TotalRecallVR

.: www.totalrecallvr.com :.

Infinity Cockpit

User Guide

February, 2024

Guide Issue 2.0

Total Recall VR Cockpit Release 20.5.0

Prolancer

Related Documents:

[1] Prolancer Pty Ltd, Total Recall VR website. Available from: http://www.totalrecallvr.com/.

[2] Prolancer Pty Ltd, Prolancer website. Available from: http://www.prolancer.com.au/.

[3] Prolancer Pty Ltd, Total Recall VR Infinity Overview User Guide, 2.0, February 2024

Table of Contents

1. Preface **7**

1.1. Conventions *7*
1.1.1. Notes & Warnings 7
1.1.2. Typographic Conventions 7
1.1.3. Procedures 9

1.2. We Need Feedback *9*

2. Introduction **10**

2.1. About this Guide *10*

2.2. What is Total Recall VR Infinity? *10*

2.3. What is Total Recall VR Infinity Cockpit? *10*

3. Start Here **13**

3.1. System Requirements *13*

3.2. Compatibility *14*

3.3. Working Mode *14*
3.3.1. Workstation Mode 14
3.3.2. Workgroup Mode 15

3.4. Network Ports *16*

3.5. Pre-installation – Windows Device *18*
3.5.1. Visual C++ 2019 Redistributable 19
3.5.2. FTDI 2DXX Drivers 19

3.6. Application Configuration Database *20*
3.6.1. Derby Server 20
3.6.2. H2 Server 21
3.6.3. PostgreSQL Server 24
3.6.4. MariaDB or MySQL Server 25
3.6.5. Microsoft SQL Server 26

3.7. Application Installation – Windows Device *27*

3.8. Application Activation *27*

3.9. Default User *35*

3.10. Application Preferences *36*
3.10.1. Locale 37
3.10.2. Database 37
3.10.3. Audit Log 39
3.10.4. E-Mail Server 41
3.10.5. Playlist 41
3.10.6. Cache 41
3.10.7. Digital Certificates 43

3.11. Application Upgrade – Windows Device *43*

3.12. Application Upgrade – Appliance Recorder *44*

3.13. Application Support *44*

4. User Interface **48**

4.1. Application Views *48*

4.2. Application Menu *49*

4.3. Application Menu Bar *49*
4.4. Touch Gestures *51*
4.5. On Screen Keyboard *51*
4.6. Forms *53*

5. User Configuration **56**
5.1. Authentication *56*
5.2. Authorisation – Application *56*
5.3. Authorisation – Recordings *56*
5.4. User Management *59*

6. Filtering and Searching **61**
6.1. Anatomy of a Filter *61*
6.2. Instant Filter Builders - Recordings *63*
6.3. Advanced Filter Builder - Recordings *65*
6.4. Instant Filter Builders – Audit Events *74*
6.5. Advanced Filter Builder – Audit Events *74*

7. Recording Management **75**
7.1. Recording Repositories *75*
7.1.1. Web Repository 76
7.1.2. Network Repository 77
7.1.3. Portable Repository 78
7.2. Recording Browser *79*

8. Event Reconstruction & Replay **84**
8.1. Event Timeline *84*
8.2. Event Sharing *88*
8.3. Media Player *90*

9. Live Monitoring **92**
9.1. Media Feeds *92*
9.2. In-progress Recording Monitor *93*
9.3. In-progress Recording Timeline *95*
9.4. Media Monitor *97*

10. Recorder Service Monitoring & Configuration **98**
10.1. Recorder Nodes *98*
10.1.1. Appliance Recorder Node 100
10.1.2. Custom Recorder Node 100
10.2. Service Status *100*
10.3. Service Control – All Services *102*
10.4. Service Control – Cockpit *103*
10.5. Service Control – Media Repository Archive Connector *103*
10.6. Service Control – Media Repository House Keeper *104*

10.7. Service Control – Recording Service ... *104*
10.8. Service Configuration – Audit Event REST Service ... *105*
10.9. Service Configuration – Audit Repository House Keeper ... *106*
10.10. Service Configuration – Audit Repository IPC Connector ... *108*
10.11. Service Configuration – Cockpit ... *109*
10.12. Service Configuration – Database Service ... *110*
10.13. Service Configuration – Media Repository Archive Connector ... *111*
10.14. Service Configuration – Media Repository House Keeper ... *115*
10.15. Service Configuration – Media Repository IPC Connector ... *117*
10.16. Service Configuration – Meta Data REST Service ... *119*
10.17. Service Configuration – Monitor Service ... *121*
10.18. Service Configuration – Profile REST Service ... *123*
10.19. Service Configuration – Recording Service ... *125*
10.20. Service Configuration – Recordings REST Service ... *129*
10.21. Service Configuration – RTP Media Server ... *130*
10.22. Service Configuration – RTSP Media Server ... *133*
10.23. Service Configuration – SIP Media Server ... *135*
10.24. Service Configuration – Tait VRP Media Server ... *139*
10.25. Service Tools – Profile REST Service ... *142*
10.25.1. Manage Transforms ... 143
10.25.2. Manage Policies ... 144

11. Appliance Recorder Manager ... 147
11.1. System Configuration – Data & Time ... *147*
11.2. System Configuration – Network ... *149*
11.3. System Configuration – Network Storage ... *151*
11.4. System Configuration – License ... *152*
11.5. System Configuration – Support ... *154*
11.6. System Control - Shutdown ... *156*
11.7. System Tools – Detach USB ... *156*
11.8. System Tools – Manage Disks ... *157*
11.9. System Tools – Upgrade ... *161*
11.10. System Tools – Get Logs ... *162*
11.11. System Tools – Tail Logs ... *162*
11.12. System Tools – Request License ... *163*

12. Archiving ... 165
12.1. House Keeper vs Archiver ... *166*
12.2. Manual Archiving to a Network Repository ... *167*
12.3. Manual Archiving to a Portable Repository ... *169*
12.4. Automatic Archiving to a Web Repository ... *171*
12.5. Automatic Archiving to a Network Repository ... *172*

12.6. Automatic Archiving to a Portable Repository *176*

13. Auditing **180**

13.1. Audit Repositories *180*

13.2. Audit Browser *182*

14. Software License **186**

1. Preface

1.1. Conventions

Our guides use several conventions to highlight certain words and phrases and draw attention to specific pieces of information.

1.1.1. Notes & Warnings

We use the following visual styles to draw attention to information that might otherwise be overlooked:

Notes are tips, shortcuts or alternative approaches to the task at hand. Ignoring a note should have no negative consequences, but you might miss out on information that makes your life easier.

Important boxes detail things that are easily missed. Ignoring the information will not cause data loss but may cause irritation and frustration.

Warnings should not be ignored. Ignoring warnings will most likely cause data loss or incorrect function.

1.1.2. Typographic Conventions

We use typographic conventions to call attention to specific words and phrases. These conventions and the circumstances they apply to are as follows.

Example	***Meaning***
Select Guide to display ...	Locate the link named "Guide" on the screen and then either: • Position the cursor over the link and then depress the appropriate mouse button to follow the link; or

	• Tap on the link with a single finger to follow the link.
Select **Add** to ...	Locate the button or menu item named "Add" on the screen and then either: • Position the cursor over the button or menu item and then depress the appropriate mouse button to initiate an action; or • Press the button with a single finger to initiate the action.
Select ↷ to ...	Locate the button or menu item with the icon "↷" on the screen and then either: • Position the cursor over the button or menu item and then depress the appropriate mouse button to initiate an action; or • Press the button with a single finger to initiate the action.
Enter ***Commission*** ... or Set ***Commission*** ...	Locate the field named "Commission" on the screen and then either: • Position the cursor over the field and then depress the appropriate mouse button to select the field. Once the cursor appears in the field, enter a value; or • Tap on the field with a single finger to select the field. Once the cursor appears in the field, enter a value.
Choose ***Country*** ...	Locate the field named "Country" on the screen and then either: • Position the cursor over the field and then depress the appropriate mouse button to display the available options. Then position the cursor over the desired option and depress the appropriate mouse button to select it; or • Press on the field with a single finger to display the available options. Then tap with a single finger on the desired option to select it.
Tick ***Active User*** ...	Locate the check box named "Active User" on the screen and then either: • Position the cursor over the check box and depress the appropriate mouse button to place a visual tick in the box; or • Tap on the check box with a single finger to place a visual tick in the box.

Un-tick ***Active User*** ...	Locate the check box named "Active User" on the screen and then either: • Position the cursor over the check box and depress the appropriate mouse button to remove the visual tick in the box. • Tap on the check box with a single finger to remove the visual tick in the box.
Enter *$30.95* ...	Enter "$30.95" using the keys on your physical or on-screen keyboard.

1.1.3. Procedures

We use a numbered sequence of steps to define procedures for performing specific tasks. For example:

Procedure Title

1. This is the first step of the procedure.
2. This is the second step of the procedure.
    a. This is the first sub-step of step two.
    b. This is the second sub-step of step two.
3. This is step three.

1.2. We Need Feedback

If you find a typographical error in this guide, or if you have thought of a way to make this guide better, then we would love to hear from you.

Please submit your feedback to mailto:feedback@prolancer.com.au.

If you have a suggestion for improving the guide, try to be as specific as possible when describing your suggestion. Otherwise, if you have found an error, please include the section number and some of the surrounding text to help us locate it.

2. Introduction

2.1. About this Guide

This is the definitive user guide for the Total Recall VR Infinity Cockpit application.

The guide is intended for the end users of Total Recall VR Infinity Cockpit. It describes how to use the application to achieve desired outcomes. Please keep a copy of this guide handy for a quick reference.

2.2. What is Total Recall VR Infinity?

Total Recall VR Infinity is the latest generation technology that powers Total Recall VR professional audio logging and call recording appliances, custom recorders and associated applications.

Total Recall VR has more than 20 years of history of creating professional audio logging and call recording systems that are self-contained, fully featured and cost-effective. Enterprises and governments worldwide use Total Recall VR products to create electronic records of many forms of audio communication, including telephone, 2-way radio, broadcast radio, public address, intercoms, room microphones and much more.

Total Recall VR products and applications are the ideal solution for:

- Recording business telephone conversations;
- Recording agent calls in contact centres;
- Logging emergency response communication;
- Logging business operations communication;
- Logging radio broadcasts;
- Logging public announcements;
- Logging Air Traffic Control communication;
- Creating audio records of meetings, legal proceedings, public enquiries and similar events; and
- Creating compliance records to meet duty of care and legal requirements.

When audio records are critical to your operations, Total Recall VR products and applications deliver. It is a professional, reliable and fully self-contained solution for audio logging and call recording that comes at an affordable price.

2.3. What is Total Recall VR Infinity Cockpit?

Total Recall VR Infinity Cockpit (or just Total Recall VR Cockpit) is the user interface for the latest generation Total Recall VR Infinity appliance and custom recorders.

It is based on the "*one interface, infinite possibilities*" principle. As a result, it can be used as a stand-alone application on your Windows and Linux device (PC, tablet, etc.),

as well as an embedded application on Total Recall VR appliances and custom recorders with a built-in screen (touch or traditional).

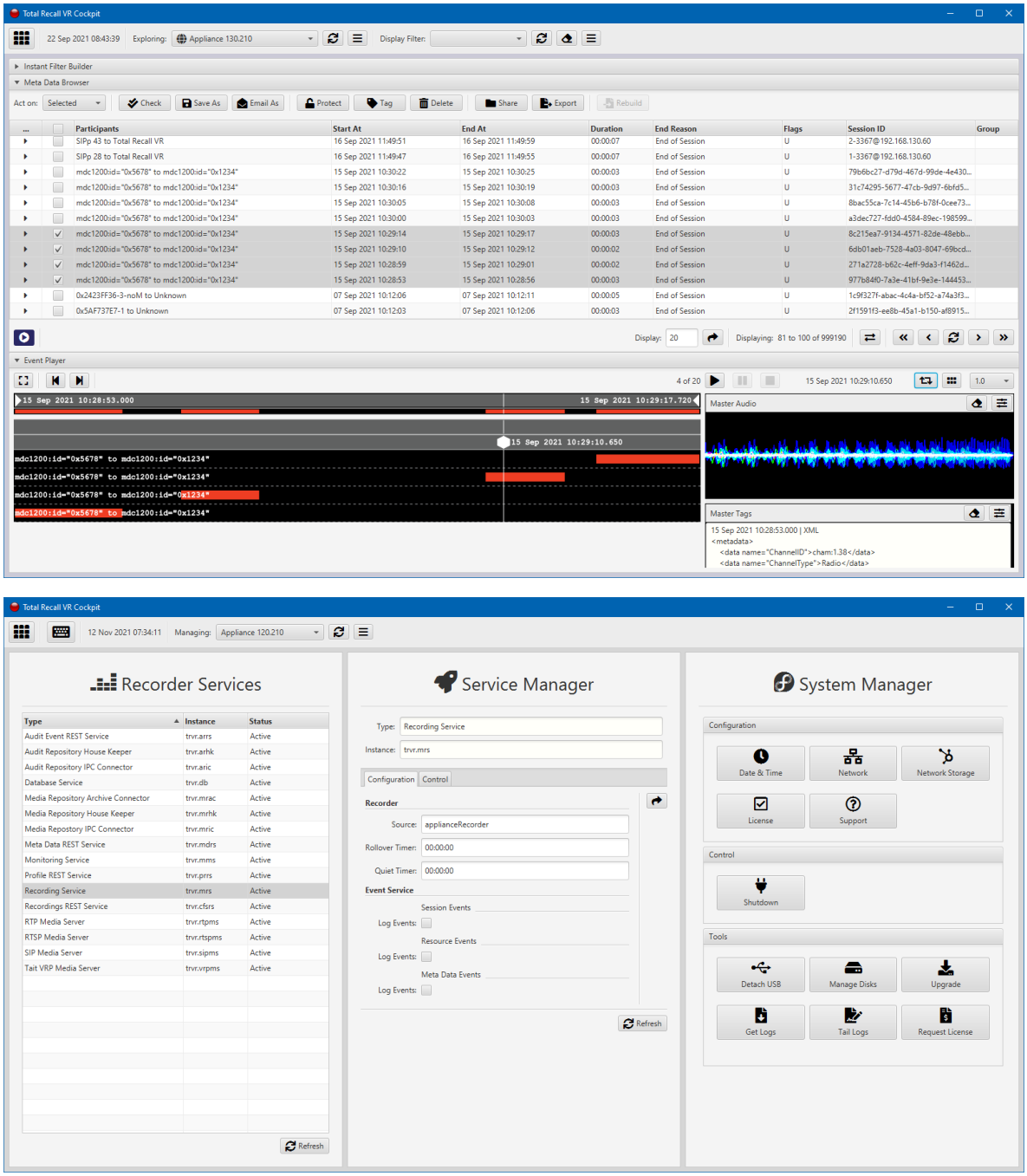


Figure 1: Total Recall VR Cockpit

Total Recall VR Cockpit has all the functions that you would expect from the user interface of a modern audio logging and call recording system. This includes (and not limited to):

- User-configurable and flexible role-based access control for all application features and recordings.

- Multiple working modes to best support standalone, single and multiple-user environments and embedded devices.
- Advanced recording management tools that work on recordings stored in different recording (media) repositories.
- Natural language search and filter query builder for recordings and audit events.
- Event (incident) reconstructions and replay.
- Live event (incident) monitoring.
- Comprehensive audit log.
- Productivity tools including an integrated e-mail client, advanced export tools for recordings (media and metadata), recording integrity verification tools and recording archive repair tools.
- Configuration, control and status monitoring of recording services.
- Appliance recorder system configuration, monitoring and repair tools.

All aspects of Total Recall VR Cockpit are touch-enabled, which makes the application suitable for use with traditional (keyboard/mouse), modern (touch only), and transitional (keyboard/mouse and touch) devices.

Total Recall VR Cockpit is a licensed application. You must purchase an Activation License to use the application.

3. Start Here

This section contains information to help you set up and activate an instance of the Total Recall VR Cockpit on your Windows or Linux device.

If you already have an active instance of the Total Recall VR Cockpit on your device and wish to upgrade it, skip directly to section 3.11 Application Upgrade.

3.1. System Requirements

Total Recall VR Cockpit is a GUI application based on the latest generation of user interface technologies. It is designed to run on a Windows or Linux device as a standalone application. In addition, it can run as an embedded application on Total Recall VR appliances and custom recorders with a built-in screen (touch or traditional).

Please use a device with the following minimum specifications for best experience with the application:

- Windows 10 (or better) with the latest updates, or CentOS 9 (or better) with the GNOME desktop and latest updates.
- 100MiB free disk space. Additional disk space may be needed for larger than default recordings cache, personal recording archives, etc. We recommend that you allocate the disk space on an NVRAM disk.
- 16GiB, or better, memory (RAM).
- 10th generation, or better, Intel® Core™ i7 processor (CPU).
- 24”, or larger, multi-point touch display that supports the HD resolution (1920 x 1080).
- Sound system with built-in external speakers or headphones.
- 1000Mbps (1Gbps) Ethernet network interface (NIC).
- Optionally, at least one free USB 3.0 (or better) port to access recording archives on removable disks.

Total Recall VR Cockpit requires AMBE decoders to play recordings stored in an AMBE audio format.

3.2. Compatibility

Total Recall VR Cockpit can be used with the latest generation Total Recall VR Infinity appliances and custom recorders (all versions).

Using Total Recall VR Cockpit with older generation Total Recall VR recorders is not possible. This includes 4th generation LinX II and LinX recorders, 3rd generation MAX recorders and 2nd generation Classic recorders.

3.3. Working Mode

Total Recall VR Cockpit can operate in one of the following working modes: workstation or workgroup.

Total Recall VR Cockpit is pre-configured to work in the workstation mode out of the box.

You can switch between the working modes anytime, see section 3.10 Application Preferences.

You may be unable to log in with Total Recall VR Cockpit after switching mode. To avoid this problem, please ensure that the target mode's configuration database has a user that you can use to log in after you switch mode.

3.3.1. Workstation Mode

In this mode, each Total Recall VR Cockpit instance uses its private configuration database that other Total Recall VR Cockpit instances cannot access.

This mode is best when you need a single Total Recall VR Cockpit instance on a single device. A single user or multiple users can use this instance of the application on the device, one at a time.

Installing multiple Total Recall VR Cockpit instances on multiple devices and using all instances in workstation mode is possible. However, note that in this mode, each instance is independent from all other instances and must be configured separately from all other instances.

The following diagram illustrates the workstation mode.

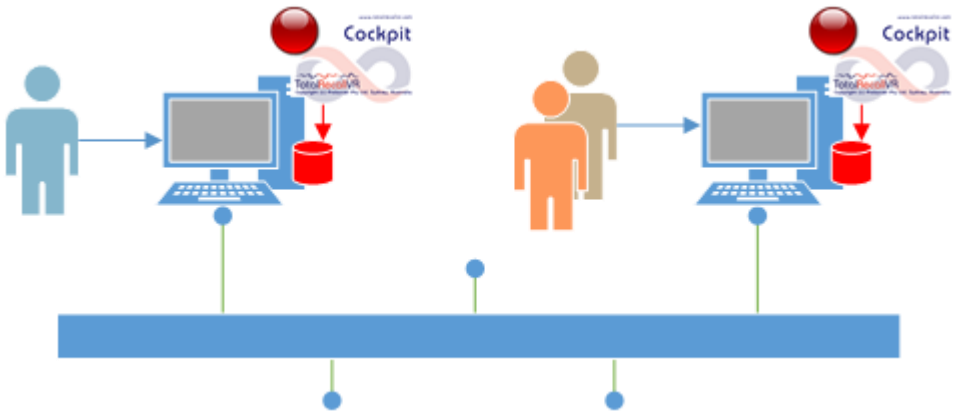


Figure 2: Workstation Mode

The diagram shows two Total Recall VR Cockpit instances on two separate devices. Each instance of Total Recall VR Cockpit uses its private configuration database on its device. Multiple users, each with their application account, can use either of the instances, but only if they have an application user account.

3.3.2. Workgroup Mode

Multiple Total Recall VR Cockpit instances use a shared configuration database in this mode.

This mode is best when you allow multiple users to use multiple instances of Total Recall VR Cockpit, each on a different device and not necessarily on the same device every time (for example, a hot-desk environment).

You can manage the configuration for all instances of Total Recall VR Cockpit with any of the installed instances, as all of the installed instances use the same shared configuration database. This simplifies and dramatically reduces the configuration effort (as opposed to configuring each instance of the application when it is running in the workstation mode).

The following diagram illustrates the workgroup mode.

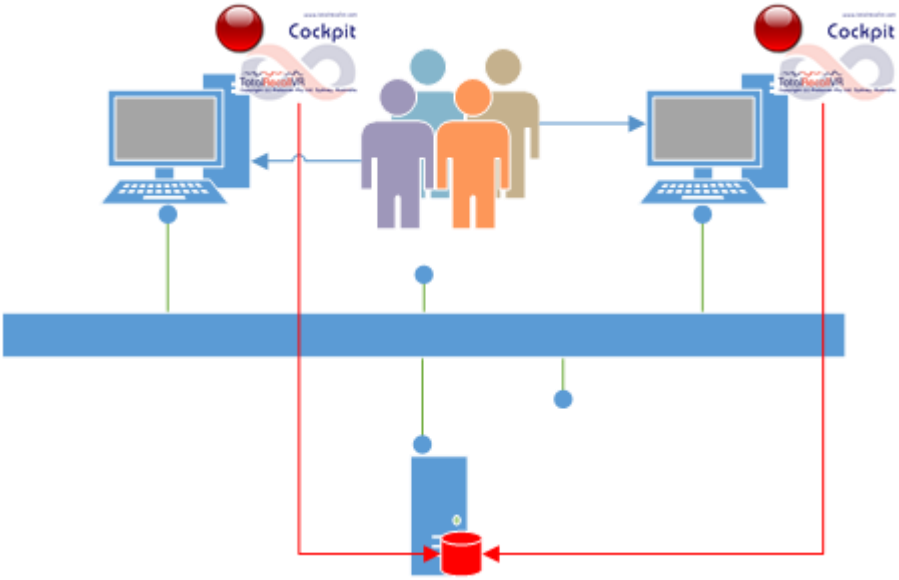


Figure 3: Workgroup Mode

The diagram shows two instances of Total Recall VR Cockpit on two separate devices. All Total Recall VR Cockpit instances use the same application configuration database, which resides on a different server. Multiple users, each with their application user account, can use an instance of Total Recall VR Cockpit on any of the devices.

3.4. Network Ports

Total Recall VR Cockpit depends on an Ethernet network to access its configuration database (when it is used in the workgroup mode), appliance and custom recorders, network drives that host recording (media) archives, network services such as name servers (DNS), e-mail servers, etc.

In all cases, Total Recall VR Cockpit acts as a client when setting up network connections. This greatly reduces the burden of configuring the firewall elements on your network, and in most cases, you will not need to change or add to any of the existing firewall rules.

However, in the rare cases when you do, the following table shows the network ports and protocols that Total Recall VR Cockpit may use.

Port	***Type***	***Protocol***	***Usage***
Default	Default	SMB/CIFS	Access Windows network drives.
Default	Default	NFS	Access Linux network drives.
Default	Default	SMTP	Send e-mail messages.
Default	Default	DNS	Host name mapping to IP address.

22	TCP	SSH/SCP	Execute system commands on recorder appliances and copy files. Not used with custom recorders.
1433 (*1)	TCP	JDBC	Access to the configuration database on a SQL Server when used in the workgroup mode.
1527 (*1)	TCP	JDBC	Access to the configuration database on a Derby server when used in the workgroup mode.
1554 (*1)	TCP	RTPS	Stream audio from the “Monitoring Service” on recorders.
1099 (*2)	TCP	RMI	Java remote object registry queries.
3010 (*2)	TCP	RMI	Configuration, control and status monitoring of the “Database Service” on recorders.
3020 (*2)	TCP	RMI	Configuration, control and status monitoring of the “Recording Service” on recorders.
3030 (*2)	TCP	RMI	Configuration, control and status monitoring of the “Monitoring Service” on recorders.
3050 (*2)	TCP	RMI	Configuration, control and status monitoring of the “SIP Media Server” on recorders.
3060 (*2)	TCP	RMI	Configuration, control and status monitoring of the “RTP Media Server” on recorders.
3070 (*2)	TCP	RMI	Configuration, control and status monitoring of the “VRP Media Server” on recorders.
3080 (*2)	TCP	RMI	Configuration, control and status monitoring of the “RTSP Media Server” on recorders.
3200 (*2)	TCP	RMI	Configuration, control and status monitoring of the “Audit Event REST Service” on recorders.
3210 (*2)	TCP	RMI	Configuration, control and status monitoring of the “Audit Repository IPC Connector” on recorders.
3220 (*2)	TCP	RMI	Configuration, control and status monitoring of the “Audit Repository House Keeper” on recorders.
3230 (*2)	TCP	RMI	Configuration, control and status monitoring of the “Recordings REST Service” on recorders.

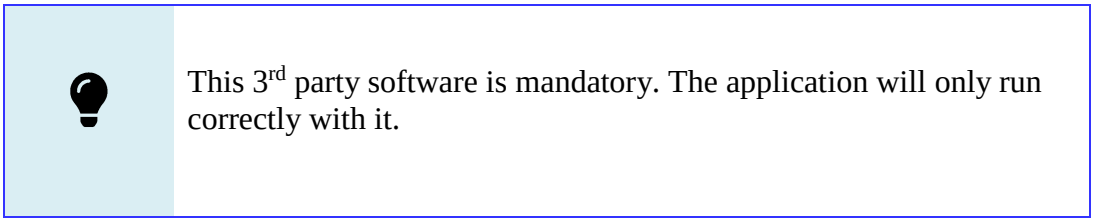
3240 (*2)	TCP	RMI	Configuration, control and status monitoring of the “Meta Data REST Service” on recorders.
3250 (*2)	TCP	RMI	Configuration, control and status monitoring of the “Media Repository House Keeper” on recorders.
3260 (*2)	TCP	RMI	Configuration, control and status monitoring of the “Media Repository IPC Connector” on recorders.
3270 (*2)	TCP	RMI	Configuration, control and status monitoring of the “Media Repository Archive Connector” on recorders.
3280 (*2)	TCP	RMI	Configuration, control and status monitoring of the “Media Repository Export Connector” on recorders.
3300 (*2)	TCP	RMI	Configuration, control and status monitoring of the “Profile REST Service” on recorders.
3306(*1)	TCP	JDBC	Access to the configuration database on a MariaDB or MySQL server when used in workgroup mode.
4010 (*1)	TCP	HTTP	Access to recording files via the “Recordings REST Service” on recorders.
4020 (*1)	TCP	HTTP	Access to metadata via the “Meta Data REST Service” on recorders.
4030 (*1)	TCP	HTTP	Access to profiles via the “Profile REST Service” on recorders.
4040 (*1)	TCP	HTTP	Access to audit events via the “Audit Event REST Service” on recorders.
5432 (*1)	TCP	JDBC	Access to the configuration database on a PostgreSQL server when used in workgroup mode.
9092 (*1)	TCP	JDBC	Access to the configuration database on a H2 server when used in workgroup mode.

(*1) Indicates a default port that users may set.
(*2) Indicates a default port that users may set on custom recorders only.

3.5. Pre-installation – Windows Device

Total Recall VR Cockpit requires 3rd party software and drivers, which you may need to install on your Windows device before installing an instance of Total Recall VR Cockpit.

3.5.1. Visual C++ 2019 Redistributable



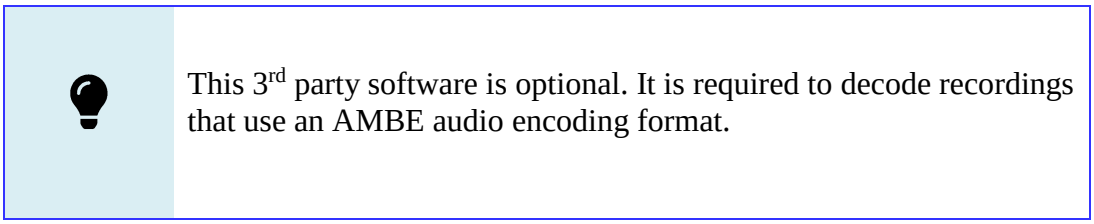
This 3rd party software is mandatory. The application will only run correctly with it.

Total Recall VR Cockpit uses native Windows libraries when running on a Windows device, and as such, it requires the Visual C++ 2019 redistributable to run.

You can download a copy of the Visual C++ 2019 Redistributable installer from https://visualstudio.microsoft.com/downloads/.

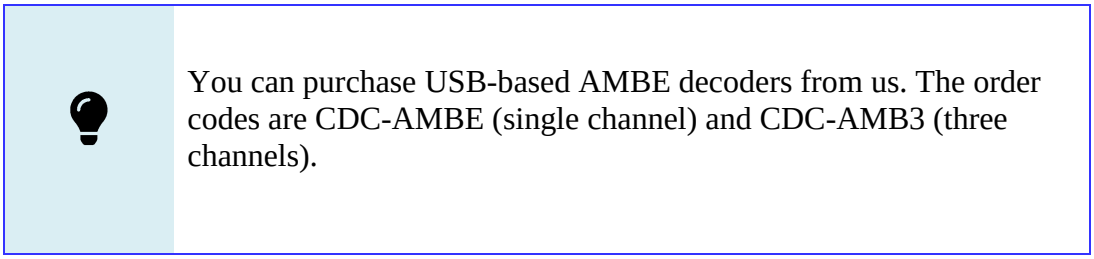
You may already have a Visual C++ 2019 Redistributable on your device. Ask your friendly technical staff to help you determine this if you need help with how to check.

3.5.2. FTDI 2DXX Drivers



This 3rd party software is optional. It is required to decode recordings that use an AMBE audio encoding format.

Total Recall VR Cockpit uses USB-based AMBE decoders to decode AMBE-encoded audio.



You can purchase USB-based AMBE decoders from us. The order codes are CDC-AMBE (single channel) and CDC-AMB3 (three channels).

The USB devices require FTDI D2XX drivers to work.

You must install FTDI's D2XX version 2.12.06, or better, WHQL-certified drivers on your Windows PC to enable Total Recall VR Cockpit to play recordings in an AMBE format. You can download an installer for the drivers from http://www.ftdichip.com/Drivers/D2XX.htm.

3.6. Application Configuration Database

You can safely skip this section if you intend to use Total Recall VR Cockpit in the workstation mode, see section 3.3.1 Workstation Mode.

Total Recall VR Cockpit stores its configuration and operating parameters using a configuration database.

By default, Total Recall VR Cockpit uses a private Derby database as its configuration database when used in the workstation mode, see section 3.3.1 Workstation Mode. It configures the Derby database automatically at installation time.

However, suppose you intend to use Total Recall VR Cockpit in the workgroup mode, see section 3.3.2 Workgroup Mode. In that case, you must configure a shared configuration database, which will be used by all Total Recall VR Cockpit instances on your network. The configuration database can reside on different servers, including Derby, H2, PostgreSQL, MariaDB, MySQL, and Microsoft SQL.

3.6.1. Derby Server

You can use a Derby database server to manage the shared configuration database.

We tested the application with Derby version 10.15 and recommend using this version.

You must create a database user and a database before connecting with the first instance of Total Recall VR Cockpit to the database. This is best done with the “ij” application. For example (adjust as necessary to fit your requirements for password, collation, etc.):

```
ij version 10.15
ij> connect
'jdbc:derby://192.168.120.200:1527/CockpitDB;create=true;user=trvr_cockpit';
ij> CALL
SYSCS_UTIL.SYSCS_SET_DATABASE_PROPERTY('derby.connection.requireAuthentication',
'true');
0 rows inserted/updated/deleted
ij> CALL SYSCS_UTIL.SYSCS_SET_DATABASE_PROPERTY('derby.authentication.provider',
'BUILTIN');
0 rows inserted/updated/deleted
ij> CALL SYSCS_UTIL.SYSCS_SET_DATABASE_PROPERTY('derby.user.trvr_cockpit', 'mypwd');
0 rows inserted/updated/deleted
ij> CALL
SYSCS_UTIL.SYSCS_SET_DATABASE_PROPERTY('derby.database.defaultConnectionMode',
'noAccess');
0 rows inserted/updated/deleted
ij> CALL SYSCS_UTIL.SYSCS_SET_DATABASE_PROPERTY('derby.database.fullAccessUsers',
'trvr_cockpit');
0 rows inserted/updated/deleted
ij>
```

To access the database you can use a JDBC URI similar to the following:

```
jdbc:derby://192.168.120.200:1527/CockpitDB
```

Assuming:

- The Derby server provides service on IP address 192.168.120.200 and port 1527.
- The name of the database is CockpitDB.

3.6.2. H2 Server

You can use an H2 database server to manage the shared configuration database.

We tested the application with H2 version 1.4.200 and recommend using this version.

Suppose an existing H2 database server runs with the “-ifNotExist” option set. In that case, creating a database user and a database that will act as the configuration database for Total Recall VR Cockpit is unnecessary. The first instance of Total

Recall VR Cockpit that will connect to the server will create both the database user and the database.

Otherwise, you must create a database user and a database before connecting to it with the first instance of Total Recall VR Cockpit. For instructions, see http://www.h2database.com/html/tutorial.html#creating_new_databases.

To access the database you can use a JDBC URI similar to the following:

```
jdbc:h2:tcp://192.168.120.200:9092/CockpitDB
```

Assuming:

- The H2 server provides service on IP address 192.168.120.200 and port 9092.
- The name of the database is CockpitDB.

If you do not have an H2 database server, you can set one up as follows.

You can download an installation package for the H2 database server for Windows from http://www.h2database.com/html/download.html.

The H2 database installation instructions for Windows should be more precise when explaining how to get an H2 database server going. The following is a summary of the steps. It can be used as a guide when setting up an H2 database server on Windows; however, it does not aim to replace the official H2 database documentation.

The following procedure assumes that the H2 database server will run on a server with an IP address of 192.168.120.200 and provide service on TCP port 9092. The same database server will provide web management service on TCP port 8082.

Please adjust the IP address and ports based on your requirements and network configuration.

Install an H2 database server

1. Download the latest stable Windows installer from http://www.h2database.com/html/download.html. We downloaded a file named ‘h2-setup-2019-10-14.exe’ for this example.
2. Run the installer file, which will install the software in “c:\Program Files (x86)\H2” by default.
3. Step 2 does not install the H2 database service automatically. You must manually install it after configuring it, as follows.

   The service ensures that the H2 database starts when the Windows server restarts.
4. The service configuration is in the “c:\Program Files (x86)\H2\service\wrapper.conf” file. We modified the following to tailor the service to our environment:

   ```
   # Application parameters. Add parameters as needed starting from 1
   ## -- Make sure to allow tcpPort on the firewall -- ##
   wrapper.app.parameter.1=org.h2.tools.Server
   wrapper.app.parameter.2=-tcp
   wrapper.app.parameter.3=-tcpPort 9092
   wrapper.app.parameter.4=-tcpAllowOthers
   wrapper.app.parameter.5=-web
   wrapper.app.parameter.6=-webPort 8082
   wrapper.app.parameter.7=-webAllowOthers
   wrapper.app.parameter.8=-webAdminPassword 23h209
   wrapper.app.parameter.9=-ifNotExists
   wrapper.app.parameter.10=-baseDir "c:/worktemp/db"
   ```

   In summary, we want the service to store database files in the “c:\worktemp\db” directory on the local machine and run on TCP port 9092. Also, we want the service to use TCP port 8082 for web management.
5. With the above changes, open a terminal window and change to the “c:\Program Files (x86)\H2\service” directory. Then:
   a. Run the *1_install_service.bat* script to install the service on the server. This adds the “H2 Database Engine Service” to the set of services on the server.
   b. Run the *2_start_service.bat* script to start the service.
   c. To ensure the service runs, start a browser on the same server using the *3_start_browser.bat* script. This should show the login page for the database server management console.
6. Edit the firewall configuration for the server and make sure that TCP ports 9092 and 8082 (if you are using our configuration from step 4) are not blocked.

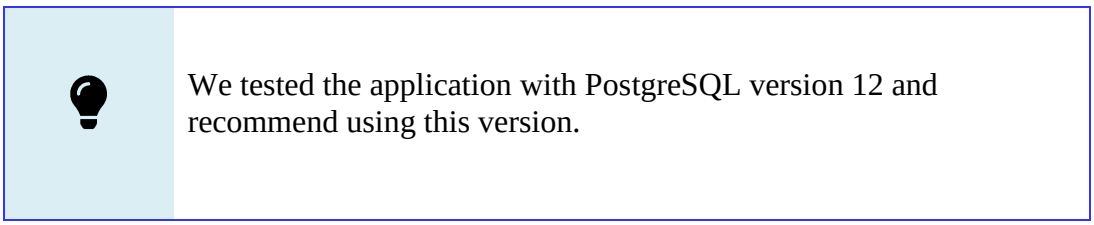
   How you complete this step depends on the firewall application that you are using. Please consult the documentation for your firewall application.

7. Once the firewall is allowing communication to TCP ports 9092 and 8082, open a browser on a different device and attempt to access the H2 server web management console using http://192.168.120.200:8082 (if you are using our configuration from step 4) to make sure that remote access to the server is possible.

Note that the "-ifNotExist" option is set in the H2 server configuration (see step 4). As a result, creating a database user and a database that will act as the configuration database for Total Recall VR Cockpit is unnecessary. The first instance of Total Recall VR Cockpit that will connect to the server will create both the database user and the database.

3.6.3. PostgreSQL Server

You can use a PostgreSQL database server to manage the shared configuration database.



You must create a database user and a database before connecting with the first instance of Total Recall VR Cockpit to the database. This is best done with the "pgAdmin" application. For example (adjust as necessary to fit your requirements for password, collation, etc.):

```
-- DB user that will be used to access the shared configuration database
CREATE ROLE trvr_cockpit WITH
  LOGIN
  NOSUPERUSER
  INHERIT
  NOCREATEDB
  NOCREATEROLE
  NOREPLICATION
  ENCRYPTED PASSWORD 'md5438ade72ac392291670512595d60e2ca'
  VALID UNTIL 'infinity';
-- DB that will be used as a shared configuration database
CREATE DATABASE CockpitDB
    WITH
    OWNER = trvr_cockpit
    ENCODING = 'UTF8'
    LC_COLLATE = 'en_AU.UTF-8'
    LC_CTYPE = 'en_AU.UTF-8'
    TABLESPACE = pg_default
    CONNECTION LIMIT = -1;
```

In addition, you may have to configure access to the database in the *pg_hba.conf* file.

To access the database you can use a JDBC URI similar to the following:

```
jdbc:postgresql://192.168.120.200:5432/CockpitDB
```

Assuming:

- The PostgreSQL server provides service on IP address 192.168.120.200 and port 5432.
- The name of the database is CockpitDB.

3.6.4. MariaDB or MySQL Server

You can manage the shared configuration database using a MariaDB or MySQL database server.

We tested the application with MariaDB 10.5 and recommend using this version.

You must create a database user and a database before connecting with the first instance of Total Recall VR Cockpit to the database. This is best done with the "MySQL Workbench" application. For example:

```
-- DB user that will be used to access the shared configuration database
mysql -e "CREATE USER 'trvr'@'192.168.130.*' IDENTIFIED BY 'cocpit09'"
-- DB that will be used as a shared configuration database
mysql -e "CREATE DATABASE CockpitDB CHARACTER SET utf8"
mysql -e "GRANT ALL PRIVILEGES ON CockpitDB.* TO 'trvr'@'192.168.130.*'"
mysql -e "FLUSH PRIVILEGES"
```

To access the database you can use a JDBC URI similar to the following:

```
jdbc:mysql://192.168.120.200:3306/CockpitDB
```

Assuming:

- The MariaDB or MySQL server provides service on IP address 192.168.120.200 and port 3306.
- The name of the database is CockpitDB.

3.6.5. Microsoft SQL Server

You can use an SQL Server database server to manage the shared configuration database.

We tested the application with SQL Server version 15 and recommend using this version.

You must create a database user and a database before connecting with the first instance of Total Recall VR Cockpit to the database. This is best done with the “SQL Server Management Studio” application. For example (not a complete SQL):

```
-- DB user that will be used to access the shared configuration database
CREATE LOGIN [trvr] WITH
  PASSWORD=N'...',
  DEFAULT_DATABASE=[master],
  DEFAULT_LANGUAGE=[...],
  CHECK_EXPIRATION=OFF,
  CHECK_POLICY=OFF
GO
ALTER SERVER ROLE [dbcreator] ADD MEMBER [trvr]
GO
-- DB that will be used as a shared configuration database
CREATE DATABASE [CockpitDB]...
GO
```

In addition, you may have to configure remote access to the database and the server instance.

To access the database you can use a JDBC URI similar to the following:

```
jdbc:sqlserver://192.168.120.200:1433;DatabaseName=CockpitDB
```

Assuming:

- The SQL Server provides service on IP address 192.168.120.200 and port 1433.
- The name of the database is CockpitDB.

3.7. Application Installation – Windows Device

A Windows installation package for Total Recall VR Cockpit is available on our website. We do not ship installation media for Total Recall VR Cockpit.

Please visit http://www.totalrecallvr.com/applications/total-recall-vr-cockpit to download the Windows installation package for Total Recall VR Cockpit.

The application installer is a wizard-based installer that will guide you through the installation steps. You will be asked to specify the following during the installation process:

1. **Installation location (directory)**. The default location is "C:\Program Files\TRVR Cockpit".
2. **Application data location (directory)**. The default location is "C:\Program Files\Common Files\TRVR Cockpit". The application will use this location for its preferences, licenses, recording cache, working playlist, configuration database (when used in the workstation mode), private audit log and log files.

DO NOT use the same application data location (directory) for multiple Total Recall VR Cockpit instances.

To install Total Recall VR Cockpit on your Windows device:

Install Total Recall VR Cockpit

1. Extract the *TRVRCockpit-<version>.exe* file from the *TRVRCockpit - <version>.zip* file you downloaded from our website.
2. Double-click on the *TRVRCockpit-<version>.exe* file to launch the installer.
3. Follow the prompts to complete the installation.

3.8. Application Activation

Total Recall VR Cockpit requires a valid activation license to run. As a result, when running Total Recall VR Cockpit for the first time, it will prompt you to activate the

application with an activation token or an activation license, as shown in the following screen capture.

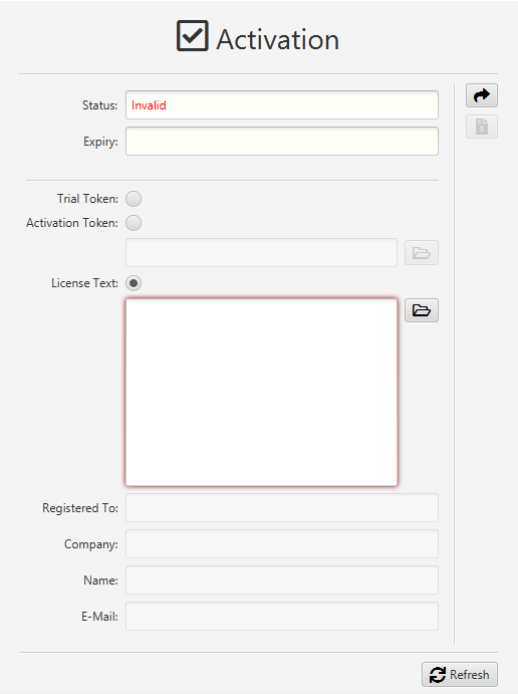


Figure 4: Activation Form

You can select one of the following activation methods:

1. **Trial Token** activation is used to activate a 10-day application trial. The device that will run the application must have a working Internet connection if you wish to use this method.

   Note that you will be able to activate one, and only one, trial of the application on a given device. Once the 10-day trial is complete, activating another trial for the application on the same device will not be possible. Please contact us if you wish to extend the application trial on a given device (we reserve the right to refuse trial extension requests).

2. **Activation Token** activation activates the application for a limited time or perpetually. The device that will run the application must have a working Internet connection if you wish to use this method.

   Use this activation method when you receive an Activation Token after purchasing an activation license for the application. Based on the number of licenses you purchase and the type of token that we send you, you may be able to activate the application with the same token on one device or multiple devices. Please consult the instructions that come with the token for more details.

3. **License Text** activation to activate the application for a limited time or perpetually. The device that will run the application does not need a working Internet connection if you wish to use this method.

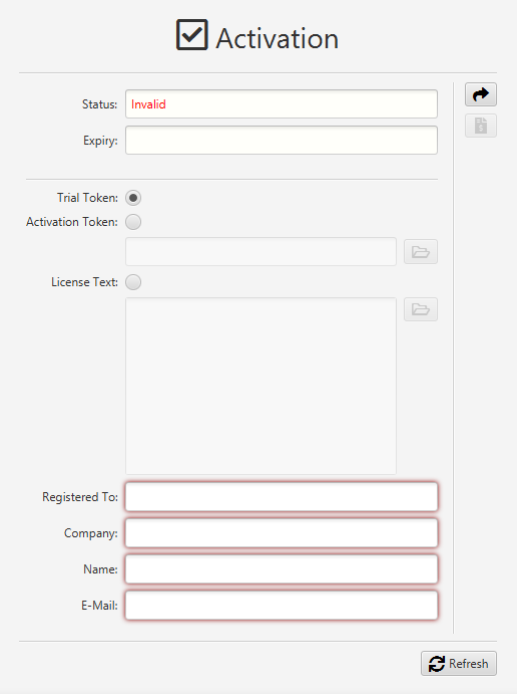
Use this activation method to re-apply existing licenses when lost or misplaced or to activate the application for the first time when the device has no Internet connection. Please get in touch with us for instructions on how to proceed to recover lost activation licenses or receive an activation license for devices that do not have Internet access.

You can use the built-in trial activation token to activate a limited duration (10 days from activation) trial of the application. During the trial period, the application is fully functional without any restrictions.

To activate a limited-duration trial:

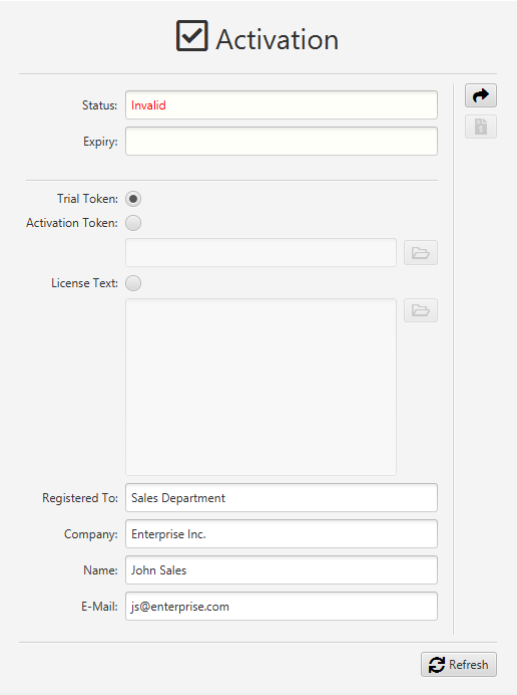
Activation with the Trial Token

1. Select ***Trial Token***.



2. Enter ***Registered To***, ***Company***, ***Name*** and ***E-Mail*** as desired. The details you enter here will be used to recover the trial activation license if lost or misplaced, so record them and keep them safe.

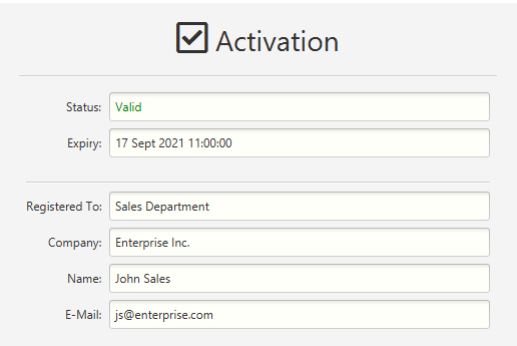
   For example:



3. Select ↱ to attempt activation. The application will attempt activation (over the Internet) with the Total Recall VR licensing server. If you receive the following error message, a trial of the application was previously activated on the device.

   As a result, the Trial Token cannot be used to activate the application (again). Please contact us if you wish to extend the application trial on a given device (we reserve the right to refuse trial extension requests).

4. In most cases, the activation will be successful. For example:



If you received an activation token from us, you can activate the application with the token. In most cases, the token will activate the application on a perpetual basis; however, in some rare cases, it may activate a limited-duration trial.

The following is an example of an activation token (note, this is an example of a token, and as such, it is invalid and cannot be used to activate the application on any device):

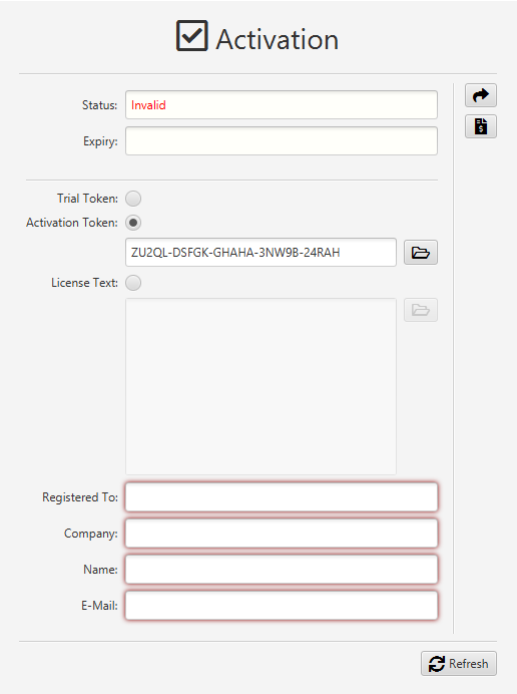
```
ZU2QL-DSFGK-GHAHA-3NW9B-24RAH
```

To activate the application with the token:

Activation with an Activation Token

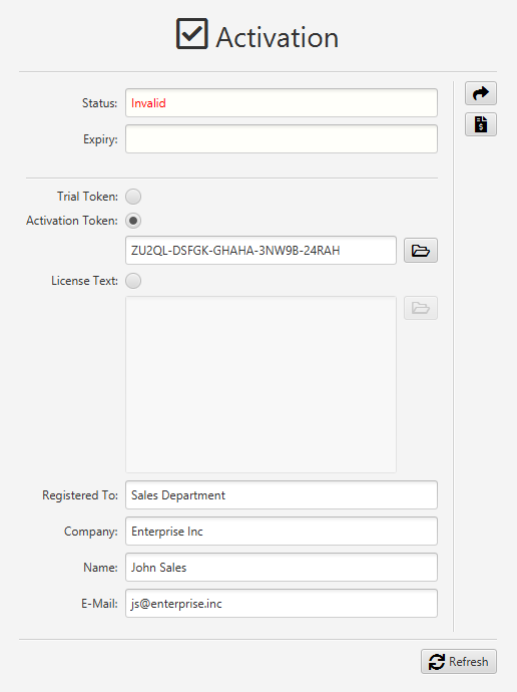
1. Select ***Activation Token*** and manually enter the token you received from us. Alternatively, select 🗁 to load the token from a file you received from us.

   For example:



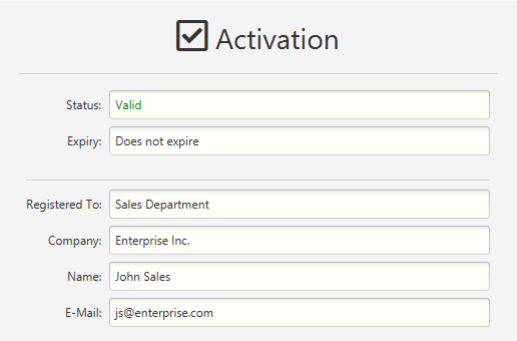
2. Enter ***Registered To***, ***Company***, ***Name*** and ***E-Mail*** as desired. The details you enter here will be used to recover the activation license if it is lost or misplaced, so record them and keep them safe.

   For example:



3. Select ↱ to attempt activation. The application will attempt activation (over the Internet) with the Total Recall VR licensing server. If you receive the following error message, the token is no longer valid or was previously used to activate the application on the same device.

4. In most cases, the activation will be successful. For example:



We may send you the license text of an activation license if you cannot activate the application over the Internet or if you have activated the application before and misplaced your activation license for a particular device.

The following is an example license text (most lines were removed to save space):

```
# Total Recall VR Cockpit Node License (id: 1511837763868)
6729c0c1fc5b9b29b19c4336e2068b75b231474c87cbce079ff39ea741b0
        :
5cde6395e2493adb54960307e8083ae8
```

Note:

a. The application's device does not need Internet access to (re)activate the application with license text.

b. When activating for the first time, the license text we will send you is for a new license, which activates the application on a particular device with the same hardware as the hardware when you generated the activation request file for the device.

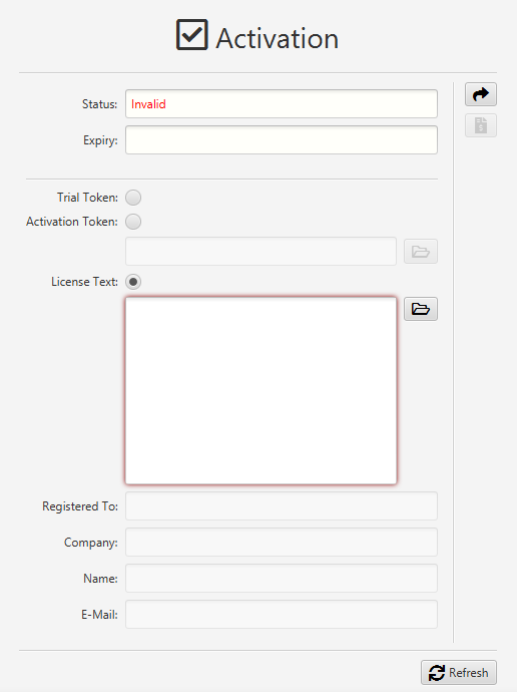
c. When reactivating after a lost license, the license text we will send you is for an existing license, which activates the application on a particular device with the same hardware as the hardware when the application was activated for the first time.

d. If the activation license is lost due to a damaged hard disk or motherboard, and you replace the faulty hardware, then the license text of the existing license (which we will send you) will no longer be valid as the device's hardware changes. You must purchase a new activation license for the modified hardware in such cases.

To activate the application with the license text:

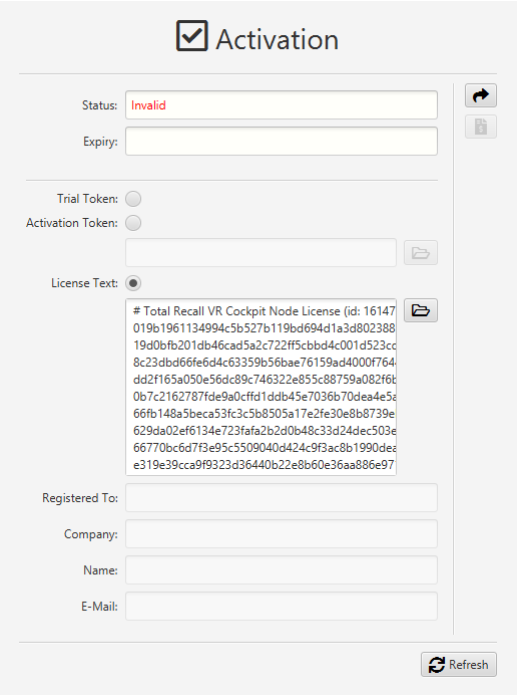
(Re)Activation with License Text

1. Select ***License Text***.



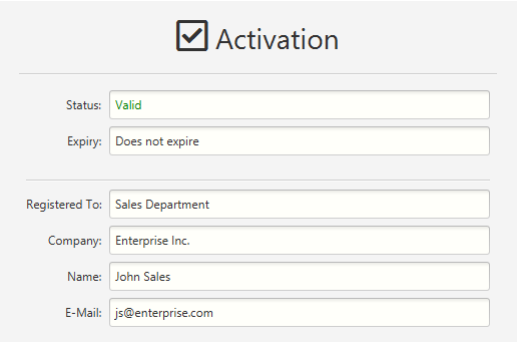
2. Select 🗁 to load the license text from the file you received from us.

   For example:



3. Select ↱ to attempt activation. If you receive the following error message, the activation license is no longer valid or is for a different application or device with different hardware.

4. In most cases, the activation will be successful. For example:



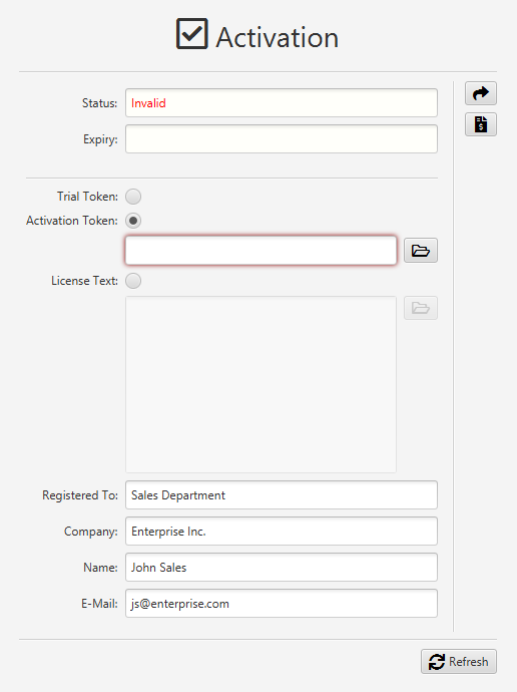
Finally, we may ask you to generate an activation request file for the application when you decide to purchase an activation license (after a trial, for example) or if you need to activate the application for the first time on a device that does not have Internet access.

To generate an activation request file:

Generate an activation request file

1. Select ***Activation Token*** and enter ***Registered To***, ***Company***, ***Name*** and ***E-Mail*** as desired. The details you enter here will be used to create the activation license.

   For example:



2. Select to display the File Selector dialog, where you can choose a location and name for the activation request file.
3. Select **Open** in the File Selector dialog to create the activation request file, which you can then send to us along with your purchase order.

3.9. Default User

Total Recall VR Cockpit comes pre-configured with a single user with administrative privileges (full access to all aspects of the application). Use this user to sign in with the application for the first time.

The sign-in credentials for the default user are:

- Username: admin
- Password: changeme

We recommend changing the default user's password immediately after you sign in for the first time.

However, note that it is only possible to recover the default user's password if misplaced if you create another user with privileges to manage user accounts, and you can sign in as that user to set a new password for the default user.

3.10. Application Preferences

Total Recall VR Cockpit is pre-configured to work in the workstation mode out of the box, see section 3.3.1 Workstation Mode.

Suppose you intend to use Total Recall VR Cockpit in the workstation mode, see section 3.3.1 Workstation Mode. In most cases, you do not need to change the application preferences. You can start using it as soon as you activate it.

To access the application preferences, you must sign in with a user with the ‘Preferences’ permission set in the ‘Cockpit Configuration’ domain. The default user, see section 3.9 Default User, has this permission by default, so when you sign in with the application for the first time, you can access and modify the application preferences.

To display the Preferences form, select to display the application menu and then select **Preferences** from the menu.

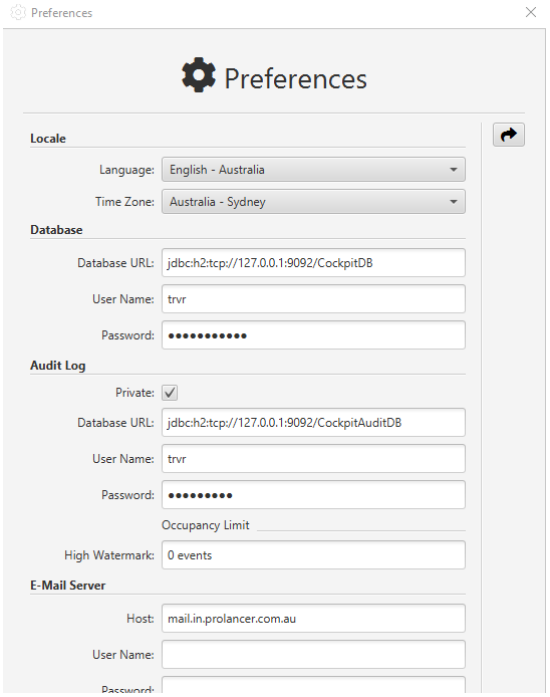


Figure 5: Preferences Form

As with all application forms, do not forget to select ↷ to apply the changes that you make to the application preferences.

The application preferences are organised into multiple categories. The following sections explain the preferences in each category.

3.10.1. Locale

The locale category contains preferences for the display language and time zone, including:

Parameter	***Default Value***	***Comment***
Language	English - Australia	
Time Zone	Australia – Sydney	

The application will show all information in the selected language and all times (for example, recording start time) in the selected time zone.

3.10.2. Database

The database category contains preferences for the application configuration database, including:

Parameter	*Default Value*	*Comment*
Database URL	jdbc:derby:CockpitDB	The application uses this configuration database.
User Name	trvr_cockpit	If set, the application uses this user to access the configuration database.
Password	********** (withheld)	If set, the application uses this password to access the configuration database.

If you intend to use the application in the workstation mode, see section 3.3.1 Workstation Mode, then leave the values of all database preferences set to their default values.

Suppose you intend to use the application in the workgroup mode, see section 3.3.2 Workgroup Mode. In that case, you can use different types of database servers, see section 3.6 Application Configuration Database, to house the shared application configuration database. In this case, set ***Database URL*** to a value compatible with the database server you are using. For example:

Database Server	*Database URL (example)*
Derby	`jdbc:derby://192.168.120.210:1527/CockpitDB` where: • The server is providing service on IP address 192.168.120.210 and TCP port 1527. • The name of the database is “CockpitDB”.
H2	`jdbc:h2:tcp://192.168.120.210:9092/CockpitDB` where: • The server is providing service on IP address 192.168.120.210 and TCP port 9092. • The name of the database is “CockpitDB”.
PostgreSQL	`jdbc:postgresql://192.168.120.200:5432/CockpitDB` where: • The server is providing service on IP address 192.168.120.200 and TCP port 5432.

	• The name of the database is “CockpitDB”.
MariaDB	`jdbc:mariadb://192.168.120.200:3306/CockpitDB` where: • The server is providing service on IP address 192.168.120.200 and TCP port 3306. The name of the database is “CockpitDB”.
MySQL	`jdbc:mysql://192.168.120.200:3306/CockpitDB` where: • The server is providing service on IP address 192.168.120.200 and TCP port 3306. The name of the database is “CockpitDB”.
SQL Server	`jdbc:sqlserver://192.168.120.220:1433;DatabaseName=CockpitDB` where: • The server is providing service on IP address 192.168.120.220 and TCP port 1433. • The name of the database is “CockpitDB”.

In addition, set ***User Name*** and ***Password*** to the access credentials of the database user that can access the database.

3.10.3. Audit Log

The audit log category contains preferences for the audit event log, including:

Parameter	***Default Value***	***Comment***
Audit log		
Private	Ticked	If ticked, the application uses a private audit repository (log).
Database URL	jdbc:derby:CockpitAuditDB	The application uses this database as an event log.
User Name	trvr_audit	If set, the application uses this user to access the database.

Password	********** (withheld)	If set, the application uses this password to access the database.
Occupancy Limit		
Occupancy Limit	10,000 events	The maximum number of audit events in the private audit log. The application automatically deletes audit events, the oldest first, when it detects this limit to make space for new events. Set the limit to *0 events* for unlimited capacity (use with caution, not recommended). It must be between *0 events* and *10,000 events*.

The application uses the event log to log all user and application activity, for example, deletion of recordings, changes of recorder configuration, etc.

If you intend to use the application in the workstation mode, see section 3.3.1 Workstation Mode, then leave the values of all audit log preferences set to their default values. In this mode, the application uses its private audit log. You can access the private audit log from the application.

Suppose you intend to use the application in the workgroup mode, see section 3.3.2 Workgroup Mode. In that case, it is best to change the audit log preferences so that the application will forward all of its audit events to a central audit log, for example, the audit log on one of your appliance recorders. For example (adjust as necessary):

Parameter	***Default Value***	***Comment***
Audit log		
Private	Not ticked.	The audit log is not private.
Base URL	http://192.168.1.100:4040/audit	The base URL of the “Audit Event REST Service” on a recorder or archive appliance which acts as a central audit log.

If you do this, you can access all audit events from all application instances with this configuration from one central audit log.

3.10.4. E-Mail Server

The e-mail server category contains preferences for the e-mail server, including:

Parameter	*Default Value*	*Comment*
Host		If set, the application uses this SMTP server to send e-mail messages. It must be a valid IP address or hostname.
User Name		If set, the application uses this user to authenticate with the SMTP server.
Password		If set, the application uses this password to authenticate with the SMTP server.

The application will use the e-mail server, if set, to send e-mail messages on user requests from the application. For example, a user can send copies of recordings via e-mail directly from the application.

3.10.5. Playlist

The playlist category contains preferences for the private playlist, including:

Parameter	*Default Value*	*Comment*
Directory	C:\Program Files\Common Files\TRVR Cockpit\playlist	The application uses this directory to store the content of its private playlist.

The application uses a private playlist during incident reconstruction and replay. The preferences in the playlist category specify the location of the playlist. The location is usually a directory on the local disk.

In most cases, there is no need to change the playlist preferences. However, you may wish to change the location of the playlist to a faster disk, for example, an NVMe disk, for a better experience with the application.

3.10.6. Cache

The cache category contains preferences for the private cache, including:

Parameter	***Default Value***	***Comment***
Directories	C:\Program Files\Common Files\TRVR Cockpit\cache	The application uses this directory directory to store the content of its private cache. You can specify multiple directories to configure the application to use the set of directories in a "load-balancing" fashion.
Occupancy Limit		
High Watermark	1,000 files	The maximum number of recording files in the cache. The application automatically deletes recording files, the oldest first, when it detects this limit. It must be between *100 files* and *10,000 files*.
Low Watermark	800 files	The minimum number of recording files to leave in the cache when deleting files after reaching the high watermark. It must be between *100 files* and *10,000 files*.

The application uses a private cache to temporarily store recordings that reside on recorders and archives with network access when users access them. For example, suppose a user attempts to listen to a recording located on a recorder. In that case, the application will fetch a copy of the recording first and store the copy in the cache before playing it. Then, when the user attempts to play it again (a typical scenario), the application will play the recording from its cache.

The cache location is usually a single directory on the local disk. However, if required, the cache can use multiple directories, each located on a different disk.

Further, the occupancy limits control the size of the cache. The cache will contain at most ***High Watermark*** recordings (files). The cache will automatically remove files when its occupancy reaches the high watermark and bring the occupancy down to or below the ***Low Watermark***.

In most cases, there is no need to change the cache preferences. However, you may wish to change the location of the cache to a faster disk, for example, an NVMe disk, for a better experience with the application.

3.10.7. Digital Certificates

The digital certificates category contains preferences for the keystore and truststore of digital certificates, including:

Parameter	*Default Value*	*Comment*
Keystore	./trvr.cockpit.p12	If set, the application uses the certificates in this file to encrypt the communication with servers (HTTPS instead of HTTP), sign reports, etc.
Keystore Password	********** (withheld)	If set, the application uses this password to access the information in the keystore file.
Keystore Key Password	********** (withheld)	If set, the application uses this password to access the keys in the keystore file.
Truststore	./trvr.cockpit.p12	If set, the application uses the certificates in this file to authenticate with servers.
Truststore Password	********** (withheld)	If set, the application uses this password to access the information in the truststore file.

The application uses several digital certificates for various purposes, including encryption of communication with recorders, signing reports, etc.

Leave the values of all digital certificate preferences set to their default values.

3.11. Application Upgrade – Windows Device

To upgrade the Total Recall VR Cockpit on your Windows device:

- If you wish to keep the application's previous configuration and activation license, simply follow the installation procedure. Do not uninstall the previous version of the application.
- If you wish to have a clean application installation with a new configuration, uninstall the previous version and then install the latest version. Please make a copy of your activation license file and the support token file before uninstalling the old version of the application. You will need the activation license for the new version of the application. The default activation license file is "*C:\Program Files\Common Files\TRVR Cockpit\etc\activation.lic*". In addition, you will need the support token to receive support for the new version of the application. The

default support token file is: "*C:\Program Files\Common Files\TRVR Cockpit\etc\support.lic*".

3.12. Application Upgrade – Appliance Recorder

Please follow the appliance recorder upgrade procedure to upgrade the Total Recall VR Cockpit on your appliance recorder, see section 11.9 System Tools – Upgrade.

3.13. Application Support

If after using this manual you still have questions about Total Recall VR Cockpit, or you are experiencing problems with Total Recall VR Cockpit, then:

1. Please visit the Total Recall VR online forums, http://www.totalrecallvr.com/forum, to find answers to common problems you may experience when installing and using Total Recall VR products.
2. Please browse the Total Recall VR online articles and tutorials, http://www.totalrecallvr.com/articles-and-tutorials, where you may find information on how to use Total Recall VR products combined with products from other manufacturers.

If you continue to experience problems, then in all cases, you should seek support from the point of purchase first.

If you need to contact us directly and require remote support, please write to itsupport@prolancer.com.au to book a remote support session.

You need to provide a valid and active support token or purchase one to receive support for a Total Recall VR Cockpit instance.

Please note the following regarding the support token:-

a. You do not need to purchase support tokens for any of your Total Recall VR products if you do not wish to receive support directly from us. Please discuss your support options with a representative from the point of purchase. They may and should offer support options that are likely to be tailored to your case compared to the remote support we provide as the manufacturer of the products.

b. Support tokens are valid for one (1) year starting from the date that is exactly one (1) month after the date when the product that it relates to was shipped from our factory. Support for the first month after the shipment date is free and does not require a valid support token. So, during the first year, if you purchase a support token for a product at the same time when you purchase the product, then you will receive thirteen (13) months of support from the shipment date of the related product. You will receive twelve (12) months each subsequent year if you renew the support token.

c. Each token relates to one instance of a Total Recall VR product and cannot be transferred to another instance of the same Total Recall VR product or used to get support for an instance of another Total Recall VR product.

d. On expiry, support tokens can be renewed on a back-charging basis. You must pay for years missed and the current year when you renew an expired token. For example:

   Suppose you purchased a support token when purchasing an instance of the Total Recall VR Cockpit. Further, let's take the fact that you did not renew the token or buy a new one after it expired at the end of the first year. If you request support in year 3 of ownership, you must pay for two years of support (to cover support for years 2 and 3) to renew your existing token or purchase a new one. The purchase will give you a token expiring at the end of year 3.

e. You can purchase a support token anytime on a back-charging basis for any Total Recall VR product instance. For example:

   Let's assume you did NOT purchase a support token when you purchased an instance of Total Recall VR Cockpit. If you request support in year 3 of ownership, you must pay for three years of support (to cover support for years 1, 2 and 3) to purchase a new support token. The purchase will give you a token expiring at the end of year 3.

In summary, if you wish to receive support directly from us for an instance of a Total Recall VR product, then you need a valid and active support token for the instance of the Total Recall VR product.

However, you do not need to purchase support from us. Instead, please discuss your support options with a representative from the point of purchase. They may and should offer support options that will likely be tailored to your case compared to the remote support we provide as the manufacturer of Total Recall VR products.

You can apply a support token to an instance of Total Recall VR Cockpit as shown in the following screen capture:

Figure 6: Support Form

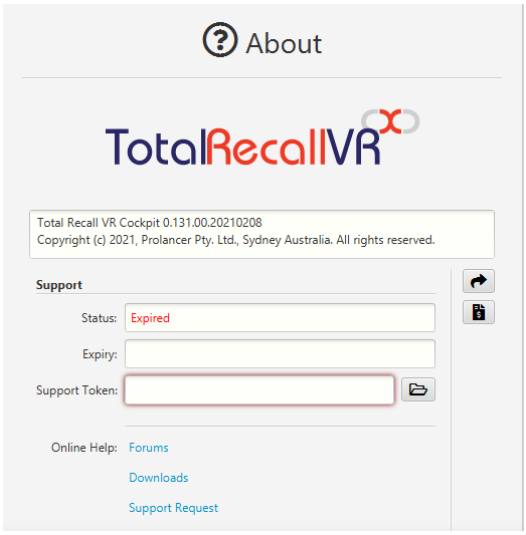
If you do so, then the token and its status are always handy when and if you need them.

To apply a token to an instance of Total Recall VR Cockpit:

Apply a Support Token

1. Select 🗁 to load the token from the support token file you received from us.

   For example:



2. Select ➦ to attempt to apply the token. If you receive the following error message, the support token is no longer valid, or it is for a different product or application or a device with different hardware.

3. In most cases, it will be successful. For example:

If the Total Recall VR Cockpit is part of a Total Recall VR appliance, then the support token for the appliance applies to the Total Recall VR Cockpit instance. In such cases, you do not need to purchase a separate support token for the Total Recall VR Cockpit instance.

For instructions on how to apply a support token to a Total Recall VR appliance, see section 11.5 System Configuration – Support.

4. User Interface

This section contains general information about the Total Recall VR Cockpit user interface that will help you get the best possible experience with the application.

We recommend that you at least skim over the information in this section, even if you are an experienced touch application user.

All aspects of Total Recall VR Cockpit are touch-enabled, which makes it suitable to use with traditional (keyboard/mouse), modern (touch only) and transitional (keyboard/mouse and touch) devices.

Total Recall VR Cockpit is based on the "*one interface, infinite possibilities*" principle. As a result, it can be used as a stand-alone application on your Windows and Linux device (PC, tablet, etc.), as well as an embedded application on Total Recall VR appliance and custom recorders with a built-in screen (touch or traditional).

The information in this section applies to all devices.

4.1. Application Views

The user interface comprises multiple views. The views are:

View	*Description*
 Sentinel	Application activation, user access and user management tools.
 Explorer	Recording browsing and tools for recording management, export, integrity verification and replay. Event (incident) reconstruction and event (incident) replay.
 Monitor	Recording and event (incident) real-time monitoring.
 Manager	Appliance and custom recorder services configuration, control and status monitoring. Appliance recorder system configuration, control and maintenance tools.
 Auditor	Audit event browsing and tools for audit event management, export and reporting.

In general, you will interact with the application through one view at a time; however, activities that you start on a view will continue while interacting with the application through another view. For example, you can start replaying a recording or an incident, and while it is replaying, you can switch to a different view and perform actions on that view (for example, search the audit log).

Use the application menu to switch between views.

You can access views only if you have permission to do so.

4.2. Application Menu

Total Recall VR Cockpit has a simple application menu that you can access anytime.

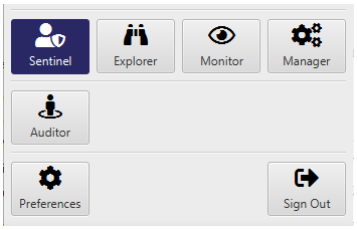


Figure 7: Application Menu

Select ⊞ (located in the left-hand corner of the application menu bar) to display the application menu. Once you choose, the menu will disappear (slide up) from the screen.

4.3. Application Menu Bar

Total Recall VR uses a dynamic menu bar with permanent and view-specific content.

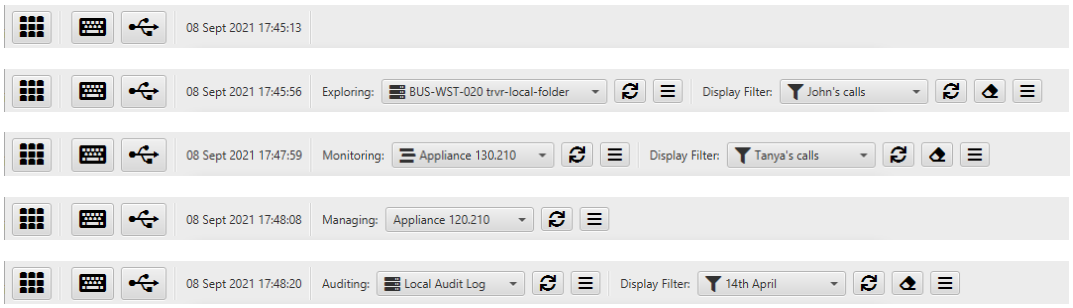


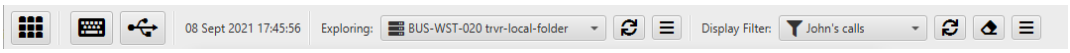
Figure 8: Application Menu Bar

The items that appear permanently on the menu bar are:

Item	*Description*
	Displays the application menu.
	Displays the built-in on-screen keyboard if, and only if, the active object on the screen accepts keyboard input.
	Initiates the process to detach a USB disk. This item appears only when the application runs in embedded mode on an appliance or a custom recorder.
08 Sep 2021 17:48:20	The current system time.

Each view may add items to the menu bar that are specific to the view. In general, each view adds at least a selector box that allows you to define the view's context. In addition, when applicable, views add a second selector box that will enable you to specify a display filter that controls which records or audit events are shown on the view.

For example, when you switch to the Explorer view, the menu bar looks as shown in the following screen capture:



In this case, the ***Exploring*** selector box sets the context of the Explorer view; it allows you to select the location of the recordings (recorder, archive, etc.) to explore. The ***Display Filter*** selector box allows you to select a filter that will define which recordings are shown in the Explorer view as you are exploring.

The items that may appear next to a selector box are:

Item	*Description*
	Refreshes the content of the selector box with the up-to-date content of the configuration database. For example, if another user creates a new location with recordings to explore, select this button to make the location appear in the selector box.
	Displays a form allowing you to create new entries, modify existing entries and remove entries shown by the selector box. For example, select this button to add a new location for recordings to explore.

	Clears the selected item. For example, select this button to deactivate the current display filter.

4.4. Touch Gestures

Total Recall VR Cockpit responds to the following touch gestures:

Item	*Description*
	Tap once with one finger – single tap.
	Tap twice with one finger – double tap.
	Press, hold, and while holding, slide to the right.
	Press, hold, and while holding, slide to the left.

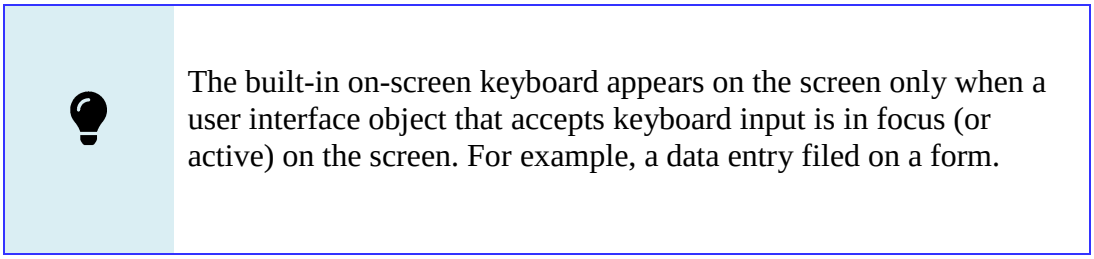
4.5. On Screen Keyboard

Total Recall Cockpit has a built-in on-screen keyboard, as shown in the following screen capture.

Figure 9: On-Screen Keyboard

The built-in on-screen keyboard is the only one you can use when Total Recall VR Cockpit runs in embedded mode on an appliance or a custom recorder with a built-in touch screen.

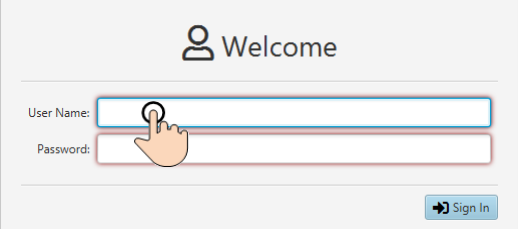
You can use the built-in on-screen keyboard in addition to your physical keyboard and the on-screen keyboard provided by the operating system on your device when Total Recall VR Cockpit is running in stand-alone mode.



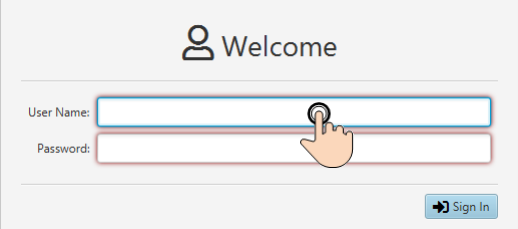
To show the built-in on-screen keyboard:

Display the on-screen keyboard

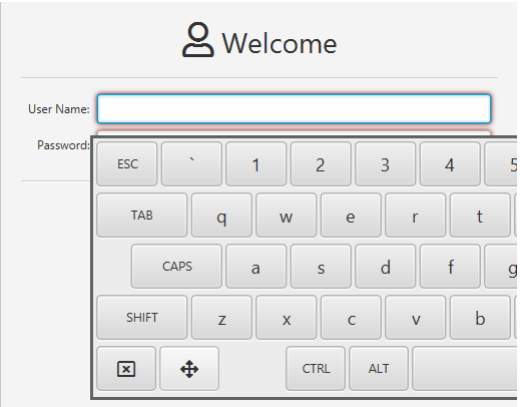
1. Make a screen object that accepts keyboard input active by clicking on it with the mouse or a single tap with a finger. For example, the ***User Name*** field on the Welcome form (note the light blue glow around the edge of the ***User Name*** field, which indicates that it is accepting keyboard input):



2. Double tap with a single finger in the area of the active object.



3. Alternately, double-click in the area of the active object.
4. Alternately, select ⌨ from the application menu.
5. The actions in the previous three steps should show the built-in on-screen keyboard. For example:



Once the keyboard is on the screen, you can use it just like any other. In addition, the following buttons that appear on the keyboard have a particular purpose:

Item	*Description*
	Hides the keyboard.
	Press and hold, then while holding, move the mouse or finger in any direction to change the position of the keyboard on the screen.

4.6. Forms

Total Recall VR Cockpit uses forms with consistent structure to present and accept data.

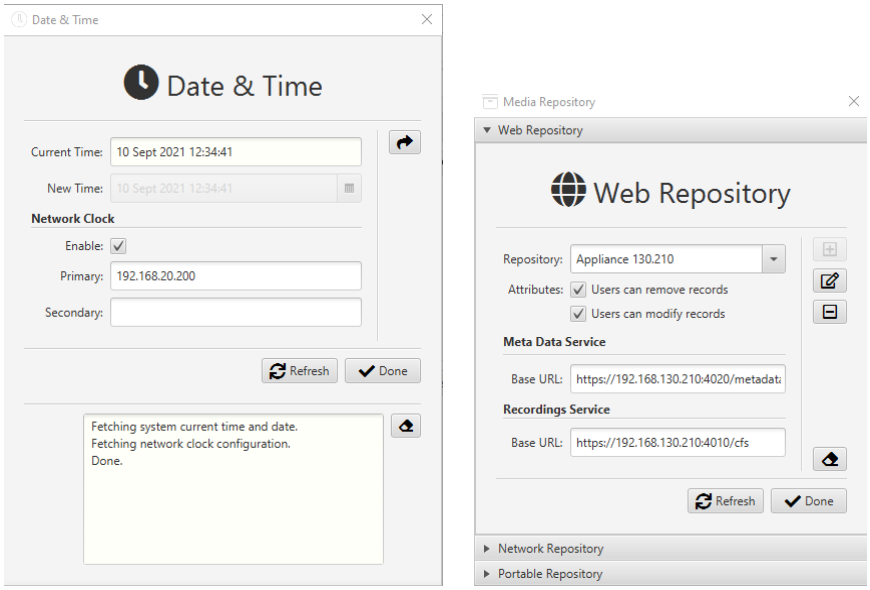
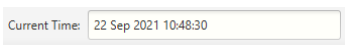


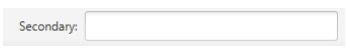
Figure 10: Example Forms

The background and glow colour of the data entry fields on the forms provide additional information for the field. For example:

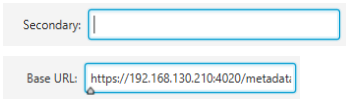
A white background indicates that the field displays and accepts data.



A Yellow background indicates that the field displays data only.

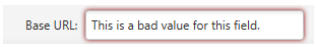


An empty field with a white background and no glow colour indicates that the data is optional.



An empty field, or a field with data and a blue glow, indicates that the field is focused and consumes all of the keyboard input.

An empty field with a red glow indicates that the data is mandatory.



A field with data and a red glow indicates that the field does not accept the data.

In addition to the form fields, some forms contain a status and progress area at the bottom. It shows information on the progress of the actions that can be triggered from the form. For example, in the previous screen capture, the area at the bottom of the Date & Time form.

Further, the following buttons may appear on a form:

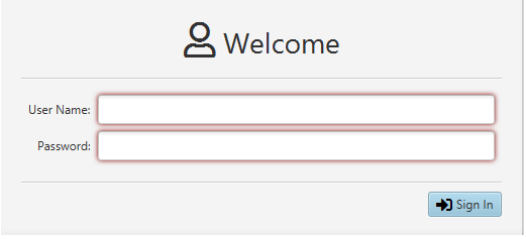
Item	***Description***
	Attempts to apply the changes entered on the form to the form's target. For example, it will attempt to set the system date and time on the Date & Time form.
	Creates a new record using the data from the form fields. For example, it will create a new repository record on the Web Repository form.
	Removes the record that is shown on the form. For example, it will remove (delete) the repository record shown on the Web Repository form.
	Updates an existing record using the data from the form fields. For example, it will update the repository record shown on the Web Repository form.
	Clear all fields on the form. For example, it will clear all fields on the Web Repository form and allow you to create a new repository entry.
	Cancels (stops) a long-running action initiated from the form while the action is in progress.
	Fetches the latest data and displays it on the form. For example, it will get and display the current system date and time on the Date & Time form.
	Hides (disposes of) the form without taking any action.

Finally, you can increase and decrease the width of the form. This is handy if you cannot see all the data in the form fields.

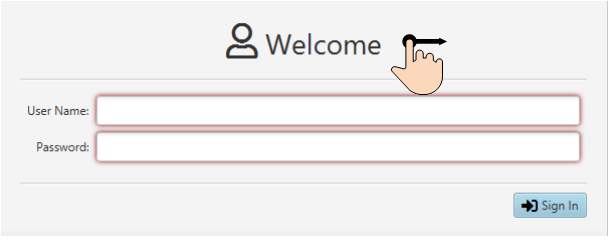
To change the width of a form:

Change the width of a form

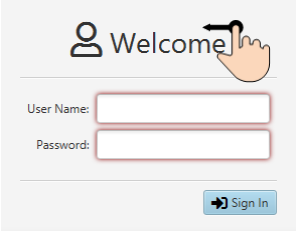
1. Click and hold, or touch with a single finger and hold, at any point in the title area of the form. For example, on the word “Welcome” in the title area of the Welcome form:



2. Move the mouse or finger to the right to increase the form's width while holding. For example:



3. Alternatively, move the mouse or finger to the left while holding to reduce the form's width. For example:



5. User Configuration

Total Recall VR Cockpit uses its authentication and authorisation database to control access to the application, features, and recordings.

5.1. Authentication

Total Recall VR Cockpit uses a standard username and password strategy for user authentication.

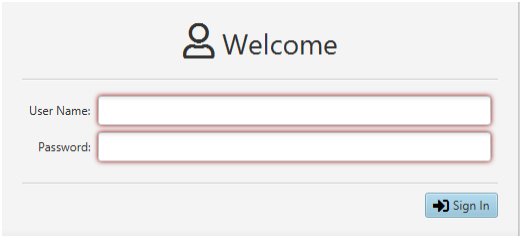


Figure 11: Welcome Form – Sign In

Both the username and password are mandatory. In addition, the password must comply with the following rules:

- Minimum 8 and maximum 16 characters.
- Contains at least one alpha and one numeric character.
- Does not contain the same character (alpha or numeric) more than three times.
- Cannot have two or more characters at the same position as the current password, if any.

5.2. Authorisation – Application

Total Recall VR Cockpit uses a set of permissions to control access to various application features.

Unlike other applications, there are no predefined roles (permission sets), so you can set different permissions for each user. This has the effect of defining a custom role for each user while, at the same time, all users with the same set of permissions belong to the same custom role.

Generally, there is permission for every action a user can initiate via the user interface.

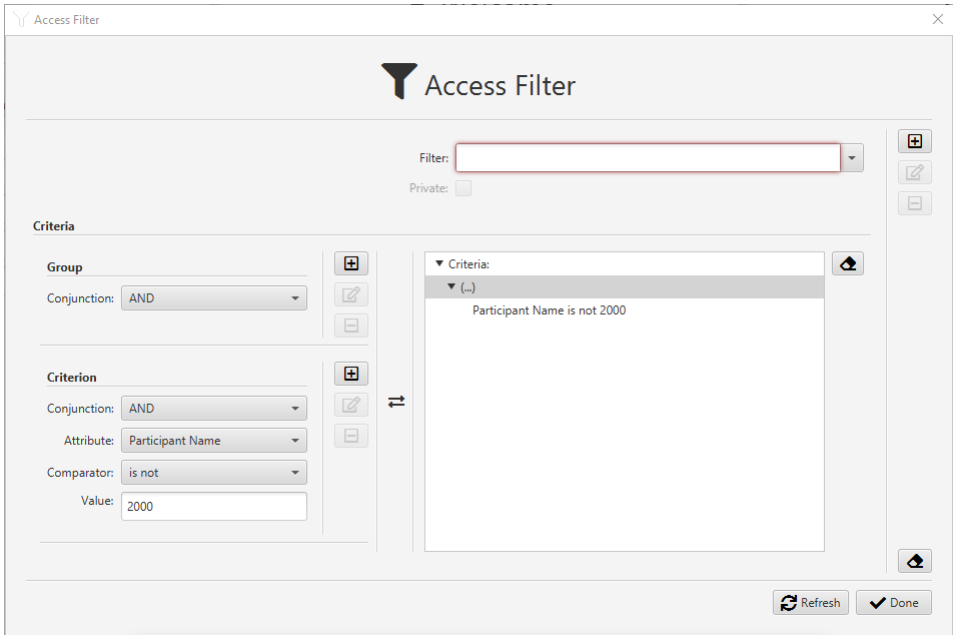
5.3. Authorisation – Recordings

Total Recall VR Cockpit uses an optional access filter to control access to recordings for each user.

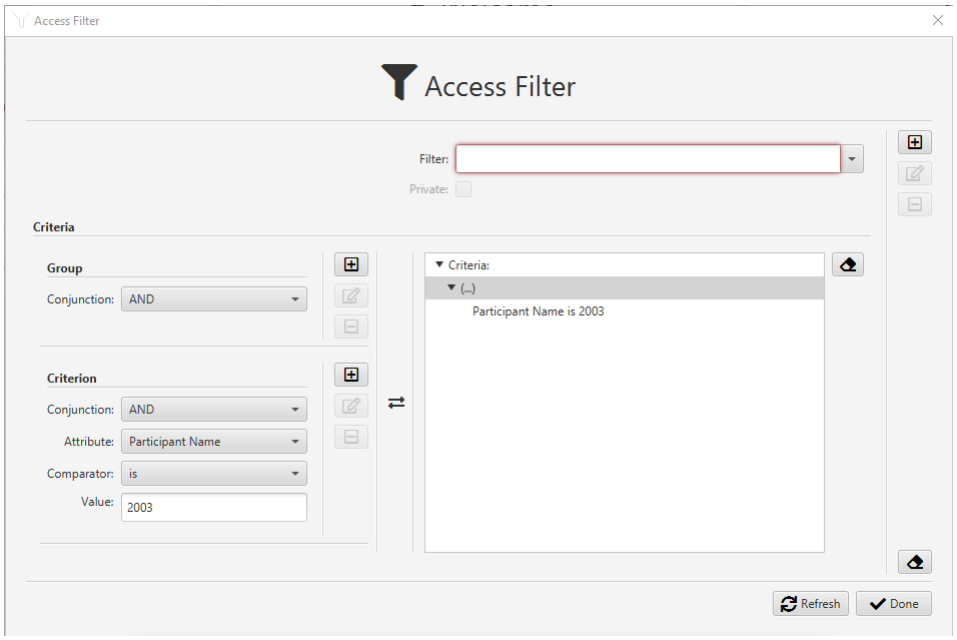
If set, the access filter is automatically added to the display filters for recordings on the recording Explorer and Monitor views. As a result, the access filter is automatically applied to both views, and the user cannot disable this action.

See section 6.3 Advanced Filter Builder - Recordings for information on creating and modifying access filters for recordings you can assign to users.

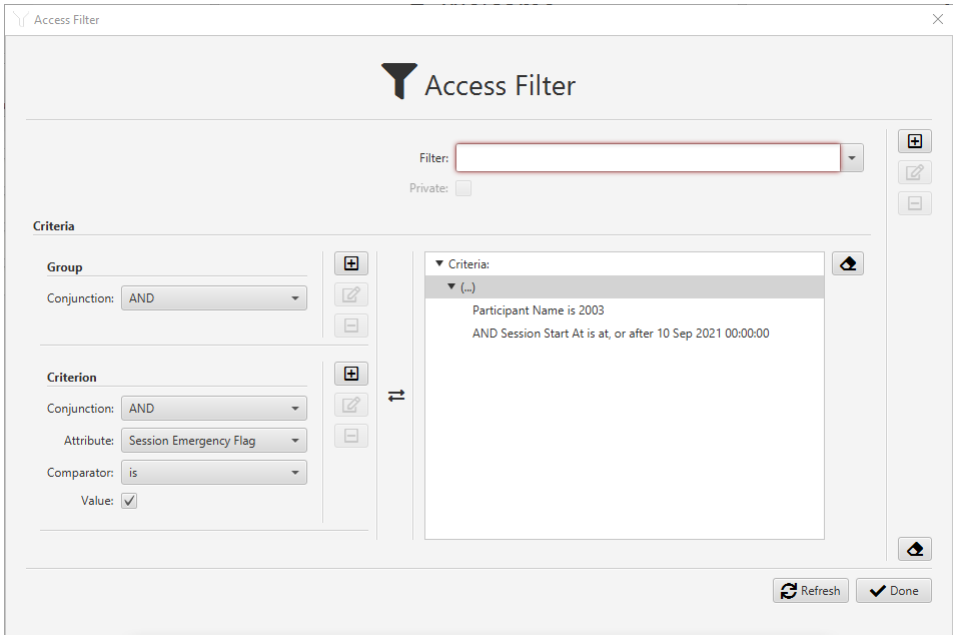
Note that there are no rules on structuring a filter; you can choose to use an exclusion, an inclusion or a combined filter. For example, the following is an exclusion filter that will exclude (filter out) all recordings that involve extension 2000 (as a result, the user will not be able to access any recordings that involve extension 2000):



The following is an example of an inclusive filter that will include (match) only recordings that involve extension 2003 (as a result, the user will only be able to access recordings that involve extension 2003):



Finally, the following is an example of a combined filter that includes recordings that involve extension 2003 but only recordings made after the 10th of September 2021 (as a result, the user will be able to access only recordings that involve extension 2003 that were made on or after the 10th of September 2021):



The possibilities are endless. As you may have noticed from the last screen capture, filtering on any recording attribute is possible.

5.4. User Management

Users with user management permission (the User permission in the Cockpit Configuration domain) can manage (create, update and remove) users via the Welcome form.

Users with user management permission can also manage their user records. As a result, such users can change their recording access filter and application permissions. In addition, such users can remove other users with administrative (full) permissions.

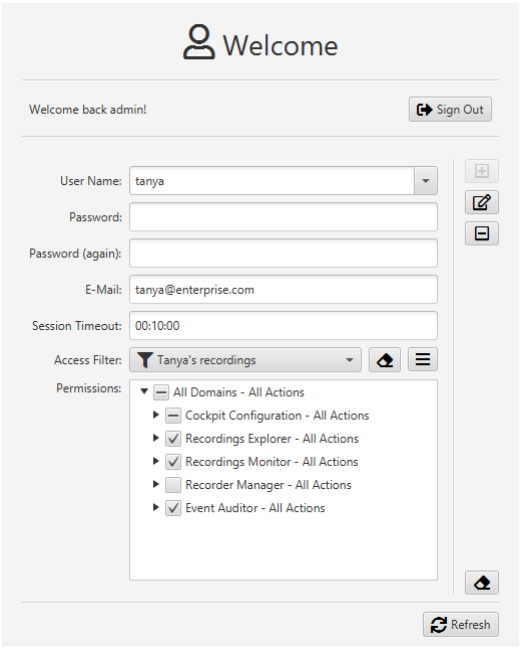


Figure 12: Welcome Form – User Management

All of the fields are self-explanatory on the Welcome form. However:

- When setting the password for a new user or modifying it for an existing user, the password must meet the password rules listed in section 5.1 Authentication.
- Set ***Session Timeout*** to *00:00:00* to prevent automatic timeout of the user's sessions due to inactivity.

Unlike users with user management permissions, users without such can change their password and e-mail address only via the **Welcome** form.

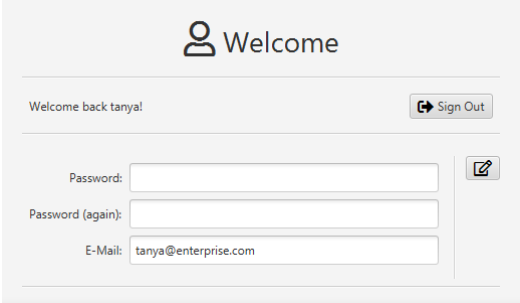


Figure 13: Welcome Form – Self Service

In such cases, and if the user attempts to change their password, the password must meet the rules listed in section 5.1 Authentication.

6. Filtering and Searching

Total Recall VR Cockpit has an integrated natural language filter processor for recordings and audit events.

In general, there are two types of filters:

- Instant filters. The lifetime of an instant filter is the same as the lifetime of the user session with the application. That is, if an application user creates an instant filter during a session with the application, the user can use the filter until they sign out. Further, application users cannot share instant filters.
- Persistent filters. As the name suggests, the lifetime of a persistent filter is as long as the filter exists in the application's configuration database. As a result, persistent filters can be used during multiple sessions with the application. Further, application users can share persistent filters or make such filters private.

Total Recall VR Cockpit has several filter builders that facilitate the creation of filters with different levels of complexity. The following sections explain how to use the different filter builders to create display and access filters for recordings and display filters for audit events.

6.1. Anatomy of a Filter

Filters are a single criterion or a collection of criteria that may be organised into groups. If the filter comprises criteria, groups of criteria, or both, the criteria and groups must be combined with the logical 'AND' or 'OR' operators.

The main building blocks of each filter are criteria. For example:

- ***Session Start At*** is at, or after *10 Sep 2021 10:00:00*.
- ***Participant Name*** is *2006*
- ***Category*** is *Error*

Each criterion specifies a recording or audit event attribute (***Session Start At***, ***Participant Name*** and ***Category*** in the previous examples) to filter on, a value (*10 Sept 10:00:00, 2006* and *Error* in the previous examples) for the attribute to filter on, and a filter comparator to apply ("is at, or after" and "is" in the previous examples).

The filter processor is capable of processing the following comparators (most are self-explanatory):

Comparator	***Description***
is	Match the specified value.
is not	Match values that are NOT the specified value.
is less than	Match values that are less than the specified value.
is, or less than	Match the specified values and values that are less than it.

is more than	Match values that are more than the specified value.
is, or more than	Match the specified values and values that are more than it.
is at	Match the specified time.
is not at	Match times that are NOT the specified time.
is before	Match times that are before the specified time.
is at, or before	Match times that are exactly the specified time or before it.
is after	Match times that are after the specified time.
is at, or after	Match times that are exactly the specified time or after it.
matches	Match values that satisfy the specified pattern. The pattern comprises of alphanumeric characters and the following wildcard characters: * - (star) - matches zero or more alphanumeric characters. For example: 10* matches any sequence of characters that start with 10. To match the actual * character use '*'. **%** - (percent) - same meaning as *. **_** - (underscore) - matches exactly one character. For example: 10_ matches any sequence of 3 characters that start with 10. To match the actual _ character use '_'.

Criteria can be combined with the logical 'AND' or 'OR' operators to create conjunctions and disjunctions. For example:

- ***Session Start At*** is at, or after *10 Sep 2021 10:00:00* AND ***Participant Name*** is *2006*
- ***Category*** is *Error* OR ***Category*** is *Warning*

Finally, criteria can be organised into groups combined with the logical 'AND' or 'OR' operators to create complex filters. For example:

- ***Session Start At*** is at, or after *10 Sep 2021 10:00:00* AND (***Participant Name*** is *2006* OR ***Participant Name*** matches *2006**)
- ***(Session Start At*** is at, or after *10 Sep 2021 10:00:00* AND ***Session Start At*** is at, or before *10 Sep 2021 14:00:00*) AND (***Participant Name*** is *2006* OR ***Participant Name*** is *2010*)

Filters do not limit the number of criteria and groups of criteria. However, different filter builders may do this.

6.2. Instant Filter Builders - Recordings

There are three filter builders for instant filters for recordings, all of which are accessible from the Instant Filter Builder area of the application view, where you may need to use a filter—for example, the Explorer and Monitor views.

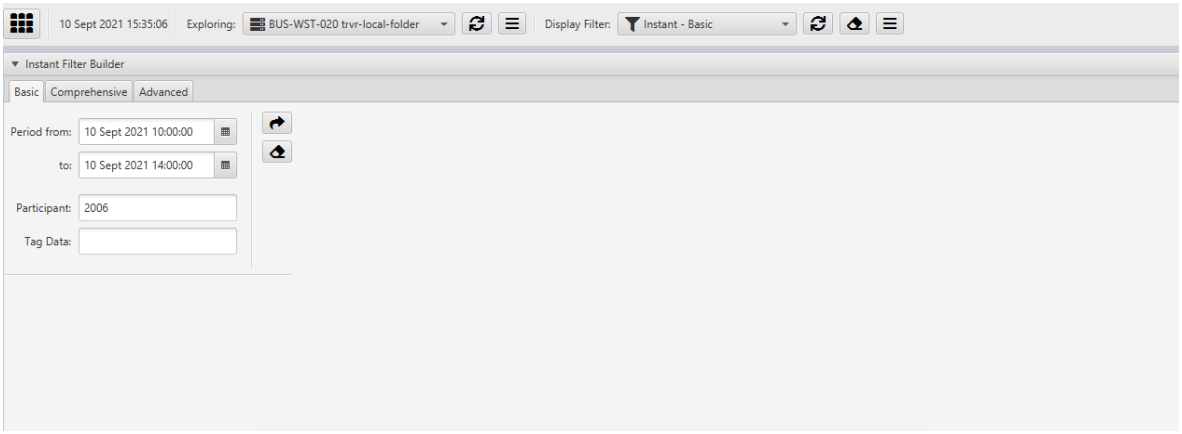
The instant filter builders for recordings work the same way, irrespective of the application view they appear on.

The three different builders for instant filters for recordings are named:

1. Basic;
2. Comprehensive; and
3. Advanced.

As the names suggest, the complexity of using an instant filter builder increases with each builder; however, at the same time, the filters that you can create become more advanced and comprehensive with each builder.

The Basic filter builder can create simple filters you will likely use most of the time, as shown in the following screen capture.



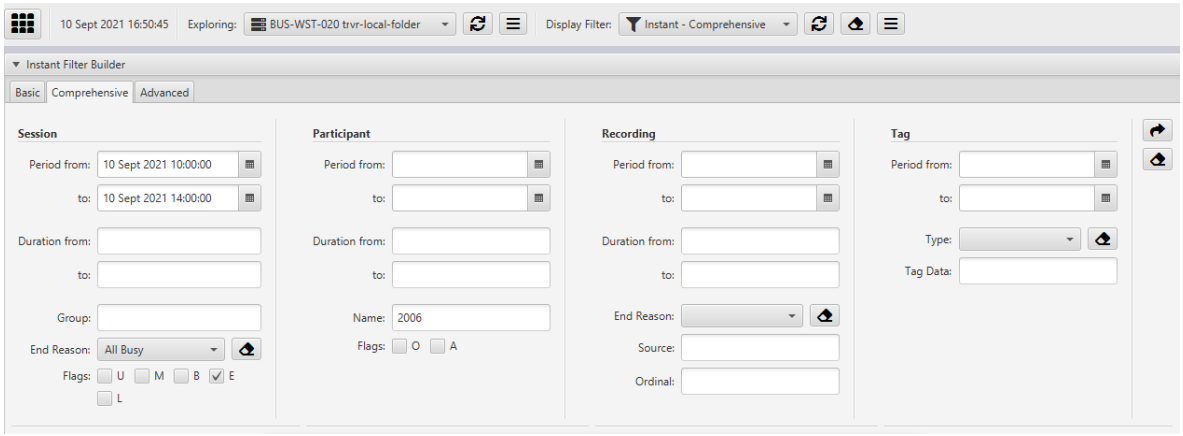
For example, to find all recordings that involve extension 2006 between 10am and 2pm on the 10th of September 2021:

Create a Basic instant filter

1. Set ***Period from*** to *10 Sept 2021 10:00:00*.
2. Set ***Period to*** to *10 Sept 2021 14:00:00*.

3. Set ***Participant*** to *2006*.
4. Select ↱ to create the filter and make it the active ***Display Filter*** for the view (note the value of ***Display Filter*** – it will show "Instant – Basic", the default name for a Basic instant filter).

If you need to filter on additional recording attributes, use the Comprehensive filter builder, which gives you access to all recording attributes.



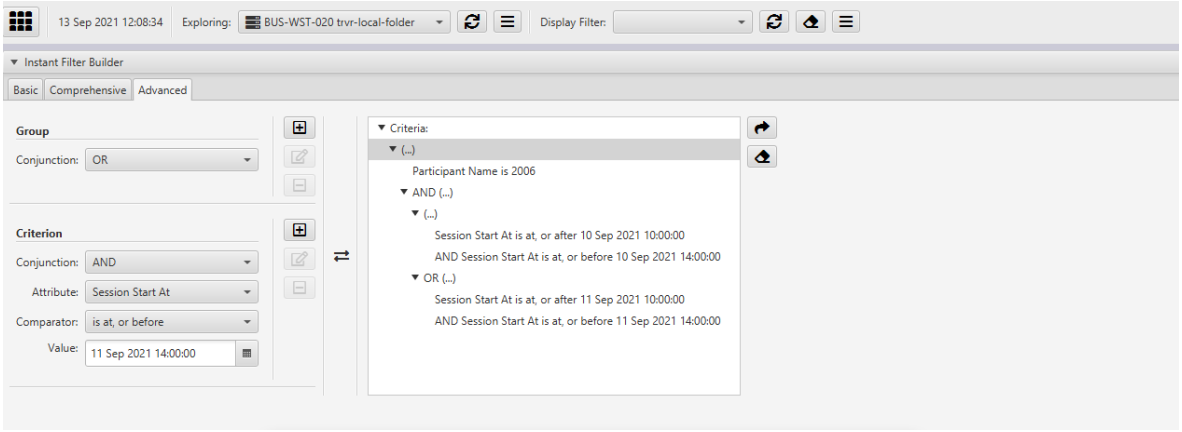
For example, to find all recordings of emergency calls that resulted in a busy condition and involve extension 2006 between 10am and 2pm on the 10th of September:

Create a Comprehensive instant filter

1. In the Session part of the form:
   a. Set ***Period from*** to *10 Sept 2021 10:00:00*.
   b. Set ***Period to*** to *10 Sept 2021 14:00:00*.
   c. Choose *All Busy* for ***End Reason***.
   d. Tick *E* for ***Flags***.
2. In the Participant part of the form:
   a. Set ***Participant*** to *2006*.
3. Select ↱ to create the filter and make it the active ***Display Filter*** for the view (note the value of ***Display Filter*** – it will show "Instant - Comprehensive", the default name for a Comprehensive instant filter).

The Basic and Comprehensive filter builders hide the complexity of creating filters by creating individual criteria and combining them into groups behind the scenes. However,

to create a filter of any complexity, use the Advanced filter builder, where you can work with individual and group criteria to construct a filter of any complexity.



For example, to find all recordings that involve extension 2006 between 10am and 2pm on the 10th or 11th of September 2021:

Create an Advanced instant filter

1. See section 6.3 Advanced Filter Builder - Recordings for instructions on using the advanced filter builder to create a filter.
2. Select ↱ to make it the active ***Display Filter*** for the view (note the value of ***Display Filter*** – it will show “Instant - Advanced”, the default name for an Advanced instant filter).

6.3. Advanced Filter Builder - Recordings

The advanced filter builder can create complex filters.

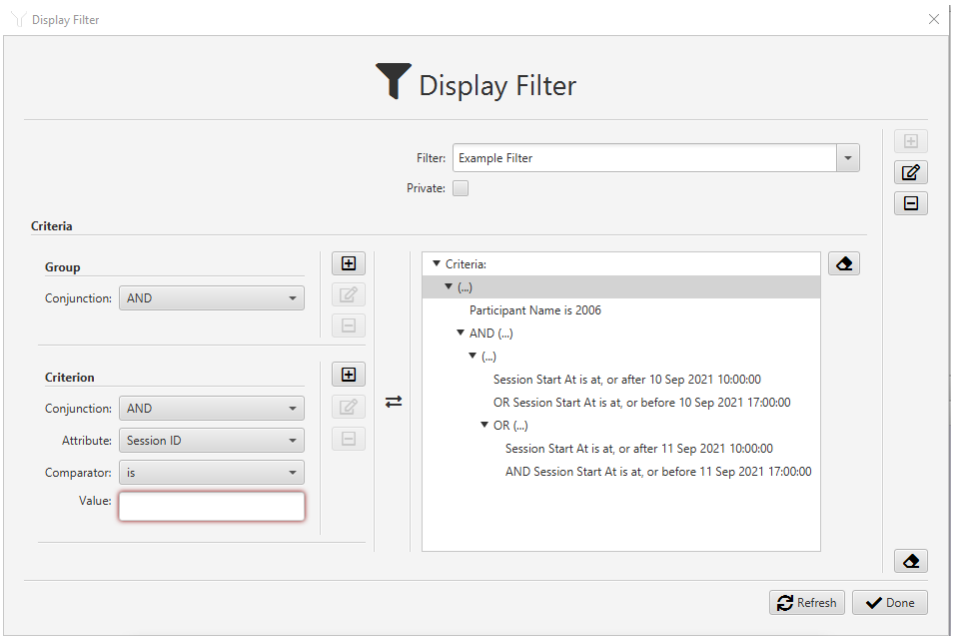


Figure 14: Advanced Recoding Filter Builder

Filters that result in the same outcomes may take different forms due to the flexibility of the advanced filter builder. Consequently, explaining how to create every possible filter here is impossible. Instead, we explain how you can create the following example filter, which should give you an idea of how to create criterions, group them and combine the criteria and groups with logical "AND" and "OR" operators:

Participant Name is *2006*

AND (

(***Session Start At*** is at, or after *10 Sep 2021 10:00:00*

AND ***Session Start At*** is at, or before *10 Sep 2021 14:00:00*)

OR

(***Session Start At*** is at, or after *11 Sep 2021 10:00:00*

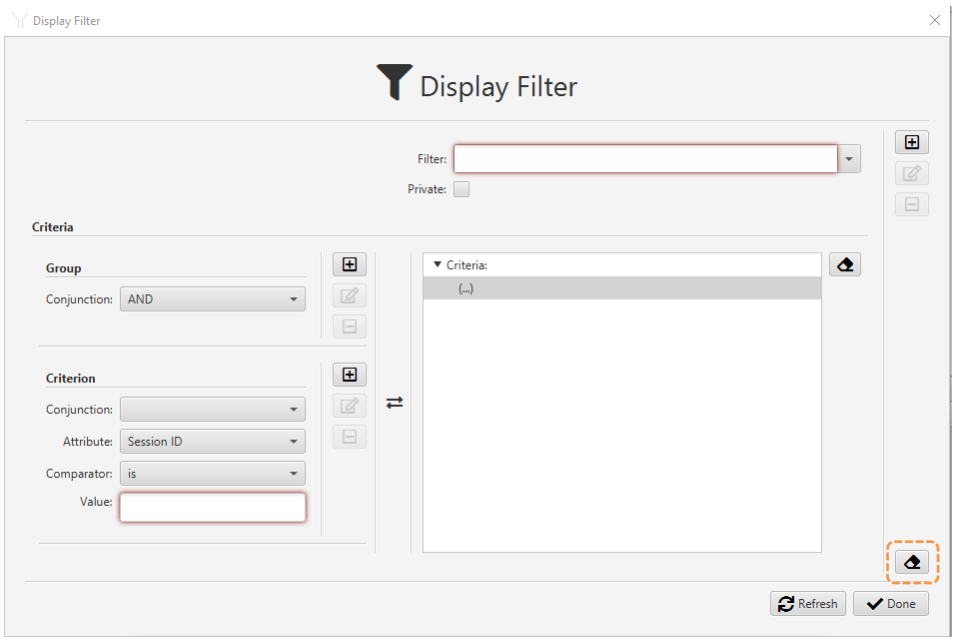
AND ***Session Start At*** is at, or before *11 Sep 2021 14:00:00*)

)

The example filter matches all recordings that involve extension 2006 and started between 10am and 2pm on the 10th of September 2021 or between 10am and 2pm on the 11th of September 2021. It comprises 5 criteria and 3 groups, one used to group two groups.

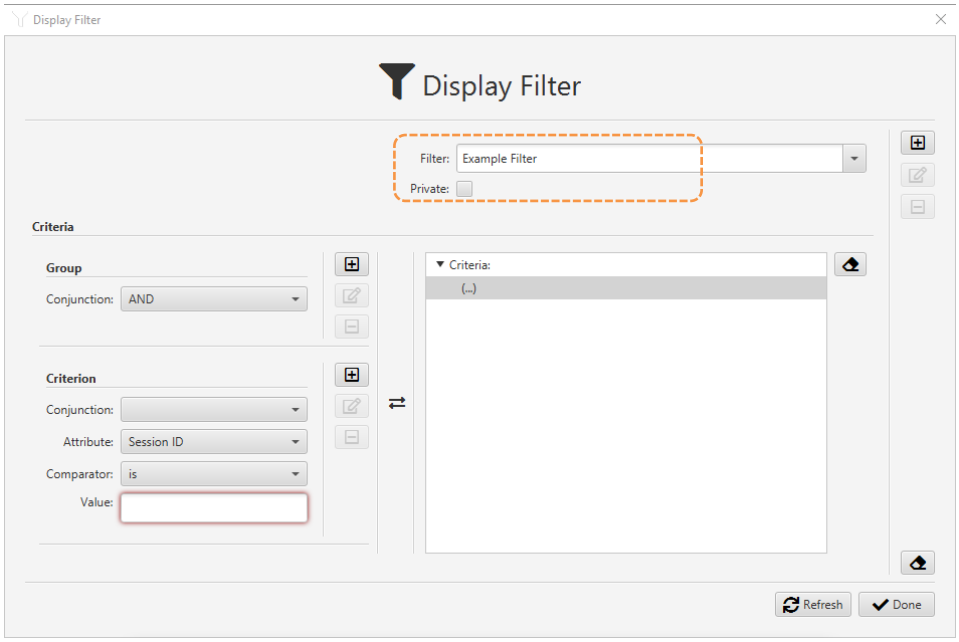
Create an Advanced instant filter

1. Start with an empty filter form. If the form is displaying a filter, then select to clear it. For example:

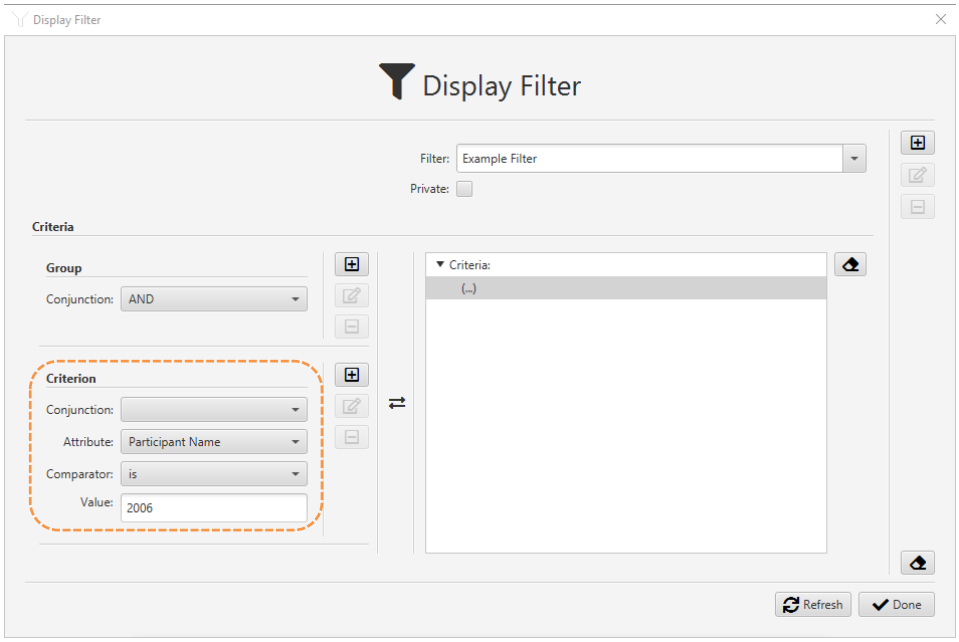


2. Enter ***Filter***. This is the filter's name that will help you identify it when you wish to use it. Then, tick ***Private*** if you do not want to share the filter with other application users.

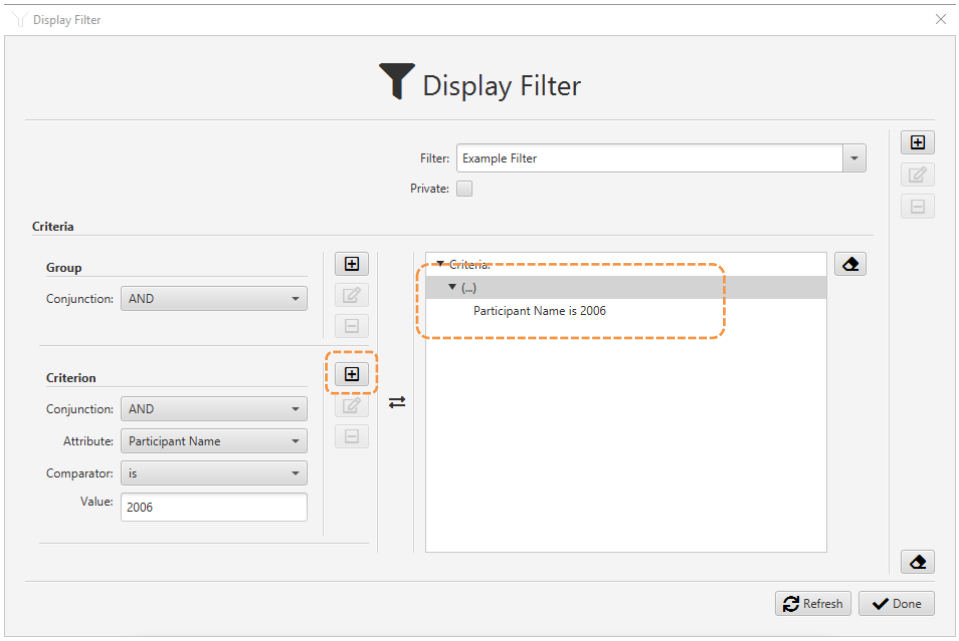
   For example, we will name the filter “Example Filter” and keep it public (so that other users can use it):



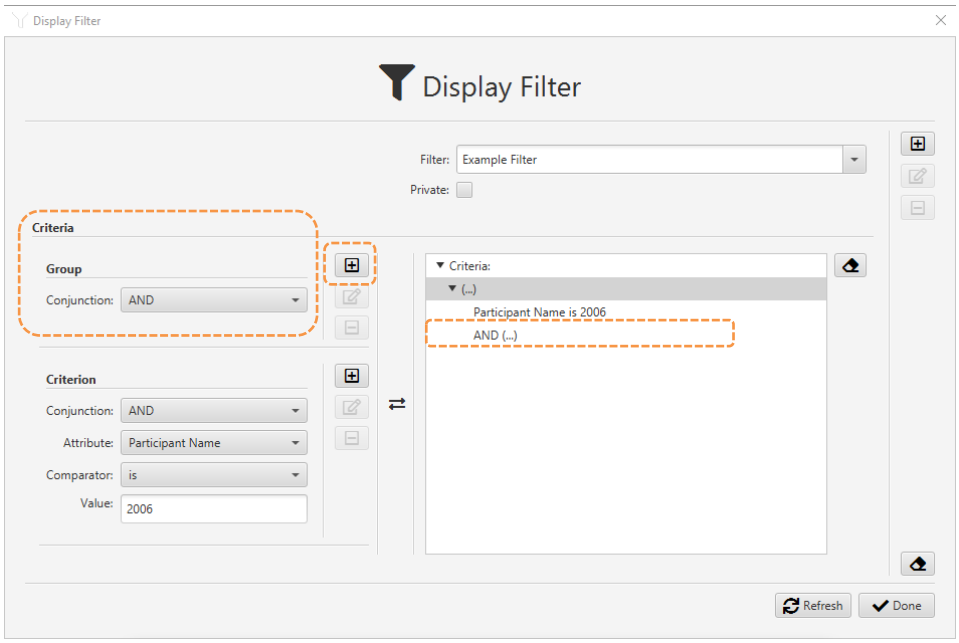
3. To create the first criterion (***Participant Name*** is *2006*), first set the fields in the Criterion area of the form as shown in the following screen capture:



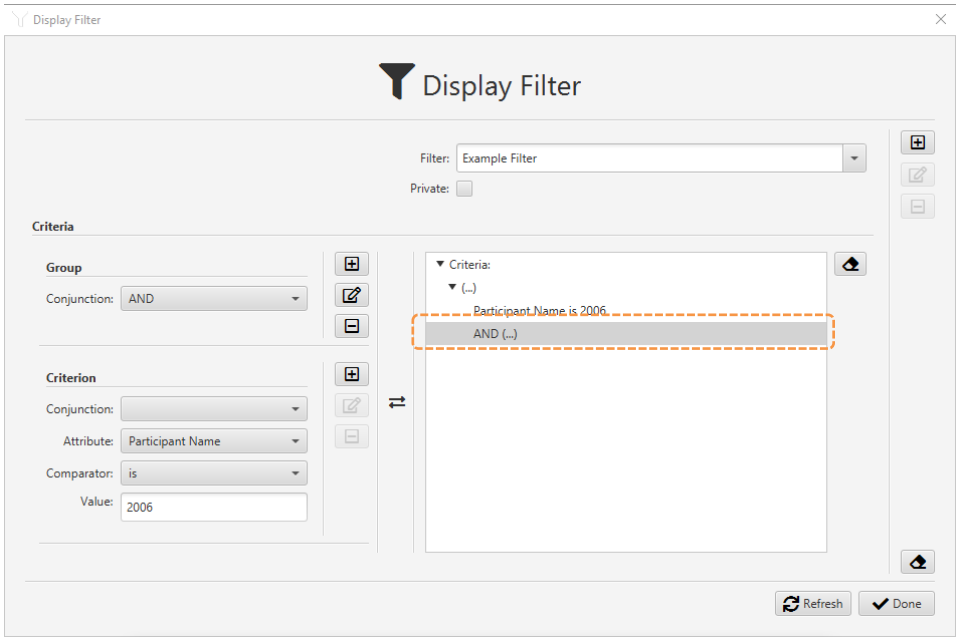
4. Next, select the main group (...) of the Criteria tree and then select ⊞ in the Criterion area of the form to add the criterion to the Criteria tree:



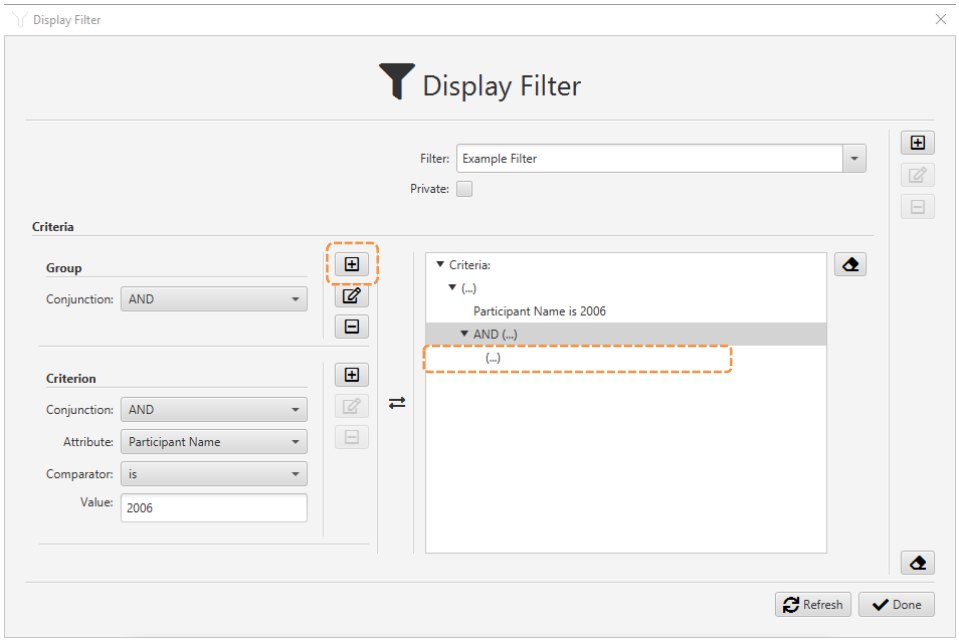
5. We need to create the group that will hold the two groups with the start time criteria. In the Group area of the form, set ***Conjunction*** to *AND*. Then select ⊞ in the Group area of the form to add the group to the Criteria tree:



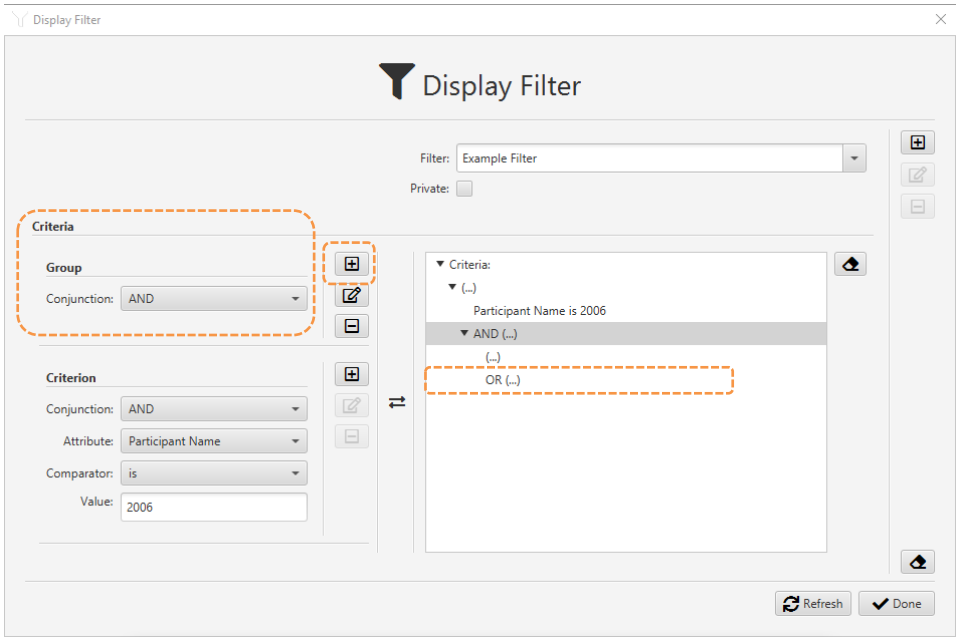
6. The new group comprises two groups, joined with the “OR” operator in our example filter. We will create the two groups first. To do so, select the group node that you just created on the Criteria tree:



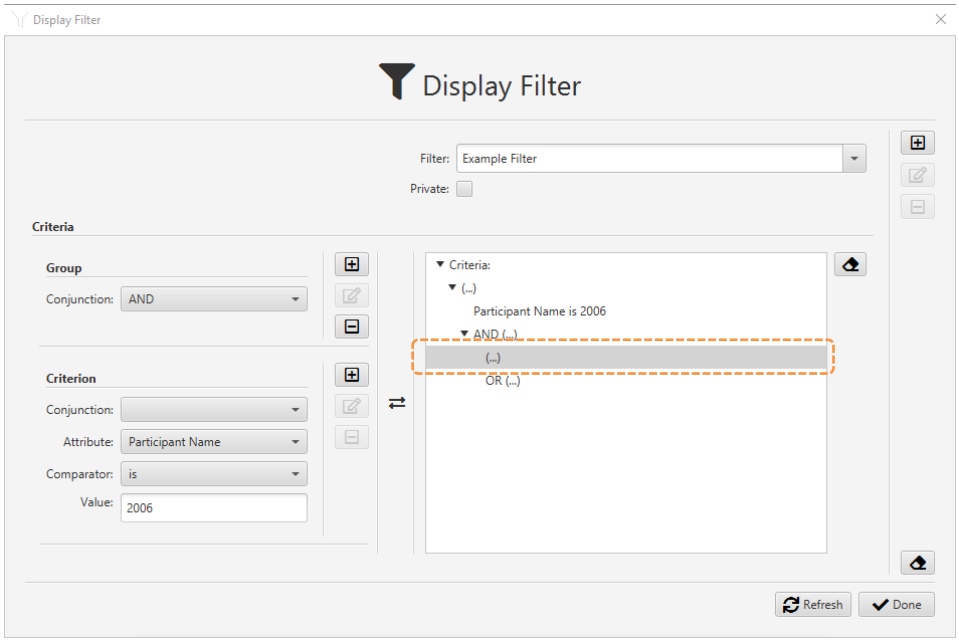
7. Select ⊞ in the Group area of the form to add a new group to the Criteria tree:



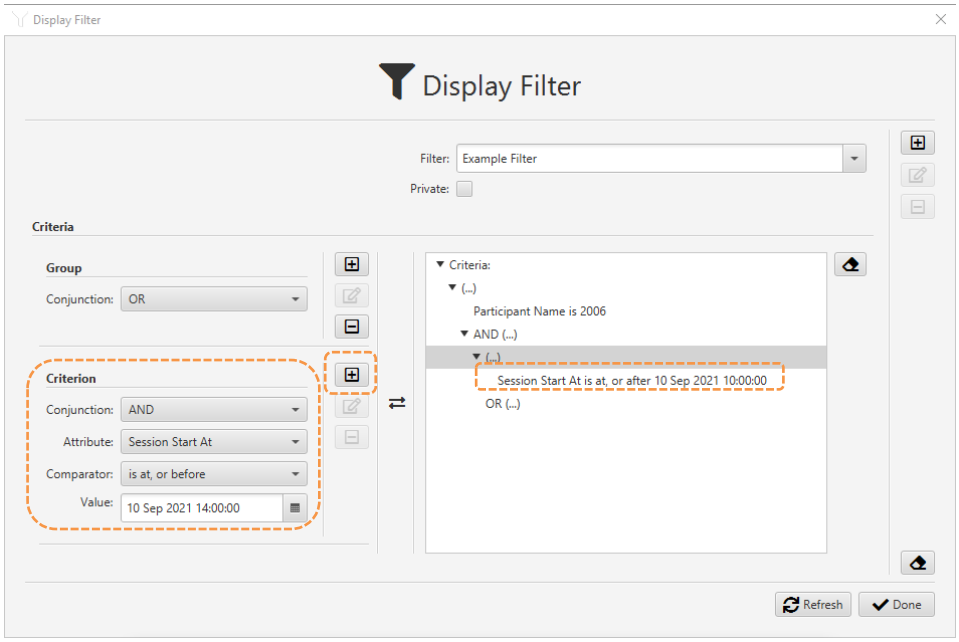
8. In the Group area of the form, set ***Conjunction*** to *OR* and then select ⊞ to add the group to the Criteria tree:



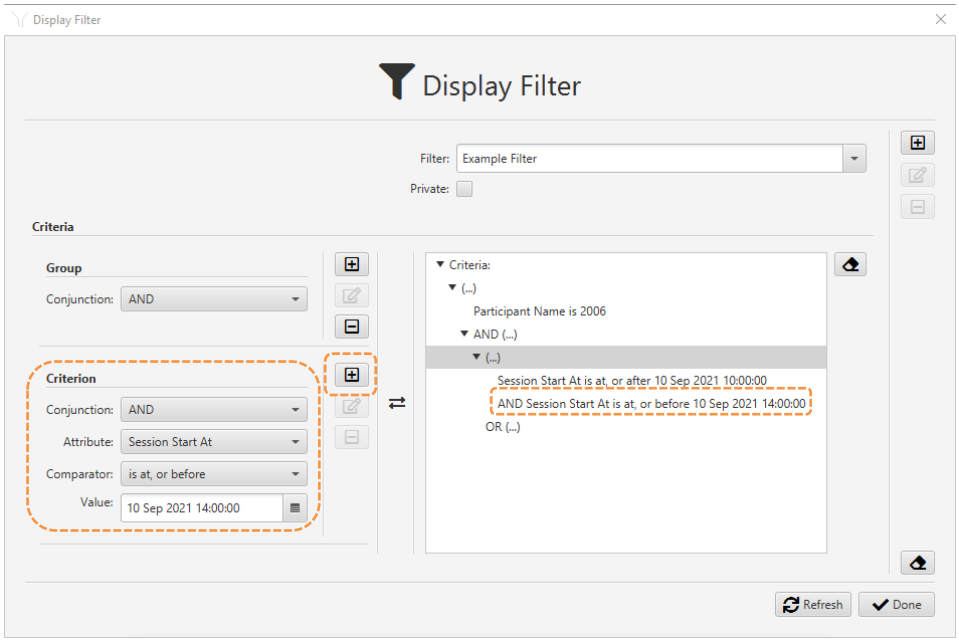
9. We will add the criteria for the 10th of September 2021. To do so, select the first sub-group in the Criteria tree:



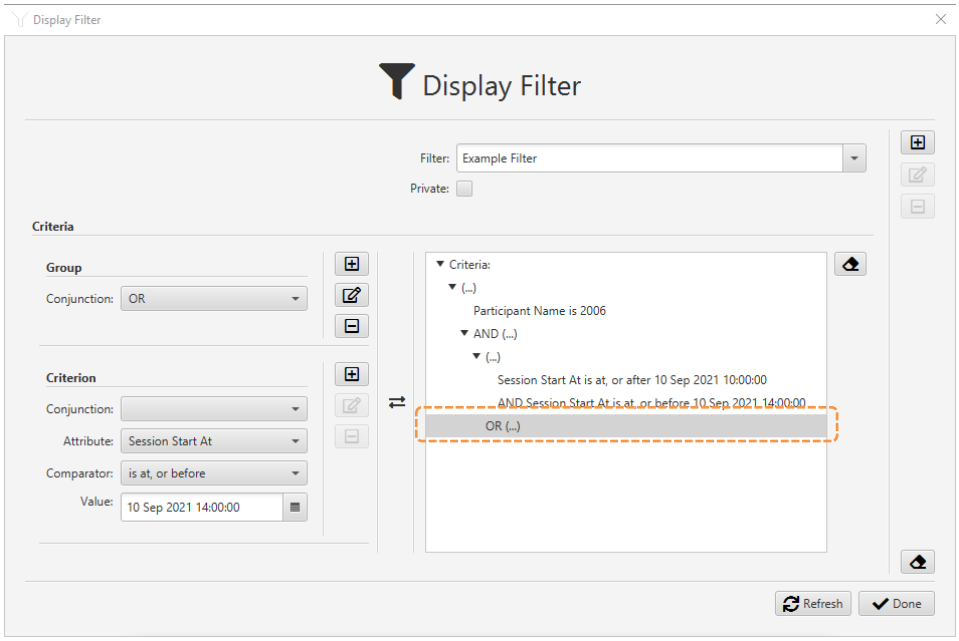
10. To create the first criterion for 10th of September 2021 (***Session Start At*** is at, or after *10 Sep 2021 10:00:00*), first set the fields in the Criterion area of the form as shown in the following screen capture, and then select ⊞ in the Criterion area of the form to add the criterion to the Criteria tree:



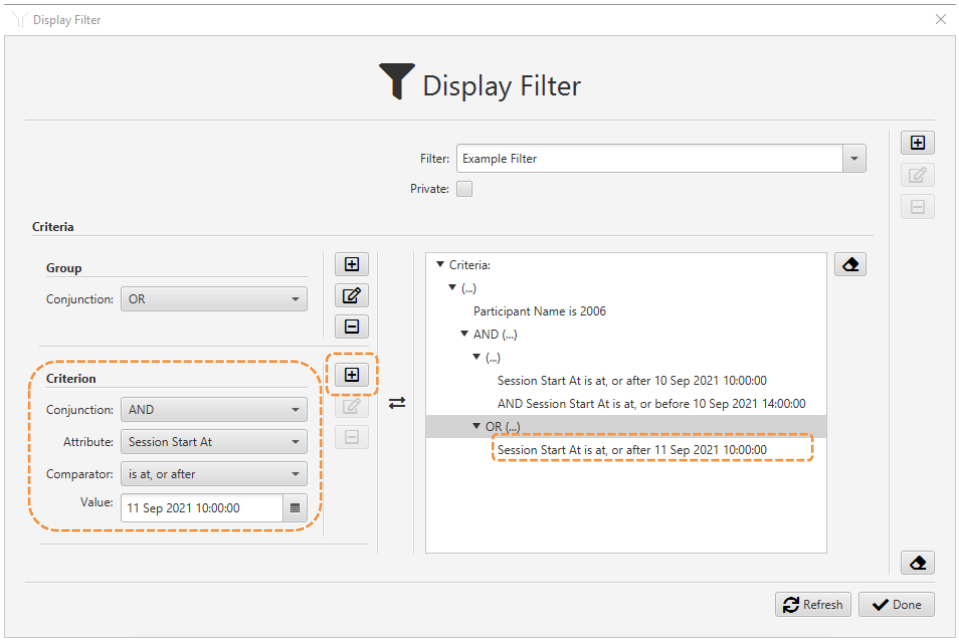
11. To create the second criterion for 10th of September 2021 (***Session Start At*** is at, or before *10 Sep 2021 14:00:00*), first set the fields in the Criterion area of the form as shown in the following screen capture, and then select ⊞ in the Criterion area of the form to add the criterion to the Criteria tree:



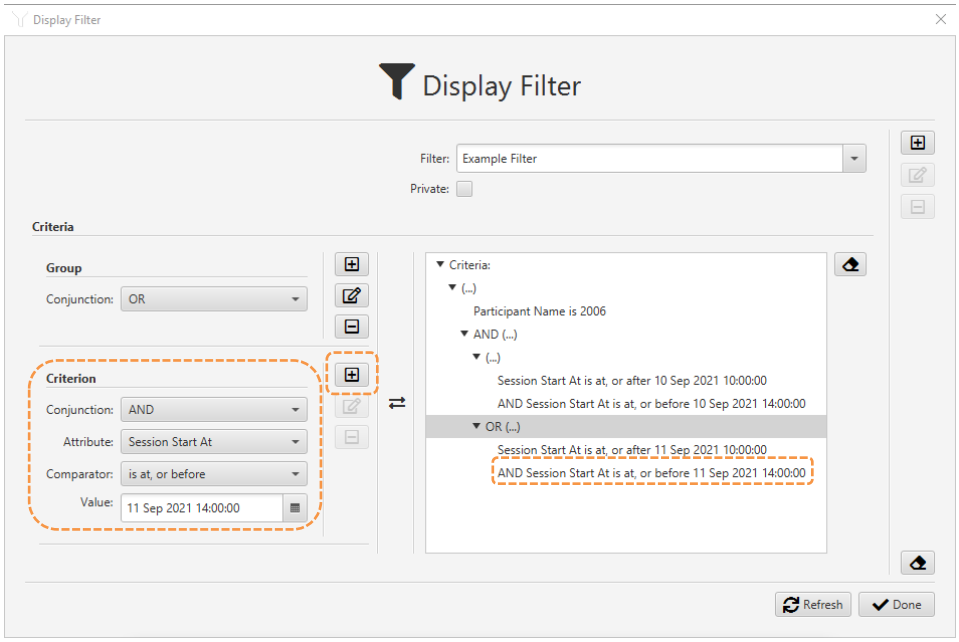
12. Finally, we will add the criteria for the 11th of September 2021. To do so, select the second sub-group in the Criteria tree first:



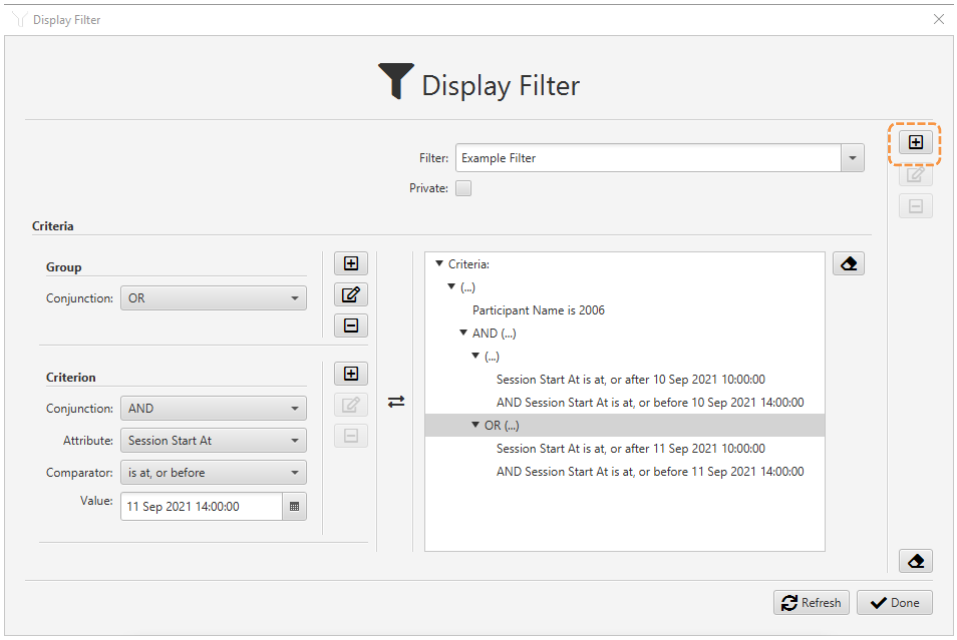
13. To create the first criterion for 11th of September 2021 (***Session Start At*** is at, or after *11 Sep 2021 10:00:00*), first set the fields in the Criterion area of the form as shown in the following screen capture, and then select ⊞ in the Criterion area of the form to add the criterion to the Criteria tree:



14. To create the second criterion for 11th of September 2021 (***Session Start At*** is at, or before *11 Sep 2021 14:00:00*), first set the fields in the Criterion area of the form as shown in the following screen capture, and then select ⊞ in the Criterion area of the form to add the criterion to the Criteria tree:



15. The filter is now complete. Select the form ⊞ (top right corner of the form) to add the filter to the application configuration database.



6.4. Instant Filter Builders – Audit Events

The instant filter builders for filters for audit events work the same as the instant filter builders for filters for recordings. The only difference is in the attributes for each criterion where:

- The instant filter builder for filters for audit events uses attributes related to audit events, for example, ***Category***, ***Priority***, ***Actor***, etc.
- The instant filter builder for filters for recordings uses attributes related to recordings, for example, ***Session Start At***, ***Participant Name***, ***Tag Data***, etc.

See section 6.2 Instant Filter Builders - Recordings for more details on how to use the instant filter builders for filters for audit events.

6.5. Advanced Filter Builder – Audit Events

The advanced filter builder for audit events works precisely like the advanced filter builder for recording filters. The only difference is in the attributes for each criterion where:

- The advanced filter builder for filters for audit events uses attributes related to audit events, for example, ***Category***, ***Priority***, ***Actor***, etc.
- The advanced filter builder for filters for recordings uses attributes related to recordings, for example, ***Session Start At***, ***Participant Name***, ***Tag Data***, etc.

See section 6.3 Advanced Filter Builder - Recordings for more details on using the advanced filter builder for filters for audit events.

7. Recording Management

The Explorer view of Total Recall VR Cockpit has a built-in browser for recordings stored in recording repositories with different types of access. The browser has a suite of recording management and productivity tools that work on recording files and metadata.

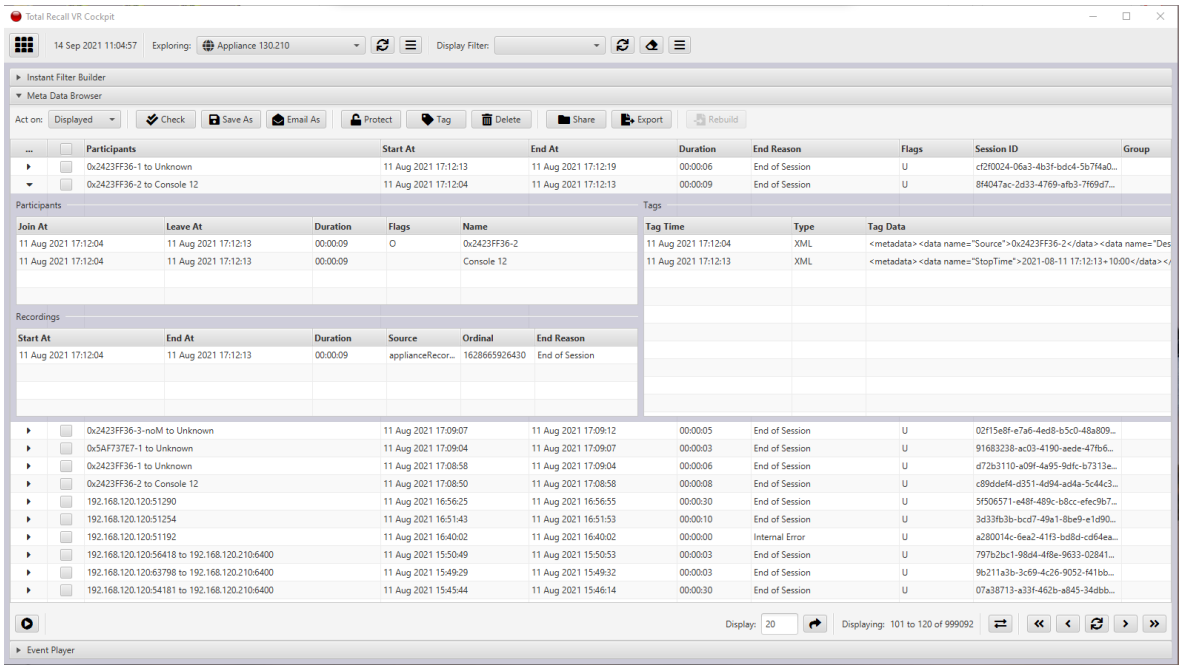


Figure 15: Recording Browser – Explorer View

The following sections explain how to use the recording browser and the recording management and productivity tools.

7.1. Recording Repositories

Each Total Recall VR recording repository (also known as a media repository) combines a set of recording files and a database of metadata (a collection of parameters) for each recording file.

Typically, a repository has one location, which can be:

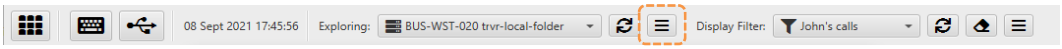
- An appliance or a custom recorder.
- An appliance or a custom recording archive device.
- A database and file system that is accessible over the network.
- A database and a file system located on a locally attached storage, for example, the disk drive that is part of your PC.
- A database and a file system located on removable storage, for example, a USB disk.

Total Recall VR Cockpit can use one of the following access mechanisms to access the recordings and their metadata in a given repository:

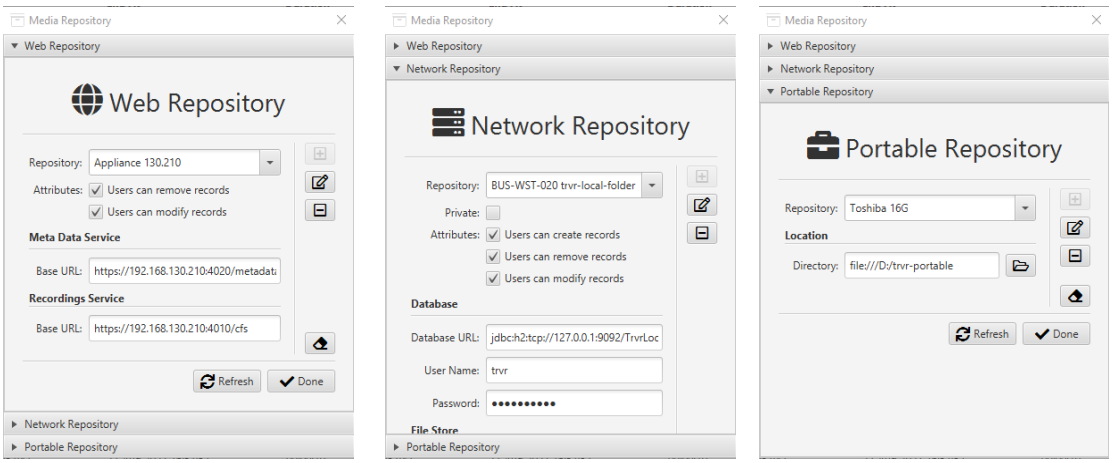
- REST interface to both the recording metadata and recording files.
- Direct network (JDBC) access to the database with recording metadata and direct access to the recording files on a local or network drive (via a network file access protocol such as NFS and CIFS).
- Direct access to a database file with recording metadata and recording files on a local file system (a locally attached disk or a removable disk).

While it may be possible to access a repository in some cases via multiple access mechanisms, such as REST and direct network access to the database with metadata and the file system with recording files, we recommend that you pick one method and stick with it in such cases. In such cases, the REST method should be preferred over the direct network access method, and the direct network access should be preferred over the local file system access method.

You can manage the records for the repositories that Total Recall VR Cockpit can access by selecting ☰, located next to the ***Exploring*** selector on the application menu bar.



It will display the Media Repository form, which you can then use to manage records for repositories with different access, as shown in the following screen captures.

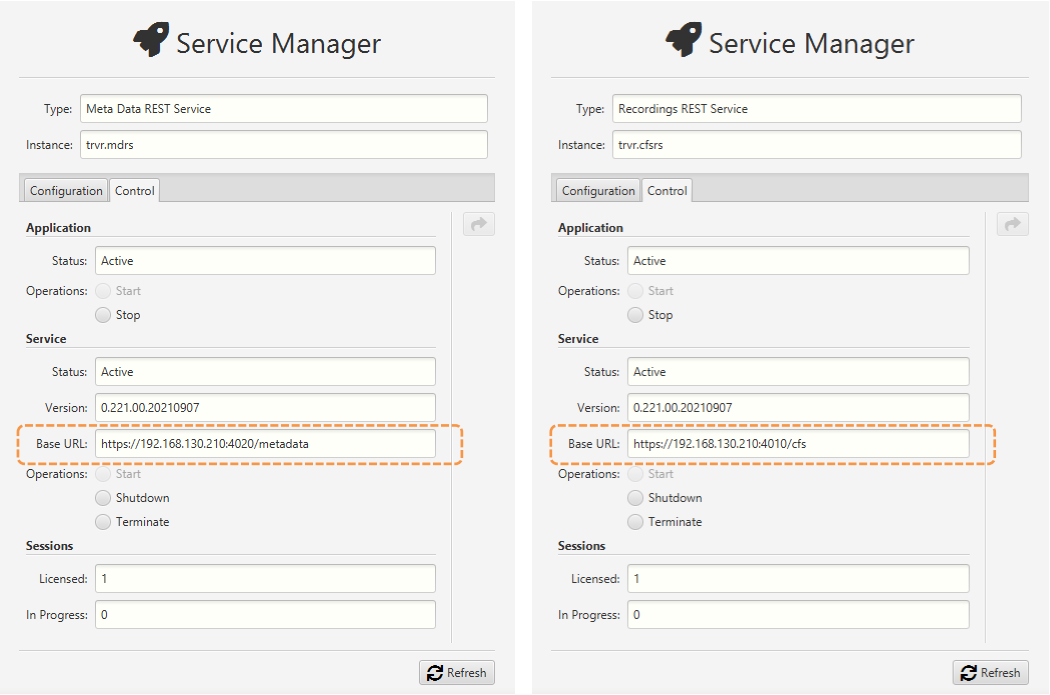


7.1.1. Web Repository

Web Repositories provide a REST interface to access the recording files and the metadata about the recordings for the recordings stored in the repository.

Repositories located on appliance and custom recorders and appliance and custom recording archive devices provide a REST interface via the “Meta Data REST Service” and the “Recordings REST Service”.

To configure a Web Repository, you need the base REST URLs for both services. You can get the base URLs from the service runtime status, for example:



7.1.2. Network Repository

Network Repositories are repositories with direct network access to both the file system with recording files and the database with metadata for the recordings.

You can create this repository type by allocating file space on network drives and creating databases on database servers with network access.

DO NOT use the same database or network file system location for multiple Network Repositories. Use a different database and network file system location for each Network Repository.

Typically, multiple Total Recall VR Cockpit users will access a Network Repository from multiple application instances simultaneously. So, Network Repositories usually contain recordings important to users who need concurrent and simultaneous access to the information in the repository. For example, a collection of recordings for an

incident or an archive (backup) of recordings that must be kept for a considerable period.

To configure a Network Repository, you will need:

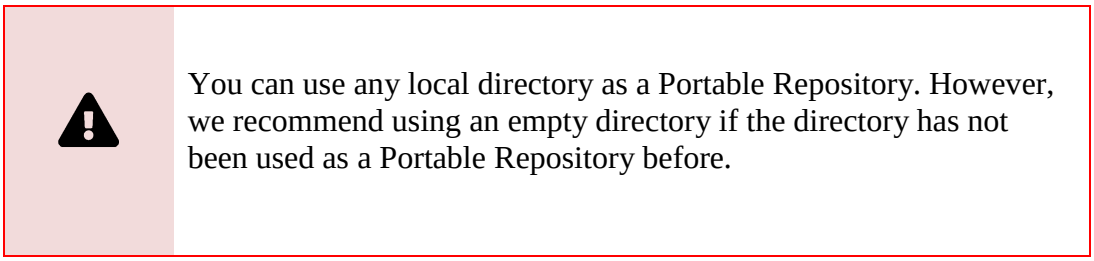
- The JDBC URL which specifies the repository database's location and name.
- The username and password of the database user that can access the database.
- The network path of the network file system housing the recording files, for example, a UNC path to a Windows share.

For more information and practice examples, see sections 12.2 Manual Archiving to a Network Repository and 12.5 Automatic Archiving to a Network Repository.

7.1.3. Portable Repository

Portable Repositories are repositories with direct local file system access to both the recording files and the database with metadata for the recordings.

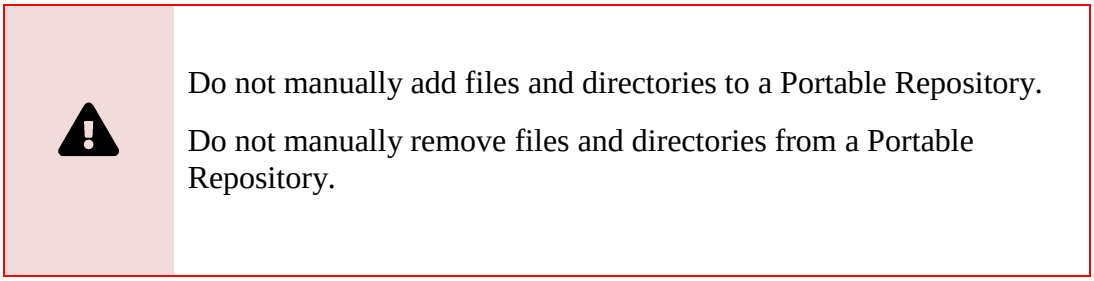
Typically, this is a repository on a removable disk, such as a USB disk or thumb drive, or a directory on the local disk of the device running an instance of Total Recall VR Cockpit.



You can use any local directory as a Portable Repository. However, we recommend using an empty directory if the directory has not been used as a Portable Repository before.

Directories used as a Portable Repository have the following subdirectories: cfs and metadata. For example, if you used the D:\trvr-portable directory as a Portable Repository, then the following subdirectories will be present:

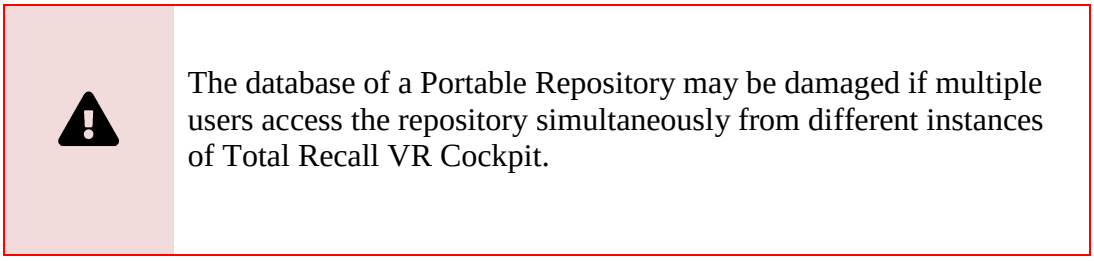
- D:\trvr-portable\cfs and
- D:\trvr-portable\metadata.



Do not manually add files and directories to a Portable Repository.

Do not manually remove files and directories from a Portable Repository.

While it is technically possible to use a directory on network file system for a Portable Repository, please avoid placing Portable Repositories on network file systems where multiple users can access them simultaneously from different Total Recall VR Cockpit instances. Portable Repositories are designed to be used by one application user from one application instance at a time.



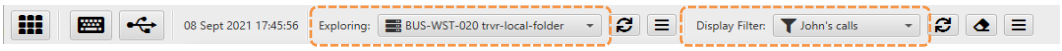
The database of a Portable Repository may be damaged if multiple users access the repository simultaneously from different instances of Total Recall VR Cockpit.

For more information and practice examples, see sections 12.3 Manual Archiving to a Portable Repository and 12.6 Automatic Archiving to a Portable Repository.

7.2. Recording Browser

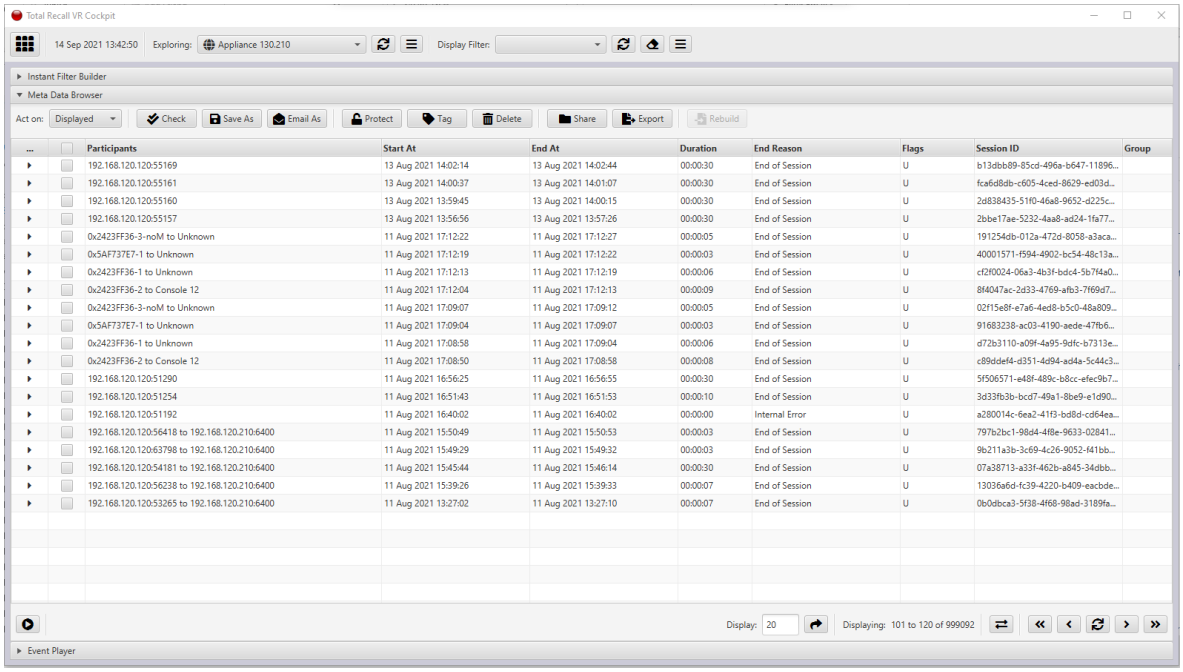
The recording browser provides a table-like view of the metadata for the recordings in the selected repository.

You can choose a repository to browse with the ***Exploring*** selector on the application menu bar. In addition, and optionally, you can choose a display filter for recordings with the ***Display Filter*** selector that is also located on the application menu bar.



If you need to configure a new repository record or update an existing one, please see section 7.1 Recording Repositories. If you need to configure a new display filter or update an existing one, please see section 6.3 Advanced Filter Builder - Recordings.

Once you choose a repository, and if Total Recall VR Cockpit can access it, it will display the metadata of the most recent recordings in the repository in a tabular form and in reverse time order (most recent recording on top).



If you choose a display filter, Total Recall VR Cockpit will use that filter while accessing the metadata in the repository and show only records that pass the filter.

A recoding access filter may be set on your user profile. If set, Total Recall VR Cockpit will automatically use it in addition to the display filter when accessing the metadata in the repository.

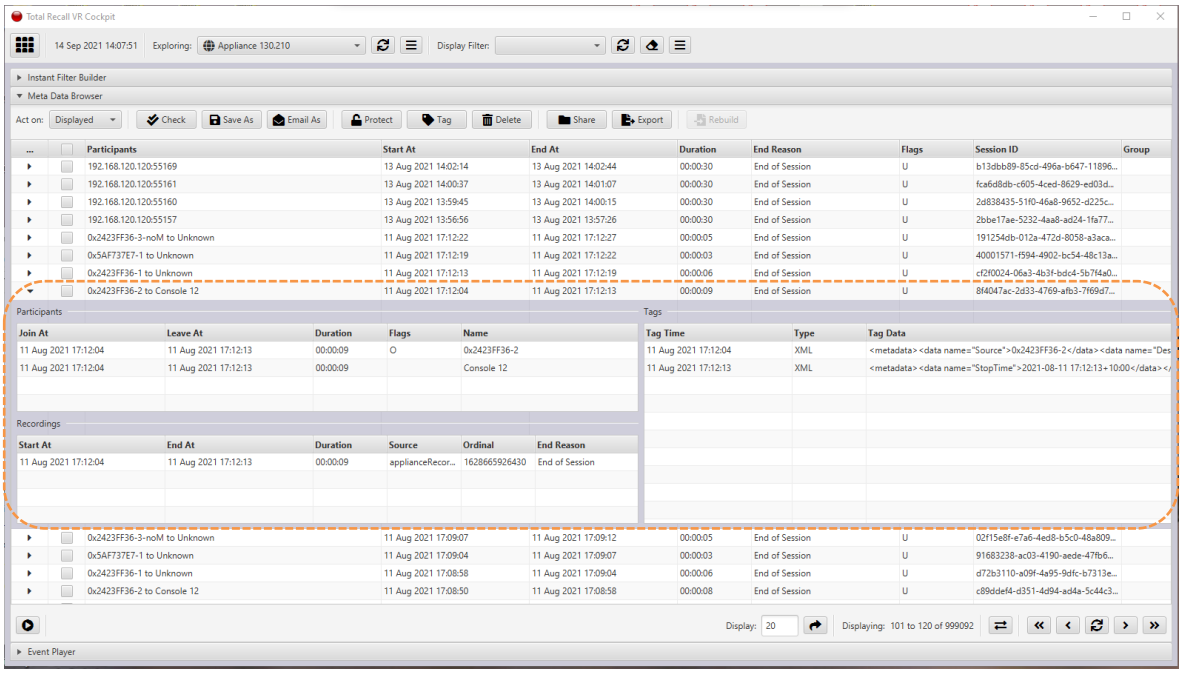
The value in the ***Display*** field specifies the number of metadata records that should appear in the table (also known as the page size), for example, 20 in the previous screen capture. To change the number of records that appear in the table (or the page size), simply enter ***Display*** and then select ↱.

Use the following controls to navigate through the metadata records in the repository:

Control	***Description***
⇄	This is a toggle control, and if set, it will automatically update the table with the metadata for the latest recordings in the repository. The update period is 60 seconds.
«	Displays the metadata for the most recent recordings in the repository, also known as the first metadata page.
‹	Displays the previous page of metadata – moving forward in time.

⟳	Refreshes the metadata that is shown.
›	Displays the previous page of metadata – moving backward in time.
»	Displays the metadata for the oldest recordings in the repository, also known as the last metadata page.

Select ▸, which appears in the first column of the row that shows the metadata for a recording, to display additional information that is part of the metadata for the recording.



Select ▾ in the same row to hide the additional information.

Finally, you can access several recording management and productivity tools via the controls above the table showing metadata.

The ***Act on*** selector defines the operating context for the management and productivity tools. The operating context can be one of the following:

1. *Selected* (default value) - The tools will operate on the selected metadata and recordings.
2. *Displayed* - the tools will operate on the displayed metadata and recordings. You may have to scroll up and down to see all of the metadata and recordings on which the tool will operate.
3. *Filtered* (use with caution) - the tools will operate on all metadata and recordings in the repository that match the selected display filter.
4. *All* (use with caution) - the tools will operate on all metadata and recordings in the repository.

Use *Filtered* and *All* with caution, as you may unexpectedly apply the tool to some metadata and recordings without intending to do so. For example, delete metadata and recordings that you do not intend to.

The following management and productivity tools are available:

Tool	***Description***
Check	Recording integrity check tool. Checks the integrity of recording files and reports on any inconsistencies that may be present.
Save As	Recording file export tool. Exports recording files to the original tamper-proof format (.trcx) or several supported standard formats (.wav, .mp3, .m4a, .ogg, etc.).
Email As	Recording e-mail tool. Export recording files to the original tamper-proof format (.trcx) or several supported standard formats (.wav, .mp3, .m4a, .ogg, etc.) and e-mail the exported recordings to one or multiple addressees.
Protect	Recording locking tool. Protects or unprotects recordings from deletion.
Tag	Tagging tool. Adds different types of tags (notes, etc.) to the recording metadata.
Delete	Deletion tool. Use this tool with caution to delete recordings. If ***Act on*** is set to *All*, it will delete all recordings in the repository. The action is not reversible.
Share	Recording file and metadata transfer tool. Transfers copies of recording files and metadata from one recording (media) repository to another.
Export	Metadata export tool. Exports recording metadata in several standard formats (XML, JSON, PDF, etc.).
Rebuild	Metadata rebuilding tool.

	Use with caution. It will remove all metadata from the database and reconstruct it from the data stored in the recording files. The tool's intended use is to repair or reconstruct damaged databases of recording metadata.

When started via the above controls, the tools may use a form to gather further information that will be used while the tools are running. For more details on using forms, please see section 4.6 Forms.

8. Event Reconstruction & Replay

The Explorer view of Total Recall VR Cockpit has a built-in event player capable of processing multiple recordings in the correct time order. Use the event player to reconstruct the timeline of events (incidents) and listen to the events as they happened in time.

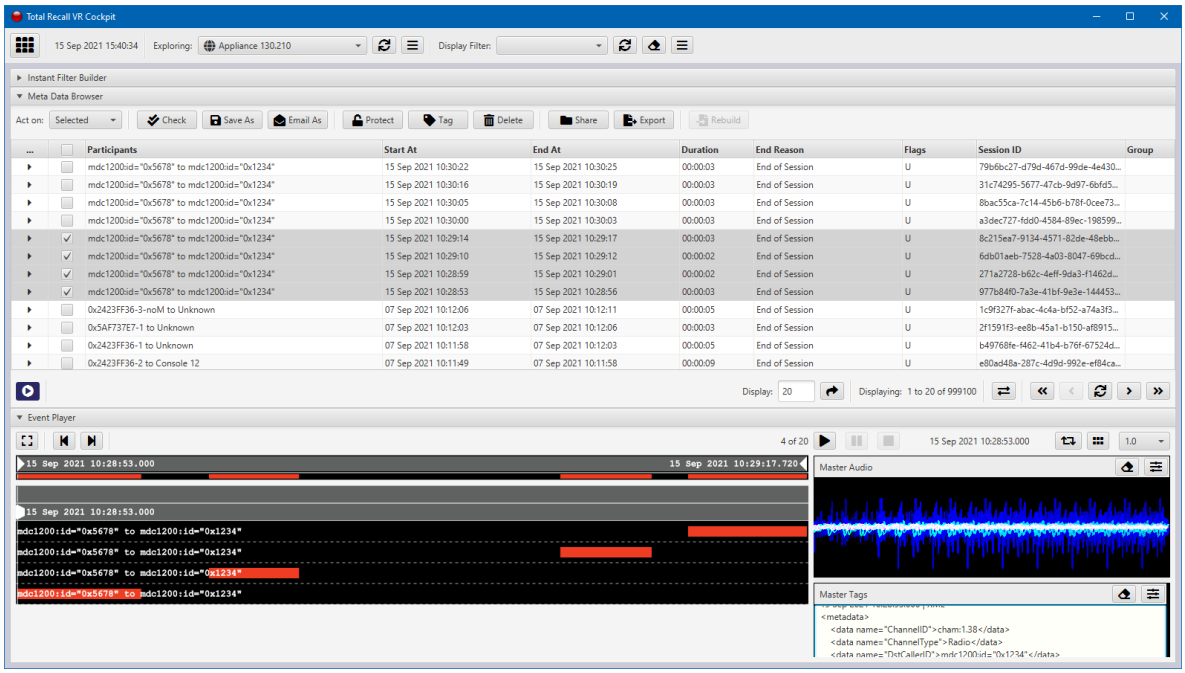


Figure 16: Event Player – Explorer View

The following sections explain how to use the event player.

8.1. Event Timeline

The event timeline is a combination of recording metadata shown by the recording browser and a visual representation of the timeline that the event player shows. The event player acts as an extension to the recording browser and adds a visual representation of the event timeline during event reconstruction and replay.

By default, the event player is not active to free up computing resources for other activities and applications.

You must activate the event player by setting the recording browser to what is known as review mode. For more details on the recording browser, see section 7.2 Recording Browser.

Set the toggle of the recording browser to enter review mode and activate the event player. Unset the same toggle to exit review mode and deactivate the event player.

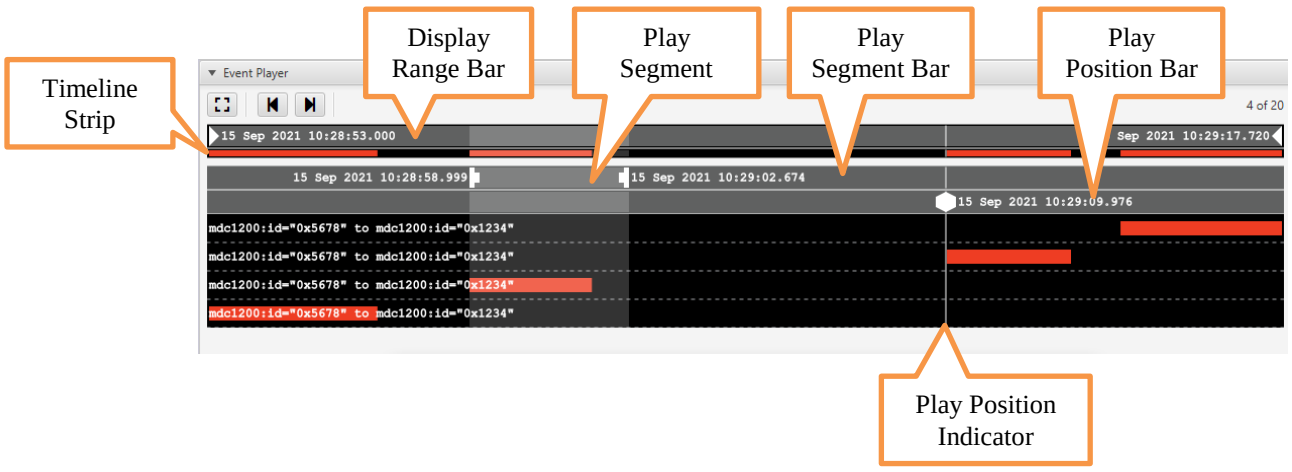
While the recording browser is in the review mode, as you select recordings in the recording browser, the selected recordings will automatically be forwarded to the event player and added to the visual representation of the event timeline in the correct time order.

> The event player limits the number of recordings that it can process to 20 at this stage. It adds recordings to the timeline on a first come, first served basis until it reaches this limit.

At the same time, as you unselect recordings in the recording browser, the event player will automatically remove the unselected recordings from the visual representation of the event timeline.

> The event player's visual representation of the timeline shows the most recent recording at the top and the oldest recordings at the bottom, the same as the recording browser.

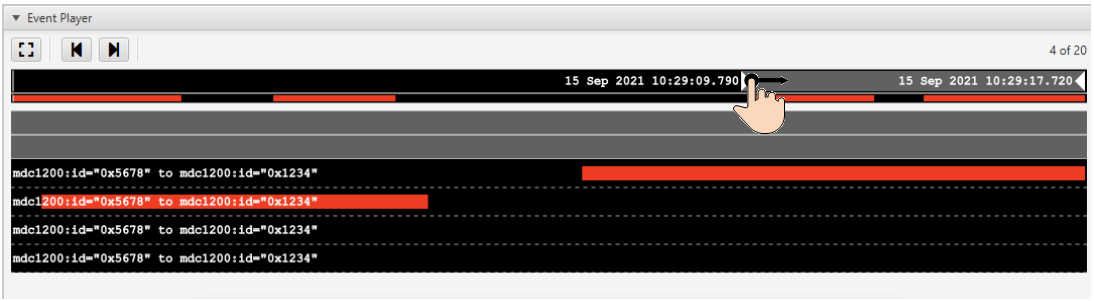
The following screen capture shows the structure of the visual timeline.



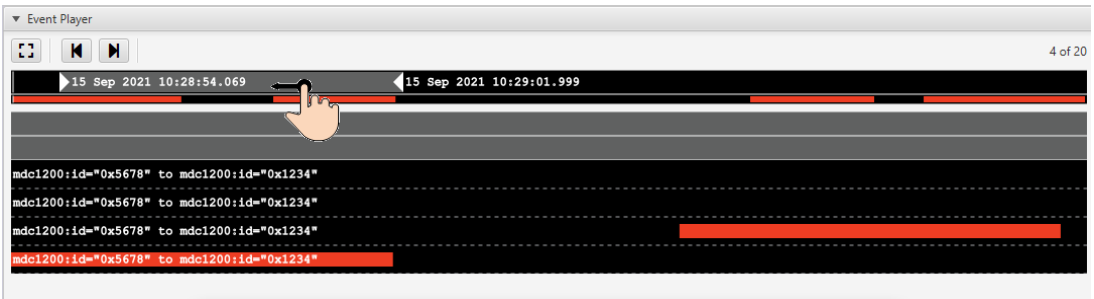
The following controls affect the visual timeline:

Control	*Description*
⛶	Resets the timeline. The timeline will show the entire duration of the event, the play position is set to the start of the event, and the play segment will be removed, if any.
⏮	Moves the play position to the start of the previous recording in the timeline, back in time, if any.
⏭	Moves the play position to the start of the next recording in the timeline, forward in time, if any.

The display range bar at the top of the timeline indicates which part of the entire timeline is displayed. You can reduce the range by moving the time range markers, ⏵ and ⏴, closer together and zooming in. For example:



To zoom out, that is to show a more extended time segment of the timeline, move the same markers further apart. Once you are happy with the display range, you can move the range to any point of the timeline. To do so, click and hold, or press and hold, in the area of the display range and then slide to the new position. For example:

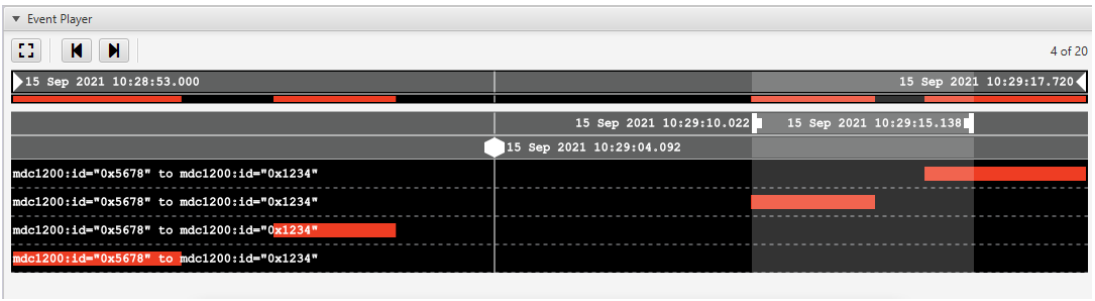


Double-click or double-tap on the display range bar to reset the display range to the timeline's entire duration.

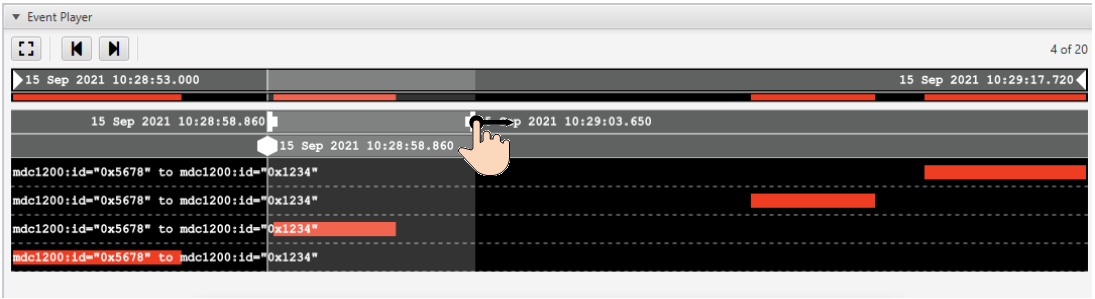
The timeline strip, located right under the display range bar, shows the time position of each recording relative to the total event duration. Its purpose is to help you visually

identify the location of recordings and gaps in the timeline so that you can quickly move to a position of interest, mainly when using a display range with a short duration.

Right under the timeline strip, the following bar is the play segment bar. Use this bar to select a segment (part) of the timeline if you wish to replay only that part. For example:



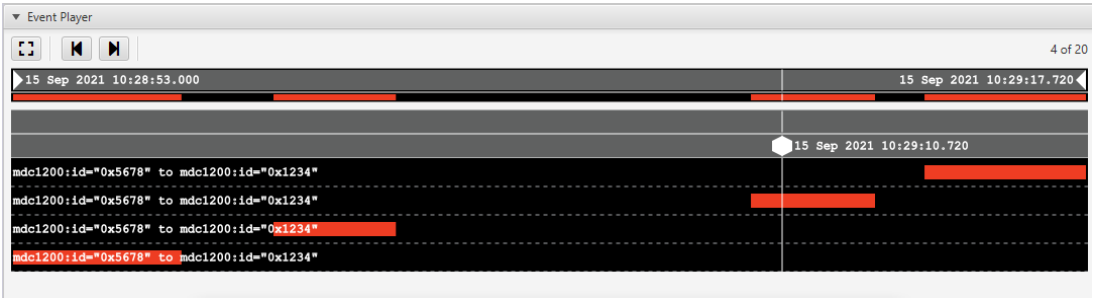
To create a play segment, click and hold, or press and hold, at (or near) the start position of the segment in the area of the play segment bar, and then while holding, slide to (or near) the end position of the segment. For example:



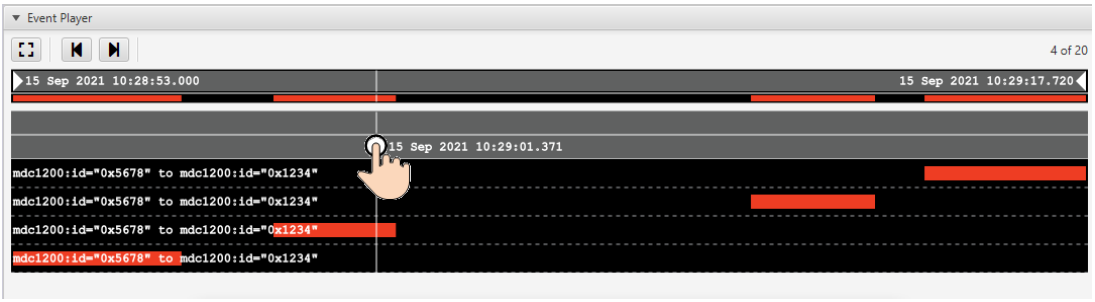
Once you are happy with the play segment, you can move the segment to any point on the timeline. To do so, click and hold, or press and hold, in the area of the play segment on the play segment bar and then slide to the new position. For example:

To remove the play segment, either double-click or double-tap on the play segment bar. Alternately, create a new play segment. The old segment will be removed automatically once you create a new one.

Finally, right under the play segment bar is the play position bar. It is the home of the play position marker. For example:



In addition to showing the current play position, you can use this bar to set the start play position. To do so, simply click in the area of the play position bar at (or near) the desired start play position. For example:



Alternatively, you can click and hold, or press and hold, the play position marker and slide it to the new play start position while holding.

To reset the play position to the event's start, double-click or double-tap on the play position bar.

8.2. Event Sharing

It is likely that in many cases, after you create an event, you will wish to share the event with others or save it so that you can get to it quickly later.

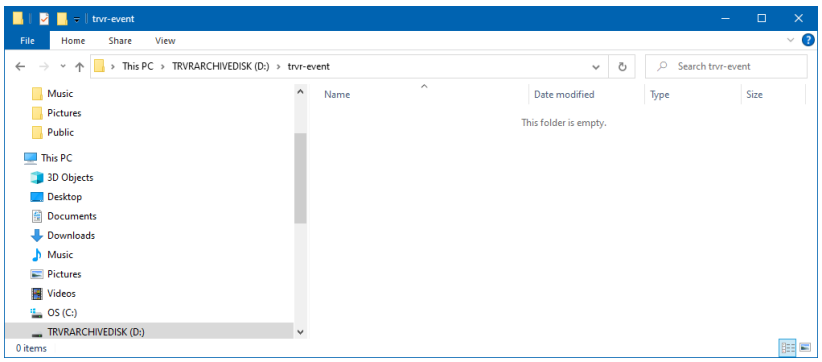
Events are a collection of recording files and metadata. Total Recall VR uses recording (or media) repositories as the structure to hold this combination of content, see section 7.1 Recording Repositories for further details.

As a result, to save and share an event, you need to create a recording repository or use an existing recording repository. In most cases, you will create a portable repository (see section 7.1.3 Portable Repository) to save an event, most likely on a USB thumb drive. However, you may use a network repository (see section 7.1.2 Network Repository) for events with a more significant number of recordings. The method of saving an event is the same for all types of recording repositories.

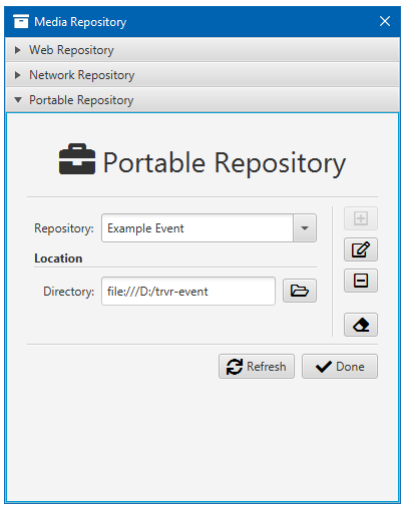
To save an event in a portable repository on a USB thumb drive:-

Save an event in a portable repository

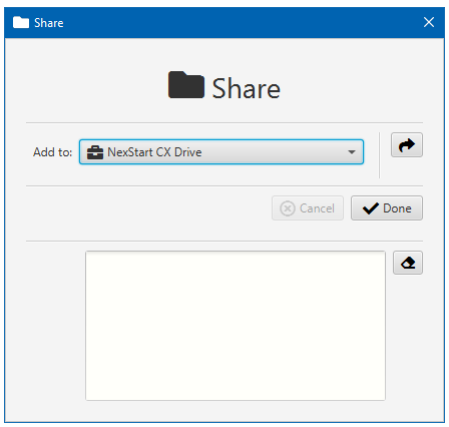
1. Attach a USB thumb drive with an empty folder portable repository. For example, we will use D:\trvr-event:



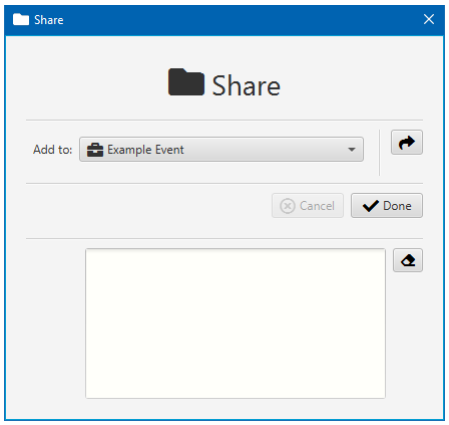
2. Add a portable repository to the Total Recall VR Cockpit configuration to access the portable repository on the USB thumb drive. We will name the repository “Example Event”:



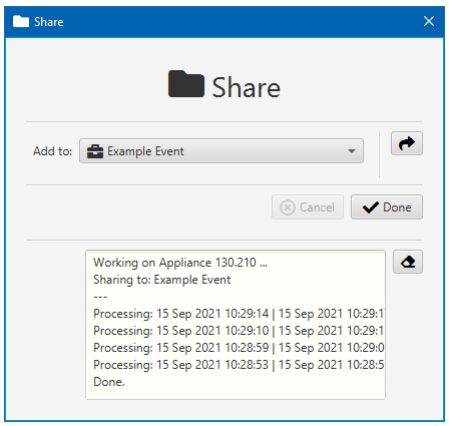
3. Set the ***Act on*** selector to *Selected*, and then select **Share** to start the recording sharing tool.



4. Choose the repository that you created during step 2 as the value for the ***Add to*** selector**:**



5. Select ↱ to save the event to the new repository:



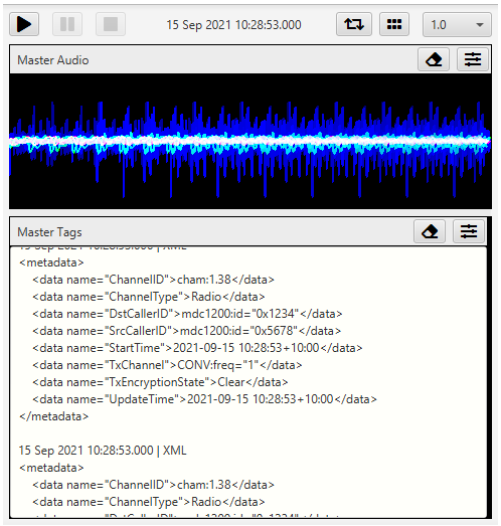
6. Select ✔ **Done** to end the tool.

At this point, you can access the repository that contains the recordings of the event just like any other recording repository and use the recording browser and event player to reconstruct the event repeatedly.

8.3. Media Player

Once you have reconstructed the event by selecting the recordings that are part of it, you can replay the event as it happened in time with the media player.

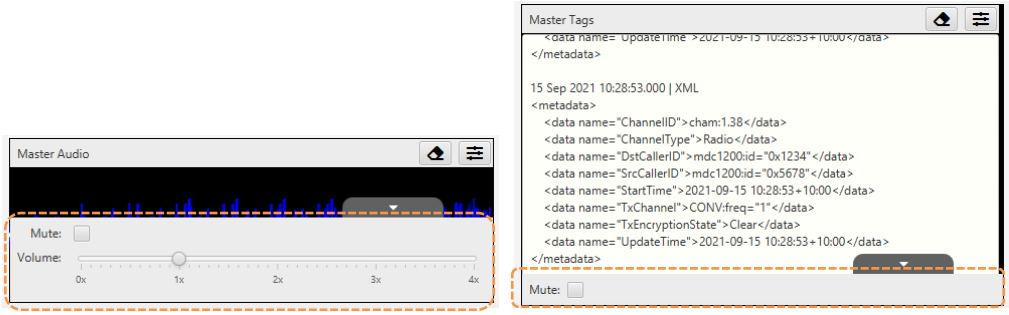
The following screen capture shows the structure of the media player:



The following player controls are available in addition to the usual player controls (play, pause and stop):

Control	***Description***
	Loop toggle. Set this toggle to play the entire event continuously or the selected segment in a loop.
	Skip gaps toggle. Set this toggle to skip the gaps, if any, between consecutive recordings when playing.
Play speed selector	Use the play speed selector to set the replay speed. A value of 1.0 specifies normal speed. Values larger than 1.0 specify faster speed, and values less than 1.0 specify slower speed.

Each visualiser that is part of the player may have additional controls specific to the visualiser. Select on the visualiser's title bar to display the control panel for that visualiser. For example:



9. Live Monitoring

The Monitor view of the Total Recall VR Cockpit provides access to the metadata of recordings in progress while the recordings are in progress. In addition, it can automatically construct a visual representation of a running timeline of the recordings in progress and play the media being recorded for the recordings appearing on the timeline. To do this, the Monitor view connects to a recording feed (a media feed).

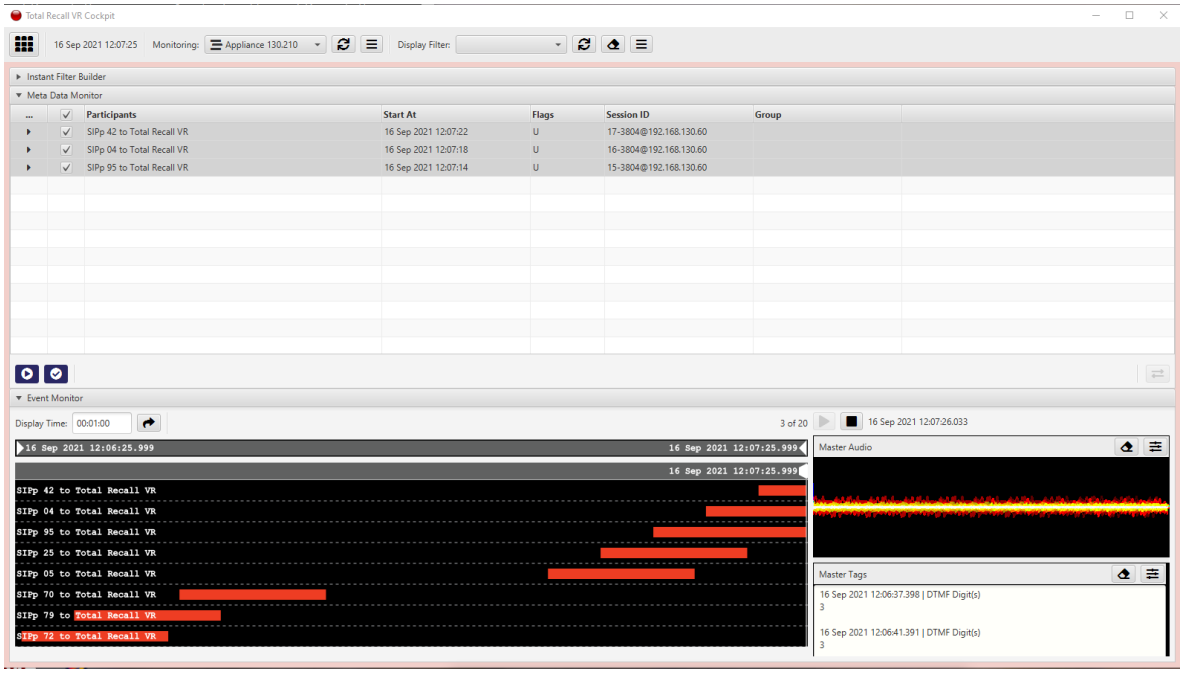


Figure 17: Monitor View

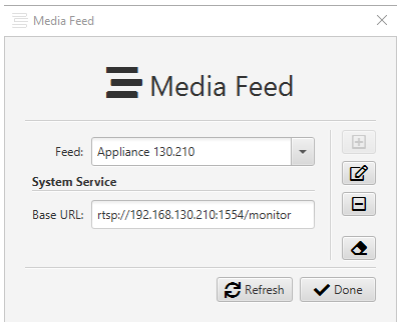
The following sections explain how to use the metadata and event monitor.

9.1. Media Feeds

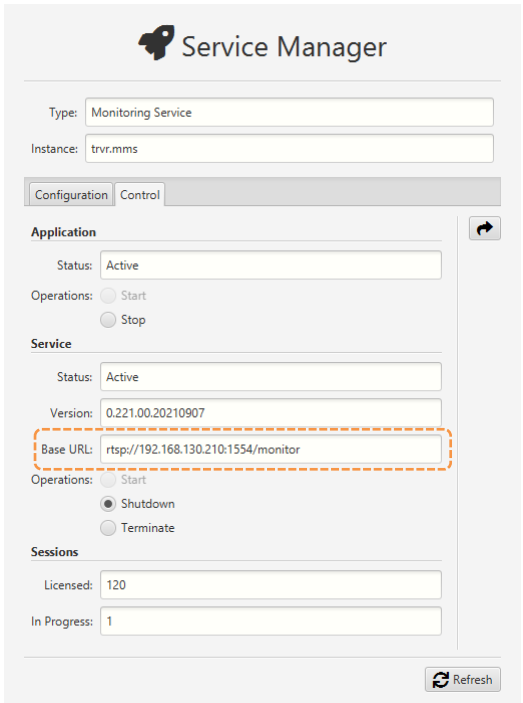
Each media feed is a streaming source of recording metadata and media for recordings in progress. Total Recall VR Cockpit connects to a feed to receive recording metadata and media for recordings in progress. It continues to receive the same until it disconnects from the feed.

You can manage the media feed records for the feeds that Total Recall VR Cockpit can access by selecting ☰, located next to the ***Monitoring*** selector on the application menu bar.

It will display the Media Feed form, which you can use to manage media feed records, as shown in the following screen capture.



To configure a Media Feed, you need the base RTSP URL of the feed. You can get the base URL from the runtime status of the "Monitoring Service" that runs on an appliance or custom recorder, for example:



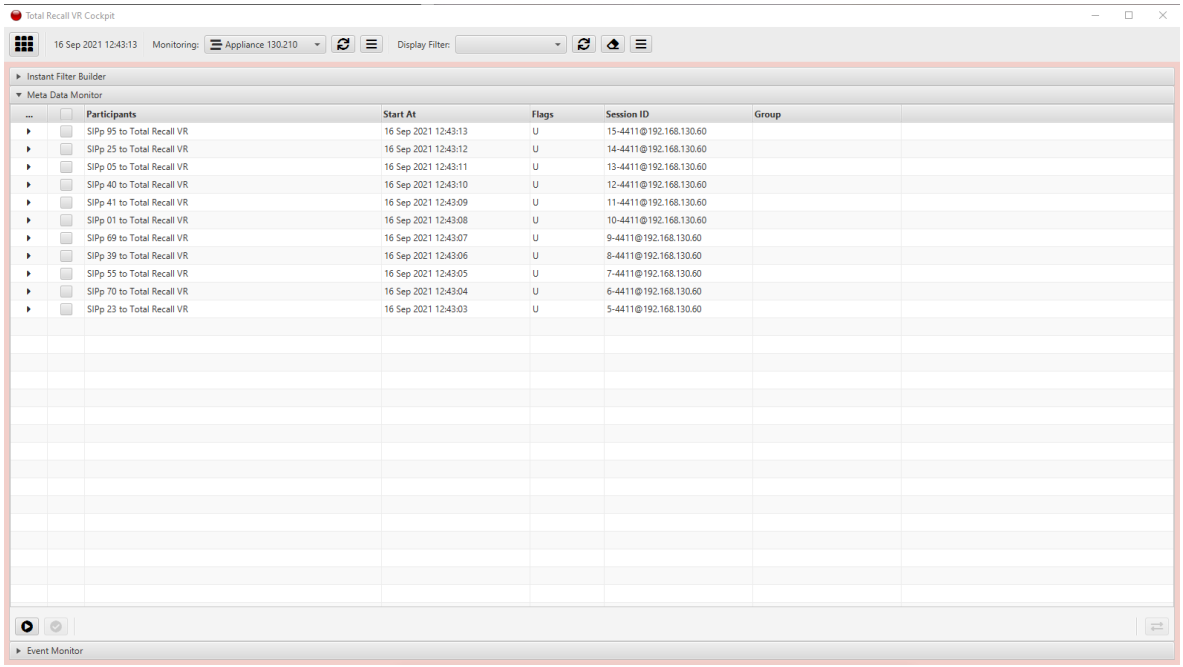
9.2. In-progress Recording Monitor

The recording monitor provides a table-like view of the metadata for the recordings that are in progress.

You can choose a media feed with the ***Monitoring*** selector on the application menu bar. In addition, and optionally, you can choose a display filter to apply to the media feed with the ***Display Filter*** selector that is also located on the application menu bar.

If you need to configure a new media feed record or update an existing one, please see section 9.1 Media Feeds. If you need to configure a new display filter or update an existing one, please see section 6.3 Advanced Filter Builder - Recordings.

Once you select a media feed, and if Total Recall VR Cockpit can access it, Total Recall VR Cockpit will display the metadata of the recordings that are in progress in a tabular form.



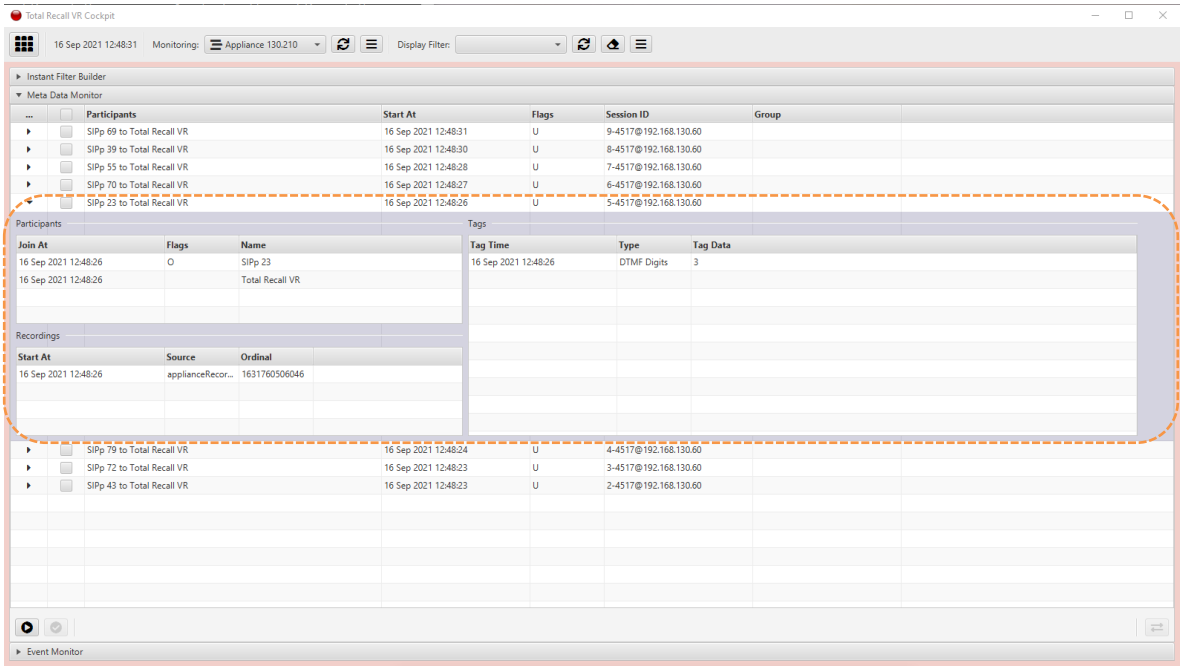
If you select a display filter as well, Total Recall VR Cockpit will use that filter as it receives metadata from the feed and shows only recordings that pass the filter.

A recording access filter may be set on your user profile. If set, Total Recall VR Cockpit will automatically use it in addition to the display filter as it receives metadata from the feed.

Use the following controls to control the feed:

Control	***Description***
⇄	Attempts to reconnect to the selected media feed when the connection is broken.

Select ▸, which appears in the first column of the row that shows the metadata for a recording, to display additional information that is part of the metadata for the recording.



Select ▾ in the same row, or wait for the recording to end to hide the additional information.

9.3. In-progress Recording Timeline

The in-progress recording timeline is a combination of recording metadata shown by the recording monitor and a visual representation of the timeline that the event monitor shows. The event monitor is an extension of the recording monitor and visually represents the timeline.

By default, the event monitor is not active to free up computing resources for other activities and applications.

You must activate the event monitor by setting the recording monitor to what is known as review mode. For more details on the recording monitor, see section 9.2 In-progress Recording Monitor.

Set the ⏵ toggle of the recording monitor to enter review mode and activate the event monitor. Unset the same toggle to exit review mode and deactivate the event monitor.

While the recording monitor is in the review mode, as you select recordings in the recording monitor, the selected recordings will automatically be forwarded to the event monitor, automatically adding the recordings to the visual representation of the event timeline in the correct time order.

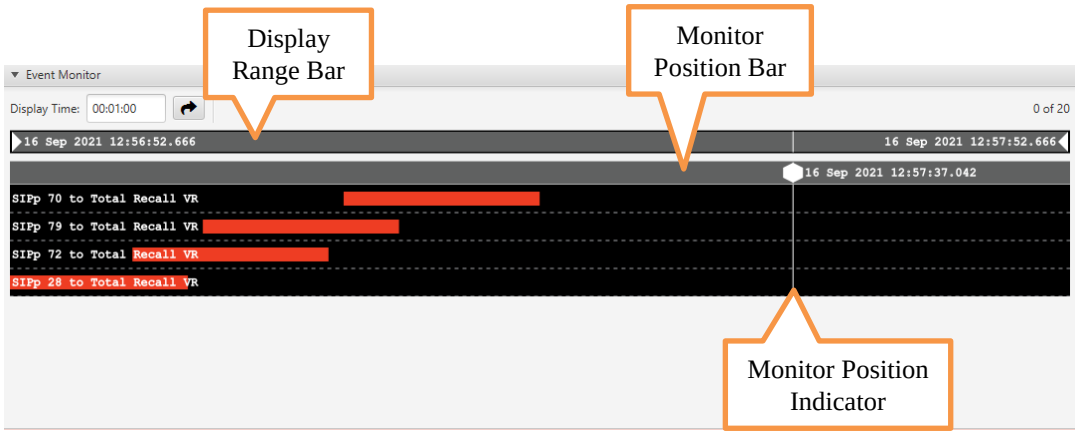
> The event monitor limits the number of recordings it can process to 20 in progress. It adds recordings to the timeline on a first come, first served basis until it reaches this limit.

At the same time, as you unselect recordings in the recording monitor, the event monitor will automatically remove the unselected recordings from the visual representation of the event timeline.

Alternately, set the ✔ toggle to automatically select recordings as they appear in the recording monitor and keep them selected until the recording ends. Unselect the same toggle to revert to manual selection.

> The event monitor's visual representation of the timeline shows the most recent recording at the top and the oldest recordings at the bottom, the same as the recording monitor.

The following screen capture shows the structure of the visual timeline.



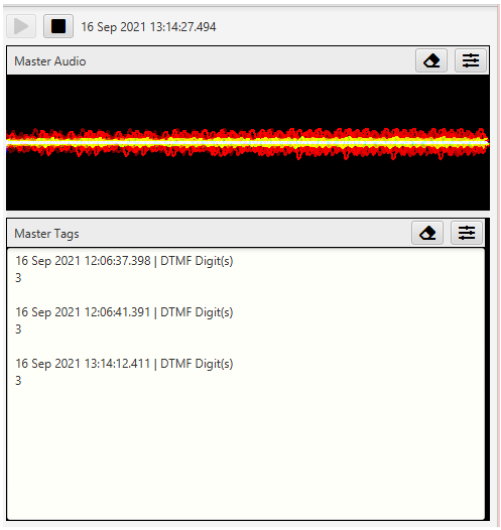
The display range bar at the top of the timeline indicates the total duration of the timeline. Set ***Display Time*** to change the display range. In effect, the display range defines the time history of the timeline.

The monitor position bar is the home of the current time position of the timeline. As monitoring happens in real-time, the monitor position will always be the present time.

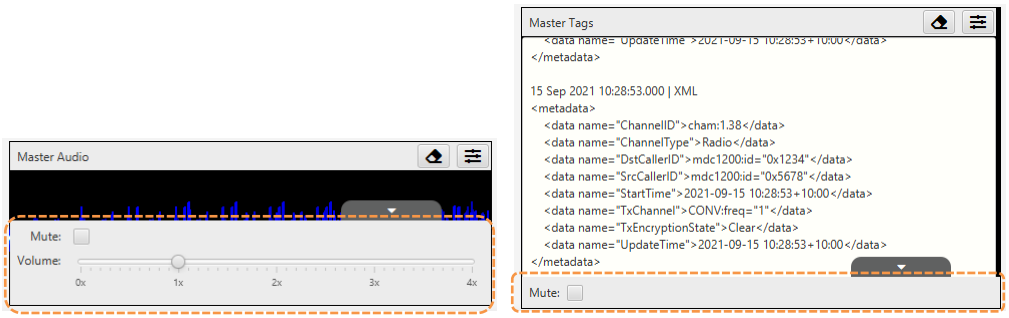
9.4. Media Monitor

Use the media monitor to listen to recordings in progress as they are added to the in-progress event timeline.

The following screen capture shows the structure of the media monitor:



Only the standard play and stop player controls are available. However, each visualiser part of the monitor may have additional controls specific to the visualiser. Select ⚌ on the visualiser's title bar to display the control panel for that visualiser. For example:



10. Recorder Service Monitoring & Configuration

The Manager view of Total Recall VR Cockpit has a built-in service status monitor and service manager for Total Recall VR recording services that run on different types of recorder nodes (physical servers, virtual machines, etc.), including appliance and custom recorder nodes.

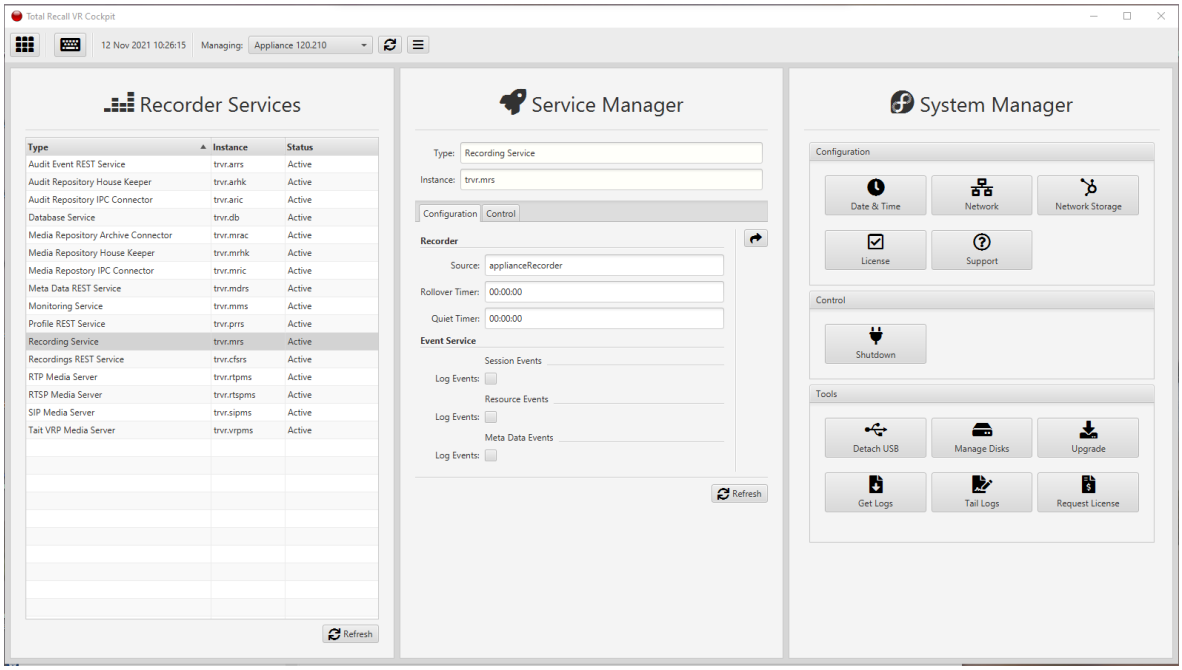


Figure 18: Manager View

The following sections explain how to use the service monitor and manager to monitor the status, control the operation and manage the configuration of Total Recall VR recorder services.

See section 11 Appliance Recorder Manager for information on how to use the system manager with appliance nodes, including appliance recorders. Total Recall VR Cockpit does not have tools for managing custom recorder nodes.

10.1. Recorder Nodes

A recorder node is any device (physical servers, virtual machines, etc.) that runs at least one of the Total Recall VR recorder services.

Some nodes run the complete suite of Total Recall VR recorder services, for example, the different Total Recall VR appliance recorders. Other nodes may run only a subset of Total Recall VR services, for example, a distributed custom Total Recall VR recorder with multiple servers (nodes) or the Total Recall VR archive appliance.

From a monitoring and management perspective, Total Recall VR Cockpit classifies nodes as follows:

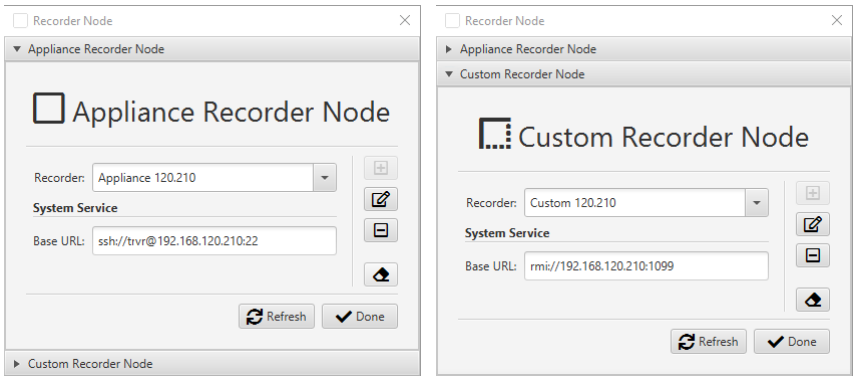
- Appliance recorder nodes – Total Recall VR Cockpit can manage and monitor the Total Recall VR recording services that run on the node and the node itself at the operating system level, for example, setting the time, configuring the network interfaces, etc. In most cases, if not all, Total Recall VR Cockpit is the only method for monitoring and managing appliance nodes.
- Custom recorder nodes – Total Recall VR Cockpit can manage and monitor the Total Recall VR recording services that run on custom nodes. However, it cannot monitor and manage any other services that may run on the node, nor can it manage the node at the operating system level; for example, it cannot set the time, configure the network interfaces, etc. In all cases, other tools must be used to monitor and manage custom nodes fully.

Total Recall VR Cockpit uses the SSH and RMI protocols to monitor and manage appliance nodes and only the RMI protocol to monitor and manage custom nodes.

Total Recall VR Cockpit does not use the SSH protocol to monitor and manage custom recorder nodes. As a result, the system management tools are not available when accessing custom recorder nodes.

You can manage the records for recorder nodes that Total Recall VR Cockpit can access by selecting ☰, located next to the ***Managing*** selector on the application menu bar.

It will display the Recorder Node form, which you can then use to configure records for different types of nodes, as shown in the following screen captures.



10.1.1. Appliance Recorder Node

To configure an appliance recorder node, you will need the SSH access URL for the node. To construct the URL, simply use one of the IP addresses assigned to one of the network interfaces of the appliance (usually the first network interface).

The URL has the following form:

```
ssh://trvr@<ip address>:22
```

Total Recall VR Cockpit dynamically constructs the RMI URL for appliance nodes from the SSH URL, so there is no need to specify it in the configuration of appliance recorder nodes.

10.1.2. Custom Recorder Node

To configure a custom recorder, you will need the RMI URL of the RMI registry service used by the Total Recall VR recorder services on the custom node.

The RMI registry service can run on the same node as the Total Recall VR recorder services or on a different one. Either way, to create the URL, you will need the IP address and port the RMI registry uses to provide the service. Assuming that you are using the default RMI registry port (1099), the format of the URL is:

```
rmi://<ip address>:1099
```

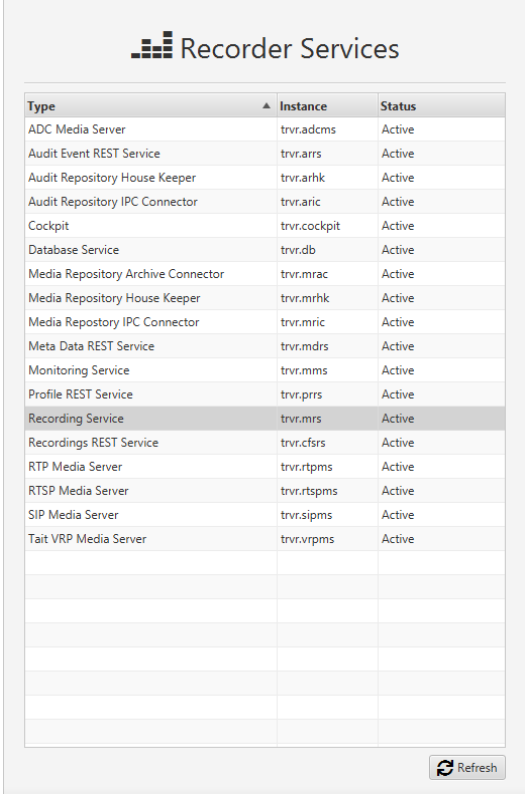
10.2. Service Status

The Recorder Services and Service Manager forms provide summary and detailed information on the Total Recall VR recorder services running on a recorder node.

Choose a recorder node with the ***Managing*** selector on the application menu bar.

If you need to configure a new record for a recorder node or update an existing one, please see section 10.1 Recorder Nodes.

Once you select a node, and if Total Recall VR Cockpit can access it, it will display a list of the Total Recall VR recorder services that run on it and a summary of their status in a tabular form. For example:



The status can be one of:

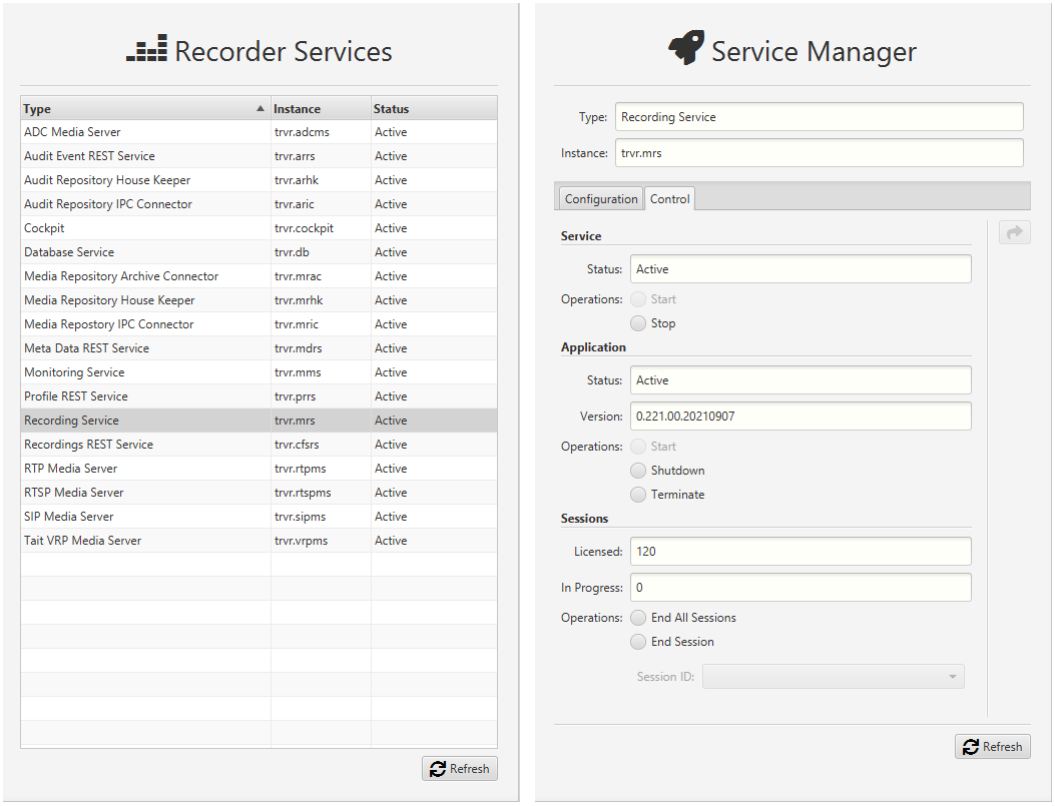
- *Active* - The service process is running. Monitoring, control and configuration are available. However, it may not be doing its job – check the detailed service status.
- *Inactive* - The service process is not running. Monitoring, control and configuration access are unavailable. The operating system is configured to restart the service process when it is not running, so you may need to wait for the operating system to restart it.

If a recorder service should be running on a node that does not appear on the list, then there is a problem with it that the operating system cannot resolve.

If this happens on an appliance node, you should contact support for further advice and support.

If this happens on a custom node, you must fix the problem before re-running the service.

To get the detailed status for a service, first select the service in the table that is part of the Recorder Services form, and then select the **Control** tab on the Service Manager form for the service, for example:



A fully operational recording service will show the *Active* status in the Service and Application sections of the form.

However, if the service shows *Active – broken* status in the Application section of the form, likely, the service does not have a valid license. If it does, then it is likely that the configuration of the service is not correct, and you need to correct it and restart the service to restore regular operation.

10.3. Service Control – All Services

In addition to viewing details on the status of recorder services, you can control the operation of the services from the **Control** tab on the Service Manager form. The following controls are available for all recording services:

Control	*Description*
Service	
Start	Starts the service that will start the application that the service should run.
Stop	Stops the service. Implies **Terminate** at the Application level (see next).
Application	
Start	Starts processing sessions, user requests, etc.
Shutdown	Initiates orderly shutdown. The application will reject all new sessions, user requests, etc., and wait to complete the existing sessions, user requests, etc., before stopping all processing.
Terminate	Initiates immediate shutdown. The application will immediately terminate all active sessions, user requests, etc., if any, and stop all processing.

Individual services may provide additional controls specific to the application the service is running. See the subsequent sections for more information.

10.4. Service Control – Cockpit

Total Recall VR Cockpit is a GUI application. Unlike all other Total Recall VR recorder services, it only provides a Restart control, which will restart the application without terminating the process that runs it.

10.5. Service Control – Media Repository Archive Connector

In addition to the standard service controls, see section 10.3 Service Control – All Services, the “Media Repository Archive Connector” provides the following additional controls:

Control	*Description*
Target Repository	
Database	
Rebuild	Initiates the process of rebuilding the database with recording metadata of the target recording (media) repository.

	It will remove all metadata in the database and then reconstruct it using the information in the recording files in the repository. The service will not archive, that is, copy new recordings from the source repository to the target repository while rebuilding the database. However, it will start to archive automatically as soon as it completes rebuilding.
Cancel Rebuild	Stops a database rebuild that is in progress. Note that if you cancel the rebuild process mid-way, the database content will be inconsistent with the recording files in the repository. As a result, browsing and searching the repository will yield inconsistent results.

10.6. Service Control – Media Repository House Keeper

In addition to the standard service controls, see section 10.3 Service Control – All Services, the "Media Repository House Keeper" provides the following additional controls:

Control	***Description***
Database	
Rebuild	Initiates rebuilding the database with recording metadata of the recording (media) repository. It will remove all metadata in the database and then reconstruct it using the information in the recording files in the repository. The repository will continue to accept new recordings while rebuilding is in progress. As a result, if the repository is used by an active "Recording Service", recording need not be interrupted.
Cancel Rebuild	Stops a database rebuild that is in progress. Note that if you cancel the rebuild process mid-way, the database content will be inconsistent with the recording files in the repository. As a result, browsing and searching the repository will yield inconsistent results.

10.7. Service Control – Recording Service

In addition to the standard service controls, see section 10.3 Service Control – All Services, the "Recording Service" provides the following additional controls:

Control	*Description*
Sessions	
End All Sessions	Immediately ends all recording sessions, if any are in progress. This may be useful after invoking the *Shutdown* control at the Application level if you do not wish to wait for sessions to end.
End Session	Immediately ends the specified recording session.

10.8. Service Configuration – Audit Event REST Service

This service provides a REST interface to a repository of audit events (audit log).

The configuration parameters that are available when the service is running on an appliance recorder node, see section 10.1 Recorder Nodes, are:

Parameter	*Default Value*	*Comment*
REST Service		
IP Address	192.168.1.100	The service binds the REST interface to this IP address.
Port	4040	The service binds the REST interface to this (TCP) port.
Log Messages	Not ticked	The service writes all HTTP messages to the service log file if ticked. Untick it in production as it considerably slows the operation of the service.
Event Service		
Audit Events		
Log Events	Not ticked	The service writes all audit events to the service log file if ticked. Untick it in production as it considerably slows the operation of the service.

The additional configuration parameters that are available when the service is running on a custom recorder node, see section 10.1 Recorder Nodes, are:

Parameter	*Default Value*	*Comment*
Digital Certificates		
Keystore	./trvr.arrs.p12	If set, the service uses the certificates in this file to encrypt the communication with clients (that is, use HTTPS instead of HTTP).
Keystore Password	********** (withheld)	If set, the service uses this password to access the information in the keystore file.
Truststore		If set, the service uses the certificates in this file to authenticate clients.
Truststore Password		If set, the service uses this password to access the information in the truststore file.
Database		
Database URL	jdbc:mariadb://127.0.0.1:9306/applianceAudit	The service uses this repository database.
User Name	trvr_ardb	If set, the service uses this user to access the repository database.
Password	********** (withheld)	If set, the service uses this password to access the repository database.
Event Service		
Base URL	kafka://127.0.0.1:2191	The service connects to this message bus.
Audit Events		
Topic Name	applianceAuditTopic	The service sends audit events to this topic on the message bus.
Client	arrsAuditTopicClient	The identifier of the service on the message bus.

10.9. Service Configuration – Audit Repository House Keeper

This service is the house keeper for a repository of audit events (also known as audit log). It keeps the content of the repository at levels specified by its configuration.

The configuration parameters that are available when the service is running on an appliance recorder node, see section 10.1 Recorder Nodes, are:

Parameter	***Default Value***	***Comment***
House Keeper		
Event Lifetime	730 days	The maximum lifetime of audit events in the repository. The service automatically deletes audit events that are older than the set lifetime. Set it to *0 days* to keep events in the repository as long as possible. The maximum value is *3650 days* (10 years).
Database		
Occupancy Limit		
High Watermark	100%	The occupancy level that will trigger the start of deletion of audit events, the oldest first, to make space for new events. It must be between *10%* and *100%* and more than the low watermark.
Low Watermark	85%	The occupancy level at which the deletion of audit events stops. It must be between *10%* and *100%* and less than the high watermark.
Event Service		
Audit Events		
Log Events	Not ticked	The service writes all audit events to the service log file if ticked. Untick it in production as it considerably slows the operation of the service.

The additional configuration parameters that are available when the service is running on a custom recorder node, see section 10.1 Recorder Nodes, are:

Parameter	*Default Value*	*Comment*
Database		
Database URL	jdbc:mariadb://127.0.0.1:9306/applianceAudit	The service uses this repository database.
User Name	trvr_ardb	If set, the service uses this user to access the repository database.
Password	********** (withheld)	If set, the service uses this password to access the repository database.
Event Service		
Base URL	kafka://127.0.0.1:2191	The service connects to this message bus.
Audit Events		
Topic Name	applianceAuditTopic	The service sends audit events to this topic on the message bus.
Client	arhkAuditTopicClient	The identifier of the service on the message bus.

10.10. Service Configuration – Audit Repository IPC Connector

This service connects an audit event repository (or audit log) to an inter-process communication (IPC) message bus that transports messages between recorder services. The service receives audit events from other recorder services on the bus and adds the events to the repository.

The configuration parameters that are available when the service is running on an appliance recorder node, see section 10.1 Recorder Nodes, are:

Parameter	*Default Value*	*Comment*
Event Service		
Audit Events		
Log Events	Not ticked	The service writes all audit events to the service log file if ticked. Untick it in production as it considerably slows the operation of the service.

The additional configuration parameters that are available when the service is running on a custom recorder node, see section 10.1 Recorder Nodes, are:

Parameter	***Default Value***	***Comment***
Database		
Database URL	jdbc:mariadb://127.0.0.1:9306/applianceAudit	The service uses this repository database.
User Name	trvr_ardb	If set, the service uses this user to access the repository database.
Password	********** (withheld)	If set, the service uses this password to access the repository database.
Event Service		
Base URL	kafka://127.0.0.1:2191	The service connects to this message bus.
Audit Events		
Topic Name	applianceAuditTopic	The service accepts audit events posted to this topic on the message bus.
Client	aricAuditTopicClient	The identifier of the service on the message bus.
Group	aricAuditTopicGroup	The service is a member of this group of message consumers.

10.11. Service Configuration – Cockpit

Comprehensive information regarding the Total Recall VR Cockpit configuration is available in section 3.10 Application Preferences.

Not all configuration parameters are accessible when the application runs on an appliance recorder node, see section 10.1 Recorder Nodes.

10.12. Service Configuration – Database Service

This service is a wrapper around a 3rd party database engine and provides a database management service.

The configuration parameters that are available when the service is running on an appliance recorder node, see section 10.1 Recorder Nodes, are:

Parameter	***Default Value***	***Comment***
Event Service		
Audit Events		
Log Events	Not ticked	The service writes all audit events to the service log file if ticked. Untick it in production as it considerably slows the operation of the service.

The additional configuration parameters that are available when the service is running on a custom recorder node, see section 10.1 Recorder Nodes, are:

Parameter	***Default Value***	***Comment***
Database Service		
Type	MariaDB	The service controls this database engine.
IP Address	127.0.0.1	The service binds the DB interface to this IP address.
Port	9306	The service binds the DB interface to this (TCP) port.
Webmin Port	9192	The service binds the engine web management interface to this (TCP) port. Used only with the H2 engine at this stage.
Base Path	/local/mariadb	The DB engine stores the database files in this directory.
Event Service		
Base URL	kafka://127.0.0.1:2191	The service connects to this message bus.

Audit Events		
Topic Name	applianceAuditTopic	The service sends audit events to this topic on the message bus.
Client	dbAuditTopicClient	The identifier of the service on the message bus.

10.13. Service Configuration – Media Repository Archive Connector

This service is the archiving service for a recording (media) repository. It automatically and in near real-time copies recordings from its repository (the source repository) to another recording (media) repository (the target repository).

For more information on different types of recording (media) repositories, see section 7.1 Recording Repositories.

The configuration parameters that are available when the service is running on an appliance recorder node, see section 10.1 Recorder Nodes, are:

Parameter	***Default Value***	***Comment***
Connector		
Archived To	01 Jan 2022 11:00:00 (example only, may not be set)	The date and time that the connector is up to. Recording sessions before this time have been archived, while recording sessions after this time have yet to be archived. You can set it to a date and time in the past or future.
Batch Size	300 sessions	The service archives up to this number of recording sessions before taking a break. It must be between *10 sessions* and *1,000 sessions*.
Batch Delay	00:01:00	The service is idle for this duration of time between batches.

		Must be between *00:00:01* (1 second) and *00:01:00* (1 minute).
Target Repository		
Type	Portable Repository	
Location		
Directory	file:///mnt/trvr/local/TRVRARCHIVE	The local file system location of the Portable Repository.
Occupancy Limit		
Database	100%	The maximum database space to use in the target repository.
File Store	95%	The maximum disk space to use in the target repository.
Event Service		
Audit Events		
Log Events	Not ticked	The service writes all audit events to the service log file if ticked. Untick it in production as it considerably slows the operation of the service.

The service treats the target repository as a Portable Repository by default, as shown in the previous table. As a result, the service will archive the recording session to an archive disk attached to the appliance. However, you can switch to a Total Recall VR archive appliance by changing the type of the target repository to a Web Repository. The configuration parameters that are available when you switch to a Web Repository are:

Parameter	***Default Value***	***Comment***
Target Repository		
Type	Web Repository	
Meta Data Service		
Base URL		The REST API URL of the “Meta Data REST Service”.
Recordings Service		
Base URL		The REST API URL of the “Recordings REST Service”.

Alternatively, you can switch to archiving to a Network Repository. The configuration parameters that are available when you change to a Network Repository are:

Parameter	***Default Value***	***Comment***
Target Repository		
Type	Network Repository	
Database		
Database URL		The JDBC URL of the repository database. The service stores recording metadata in this database.
User Name		If set, the service uses this user to access the repository database.
Password		If set, the service uses this password to access the repository database.
File Store		
Directory		The service will use this directory to store recording files.

The additional configuration parameters that are available when the service is running on a custom recorder node, see section 10.1 Recorder Nodes, are:

Parameter	***Default Value***	***Comment***
Digital Certificates		
Keystore	./trvr.mrac.p12	If set, the service uses the certificates in this file to encrypt the communication with servers (that is, use HTTPS instead of HTTP).
Keystore Password	********** (withheld)	If set, the service uses this password to access the information in the keystore file.

Truststore	./trvr.mrac.p12	If set, the service uses the certificates in this file to authenticate with server.
Truststore Password	********** (withheld)	If set, the service uses this password to access the information in the truststore file.
Source Repository		
Type	Network Repository	
Database		
Database URL	jdbc:mariadb://127.0.0.1:9306/applianceMetaData	The JDBC URL of the repository database. The service reads recording metadata from this database.
User Name	trvr_mrdb	If set, the service uses this user to access the repository database.
Password	********** (withheld)	If set, the service uses this password to access the repository database.
File Store		
Directory	/local/recorder/cache	The service accesses recording files from this directory.
Event Service		
Base URL	kafka://127.0.0.1:2191	The service connects to this message bus.
Audit Events		
Topic Name	applianceAuditTopic	The service sends audit events to this topic on the message bus.
Client	mracAuditTopicClient	The identifier of the service on the message bus.

By default, the service treats the source repository as a Network Repository, as shown in the previous table. However, you can switch to using the REST interface of the source repository, if available, by changing the type of the source repository to a Web Repository. The configuration parameters that are available when you switch to a Web Repository are:

Parameter	***Default Value***	***Comment***
Target Repository		
Type	Web Repository	
Meta Data Service		
Base URL		The REST API URL of the "Meta Data REST Service".
Recordings Service		
Base URL		The REST API URL of the "Recordings REST Service".

10.14. Service Configuration – Media Repository House Keeper

This service is the house keeper for a recording (media) repository. It keeps the content of the repository at levels specified by its configuration.

The configuration parameters that are available when the service is running on an appliance recorder node, see section 10.1 Recorder Nodes, are:

Parameter	***Default Value***	***Comment***
House Keeper		
Session Lifetime	0 days	The maximum lifetime of recording sessions in the repository. The service automatically deletes recording sessions that are older than the set lifetime. Set it to *0 days* to keep recording sessions in the repository as long as possible. The maximum value is *3650 days* (10 years).
Database		
Occupancy Limit		
High Watermark	100%	The occupancy level that will trigger the start of deletion of recording sessions, the oldest first, to make space for new sessions.

		It must be between *10%* and *100%* and more than the low watermark.
Low Watermark	85%	The occupancy level at which the deletion of recording sessions stops. It must be between *10%* and *100%* and less than the high watermark.
File Store		
Occupancy Limit		
High Watermark	95%	The occupancy level that will trigger the start of deletion of recording sessions, the oldest first, to make space for new sessions. It must be between *10%* and *95%* and more than the low watermark.
Low Watermark	80%	The occupancy level at which the deletion of recording sessions stops. It must be between *10%* and *95%* and less than the high watermark.
Event Service		
Audit Events		
Log Events	Not ticked	The service writes all audit events to the service log file if ticked. Untick it in production as it considerably slows the operation of the service.

The additional configuration parameters that are available when the service is running on a custom recorder node, see section 10.1 Recorder Nodes, are:

Parameter	*Default Value*	*Comment*
Database		
Database URL	jdbc:mariadb://127.0.0.1:9306/applianceMetaData	The JDBC URL of the repository database. The service reads recording metadata from this database.
User Name	trvr_mrdb	If set, the service uses this user to access the repository database.
Password	********** (withheld)	If set, the service uses this password to access the repository database.
File Store		
Directories	/local/recorder/cache	The service uses this repository file store.
Event Service		
Base URL	kafka://127.0.0.1:2191	The service connects to this message bus.
Audit Events		
Topic Name	applianceAuditTopic	The service sends audit events to this topic on the message bus.
Client	mrhkAuditTopicClient	The identifier of the service on the message bus.

10.15. Service Configuration – Media Repository IPC Connector

This service connects a recording (media) repository to an inter-process communication (IPC) message bus that transports messages between recorder services. The service receives messages from other recorder services on the bus and adds the recording sessions described by the messages to the repository.

The configuration parameters that are available when the service is running on an appliance recorder node, see section 10.1 Recorder Nodes, are:

Parameter	***Default Value***	***Comment***
Event Service		
Meta Data Events		
Log Events	Not ticked	The service writes all metadata events to the service log file if ticked. Untick it in production as it considerably slows the operation of the service.
Audit Events		
Log Events	Not ticked	The service writes all audit events to the service log file if ticked. Untick it in production as it considerably slows the operation of the service.

The additional configuration parameters that are available when the service is running on a custom recorder node, see section 10.1 Recorder Nodes, are:

Parameter	***Default Value***	***Comment***
Database		
Database URL	jdbc:mariadb://127.0.0.1:9306/applianceMetaData	The JDBC URL of the repository database. The service reads recording metadata from this database.
User Name	trvr_mrdb	If set, the service uses this user to access the repository database.
Password	********** (withheld)	If set, the service uses this password to access the repository database.
File Store		
Directories	/local/recorder/cache	The service uses this repository file store.
Event Service		
Base URL	kafka://127.0.0.1:2191	The service connects to this message bus.

Meta Data Events		
Topic Name	applianceMetadataTopic	The service accepts metadata events posted to this topic on the message bus.
Client	mricMetadataTopicClient	The identifier of the service on the message bus.
Group	mricMetadataTopicGroup	The service is a member of this group of message consumers.
Audit Events		
Topic Name	applianceAuditTopic	The service sends audit events to this topic on the message bus.
Client	mricAuditTopicClient	The identifier of the service on the message bus.

10.16. Service Configuration – Meta Data REST Service

This service provides a REST interface to the recording metadata for a recording (media) repository.

The configuration parameters that are available when the service is running on an appliance recorder node, see section 10.1 Recorder Nodes, are:

Parameter	***Default Value***	***Comment***
REST Service		
IP Address	192.168.1.100	The service binds the REST interface to this IP address.
Port	4020	The service binds the REST interface to this (TCP) port.
Log Messages	Not ticked	The service writes all HTTP messages to the service log file if ticked. Untick it in production as it considerably slows the operation of the service.
Event Service		
Audit Events		
Log Events	Not ticked	The service writes all audit events to the service log file if ticked.

		Untick it in production as it considerably slows the operation of the service.

The additional configuration parameters that are available when the service is running on a custom recorder node (see section 10.1 Recorder Nodes) are:

Parameter	***Default Value***	***Comment***
Digital Certificates		
Keystore	./trvr.mdrs.p12	If set, the service uses the certificates in this file to encrypt the communication with clients (that is, use HTTPS instead of HTTP).
Keystore Password	********** (withheld)	If set, the service uses this password to access the information in the keystore file.
Truststore		If set, the service uses the certificates in this file to authenticate client.
Truststore Password		If set, the service uses this password to access the information in the truststore file.
Database		
Database URL	jdbc:mariadb://127.0.0.1:9306/applianceMetaData	The JDBC URL of the repository database. The service reads recording metadata from this database.
User Name	trvr_mrdb	If set, the service uses this user to access the repository database.
Password	********** (withheld)	If set, the service uses this password to access the repository database.
Event Service		
Base URL	kafka://127.0.0.1:2191	The service connects to this message bus.
Audit Events		

Topic Name	applianceAuditTopic	The service sends audit events to this topic on the message bus.
Client	mdrsAuditTopicClient	The identifier of the service on the message bus.

10.17. Service Configuration – Monitor Service

This service provides an RTSP streaming interface for recording metadata and media for recordings in progress.

The service connects directly to an inter-process communication (IPC) message bus that transports messages between recorder services in real time and converts the messages to RTSP streams of recording metadata and media.

The configuration parameters that are available when the service is running on an appliance recorder node, see section 10.1 Recorder Nodes, are:

Parameter	***Default Value***	***Comment***
RTSP Service		
IP Address	192.168.1.100	The service binds the RTSP interface to this IP address.
Port	1554	The service binds the RTSP interface to this (TCP) port.
Public IP Address		If set, the service uses this IP address as the RTSP service IP address in RTSP messages.
Public Port		If set, the service uses this (TCP) port as the RTSP service port in RTSP messages.
Log Messages	Not ticked	The service writes all RTSP messages to the service log file if ticked. Untick it in production as it considerably slows the operation of the service.
RTP Service		
IP Address	192.168.1.100	The service binds the RTP interface to this IP address.
Base Port	7200	Starting with this, the service binds the RTP interface to (UDP) ports.

		The number of licensed sessions defines the range of UDP ports that the service uses.
Public IP Address		If set, the service uses this IP address as the RTP service IP address in RTSP messages.
Public Base Port		If set, the service uses this (UDP) port as the base RTP service port in RTSP messages. The number of licensed sessions defines the range of UDP ports that the service uses.
Event Service		
Session Events		
Log Events	Not ticked	The service writes all recording session events to the service log file if ticked. Untick it in production as it considerably slows the operation of the service.
Meta Data Events		
Log Events	Not ticked	The service writes all metadata events to the service log file if ticked. Untick it in production as it considerably slows the operation of the service.
Audit Events		
Log Events	Not ticked	The service writes all audit events to the service log file if ticked. Untick it in production as it considerably slows the operation of the service.

The additional configuration parameters that are available when the service is running on a custom recorder node, see section 10.1 Recorder Nodes, are:

Parameter	*Default Value*	*Comment*
Event Service		
Base URL	kafka://127.0.0.1:2191	The service connects to this message bus.
Session Events		
Topic Name	applianceSessionTopic	The service accepts recording session events posted to this topic on the message bus.
Client	mmsSessionTopicClient	The identifier of the service on the message bus.
Group	mmsSessionTopicGroup	The service is a member of this group of message consumers.
Meta Data Events		
Topic Name	applianceMetadataTopic	The service accepts metadata events posted to this topic on the message bus.
Client	mmsMetadataTopicClient	The identifier of the service on the message bus.
Group	mmsMetadataTopicGroup	The service is a member of this group of message consumers.
Audit Events		
Topic Name	applianceAuditTopic	The service sends audit events to this topic on the message bus.
Client	mmsAuditTopicClient	The identifier of the service on the message bus.

10.18. Service Configuration – Profile REST Service

This service provides a REST interface to a profile repository.

The configuration parameters that are available when the service is running on an appliance recorder node, see section 10.1 Recorder Nodes, are:

Parameter	*Default Value*	*Comment*
REST Service		
IP Address	192.168.1.100	The service binds the REST interface to this IP address.

Port	4030	The service binds the REST interface to this (TCP) port.
Log Messages	Not ticked	The service writes all HTTP messages to the service log file if ticked. Untick it in production as it considerably slows the operation of the service.
Resource Events		
Log Events	Not ticked	The service writes all resource events to the service log file if ticked. Untick it in production as it considerably slows the operation of the service.
Audit Events		
Log Events	Not ticked	The service writes all audit events to the service log file if ticked. Untick it in production as it considerably slows the operation of the service.

The additional configuration parameters that are available when the service is running on a custom recorder node, see section 10.1 Recorder Nodes, are:

Parameter	***Default Value***	***Comment***
Digital Certificates		
Keystore	./trvr.prrs.p12	If set, the service uses the certificates in this file to encrypt the communication with clients (that is, use HTTPS instead of HTTP).
Keystore Password	********** (withheld)	If set, the service uses this password to access the information in the keystore file.
Truststore		If set, the service uses the certificates in this file to authenticate clients.

Truststore Password		If set, the service uses this password to access the information in the truststore file.
Database		
Database URL	jdbc:mariadb://127.0.0.1:9306/applianceProfile	The service uses this repository database.
User Name	trvr_prdb	If set, the service uses this user to access the repository database.
Password	********** (withheld)	If set, the service uses this password to access the repository database.
Event Service		
Base URL	kafka://127.0.0.1:2191	The service connects to this message bus.
Resource Events		
Topic Name	applianceResourceTopic	The service sends resource events to this topic on the message bus.
Client	prrsResourceTopicClient	The identifier of the service on the message bus.
Audit Events		
Topic Name	applianceAuditTopic	The service sends audit events to this topic on the message bus.
Client	mmsAuditTopicClient	The identifier of the service on the message bus.

10.19. Service Configuration – Recording Service

This service writes recording metadata and media to a recording repository.

The configuration parameters that are available when the service is running on an appliance recorder node, see section 10.1 Recorder Nodes, are:

Parameter	***Default Value***	***Comment***
Recorder		
Source	applianceRecorder	The service adds this tag to the metadata of all recordings it creates.
Rollover Timer	00:00:00	The service will segment a session recording into multiple recording files, each with this duration or less if the recording session is longer than this. Set it to *00:00:00* to prevent segmenting recordings into multiple files.
Quiet Timer	00:00:00	The service automatically ends recording a session if it does not receive any messages for the session for this duration. Set it to *00:00:00* to keep recording until a message ends recording.
Event Service		
Session Events		
Log Events	Not ticked.	The service writes all session events to the service log file if ticked. Untick it in production as it considerably slows the operation of the service.
Resource Events		
Log Events	Not ticked.	The service writes all resource events to the service log file if ticked. Untick it in production as it considerably slows the operation of the service.
Meta Data Events		
Log Events	Not ticked.	The service writes all metadata events to the service log file if ticked.

		Untick it in production as it considerably slows the operation of the service.
Audit Events		
Log Events	Not ticked	The service writes all audit events to the service log file if ticked. Untick it in production as it considerably slows the operation of the service.

The additional configuration parameters that are available when the service is running on a custom recorder node, see section 10.1 Recorder Nodes, are:

Parameter	***Default Value***	***Comment***
File Store		
Intermediary	/local/recorder/tmp	The service uses this file store for recording sessions in progress (while actively recording).
Final	/local/recorder/cache	The service uses this file store for completed recording session.
Digital Certificates		
Keystore	./trvr.mrs.p12	If set, the service uses the certificates in this file to encrypt the communication with servers (that is, use HTTPS instead of HTTP).
Keystore Password	********** (withheld)	If set, the service uses this password to access the information in the keystore file.
Truststore	./trvr.mrs.p12	If set, the service uses the certificates in this file to authenticate with server.
Truststore Password	********** (withheld)	If set, the service uses this password to access the information in the truststore file.
Profile		

Base URL	https://192.168.1.100:4030/profile	The service uses this profile server.
Resource group	applianceProfile	The service uses this profile on the profile server.
Event Service		
Base URL	kafka://127.0.0.1:2191	The service connects to this message bus.
Session Events		
Topic Name	applianceSessionTopic	The service accepts session events posted to this topic on the message bus.
Client	mrsSessionTopicClient	The identifier of the service on the message bus.
Group	mrsSessionTopicGroup	The service is a member of this group of message consumers.
Resource Events		
Topic Name	applianceResourceTopic	The service accepts resource events posted to this topic on the message bus.
Client	mrsResourceTopicClient	The identifier of the service on the message bus.
Group	mrsResourceTopicGroup	The service is a member of this group of message consumers.
Meta Data Events		
Topic Name	applianceMetadataTopic	The service sends metadata events to this topic on the message bus.
Client	mrsMetadataTopicClient	The identifier of the service on the message bus.
Audit Events		
Topic Name	applianceAuditTopic	The service sends audit events to this topic on the message bus.
Client	mrsAuditTopicClient	The identifier of the service on the message bus.

10.20. Service Configuration – Recordings REST Service

This service provides a REST interface to the file store of a recording (media) repository.

The configuration parameters that are available when the service is running on an appliance recorder node, see section 10.1 Recorder Nodes, are:

Parameter	***Default Value***	***Comment***
REST Service		
IP Address	192.168.1.100	The service binds the REST interface to this IP address.
Port	4010	The service binds the REST interface to this (TCP) port.
Log Messages	Not ticked	The service writes all HTTP messages to the service log file if ticked. Untick it in production as it considerably slows the operation of the service.
Event Service		
Audit Events		
Log Events	Not ticked	The service writes all audit events to the service log file if ticked. Untick it in production as it considerably slows the operation of the service.

The additional configuration parameters that are available when the service is running on a custom recorder node, see section 10.1 Recorder Nodes, are:

Parameter	***Default Value***	***Comment***
Digital Certificates		
Keystore	./trvr.cfsrs.p12	If set, the service uses the certificates in this file to encrypt the communication with clients (that is, use HTTPS instead of HTTP).

Keystore Password	********** (withheld)	If set, the service uses this password to access the information in the keystore file.
Truststore		If set, the service uses the certificates in this file to authenticate clients.
Truststore Password		If set, the service uses this password to access the information in the truststore file.
File Store		
Directories:	/local/recorder/cache	The service uses this repository file store.
Event Service		
Base URL	kafka://127.0.0.1:2191	The service connects to this message bus.
Audit Events		
Topic Name	applianceAuditTopic	The service sends audit events to this topic on the message bus.
Client	cfsrsAuditTopicClient	The identifier of the service on the message bus.

10.21. Service Configuration – RTP Media Server

This service captures media and additional information (metadata) about the media from RTP streams sent directly to it by clients over a network and from RTP streams that are multicast on a network.

This service does not send RTP packets.

In addition to processing standard RTP packets, the service can extract additional information (metadata) about the media streams from different types of supported RTP extensions if such extensions are present in the RTP packets.

Typically, the service will start a recording session when it receives the first RTP packet with media for a configured RTP stream. Then, it will continue capturing media and information (metadata) about the media until there is an ‘absence’ of RTP packets with media for a configurable time (also known as VoX timeout).

The configuration parameters that are available when the service is running on an appliance recorder node, see section 10.1 Recorder Nodes, are:

Parameter	*Default Value*	*Comment*
RTP Unicast Service (for each unicast stream)		
IP Address		If set, the service binds the RTP interface to this IP address.
Port		If set, the service binds the RTP interface to this (UDP) port.
VoX Timeout	00:00:15	The service ends the current recording session when it has not received an RTP packet with media for this time.
Extension	None	The service extracts information (metadata) about the media from this RTP extension if it is present in the RTP packets.
Payload		
Events		If set, the service treats the media in RTP packets with this RTP payload type as events.
Named Events		If set, the service treats the media in RTP packets with this RTP payload type as named events.
Tone Events		If set, the service treats the media in RTP packets with this RTP payload type as tone events.
RTP Multicast Service (for each multicast service)		
IP Address		If set, the service subscribes to RTP packets that are sent to this multicast address.
Port		If set, the service subscribes to RTP packets sent to this multicast (UDP) port.
Network Device		If set, the service uses this network device to subscribe to multicasts.
VoX Timeout	00:00:15	The service ends the current recording session when it has not received an RTP packet with media for this duration.

Extension	None	The service extracts information (metadata) about the media from this RTP extension if it is present in the RTP packets.
Payload		
Events		If set, the service treats the media in RTP packets with this RTP payload type as events.
Named Events		If set, the service treats the media in RTP packets with this RTP payload type as named events.
Tone Events		If set, the service treats the media in RTP packets with this RTP payload type as tone events.
Event Service		
Session Events		
Log Events	Not ticked.	The service writes all session events to the service log file if ticked. Untick it in production as it considerably slows the operation of the service.
Audit Events		
Log Events	Not ticked	The service writes all audit events to the service log file if ticked. Untick it in production as it considerably slows the operation of the service.

The additional configuration parameters that are available when the service is running on a custom recorder node, see section 10.1 Recorder Nodes, are:

Parameter	***Default Value***	***Comment***
Event Service		
Base URL	kafka://127.0.0.1:2191	The service connects to this message bus.

Session Events		
Topic Name	applianceSessionTopic	The service sends session events to this topic on the message bus.
Client	rtpmsSessionTopicClient	The identifier of the service on the message bus.
Audit Events		
Topic Name	applianceAuditTopic	The service sends audit events to this topic on the message bus.
Client	rtpmsAuditTopicClient	The identifier of the service on the message bus.

10.22. Service Configuration – RTSP Media Server

This service captures media and additional information (metadata) about the media from RTSP sessions with clients. Combined with the "SIP Media Server" service, it can capture audio conversations in ED-137 networks, common in air traffic control environments.

Clients use the RTSP protocol to start and control a recording session with this service. Once a recording session is active, clients use RTP packets to send media to the service via independent UDP or TCP connections, or interleaved with the RTSP messages on the RTSP connection.

This service does not initiate RTSP sessions or send RTP packets during RTSP sessions.

The service is fully compliant with the "ED-137 Interoperability Standard for VoIP ATM Components, Volume 4: Recording, January 2012 (ED-137/4B)" and the "ED-137 Interoperability Standard for VoIP ATM Components, Volume 4: Recording, March 2019 (ED-137/4C)".

In addition to RTP packets, this service can capture metadata from the first RECORD message and subsequent SET_PARAMETER messages during RTSP sessions. The metadata can be in the Total Recall VR proprietary or ED-137 format.

The configuration parameters that are available when the service is running on an appliance recorder node, see section 10.1 Recorder Nodes, are:

Parameter	***Default Value***	***Comment***
RTSP Service		
IP Address	192.168.1.100	The service binds the RTSP interface to this IP address.
Port	554	The service binds the RTSP interface to this (TCP) port.

Public IP Address		If set, the service uses this IP address as the RTSP service IP address in RTSP messages.
Public Port		If set, the service uses this (TCP) port as the RTSP service port in RTSP messages.
Log Messages	Not ticked	The service writes all RTSP messages to the service log file if ticked. Untick it in production as it considerably slows the operation of the service.
RTP Service		
IP Address	192.168.1.100	The service binds the RTP interface to this IP address.
Base Port	6800	Starting with this, the service binds the RTP interface to (UDP and TCP) ports. The number of licensed sessions defines the range of UDP and TCP ports that the service uses.
Public IP Address		If set, the service uses this IP address as the RTP service IP address in RTSP messages.
Public Base Port		If set, the service uses this (UDP and TCP) port as the base RTP service port in RTSP messages. The number of licensed sessions defines the range of UDP and TCP ports that the service uses.
Event Service		
Session Events		
Log Events	Not ticked	The service writes all session events to the service log file if ticked. Untick it in production as it considerably slows the operation of the service.

Audit Events		
Log Events	Not ticked	The service writes all audit events to the service log file if ticked. Untick it in production as it considerably slows the operation of the service.

The additional configuration parameters that are available when the service is running on a custom recorder node (see section 10.1 Recorder Nodes) are:

Parameter	***Default Value***	***Comment***
Event Service		
Base URL	kafka://127.0.0.1:2191	The service connects to this message bus.
Session Events		
Topic Name	applianceSessionTopic	The service sends session events to this topic on the message bus.
Client	rtspmsSessionTopicClinet	The identifier of the service on the message bus.
Audit Events		
Topic Name	applianceAuditTopic	The service sends audit events to this topic on the message bus.
Client	rtspmsAuditTopicClient	The identifier of the service on the message bus.

10.23. Service Configuration – SIP Media Server

This service captures media and additional information (metadata) about the media from SIP sessions with clients.

This service does not initiate SIP sessions or send RTP packets during SIP sessions.

The service provides different recording services. The recording service that will apply to a SIP session depends on the user part of the SIP “To” header that appears in the SIP INVITE message:

SIP "To" Header	*Recording Service*
recorder.sip@...	Basic SIP session recording service where up to 2 audio RTP streams will be recorded.
recorder.siprec@...	SIPrec recordings service based on RFC7865 and RFC7866, where the recorder acts as an SRS.
recorder.ed137@...	ED137 recording service based on ED-137 Interoperability Standard for VoIP ATM Components, Volume 4: Recording, January 2012 (ED-137/4B) and ED-137 Interoperability Standard for VoIP ATM Components, Volume 4: Recording, March 2019 (ED-137/4C).
recorder.bib@...	Cisco IP phone-based recording based on Cisco built-in bridge (BiB). Requires Cisco UCM release 8.5 or better.
recorder.acom@...	Zetron Acom recording service based on Zetron SIP Logging Interface Specification 025-9673F Rev F, January 2017.
LoggerChan<xxx>@...	Zetron Acom recording service based on Zetron SIP Logging Interface Specification 025-9673F Rev F, January 2017. It enforces that the SIP "From" header value is "Zchan<xxx>@...".
recorder.max@...	Zetron MAX recording service based on Zetron MAX Voice Logger Interface Control ICD 025-9702A Rev A, January 2017.
Channel<xxx>@...	Zetron MAX recording service based on Zetron MAX Voice Logger Interface Control ICD 025-9702A Rev A, January 2017. It enforces that the SIP "From" header value is "VLG-channel<xxx>@...".
Any other value	Same as recorder.sip@... Basic SIP session recording service where up to 2 audio RTP streams will be recorded.

The configuration parameters that are available when the service is running on an appliance recorder node, see section 10.1 Recorder Nodes, are:

Parameter	*Default Value*	*Comment*
SIP Service		
IP Address	192.168.1.100	The service binds the SIP interface to this IP address.
Port	5060	The service binds the SIP interface to this (UDP and TCP) port.
Public IP Address		If set, the service uses this IP address in SIP messages as the SIP service IP address.
Public Port		If set, the service uses this (UDP and TCP) port as the SIP service port in SIP messages.
Log Messages	Not ticked	The service writes all SIP messages to the service log file if ticked. Untick it in production as it considerably slows the operation of the service.
RTP Service		
IP Address	192.168.1.100	The service binds the RTP interface to this IP address.
Base Port	6000	Starting with this, the service binds the RTP interface to (UDP) ports. The number of licensed sessions defines the range of UDP ports that the service uses.
Public IP Address		If set, The service uses this IP address as the RTP service IP address in SIP messages.
Public Base Port		If set, the service uses this (UDP) port as the base RTP service port in SIP messages. The number of licensed sessions defines the range of UDP ports that the service uses.
RTSP Service		
IP Address	192.168.1.100	The service responds with this IP address to queries about the RTSP service.

Port	554	The service responds with this (TCP) port to queries about the RTSP service.
Bindings (for each binding)		
Registrar		
Address		If set, the IP address of the SIP Registrar to use.
User Name		If set, the service uses this user to authenticate with the SIP Registrar.
Password		If set, the service uses this password to authenticate with the SIP Registrar.
Address of Record		
Address		If set, the service will register this address with the SIP Registrar.
User Name		If set, the service will register this user name with the SIP Registrar.
Contact Address		
Type	SIP Standard	The type of SIP binding to create with the SIP Registrar.
Lifetime	3600 seconds	The lifetime of the SIP binding. The service will automatically refresh the SIP binding with the SIP Registrar before it expires.
Event Service		
Session Events		
Log Events	Not ticked	The service writes all session events to the service log file if ticked. Untick it in production as it considerably slows the operation of the service.
Audit Events		
Log Events	Not ticked	The service writes all audit events to the service log file if ticked.

		Untick it in production as it considerably slows the operation of the service.

The additional configuration parameters that are available when the service is running on a custom recorder node, see section 10.1 Recorder Nodes, are:

Parameter	***Default Value***	***Comment***
Event Service		
Base URL	kafka://127.0.0.1:2191	The service connects to this message bus.
Session Events		
Topic Name	applianceSessionTopic	The service sends session events to this topic on the message bus.
Client	sipmsSessionTopicClient	The identifier of the service on the message bus.
Audit Events		
Topic Name	applianceAuditTopic	The service sends audit events to this topic on the message bus.
Client	sipmsAuditTopicClient	The identifier of the service on the message bus.

10.24. Service Configuration – Tait VRP Media Server

This service captures media and additional information (metadata) about the media from Tait VRP (Voice Recording Protocol) streams, which are used in Tait DMR and MPT-IP networks.

The service is a single UDP port (9999 by default) that accepts connections from Tait DMR and MPT-IP systems over a network. Multiple DMR and MPT-IP nodes can send VRP packets to each instance of this service.

The configuration parameters that are available when the service is running on an appliance recorder node, see section 10.1 Recorder Nodes, are:

Parameter	***Default Value***	***Comment***
VRP Service		
IP Address	192.168.1.100	The service binds the VRP interface to this IP address.
Port	9999	The service binds the VRP interface to this (UDP) port.
Log Messages	Not ticked	The service writes all VRP messages to the service log file if ticked. Untick it in production as it considerably slows the operation of the service.
VoX Timeout	00:00:15	According to the VRP specification, VRP call start and call end packets are sent to the recorder to specify when calls start and end. However, not all Tait networks use the call start and end packets. This parameter is relevant only to networks where the call start and call end packets are absent. This parameter defines the 'quiet time' (absence of VRP packets) during recording, which must pass before this service stops recording VRP streams.
Address Scheme	MPT 1327	The service will use this addressing scheme when processing addresses in the VRP packets.
Event Service		
Session Events		
Log Events	Not ticked	The service writes all session events to the service log file if ticked. Untick it in production as it considerably slows the operation of the service.
Audit Events		

Log Events	Not ticked	The service writes all audit events to the service log file if ticked. Untick it in production as it considerably slows the operation of the service.

If you select the *MPT 1343* or the *ANN* address scheme, you can specify fleet numbering parameters. The parameters that define the fleet numbering for the *MPT 1343* address scheme are:

Parameter	***Default Value***	***Comment***
VRP Service		
Address Scheme	MPT 1343	
Fleets		
NP	200	Number Prefix. Valid values are *200* to *327* inclusive.
FIN	2001	Fleet Individual Number. Valid values are *2001* to *4999* inclusive.
FGN	5000	Fleet Group Number. Valid values are *5000* to *6050* inclusive.
UN Digits	3	Number of digits used for Unit Numbers. Valid values are *2* and *3* (digits).
GN Digits	3	Number of digits used for Group Numbers. Valid values are *2* and *3* (digits).

The parameters that define the fleet numbering for the *ANN* address scheme are:

Parameter	***Default Value***	***Comment***
VRP Service		
Address Scheme	ANN	
Fleets		

Fleet Partitioning	3	FPP. Valid values are *0* to *10*. The sum of this parameter and the Miniaturisation Extent parameter cannot exceed 10.
Miniaturisation Extent	7	MEP. Valid values are *0* to *10*. The sum of this parameter and the Fleet Partitioning parameter cannot exceed 10.

The additional configuration parameters that are available when the service is running on a custom recorder node (see section 10.1 Recorder Nodes) are:

Parameter	***Default Value***	***Comment***
Event Service		
Base URL	kafka://127.0.0.1:2191	The service connects to this message bus.
Session Events		
Topic Name	applianceSessionTopic	The service sends session events to this topic on the message bus.
Client	vrpmsSessionTopicClient	The identifier of the service on the message bus.
Audit Events		
Topic Name	applianceAuditTopic	The service sends audit events to this topic on the message bus.
Client	vrpmsAuditTopicClient	The identifier of the service on the message bus.

10.25. Service Tools – Profile REST Service

Profiles are a collection of configuration and other information that can be used to tailor the operation of Total Recall VR recording services.

At this stage, the following Total Recall VR services use profiles:

- Recording Service – see section 10.19 Service Configuration – Recording Service.

The Profile REST Service provides the following tools to manager profiles:

Tool	*Description*
Manage Transforms	Define and manage address transforms (mappings).
Manage Policies	Define and manage recording policies.

The subsequent sections explain how to use the tools.

10.25.1. Manage Transforms

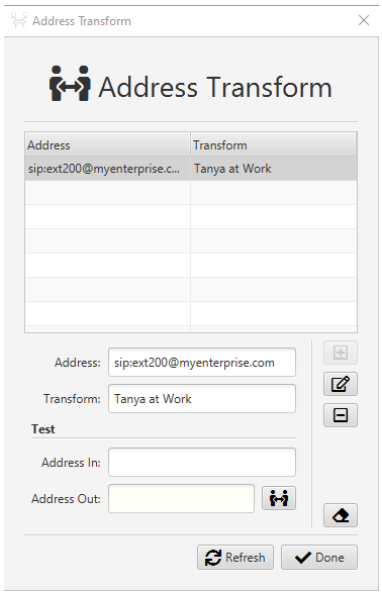
In addition to media, Total Recall VR recording services capture additional information (metadata) about the media while recording a session. This additional information includes the session participants' addresses (also known as the names).

The recording services extract the addresses (names) of the participants from identifiers that appear in the media itself or identifiers that appear in the out-of-band information about the media. As a result, the identifiers may take different forms and may not be suitable for human consumption. For example, in most cases, an identifier such as “sip:ext200@myenterprise.com” is meaningless to most of us, while an identifier such as “Tanya at Work” is meaningful.

But what if “sip:ext200@myenterprise.com” and “Tanya at Work” are the same thing; that is, the former is the not-so-user-friendly identifier of the latter?

If so, then all of us would prefer to search using “Tanya at Work” rather than “sip:ext200@myenterprise.com”.

The address transform tool allows you to define transforms for participants' addresses (names). Using the tool, you can map “sip:ext200@myenterprise.com” to “Tanya at Work” so that the latter, instead of the former, appears in the recording metadata as shown in the following screen capture:



You can set ***Address*** to a regular expression that matches multiple identifiers and map all matching identifiers to more human-friendly values. Also, you can use regular expression groups in the value for ***Transform*** to create mappings that take part of the original address.

Regular expressions basic syntax reference:
http://docs.oracle.com/javase/tutorial/essential/regex/

For example:

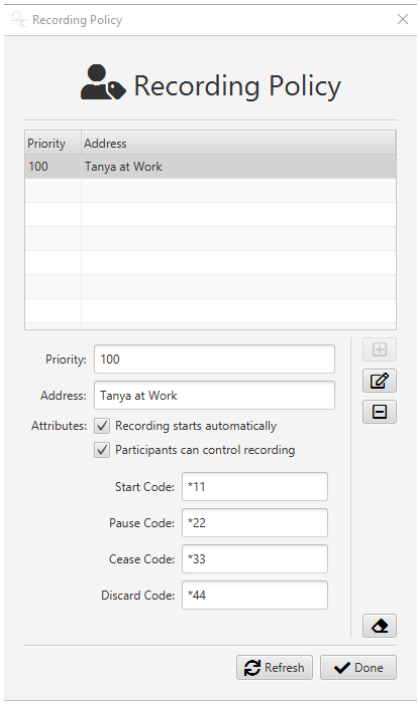
Address	***Transform***	***Address In***	***Address Out***
61298762100	*100*	61298762100	100
		4456789999	4456789999
61298762101	*Tanya's Phone*	61298762101	Tanya's Phone
		61298762102	61298762102
61298762([0-9]{3})	*Extension $1*	61298762101	Extension 101
		61298762229	Extension 229
		4456789999	4456789999
*sip:ext([0-9]{2})@.**	*$1*	sip:ext76@mysip.com	76
		4456789999	4456789999
		sip:90@mysip.com	sip:90@mysip.com
sip:([^@])@.**	*$1*	sip:igor@sipco.com	igor
		sip:90@mysip.com	90
192.168.130.100:700[0-9]	*PA Speaker*	192.168.130.100:7000	PA Speaker
		192.168.130.100:7010	192.168.130.100:7010

10.25.2. Manage Policies

Recording policies specify how a session recording should proceed when a particular participant is in the session.

By default, Total Recall VR recording services start capturing and recording media and additional information (metadata) about the media as soon as a session begins, and the session participants cannot control the recording in any way.

The default applies to all sessions unless there is a recording policy for at least one of the session participants, as shown in the following screen capture:



In such cases, the policy will affect the recording of the session. As you may have observed from the previous screen capture, recording may not start when the session starts, and participants may be allowed to control the recording.

A single policy may apply to multiple participants. You can define such a policy by using a regular expression as a value for ***Address***.

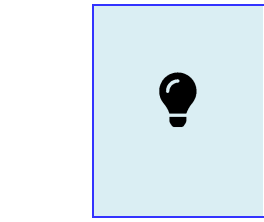
Regular expressions basic syntax reference:
http://docs.oracle.com/javase/tutorial/essential/regex/

When there are policies for multiple session participants, the policy with the highest ***Priority*** will define how the session is recorded. The recording services will disregard all other policies.

Finally, when there are multiple policies with the same ***Priority*** for multiple session participants, the first policy on the list of policies with the highest priority will define how the session is recorded.

11. Appliance Recorder Manager

The Manager view of Total Recall VR Cockpit has a built-in system manager for appliance recorder nodes.



Total Recall VR Cockpit does not have tools for system management of custom recorder nodes, see section 10.1 Recorder Nodes.

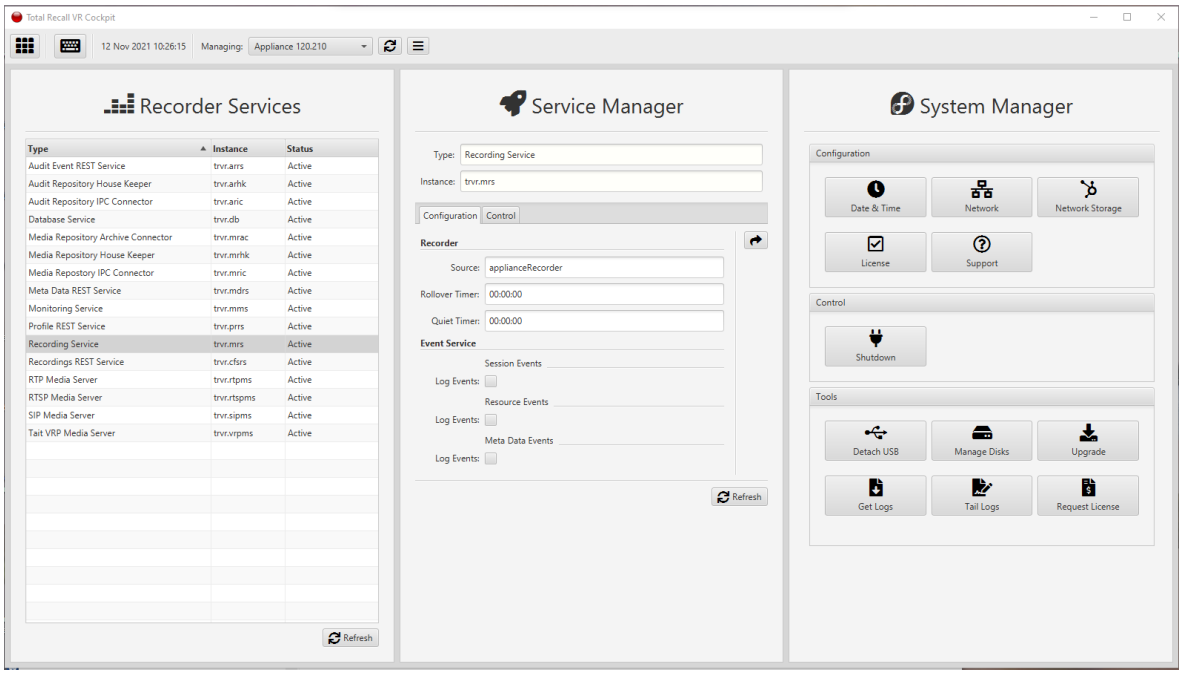


Figure 19: Manager View

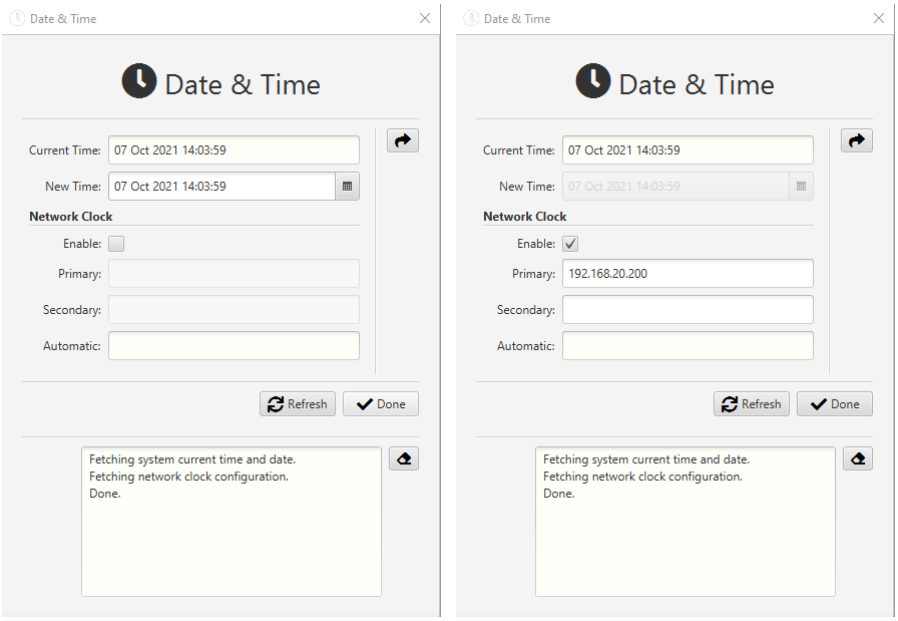
The following sections explain how to use the system manager.

11.1. System Configuration – Data & Time

Total Recall VR appliances use an internal clock to time stamp recordings and metadata, execute periodic activities, etc.

The internal clock uses UTC. As a result, all time stamps are in the UTC. However, The Total Recall VR Cockpit shows time stamps in the time zone set in its configuration database, see section 3.10.1 Locale.

The system clock of the appliance can be either its internal hardware clock (the default configuration) or a network clock that uses the NTP protocol, as shown in the following screen capture.



When the configuration specifies two NTP servers, the appliance will synchronise its time with the ***Primary*** server. When the ***Primary*** server is unavailable, the appliance will switch to the ***Secondary*** server. However, the appliance will switch back to the ***Primary*** server as soon as the ***Primary*** server becomes available.

To connect and continually synchronise the system clock of an appliance to an NTP source:

1. Make sure that the appliance has a working network connection. See section 11.2 System Configuration – Network for details on configuring the network interfaces.

2. Ensure the appliance can access the NTP server(s) over the network. This may require network infrastructure configuration, such as routers and firewalls.

3. Do not use the same IP address for the ***Primary*** and ***Secondary*** NTP servers. If you have only one NTP server, set ***Primary*** and leave ***Secondary*** blank.

4. Avoid synchronising with *ntp.org* servers. Their IP addresses change constantly. As a result, appliances may not be able to connect to an NTP server reliably.

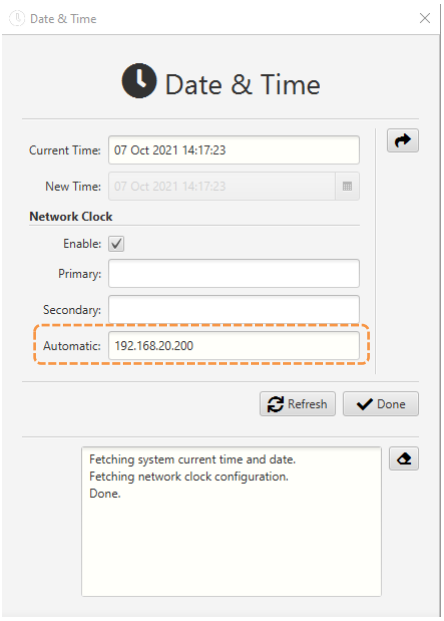
4. Make sure the NTP servers provide UTC time.

When you select ↱, the appliance will synchronise its date and time to the primary NTP server. This may result in a substantial one-off time shift. The substantial time shift may

cause unexpected behaviour by the appliance; for example, if the time shift is back in time, some regular activities may not run until the clock catches up. To avoid this, set the internal clock to a time as close as possible to the network time and then configure the appliance to use the network clock. Alternatively, restart the appliance immediately after switching it to the network clock.

Subsequently, the appliance will continue synchronising its time with the NTP servers regularly, which may result in very small time shifts that do not affect the appliance's operation.

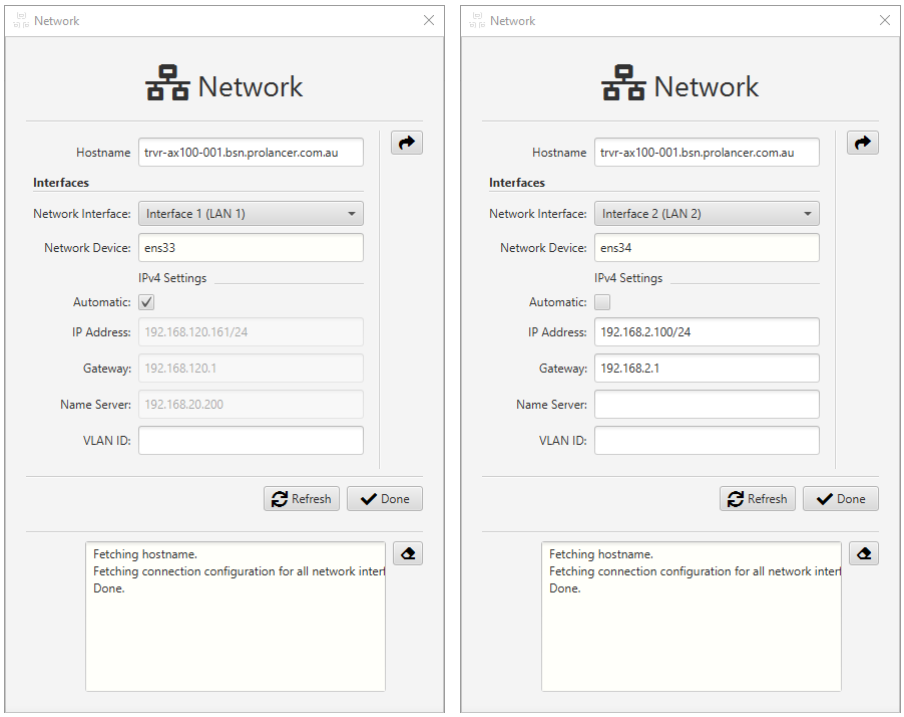
Finally, ***Automatic*** may show the IP addresses of the NTP servers that were automatically configured, for example, when using DHCP to configure the network interfaces of the appliance, as shown in the following screen capture.



However, note that you can specify a ***Primary*** and a ***Secondary*** NTP server to use in addition to the automatically configured NTP servers. In most cases, you will use the automatically configured NTP servers and leave both ***Primary*** and ***Secondary*** blank (as shown in the previous screen capture).

11.2. System Configuration – Network

Total Recall VR appliances have two network interfaces. Use one (usually the first one) to connect the appliance to the enterprise network and the other (usually the second) for recording.



As shown in the previous screen captures, you can use static or automatic configuration (via DHCP) for each network interface.

All Total Recall VR recorder appliances ship with both network interfaces set for automatic configuration (via DHCP).

We recommend a static configuration for both network interfaces.

Exercise extreme caution when changing the configuration of the network interfaces – you may lose connection to the appliance if you are configuring the network interfaces remotely and misconfigure the network interface used for the current connection to Total Recall VR Cockpit.

To use automatic configuration, tick ***Automatic***. To use static, untick ***Automatic*** and specify ***IP Address***, ***Gateway***, and ***Name Server***. In both cases, set ***VLAN ID*** if you use VLANs on your networks.

Suppose you change the configuration of a network interface from static to automatic. In that case, it may take some time for all recorder services to restart with the new configuration (as long as 10-15 minutes), so please be patient.

Connecting a Total Recall VR appliance to two different networks is possible as appliances have two network interfaces.

If a Total Recall VR appliance is connected to two different networks, then the appliance cannot be used to route packets between the networks. That is, it cannot be used as a routing device.

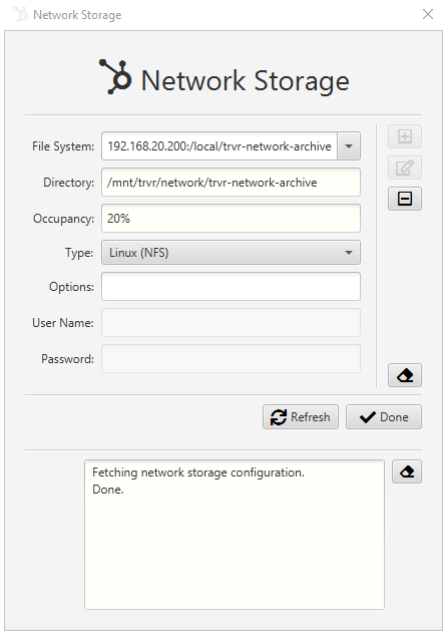
Total Recall VR appliances use a source-based routing strategy for IP packets, so the network traffic on one interface is separate from the network traffic on the other.

The source-based routing strategy allows for a separate gateway for each interface. However, the first interface's gateway is the appliance's default gateway. As a result, packets to services such as DNS, NTP, etc., if not on one of the networks connected to the appliance interfaces, will be sent via the first interface. This is one of the reasons why we recommend connecting the first interface to your enterprise network and using the second interface for recording.

In addition, you can connect both interfaces to the same network, assign them a different IP address on that network and set them to use the same gateway. However, even in this case, internally, the traffic on the first interface will be completely separate from the traffic on the second interface. As a result, both interfaces can be used to their maximum capacity.

11.3. System Configuration – Network Storage

Total Recall VR appliances can use network storage on Windows and Linux storage servers.



Appliances use the CIFS protocol to access storage on Windows servers and the NFS protocol to access storage on Linux servers. As a result, you must set ***File System*** to either a Windows UNC path or a Linux NFS path, based on the type of the storage server.

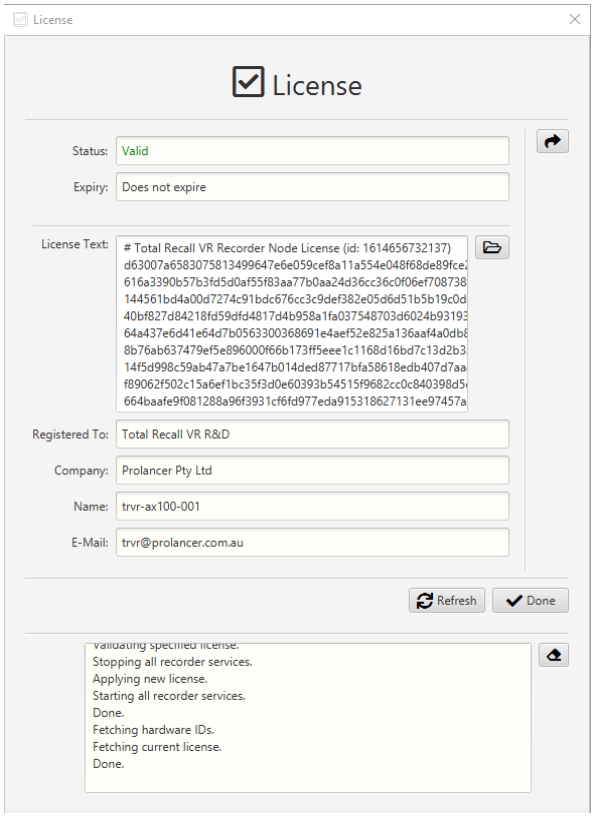
Further, you can fine-tune the storage server access by specifying ***Options***. The options that are accepted are all of the mount options that are available with the CIFS and NFS mounters on a Linux system. However, in most cases, you do not need to specify any ***Options***. The following table shows the options that are automatically set for each type of storage:

Type	***Default Options***
NFS	rw,relatime,rsize=1048576,wsize=1048576,namlen=255,hard,proto=tcp,timeo=600,retrains=2,sec=sys,local_lock=none
CIFS	rw,relatime,cache=strict,noforceuid,noforcegid,filemode=0755,dirmode=0755,soft,nounix,serveino,mapposix,rsize=4194304,wsize=4194304,bsize=1048576,echo_interval=60,actimeo=60

11.4. System Configuration – License

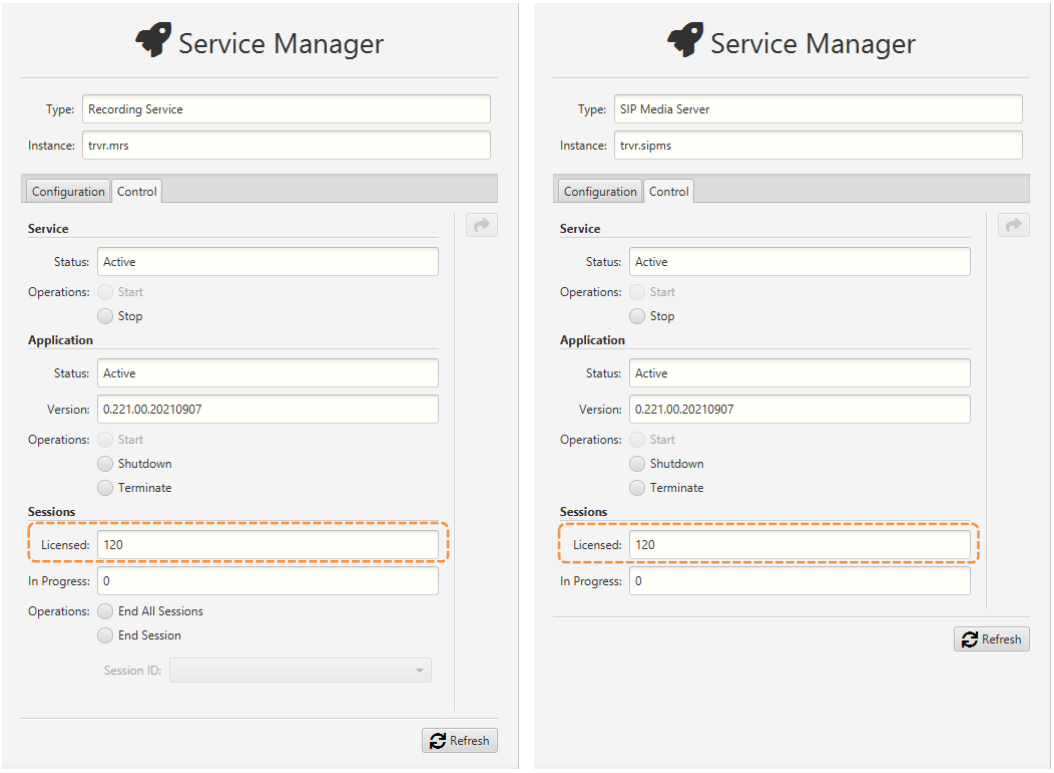
The Total Recall VR recorder services that run on a Total Recall VR appliance require a valid activation license.

Total Recall VR appliances ship from the factory with a valid activation license. However, you can change the license at any time, for example, to increase the recording channel count as shown in the following screen capture:



To change the license, either set ***License Text*** to the text of the new license you received by cutting and pasting or select 🗁 to load the license text from a license file you received.

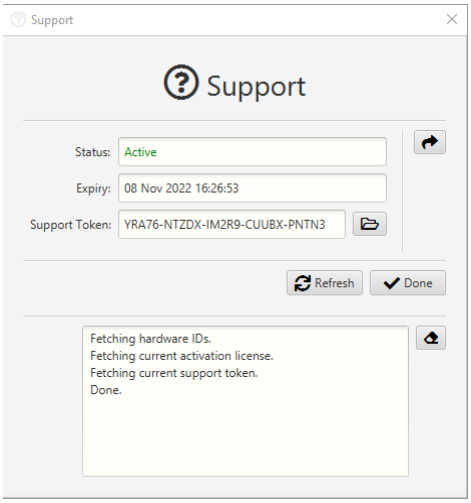
You may have noticed that the number of licensed channels, sessions, etc., does not appear on the License form (see previous screen capture). To determine the actual number of licensed channels, sessions, etc., visit the **Control** tab for each of the services in the Service Manager, for example:



11.5. System Configuration – Support

To receive support directly from us for your Total Recall VR appliance, you need to provide a valid and active support token for the appliance when you seek support.

If you purchased support for your Total Recall VR appliance at the time of purchase, then the appliance will ship from the factory with a valid support token, as shown in the following screen capture:



However, when you renew the support token or purchase a new one, you can apply the token to your appliance. If you do so, the token and its status will be handy during a subsequent support call.

To apply a support token, select 🗁 to load the token from a support token file that you received and then select ↱.

Please note the following regarding the support token:-

a. You do not need to purchase support tokens for any of your Total Recall VR products if you do not wish to receive support directly from us. Please discuss your support options with a representative from the point of purchase. They may and should offer support options that are likely to be tailored to your case compared to the remote support we provide as the manufacturer of the products.

b. Support tokens are valid for one (1) year starting from the date that is exactly one (1) month after the date when the product that it relates to was shipped from our factory. Support for the first month after the shipment date is free and does not require a valid support token. So, during the first year, if you purchase a support token for a product at the same time when you purchase the product, then you will receive thirteen (13) months of support from the shipment date of the related product. You will receive twelve (12) months each subsequent year if you renew the support token.

c. Each token relates to one instance of a Total Recall VR product and cannot be transferred to another instance of the same Total Recall VR product or used to get support for an instance of another Total Recall VR product.

d. On expiry, support tokens can be renewed on a back-charging basis. You must pay for years missed and the current year when you renew an expired token. For example:

   Suppose you purchased a support token when purchasing an instance of the Total Recall VR Cockpit. Further, let’s take the fact that you did not renew the token or buy a new one after it expired at the end of the first year. If you request support in year 3 of ownership, you must pay for two years of support (to cover support for years 2 and 3) to renew your existing token or purchase a new one. The purchase will give you a token expiring at the end of year 3.

e. You can purchase a support token anytime on a back-charging basis for any Total Recall VR product instance. For example:

   Let’s assume you did NOT purchase a support token when you purchased an instance of Total Recall VR Cockpit. If you request support in year 3 of ownership, you must pay for three years of support (to cover support for years 1, 2 and 3) to purchase a new support token. The purchase will give you a token expiring at the end of year 3.

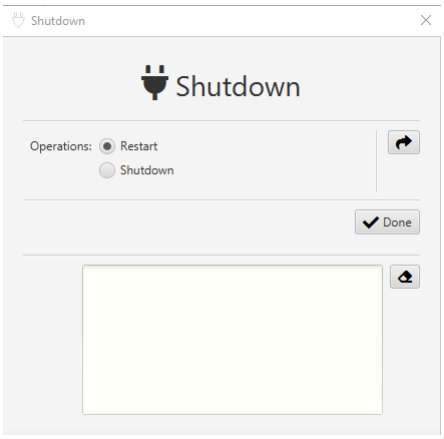
In summary, if you wish to receive support directly from us for an instance of a Total Recall VR product, then you need a valid and active support token for the instance of the Total Recall VR product.

However, you do not need to purchase support from us. Instead, please discuss your support options with a representative from the point of purchase. They may and should offer support options that will likely be tailored to your case compared to the remote support we provide as the manufacturer of Total Recall VR products.

11.6. System Control - Shutdown

Use this system control to remotely power cycle Total Recall VR appliances.

You can select either to restart or to shutdown the appliance, as shown in the following screen capture:



However, if you shut down an appliance, you will need to power it up, so avoid shutting down appliances when you do not have physical access to them.

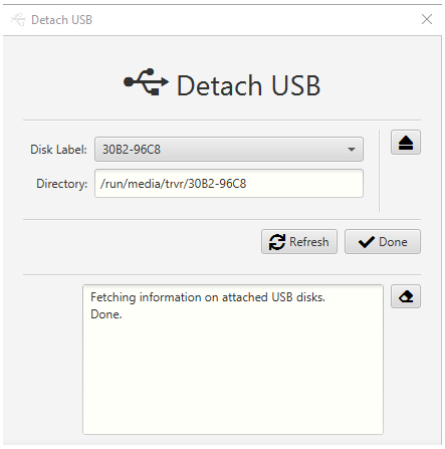
11.7. System Tools – Detach USB

Use this system tool to safely detach a USB storage device (thumb drive, disk, etc.) that you may have attached to a Total Recall VR appliance.

You will damage the files and file system on the USB device if you physically detach it from the appliance while the file systems and files on it are in use. This is similar to what may happen to a USB thumb drive if you physically detach it from your Windows PC while applications are using it.

This tool enables you to prepare the USB device to physically detach it from the appliance so that you can physically detach it without damaging its content.

To detach a USB device, simply choose the device with the ***Disk Label*** selector and then select ⏏, as shown in the following screen capture:

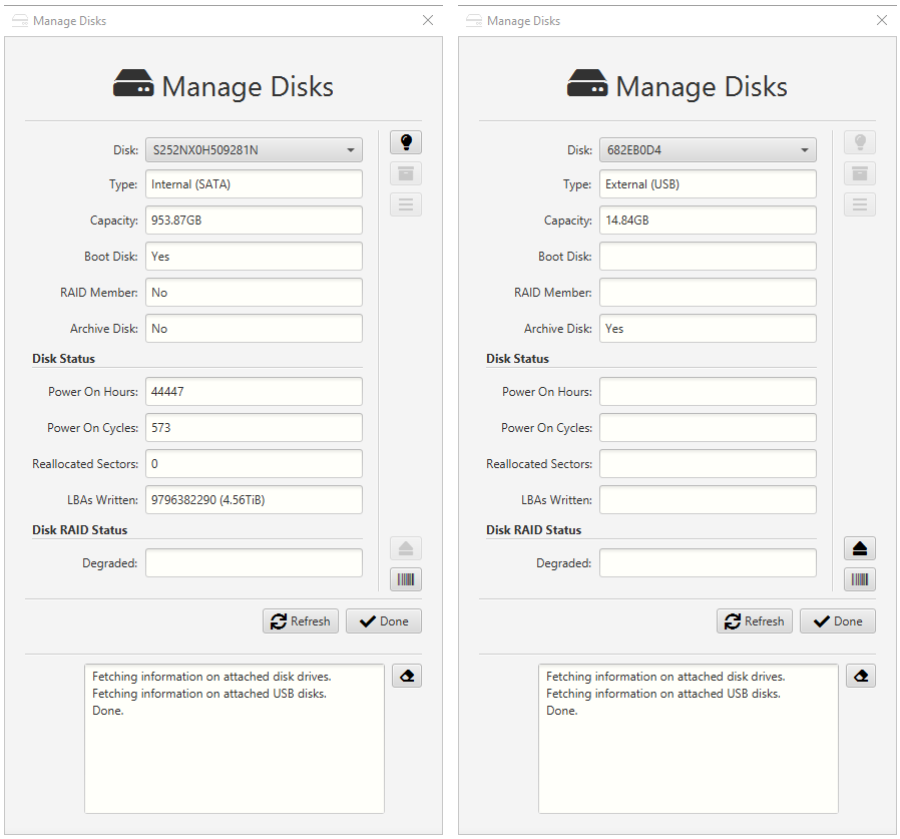


The operation status will tell you if it is safe to detach the USB device from the appliance physically. You may have to stop or reconfigure some recorder services if they are using the USB device to disconnect the USB device.

11.8. System Tools – Manage Disks

This system tool is a collection of disk status and maintenance utilities.

The disk status utilities fetch various disk operating parameters automatically when you choose a disk with the ***Disk*** selector, as shown in the following screen capture:



The following disk maintenance utilities are available:

Utility	***Description***
	Disk blink utility. Flashes the disk LED for a short period.
	Disk attach utility for archive disks. Attaches a disk as an archive disk to the appliance. The “Media Repository Archive Connector” can then use this disk to house a target recording (media) repository.
	Disk attach utility for RAID system disks. Attaches a disk as a system disk to the appliance and adds it to the RAID of system disks.
	Disk detach utility. Prepares the disk so it can be physically detached from the appliance. You may have to stop or reconfigure some recorder services if they use the disk to detach it.
	Disk rescan utility.

	Rescans the system for newly attached disks. In most cases, the system will detect newly attached disks automatically; however, you can force it to rescan all disks if it does not.

Please follow one of the following procedures to replace a disk safely.

The “Media Repository Archive Connector” service uses archive disks (which can be either external USB or internal disks) to archive recording files and metadata. It creates a recording (media) repository, see section 7.1 Recording Repositories, on such disks. It adds until it reaches physical disk limits or other limits specified in its configuration, see section 10.13 Service Configuration – Media Repository Archive Connector. Once the service reaches a limit, it will stop archiving until a new archive disk with available space is attached to the appliance.

To replace an archive disk:

Replace an archive disk

1. Stop the “Media Repository Archive Connector” service using the *Stop* control that is available on the **Control** tab for the service in the Service Manager.
2. Select **Manage Disks** in the System Manager to start the disk management tool.
3. Use the ***Disk*** selector to choose the current archive disk and display its status information. The disk status of an archive disk shows *Yes* as the value for the ***Archive Disk***.
4. Skip this step for external USB disks. Select for internal disks to flash the disk LED, which will help you identify the physical disk caddy that houses the archive disk.
5. Select to prepare the disk to be physically detached from the appliance. The process may take a short time to complete. Once it completes, you can safely physically detach the disk from the appliance.

   MAKE SURE TO DETACH THE CORRECT DISK. IF YOU DETACH A SYSTEM DISK INSTEAD, THE APPLIANCE WILL STOP WORKING AND MAY NOT BE POSSIBLE TO RECOVER IT FROM THE DISKS.
6. Attach a new unformatted disk or a USB disk to the appliance.
7. Select to force the disk tool to rescan and reload the disks so that the new disk appears in the list of available options for the ***Disk*** selector.
8. Use the ***Disk*** selector to choose the new disk.
9. Select to configure and attach the new disk as an archive disk.
10. Select **Done** to exit the disk management tool.
11. Check the “Media Repository Archive Connector” configuration and ensure it points to the new disk's file system.

12. Start the “Media Repository Archive Connector” service using the *Start* control that is available on the **Control** tab for the service in the Service Manager.

Your appliance may be using a RAID disk configuration for its system disks. In such cases, if a disk is failing, showing a degraded status or has been operating for four or more years, you can use the disk maintenance tools to replace it.

If your Total Recall VR appliance uses a hardware RAID disk controller, this system tool will report a single non-RAID disk. You must use the hardware RAID tools that come with the hardware to manage the RAID and the disks that are part of it.

Exercise extreme caution when replacing RAID disks.

To replace a system disk on appliances with a RAID disk configuration:

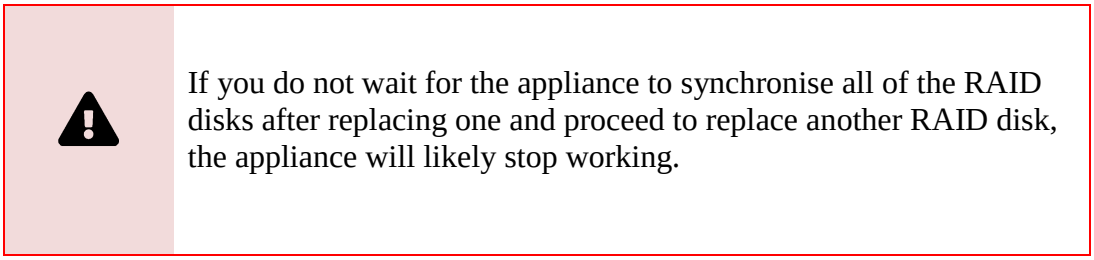
Replace a system disk (only for appliances with RAID system disk configuration)

1. Select **Manage Disks** in the System Manager to start the disk management tool.
2. Use the ***Disk*** selector to choose the system RAID disk you wish to replace and display its status information. The disk status of a system RAID disk shows *Yes* as the value for the ***Boot Disk***. Note that the status may show *Yes* as a value for the ***RAID Disk*** status or *No* if the operating system has excluded the disk from the RAID. The ***Degraded*** status will show a value as well for system RAID disks.
3. Select to flash the LED to help identify the physical disk caddy that houses the disk.
4. Select to prepare the disk to be physically detached from the appliance. The process may take a short time to complete. Once it completes, you can safely physically detach the disk from the appliance.

   MAKE SURE TO DETACH THE CORRECT DISK. IF YOU DETACH THE ACTIVE RAID DISK, THE APPLIANCE WILL STOP WORKING AND CANNOT BE RECOVERED FROM ANY OF THE RAID DISKS.
5. Attach a new unformatted disk to the appliance. This disk must be the same brand and model as the disk you are replacing.
6. Select to force the disk tool to rescan and reload the disks so that the new disk appears in the list of available options for the ***Disk*** selector.

7. Use the ***Disk*** selector to choose the new disk.
8. Select ☰ to configure and attach the new disk as a system RAID disk.
9. Select ✔ **Done** to exit the disk management tool.

If you intend to replace another RAID disk now, give the appliance enough time to synchronise all RAID disks before proceeding. The synchronisation may take several hours (typically as much as 3 hours for a RAID with 1TiB disks).

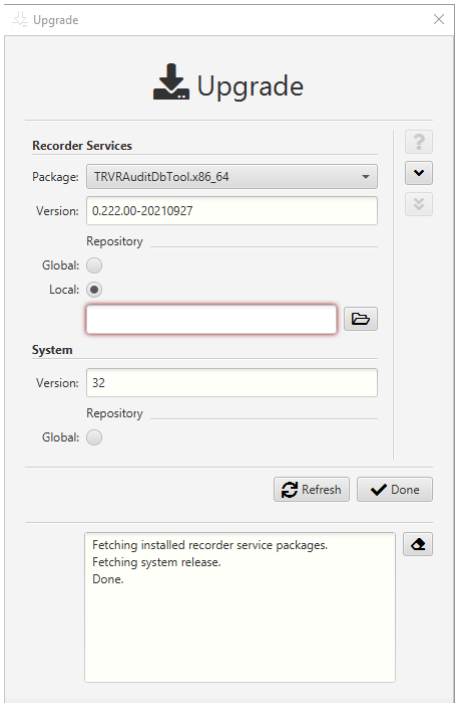


If you do not wait for the appliance to synchronise all of the RAID disks after replacing one and proceed to replace another RAID disk, the appliance will likely stop working.

11.9. System Tools – Upgrade

Use this system tool to upgrade the recorder services and the system software on a Total Recall VR appliance.

In most cases, you will use this tool to upgrade the recorder services either from the global Total Recall VR software repository or from a local copy of a Total Recall VR software repository (for example, a repository on a USB thumb drive), as shown in the following screen capture:



The appliance must have Internet access to upgrade from the global Total Recall VR software repository.

If the appliance lacks Internet access, download a Total Recall VR software repository ZIP package from our website. Subsequently, use the ZIP file (do not extract the content) as a local Total Recall VR software repository during the upgrade process.

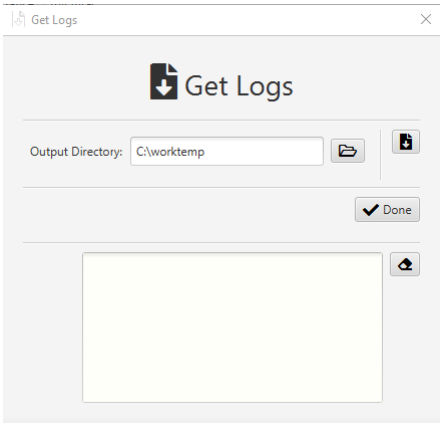
All ZIP packages of Total Recall VR software repositories are cryptographically signed. The upgrade tool will refuse to use a ZIP package without or with an invalid signature to protect the integrity of your appliance.

On occasion, we may release updates for the system software as well. In such cases, you can upgrade the system software from the global Total Recall VR repository. System software updates are simply too large to release as a ZIP package.

11.10. System Tools – Get Logs

Use this system tool to download a copy of the operating logs of a Total Recall VR appliance.

The tool creates a ZIP package of all operating logs and other information and then downloads and stores the package in the specified directory, as shown in the following screen capture:

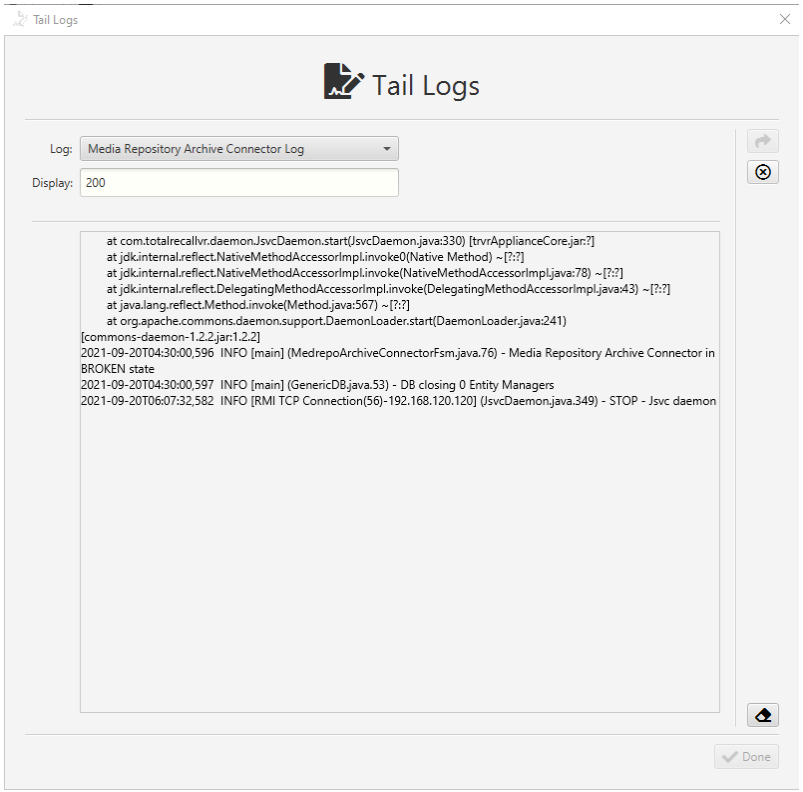


All of the files in the ZIP package are text files, so you can use your favourite text editor to browse the content of the files after extracting the files from the ZIP package.

11.11. System Tools – Tail Logs

Use this system tool to display the information being written in the log files for various Total Recall VR recorder services in near real-time (as it happens).

This is useful when diagnosing problems, as shown in the following screen capture:

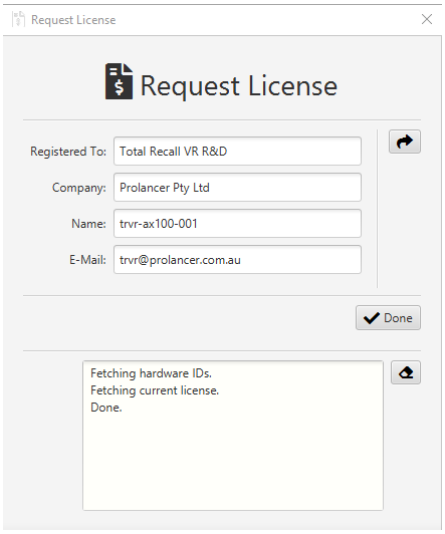


To tail the log of a recorder service, choose the service with the ***Log*** selector and then select ↱ to start tailing the log for that service. Subsequently, select ⊗ to stop tailing the log at any time.

11.12. System Tools – Request License

Use this system tool to generate a license request file or a support token file if and when you wish to request a new activation license or support token for your appliance.

The tool allows you to modify the license ownership information as shown in the following screen capture:



However, in most cases, you will keep the ownership information the same and simply generate the license request file.

You must send us the license request file with your order for a new activation license or support token for your Total Recall VR appliance. We cannot process your order without the license request file.

12. Archiving

All Total Recall VR appliance recorders have a built-in recording (media) repository and store new recordings in this repository when recording. To avoid stopping recording when the repository is full, all appliance recorders manage the space in the repository automatically. An integrated auto-cleaning function ensures enough free space to continue recording endlessly.

The auto cleaning function is performed by the "Media Repository House Keeper" service, see section 10.14 Service Configuration – Media Repository House Keeper. By default, it automatically starts deleting recordings when the database occupancy reaches 100% or the disk occupancy reaches 95%, whichever occurs first. It removes the oldest recordings until the database occupancy is at or below 85% and the disk occupancy is below 80%.

However, you may be using different limits on your appliance, so check the configuration of the "Media Repository House Keeper" service.

You must implement a working archiving strategy to avoid losing recordings due to auto-cleaning.

Archiving is the process of copying recordings and the related metadata from one recording (media) repository (the source repository) to another (the target repository). You can archive manually on an ad-hoc basis, automatically on a near real-time basis (as recordings are added to the source repository, they are automatically copied to the target one), or both.

To archive manually, use the Recording Browser on the Explore view of Total Recall VR Cockpit (see section 7.2 Recording Browser, particularly the **Share** tool, which is the recording and metadata transfer tool). In this case, you have great flexibility when deciding which recordings to archive; for example, archive all recordings in the source repository in one go, create a comprehensive filter (see section 6 Filtering and Searching) to archive recordings that match the filter selectively, etc.

To set up automatic archiving, configure the "Media Repository Archiving Connector" service, see section 10.13 Service Configuration – Media Repository Archive Connector, using the Manager view of Total Recall VR Cockpit. This service archives all recordings in near real-time. It copies recordings and related metadata to the target repository as soon as they are added to the source repository.

To access the recordings in the target repository, use the Recording Browser on the Explore view of Total Recall VR Cockpit to create a Media Repository record for the target repository and then use it to explore the repository, see section 7 Recording Management.

As you may already know, there are three types of repositories, see section 7.1 Recording Repositories. The following sections explain how to either manually or automatically archive from any source repository to a specific target repository. In summary:

- If you wish to archive to a Total Recall VR archive appliance, read the sections explaining how to archive to a Web Repository.

- If you wish to archive to a repository using a network file system and a database server, read the sections explaining how to archive to a Network Repository.
- If you wish to archive to a portable drive, usually a USB drive, then read the sections that explain how to archive to a Portable Repository

12.1. House Keeper vs Archiver

The operation of the “Media Repository House Keeper” service may have an undesirable impact on manual and automatic archiving.

As we explained in the previous section, the “Media Repository House Keeper” service automatically manages the space in the recording (media) repository. It automatically starts deleting recordings to free space in the repository for new recordings when the database occupancy or the file store occupancy reaches configurable limits.

The house keeper when auto cleaning is much faster than all types of archivers when archiving, manual or automatic. As a result, auto-cleaning may delete recordings while archiving is in progress. Consequently, in some cases:

- Recordings that should have been (or you expected them to be) archived may not be archived simply because they were auto-cleaned (deleted) just before the archiver got to them or,
- Archiving may fail while trying to archive a recording that is auto-cleaned simultaneously. In this case, the archiver will fail, not the house keeper, as archiving is considered secondary to auto cleaning, which frees space for new recordings.

The undesirable outcomes are more likely to happen if you start archiving the oldest recordings in the repository, the repository is at capacity (that is, it is full), and the auto cleaning is about to start or is in progress.

To avoid undesirable outcomes, you may have to stop the “Media Repository House Keeper” service and keep it inactive while manually archiving the oldest recordings in the repository.

Further, always start automatic archiving as soon as you start recording. With time, this will ensure that the auto cleaner works on the oldest recordings while the auto archiver works on the youngest recordings.

12.2. Manual Archiving to a Network Repository

Network Repositories are repositories with direct network access to both the file system with recording files and the database with metadata for the recordings, see section 7.1.2 Network Repository.

To archive to a Network Repository, you must create one first. To do so, you will need:

- A database on a supported database server (Derby, H2, MariaDB, PostgreSQL or Microsoft SQL).
- A user that can access the database over the network, create tables, indices and other database structures, and add to, remove from and update records in the tables.
- A file system with network access via the NFS or CIFS protocol.

Based on the database server, you may need to create a database and a database user before using it as a repository database. The same rules apply to using different database servers for the configuration database for Total Recall VR Cockpit, see section 3.6 Application Configuration Database.

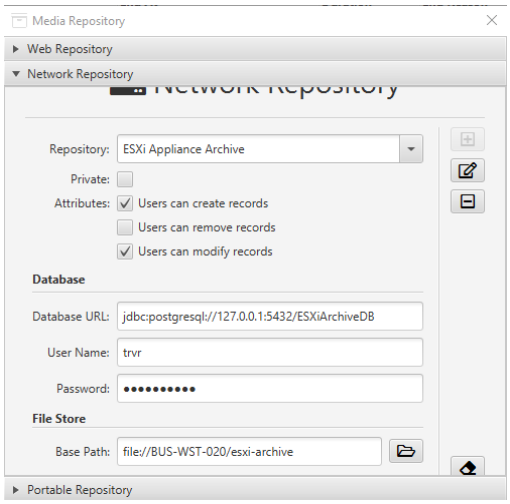
DO NOT use the same database, nor the same network file system, for multiple Network Repositories. Use a different database and network file system for each Network Repository.

Total Recall VR Cockpit must be able to access the database and the file system over your network.

Once you have all of the above ready, you will need the following information to configure archiving:

- The JDBC URL that specifies the location and name of the database.
- The user name and password of the database user that can access the database.
- The network path of the network file system location, for example a UNC path to a Windows share.

Armed with all of the above information, you can proceed to configure a Network Repository record in the Explorer view, for example:



In this example, we named the Network Repository "ESXi Appliance Archive". Note that we left ***Private*** unticked. As a result, all Total Recall VR Cockpit users who have permission to use the **Share** tool can archive to this repository.

Further, note the ***Attributes***; in particular, we ticked the *Users can create records* attribute. Adding recordings to the repository will only be possible if this attribute is set.

Next, note the value of the ***Database URL***. The URL structure will change based on the database server you are using and the database name you created. In addition, the ***User Name*** and ***Password*** in the Database section of the form must be set to the credentials of the user that can access the database.

Finally, note that we used the path to the network file system as a value for the ***Directory***.

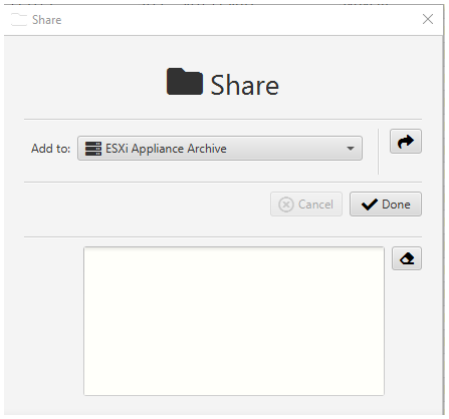
With this entry in place, you can manually archive recordings and related metadata from any other repository to the Network Repository. To do so (assuming the Explorer view is the active view):

Manually archive to a Network Repository

1. Choose the source repository with the ***Exploring*** selector. Typically, this will be the repository on your recorder appliance. However, it can be any other repository. The recording browser will show the latest recordings in the repository.
2. Decide which recordings you wish to archive. To do this, you may have to choose a ***Display Filter*** and choose the context for the **Share** tool with the ***Act on*** selector.

   For example, to archive all recordings in the source repository, clear ***Display Filter*** and set ***Act on*** to *All*. Alternatively, to archive only the recordings that match a filter, set ***Display Filter*** to the desired filter and then set ***Act on*** to *Filtered*.
3. Select **Share** to start the recording and metadata transfer tool.

4. On the Share form, set ***Add to*** to the name of the target Network Repository that you created earlier, for example:



5. Select ↱ to archive. This may take some time to complete.

To access the archived recordings in the target Network Repository, choose the target repository with the ***Exploring*** selector.

12.3. Manual Archiving to a Portable Repository

Portable Repositories are repositories with direct local file system access to both the recording files and the database with metadata for the recordings, see section 7.1.3 Portable Repository.

Typically, this is a repository on a removable disk, such as a USB disk, or a directory on the local disk.

You can use any local directory as a Portable Repository.

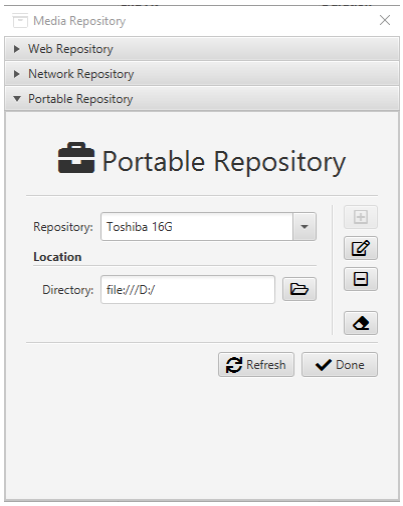
However, we recommend using an empty directory if the directory has not been used as a Portable Repository before.

While it is technically possible to use a network file system location (directory) for a Portable Repository, please avoid placing Portable Repositories on network file systems where multiple users can access them simultaneously from different Total Recall VR Cockpit instances. Portable Repositories are designed to be used by one application user from one application instance at a time.

The database of a Portable Repository may be damaged if multiple users access the repository simultaneously from different instances of Total Recall VR Cockpit.

To archive to a Portable Repository, you must create one first. You will need an empty directory on a local drive or a blank USB disk to do so.

Once you have all of the above ready, you can proceed to configure a Portable Repository record in the Explorer view, for example:



In this example, we are using a blank USB thumb drive attached to the device (Windows PC, in this case) running the Total Recall VR Cockpit instance that we will use to perform the archiving. We can access the thumb drive via the D: drive (which was allocated by Windows in this case). We named the Network Repository "Toshiba 16G".

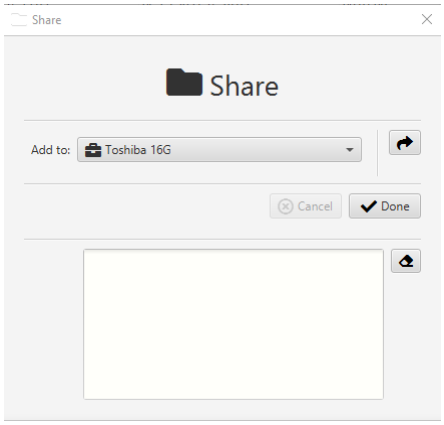
With this entry in place, you can manually archive recordings and related metadata from any other repository to the Portable Repository. To do so (assuming the Explorer view is the active view):

Manually archive to a Portable Repository

1. Choose the source repository with the ***Exploring*** selector. Typically, this will be the repository on your recorder appliance, but theoretically, it can be any other repository. The recording browser will show the latest recordings in the repository.
2. Decide which recordings you wish to archive. To do this, you may have to choose a ***Display Filter*** and choose the context for the **Share** tool with the ***Act on*** selector.

For example, to archive all recordings in the source repository, clear ***Display Filter*** and set ***Act on*** to *All*. Alternatively, to archive only the recordings that match a filter, set ***Display Filter*** to the desired filter and then set ***Act on*** to *Filtered*.

3. Select **Share** to start the recording and metadata transfer tool.
4. On the Share form, set ***Add to*** to the name of the target Portable Repository that you created earlier, for example:



5. Select to archive. This may take some time to complete.

To access the archived recordings in the target Portable Repository, choose the target repository with the ***Exploring*** selector.

12.4. Automatic Archiving to a Web Repository

You can configure all Total Recall VR appliance recorders to archive to a Web Repository automatically.

Web Repositories provide a REST interface to access both the recording files and the metadata for the recordings, see section 7.1.1 Web Repository.

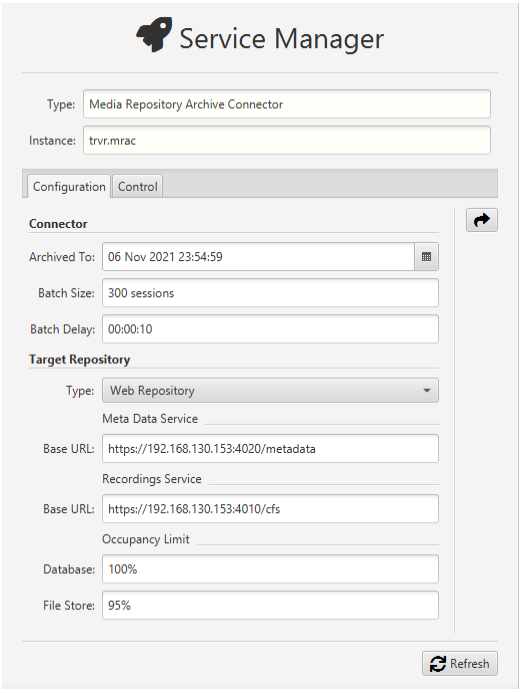
To archive to a Web Repository, purchase a Total Recall VR archive appliance or create your own custom Total Recall VR archive node.

Once you have all of the above ready, you will need the following information to configure archiving:

- The base REST URL of the “Meta Data REST Service”.
- The base REST URL of the “Recordings REST Service”.

Armed with all the above information, you can configure automatic archiving to a Web Repository on your Total Recall VR appliance recorder.

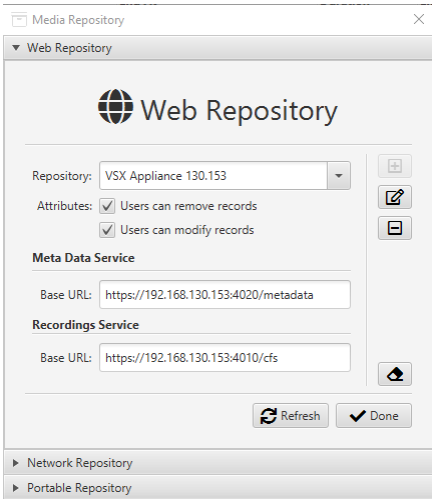
Configure the “Media Repository Archive Connector” with a Target Repository that is a Web Repository, see section 10.13 Service Configuration – Media Repository Archive Connector, for example:



Note the ***Base URL*** for the Meta Data Service and the Recordings Service. These are the base REST URLs for the "Meta Data REST Service" and the "Recordings REST Service", respectively, from the configuration of the archive appliance.

You can restart the "Media Repository Archive Connector" service with the above configurations. It will start archiving recordings to the Web Repository immediately.

You can access the archived recordings immediately, as archiving is in progress. To do so, you need to create a Web Repository record in the Explorer view, for example:



12.5. Automatic Archiving to a Network Repository

You can configure all Total Recall VR appliance recorders to archive to a Network Repository automatically.

Network Repositories are repositories with direct network access to both the file system with recording files and the database with metadata for the recordings, see section 7.1.2 Network Repository.

To archive to a Network Repository, you must create one first. To do so, you will need:

- A database on a supported database server (Derby, H2, MariaDB, PostgreSQL or Microsoft SQL).
- A user that can access the database over the network, create tables, indices and other database structures, and add to, remove from and update records in the tables.
- A file system with network access via the NFS or CIFS protocol.

Based on the database server, you may need to create a database and a database user before using it as a repository database. The same rules apply to using different database servers for the configuration database for Total Recall VR Cockpit, see section 3.6 Application Configuration Database.

DO NOT use the same database, nor the same network file system, for multiple Network Repositories. Use a different database and network file system for each Network Repository.

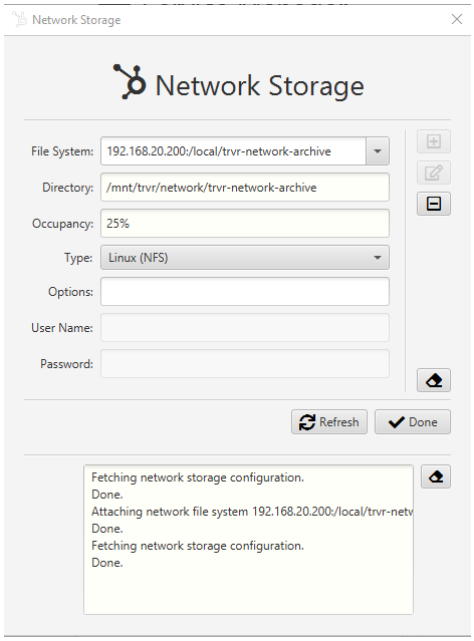
The Total Recall VR recording appliance and at least one Total Recall VR Cockpit instance must be able to access the database and the file system over your network.

Once you have all of the above ready, you will need the following information to configure automatic archiving on your Total Recall VR appliance recorder:

- The JDBC URL that specifies the location and name of the database.
- The user name and password of the database user that can access the database.
- The network path of the network file system location, for example a UNC path to a Windows share.

Armed with all the above information, you can configure automatic archiving to a Network Repository on your Total Recall VR appliance recorder.

Start by configuring access to the network file system from your Total Recall VR appliance recorder. Use the Network Storage tool in the System Manager to do this, see section 11.3 System Configuration – Network Storage, for example:

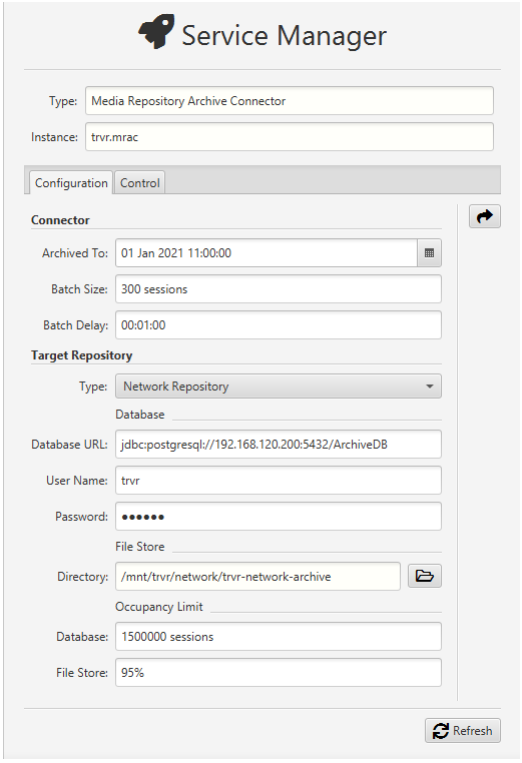


As you may have noticed, in this example, we are using a file system with NFS access on a server with an IP address of 192.168.20.200. Similarly, you can configure a file system with CIFS access (a Windows share). Note that the recording services on the Total Recall VR appliance recorder can access this file system via the following path:

```
/mnt/trvr/network/trvr-network-archive
```

This is important as this is the path that we will use next.

Then proceed to configure the “Media Repository Archive Connector” with a Target Repository that is a Network Repository, see section 10.13 Service Configuration – Media Repository Archive Connector, for example:

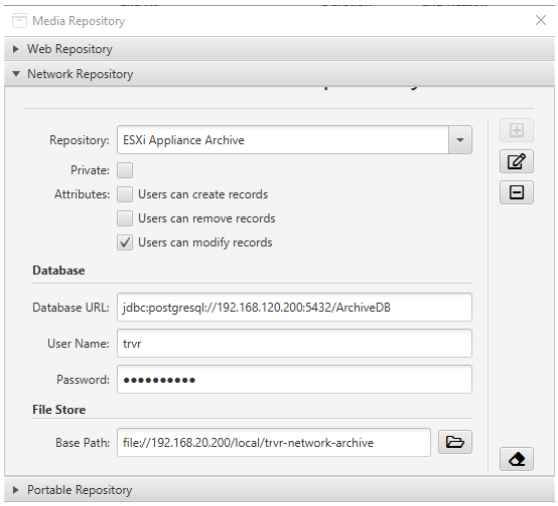


First, note that we selected the path to the network file system we created earlier as a value for the ***Directory***. This tells the service to write recording files to the network file system.

Second, note the value of the ***Database URL***. The URL structure will change based on the database server you are using and the name of the database you created. In addition, the ***User Name*** and ***Password*** in the Database section of the form must be set to the credentials of the user that can access the database.

You can restart the “Media Repository Archive Connector” service with the above configurations. It will start archiving recordings to the Network Repository immediately.

You can access the archived recordings immediately, as archiving is in progress. To do so, you need to create a Network Repository record in the Explorer view, for example, and assume that the device that is running the Total Recall VR Cockpit instance has the same network access to the database and the network file system as your Total Recall VR appliance recorder:



Note that the devices that run Total Recall VR Cockpit instances may have different network access to the repository's database (less likely) and filesystem (very likely) than the Total Recall VR recorder appliance. If so, you must adjust the configuration of the Network Repository record in the Explorer view accordingly.

Also, in our example, we use a file system with NFS access. To access such a file system from Total Recall VR Cockpit, you may need to install an NFS client on the device used to run the Total Recall VR Cockpit instance.

12.6. Automatic Archiving to a Portable Repository

As an alternative to the recommended method of archiving to a Network Repository, see section 12.5 Automatic Archiving to a Network Repository, you can configure your Total Recall VR appliance recorder to archive to a Portable Repository automatically.

Portable Repositories are repositories with direct local file system access to both the recording files and the database with metadata for the recordings, see section 7.1.3 Portable Repository.

Typically, this is a repository on a removable disk, such as a USB disk, directly attached to your Total Recall VR appliance recorder.

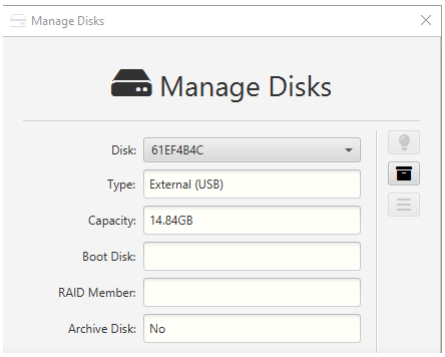
Generally, you can use any USB disk that you can attach to your Total Recall VR appliance recorder, however:

- Prefer brand new and unused disks.
- Prefer USB 3.1 or USB 3.0 disks. Avoid USB 2.0 disks at all costs.
- Disks with less than 128GiB capacity are unlikely to have enough capacity for a Portable Repository with the maximum allowed occupancy. At the same time, much space may be wasted on disks with more than 500GiB. This, of course, depends on the length of your recordings; shorter recordings have smaller file sizes, while longer ones have larger file sizes.

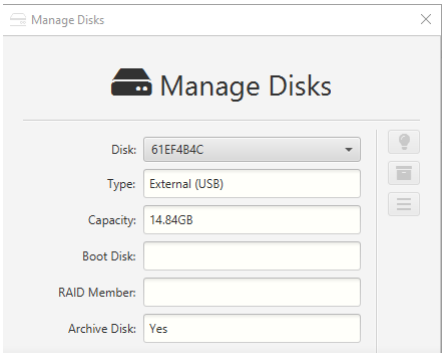
USB disks, in particular thumb drives, generally come preformatted with an NTFS file system, and as a result, they can be used straight out of the box. However, you can use unformatted disks and disks with a FAT32 and an exFAT file system.

The first thing that you need to do is to physically connect a disk to your Total Recall VR appliance recorder.

Next, attach the disk as an archive disk to the Total Recall VR appliance recorder. Use the Manage Disks tool in the System Manager to do this, see section 11.8 System Tools – Manage Disks. If the tool does not recognise the disk as present, select to force the tool to rescan and reload the disks. The tool will show the newly attached disk, for example, if the disk is a USB disk:

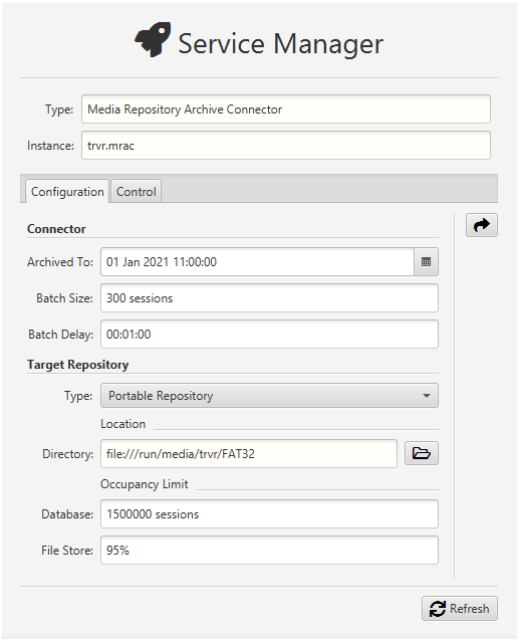


Note the value of the ***Archive Disk***. It is set to *No*, indicating that the disk is not ready to be used as a Portable Repository, select to configure it so it can be used as a Portable Repository. For example, if successful:



Note the value of the ***Archive Disk***. It is set to *Yes* now, indicating that the disk is ready to be used as a Portable Repository.

Then proceed to configure the “Media Repository Archive Connector” with a Target Repository that is a Portable Repository, see section 10.13 Service Configuration – Media Repository Archive Connector, for example:

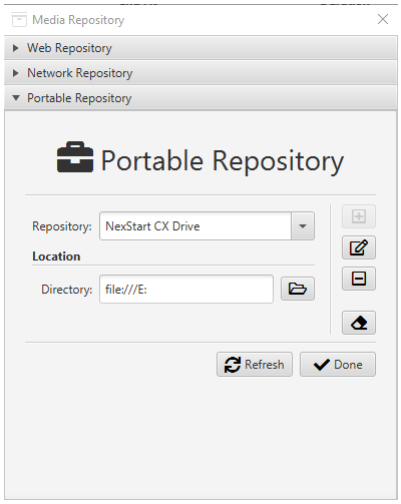


Note that we used 🗁 to select the path that was assigned by the system to the disk and set it as the value for ***Directory***.

You can restart the "Media Repository Archive Connector" service with the above configurations. It will start archiving recordings to the Network Repository immediately.

Unlike automatic archiving to a Network Repository, see section 12.5 Automatic Archiving to a Network Repository, it is not possible to access the archived recordings in the Portable Repository until you physically detach the disk from the Total Recall VR appliance recorder. Of course, this happens only after you stop archiving to the disk. Typically, you will replace the disk when the Portable Repository is full. For instructions on how to do this see section 11.8 System Tools – Manage Disks.

Once you have a disk with a Portable Repository on it, you can access the recordings in the repository by first attaching the disk to a device that runs an instance of Total Recall VR Cockpit and then creating a Portable Repository record in the Explorer view for example:


Media Repository
Web Repository
Network Repository
Portable Repository
Portable Repository
Repository:
NexStart CX Drive
Location
Directory:
file:///E:
Refresh
Done

13. Auditing

The Auditor view of Total Recall VR Cockpit has a built-in browser for audit events stored in audit repositories (also known as audit logs). The browser has a suite of event management and productivity tools that work on audit events.

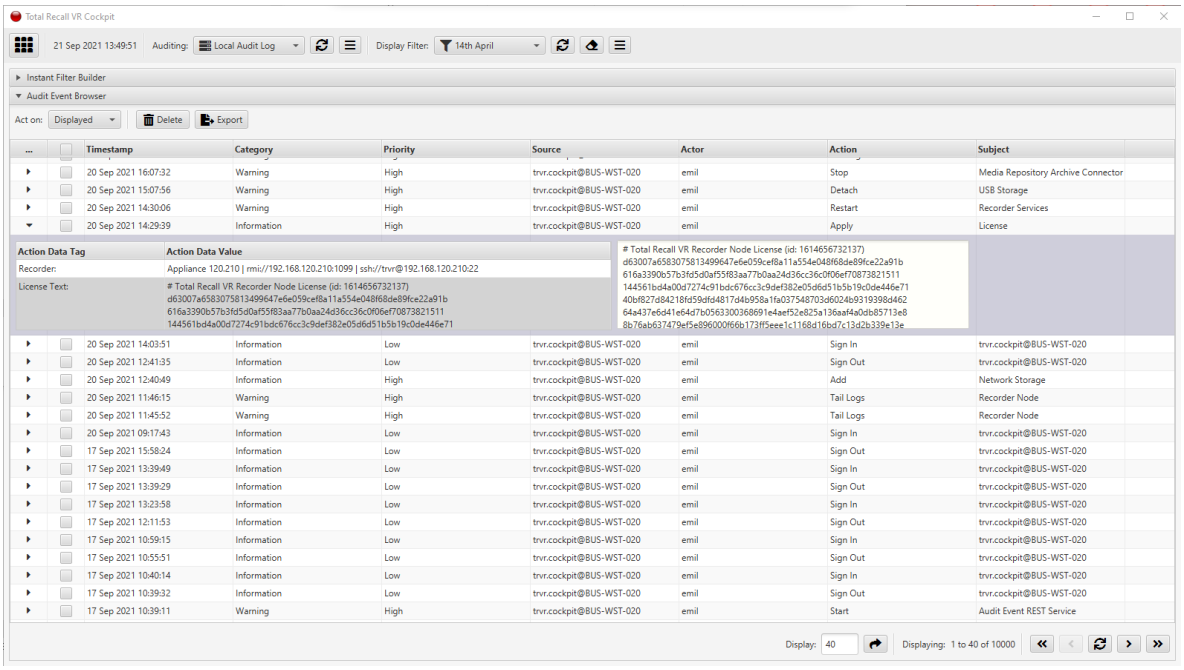


Figure 20: Audit Event Browser – Auditor View

The following sections explain how to use the audit event browser and the audit event management and productivity tools.

13.1. Audit Repositories

Each Total Recall VR audit repository (or audit log) is a collection of audit events stored in a database.

Typically, a repository has one location, which can be:

- An appliance or a custom recorder.
- An appliance or a custom audit device.
- A database that is accessible over the network.

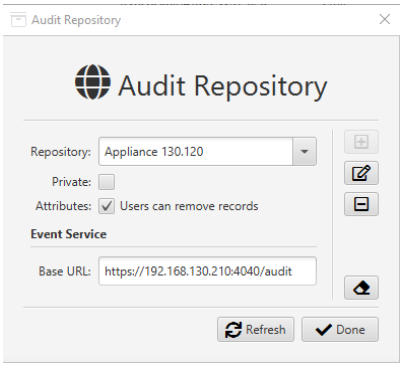
Total Recall VR Cockpit can use one of the following access mechanisms to access the audit events in a given repository:

- REST interface.
- Direct network (JDBC) access to the database with audit events.

While in some cases, it may be possible to access a repository via multiple access mechanisms, for example, REST and direct network access to the database with audit events, we recommend that you pick one method and stick with it in such cases. In such cases, the REST method should be preferred over the direct network access method.

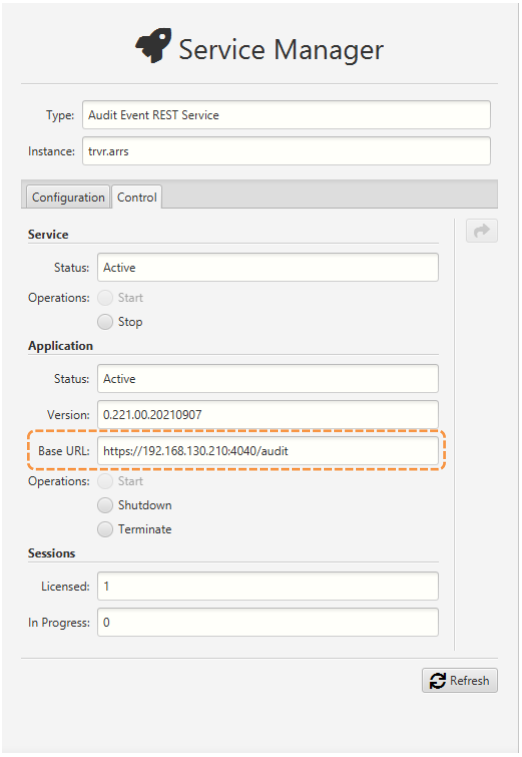
You can manage the records for the repositories that Total Recall VR Cockpit can access by selecting ☰, located next to the ***Auditing*** selector on the application menu bar.

It will display the Audit Repository form, which you can use to manage repository records with REST access, as shown in the following screen captures.



Repositories located on appliance and custom recorders and appliance and custom recording audit devices provide the REST interface via the “Audit Event REST Service”.

To configure an Audit Repository, you need the base REST URL for the service. You can get the base URLs from the service runtime status, for example:



Audit repositories with direct network (JDBC) access to the database with audit events are used exclusively by Total Recall VR Cockpit as private audit logs. Suppose a Total Recall VR Cockpit instance is configured to use a private audit log, see section 3.10.3 Audit Log. In that case, it will automatically add a Local Audit Log entry to the Auditing selector. Choose this entry to access the audit events in the private audit log.

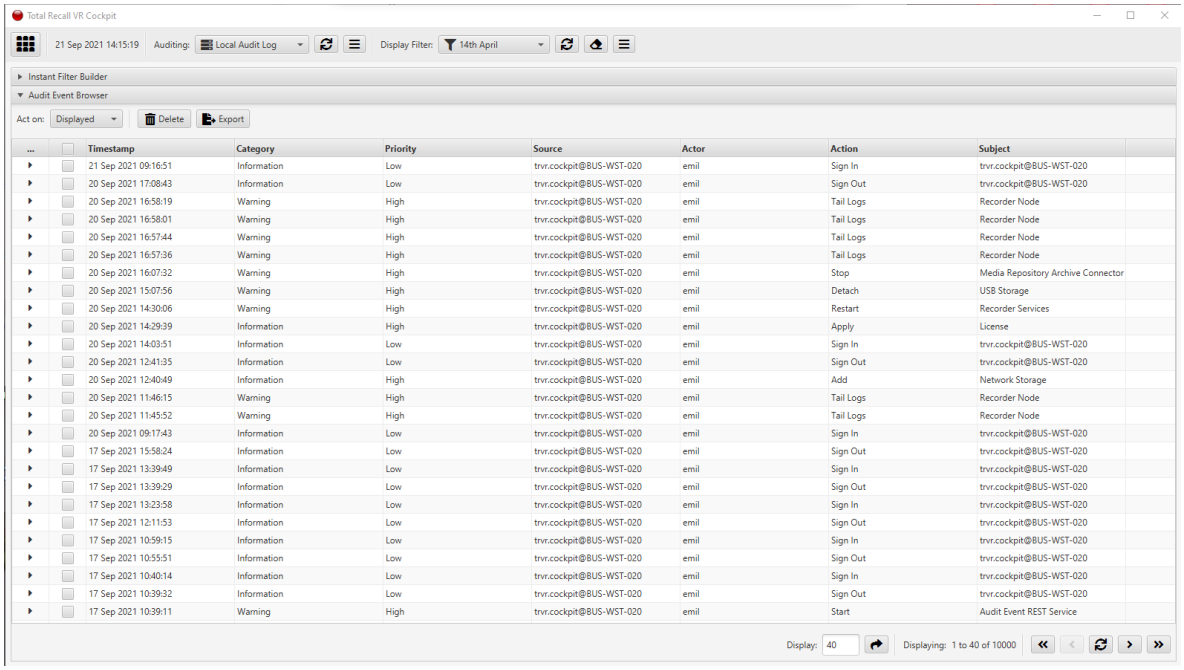
13.2. Audit Browser

The audit browser provides a table-like view of the audit events in the selected repository.

You can choose a repository to audit via the ***Auditing*** selector on the application menu bar. In addition, and optionally, you can choose a display filter for audit events via the ***Display Filter*** selector that is also located on the application menu bar.

If you need to configure a new repository record or update an existing one, please see section 13.1 Audit Repositories. If you need to configure a new display filter or update an existing one, please see section 6.5 Advanced Filter Builder – Audit Events.

Once you select a repository, and if Total Recall VR Cockpit can access it, Total Recall VR Cockpit will display the data of the most recent audit events that are in the repository in a tabular form.



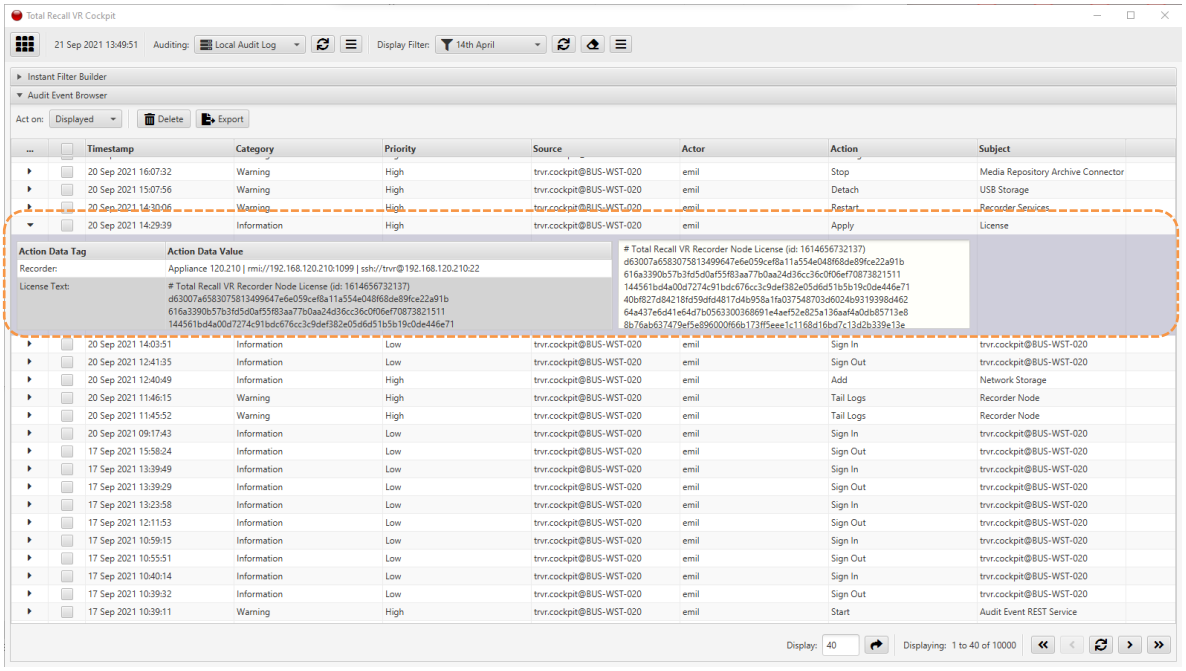
If you select a display filter as well, then Total Recall VR Cockpit will use that filter while accessing the audit events in the repository and show only records that pass the filter.

The value in the ***Display*** field specifies the number of audit events that should appear in the table (also known as the page size), for example, 40 in the previous screen capture. To change the number of records that appear in the table (or the page size), simply set ***Display*** and then select ↱.

Use the following controls to navigate through the audit events in the repository:

Control	***Description***
«	Displays the most recent audit events in the repository, also known as the first page of events.
‹	Displays the previous page of audit events – moving forward in time.
⟳	Refreshes the audit events that are shown.
›	Displays the previous page of audit events – moving backward in time.
»	Displays the oldest audit events in the repository, the last page of events.

Select ▸, which appears in the first column of the row that shows the data for an audit event, to display additional information on the event.



Select ▼ in the same row to hide the additional information.

Finally, you can access several management and productivity tools via the controls above the table showing the audit events.

The ***Act on*** selector defines the operating context for the management and productivity tools. The active context can be one of the following:

1. *Selected* (default value) - The tools will operate on the selected audit.
2. *Displayed* - The tools will operate on the displayed audit events. You may have to scroll up and down to see all audit events that the tool will operate on.
3. *Filtered* (use with caution) - The tools will operate on all audit events in the repository that match the selected display filter.
4. *All* (use with caution) - The tools will operate on all the audit events in the repository.

Use *Filtered* and *All* with caution, as you may unexpectedly apply the tool to audit events without intending to do so.

The following management and productivity tools are available:

Tool	*Description*
Delete	Deletion tool. Use with caution to delete audit events. If ***Act on*** is set to *All*, it will delete all audit events from the repository. The action is not reversible.
Export	Audit event export tool. Exports audit events in several standard formats (XML, JSON, PDF, etc.).

When started via the above controls, the tools may use a form to gather further information that will be used while the tools are running. For more details on using forms, please see section 4.6 Forms.

14. Software License

END USER LICENSE AGREEMENT

THIS SOFTWARE END USER LICENSE AGREEMENT ("EULA") IS A LEGAL AGREEMENT BETWEEN YOU (EITHER AN INDIVIDUAL OR, IF PURCHASED OR ACQUIRED BY OR FOR AN ENTITY, AN ENTITY) AND PROLANCER PTY LTD. IT PROVIDES A LICENSE TO USE THIS SOFTWARE AND CONTAINS WARRANTY INFORMATION AND LIABILITY DISCLAIMERS. BY DOWNLOADING, INSTALLING OR USING THE SOFTWARE YOU ARE INDICATING YOUR ASSENT TO THE TERMS OF THIS LICENSE. IF YOU DO NOT AGREE TO ALL OF THE FOLLOWING TERMS, DO NOT DOWNLOAD OR INSTALL THE SOFTWARE, DISCONTINUE ITS USE IMMEDIATELY AND DESTROY ALL COPIES IN YOUR POSSESSION.

1. DEFINITIONS
a) "Prolancer" means Prolancer Pty Ltd, an Australian company with ACN 115 942 357.
b) "Software" means the executable code, additional tools, libraries, source files, header files, data files, any updates or error corrections provided by Prolancer, user manuals, guides, printed materials, and online or electronic documentation.
c) "License Key" means a serial number issued to you by Prolancer to activate and use the Software.
d) "Maintenance Plan" is a time-limited right to technical support and Software updates and upgrades. Technical support only covers issues or questions resulting directly from the operation of the Software. Prolancer will not provide you with generic consultation, assistance, or advice under any other circumstances.

2. LICENSE GRANTS
2.1 This Software is licensed, not sold.
2.2 Trial Period License. Prolancer may grant You a free, node-locked, limited, non-exclusive, non-transferable, non-renewable license to copy and use the Software for evaluation purposes only and not for any commercial use. At Prolancer's discretion, Prolancer may provide limited support through email or discussion forums on Prolancer’s website. The evaluation copy of the Software contains a feature that will automatically disable the Software at the end of the Trial Period. Prolancer will have no liability to you if this feature disables the Software.
2.3 License After Trial Period. During the Trial Period, you can pay a license fee to use the Software after its expiration. Upon your payment of the license fee, Prolancer provides you with a permanent registration number ("License key") and grants you a node-locked, limited, non-exclusive, non-transferable license to:
a) use the Software on a commercial basis.
c) copy the Software in machine-readable form solely for archival and backup purposes.

3. LICENSE RESTRICTIONS
3.1 You shall undertake any necessary steps to protect the License Key against unauthorised use.
3.2 You may not alter, merge, modify, adapt or translate the Software, or decompile, reverse engineer, disassemble, or otherwise reduce the Software to a human-perceivable form.
3.3 You may not sell, rent, lease, sublicense, transfer, or resell for profit or otherwise distribute the Software or any part thereof.
3.4 You may not modify the Software or create derivative works based upon the Software.
3.5 You may not decompile, disassemble or reverse engineer the Software.
3.6 You may not remove or obscure any copyright and trademark notices relating to the Software.

4. USE OF LICENSING FUNCTIONALITY
4.1 If you have licensed a qualifying edition of the Software, you may use the functionality labelled "Licensing" solely to apply the Licensing functionality processes and/or restrictions to your products and distribute such products to your end users for their trial purposes for a predetermined period of time. To avoid doubt, the preceding limitations apply only to your use of the Licensing functionality and not your use of the Software in general.
4.2 You may not use or apply the Licensing functionality to benefit any software products you do not own.

5. OWNERSHIP AND INTELLECTUAL PROPERTY RIGHTS
5.1 This Agreement gives you limited rights to use the Software. Prolancer retains all rights, title and interest in and to the Software and all copies thereof, including copyrights, patents, trade secret rights, trademarks and other intellectual property rights. All rights not explicitly granted in this Agreement, including International

Copyrights, are reserved by Prolancer. The Software's structure, organisation and code are valuable trade secrets and confidential information of Prolancer.

6. LIMITATION OF LIABILITY
6.1 Prolancer's cumulative liability to You or any other party for any loss or damages resulting from any claims, demands, or actions arising out of or relating to this Agreement shall not exceed the license fee paid to Prolancer for use of the Software.
6.2 Prolancer shall be relieved of any obligations for any portions of the software that are revised, changed, modified, or maintained by anyone other than Prolancer.

7. PATENT AND COPYRIGHT INDEMNITY
7.1 Prolancer represents and warrants that the Software shall not infringe or misappropriate any copyrights, patents, trade secret rights, trademarks and other intellectual property rights.
7.2 In the event the Software is found to infringe, Prolancer will have the option, at its expense, to
a) modify the Software to cause it to become non-infringing;
b) substitute the Software with other Software reasonably suitable to You, or
c) if none of the preceding remedies are commercially feasible, terminate the license for the infringing Software and refund any license fees paid for the Software.
7.3 Prolancer will have no liability for any claim of infringement based on
a) code contained within the Software which Prolancer did not create;
b) use of a superseded or altered release of the Software, except for such alteration(s) or modification(s) which have been made by Prolancer or under Prolancer's direction, if such infringement would have been avoided by the use of a current, unaltered release of the Software that Prolancer provides to You, or
c) the combination, operation, or use of any Software furnished under this Agreement with programs or data not furnished by Prolancer if such infringement would have been avoided by the use of the Software without such programs or data.

8. LIMITED WARRANTIES
8.1 THE SOFTWARE IS PROVIDED ON AN "AS IS" BASIS. PROLANCER MAKES NO WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTY OR MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. WITHOUT LIMITATION, YOU ASSUME SOLE RESPONSIBILITY FOR SELECTING THE SOFTWARE TO ACHIEVE YOUR INTENDED RESULTS AND FOR THE INSTALLATION, USE AND RESULTS OBTAINED FROM THE SOFTWARE. PROLANCER MAKES NO WARRANTY THAT THE SOFTWARE WILL BE ERROR-FREE OR FREE FROM INTERRUPTIONS OR OTHER FAILURES. IN PARTICULAR, THE SOFTWARE IS NOT DESIGNED FOR USE IN HAZARDOUS ENVIRONMENTS REQUIRING FAIL-SAFE PERFORMANCE. PROLANCER EXPRESSLY DISCLAIMS ANY WARRANTY OF FITNESS FOR HIGH-RISK ACTIVITIES.
8.2 Prolancer warrants that it holds the proper rights allowing it to license the Software and is not currently aware of any actions that may affect its rights to do so.
8.3 Prolancer cannot guarantee that the Software will work at all times. If you change your operating system, the software may not work anymore. You acknowledge and agree that such changes are fair and reasonable.
8.4 You should ensure it is legal to use the Software in your country or jurisdiction. Prolancer only provides a license for You to use the software. It is Your responsibility to ensure you are allowed to use the Software.
8.5 Prolancer reserves the right at any time to cease the support of the Software and to alter the prices, features, specifications, capabilities, functions prospectively, licensing terms, release dates, general availability or other characteristics of the Software.

9. MAINTENANCE PLAN
9.1 At any time before the expiration of your Maintenance Plan and 14 days after, you may purchase an extension to the current Maintenance Plan. This additional Maintenance Plan will extend the availability of your current Maintenance Plan for a period beginning with the date when your Maintenance Plan expires.
9.2 For a limited time after the expiration of your Maintenance Plan, you may purchase a renewal of your Maintenance Plan. This will provide you with a new Maintenance Plan that will begin when the renewal is purchased.
9.3 If you do not purchase any additional Maintenance Plan, you will still have the right to use the existing Software. Still, you will lose the right to technical support and Software updates and upgrades as of the date your current Maintenance Plan expires.
9.4 A Maintenance Plan must be purchased for customers who purchase or already own multiple licenses.

9.5 Technical support is provided via electronic mail at the address specified on the website. Prolancer will use its best efforts to provide you with technical support within forty-eight (48) business hours of your request. Please check our website to find our latest contact information.

10. SUPPORT
10.1 Except as provided herein, support for the Software is provided to you free of charge while your current Maintenance Plan is valid. If Prolancer discontinues any version of the Software, Prolancer reserves the right to limit or cease product support and updates for such discontinued version. Prolancer reserves the right to discontinue free support with thirty (30) days written notice posted to the Prolancer or the Software website.

11. INTERNET-BASED SERVICES
11.1 Consent for Internet-Based Services. Certain Software features connect to Prolancer or service provider computer systems over the Internet. Sometimes, you will not receive a separate notice when they connect. You may switch off these features or not use them. BY USING THESE FEATURES, YOU CONSENT TO THE TRANSMISSION OF THIS INFORMATION. Prolancer does not use the information to identify or contact you. For more information, see Prolancer’s Privacy Policy on Prolancer’s website.
11.2 Computer Information. The Software features use Internet protocols, which send to the appropriate systems computer information, such as your Internet protocol address, the operating system type, browser name and version of the software you are using, and the language code of the device where you installed the software. Prolancer uses this information to make Internet-based services available to you.
11.3 Customer Experience Improvement Program (CEIP). The Software may use CEIP, which automatically sends Prolancer anonymous information about your hardware and how you use this software. We may use the computer information and CEIP information to improve our software and services. We may also share it with others, such as hardware and software vendors. They may use the information to improve how their products run with Prolancer software.

12. HIGH-RISK ACTIVITIES
12.1 The Software is not fault-tolerant and is not designed, manufactured or intended for use or resale as on-line control equipment in hazardous environments requiring fail-safe performance, such as in the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control, direct life support machines, or weapons systems, in which the failure of the Software could lead directly to death, personal injury, or severe physical or environmental damage ("High-Risk Activities"). Prolancer and its suppliers specifically disclaim any express or implied warranty of fitness for High-Risk Activities.

13. THIRD PARTY SITES AND SOFTWARE
13.1 The Software may direct you to third-party Web sites. Prolancer does not control, endorse, or guarantee content, including software, data or other information on such third-party sites. You agree that Prolancer is not responsible for any content, associated links, resources, or services associated with a third-party site. You further agree that Prolancer shall not be liable for any loss or damage of any sort associated with your use of third-party content. Access to these sites is provided for your convenience only.
13.2 The Software may contain third-party software. By accepting this EULA, You are also accepting the additional terms and conditions concerning such software, if any, forth herein.

14. AUDIT RIGHTS
14.1 Prolancer may audit your use of the Software to verify compliance with this Agreement. The Software is configured to enable periodic HTTP communication with Prolancer. License information is transmitted from the Software to Prolancer during this communication to ensure license compliance. The information transmitted during these periodic updates includes the operating system, license serial number, and other relevant information to verify compliance. If you are unwilling to provide this communication capability, you may opt out of ongoing communication, but you will no longer receive Software updates and search engine configuration updates. If the Software's usage is considered out of compliance with this Agreement, the Software may, without notice, cease to function.
14.2 During the audit process, Prolancer has the ability to personally identify the individual who registered with Prolancer to acquire the Software license ("Registrant") through the identification number assigned to your account at the time of registration by using the personal information the Registrant provided to Prolancer during the registration process. Such personal information will only be used by Prolancer in connection with such an audit process.

15. SEVERABILITY

15.1 If any provision hereof shall be held illegal, invalid or unenforceable, in whole or in part, such provision shall be modified to the minimum extent necessary to make it legal, valid and enforceable, and the legality, validity and enforceability of all other provisions of this Agreement shall not be affected.

16. GOVERNING LAW
16.1 This Agreement is to be governed by and construed in accordance with the laws and jurisdiction of the defending party. Service of process upon either party shall be valid if served by registered or certified mail, return receipt requested and to the most current address provided by such party. The United Nations Convention on Contracts for the International Sale of Goods shall not apply to this Agreement.

17. TERMINATION
17.1 Your license to use the Software continues until terminated. This license will terminate automatically if you fail to comply with any term hereof. No notice shall be required from Prolancer to effect such termination. You may also terminate this Agreement at any time by notifying Prolancer in writing of termination. On termination, you must destroy all copies of the Software. Your obligation to pay accrued charges and fees shall survive any termination of this Agreement.

18. ASSIGNMENT
18.1 Neither this Agreement nor any rights granted hereunder may be sold, leased, assigned, or otherwise transferred, in whole or in part, by you, whether voluntary or by operation of law. Any such attempted assignment shall be void and of no effect without the prior written consent of Prolancer.

19. ENTIRE AGREEMENT
19.1 This Agreement contains the entire agreement between Prolancer and You related to the software and supersedes all prior agreements and understandings, whether oral or written. It may be amended only by writing executed by both parties.

[End of Document]