connections from all machine IP's for IPv4:

```
# IPv4 local connections:
host    all             all             127.0.0.1/32            md5
host    all             all             0.0.0.0/0               trust
```

Configuring MS SQL Server to Allow Remote Connections:

MS SQL Server needs to be configured to allow connections from other machines on the network. By default it blocks all remote connections. You will need to edit the configuration using the SQL Server Configuration Manager utility to allow remote connections. The TCP/IP protocol must be Enabled in the SQL network client protocol configurations. See below for an example.



Downloading Log Files

When asked to do so, you may download log files for the support team to review. Each module and page have its own place to download logs from. You will be instructed which logs to download. If the files are small, under 5 MB, then email them to support@tsfactory.com. Otherwise you will be given a place to store the files for the support team.

List of Service Ports

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