Telex RDC

Documentation for Telex RDC

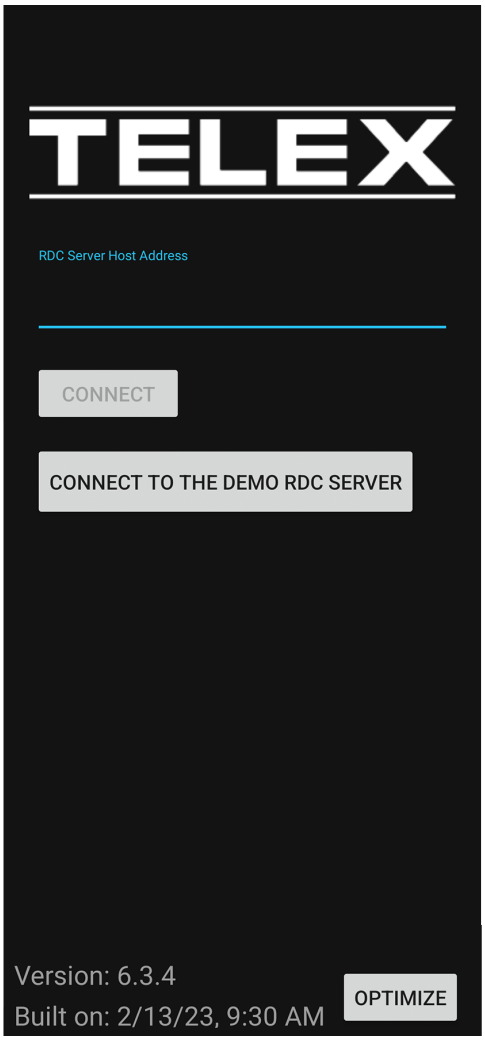
IPC

Table of contents

1. User Guide

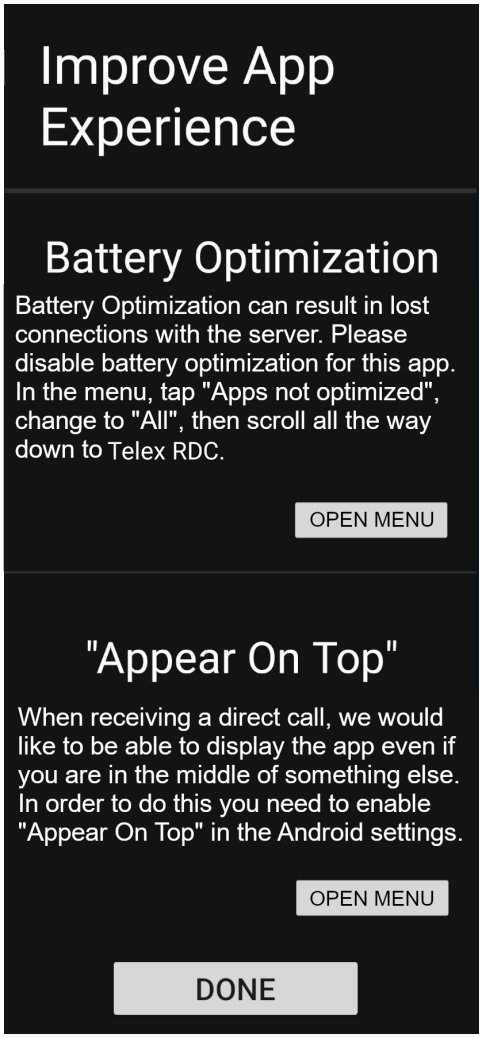
1.1 Android App Installation

1.1.1 Server Host Address



Install Telex RDC from Google Play. When prompted, enter the IP address or Domain Name for your server then press submit.

1.1.2 Optimization



Battery Optimization

Tap the Optimize button in the bottom right corner to access the Improve App Experience menu. Android may have enabled battery optimization for the Telex RDC app by default. Battery optimization can result in lost connections with the server. Tap the OPEN MENU button to access the battery optimization menu in the Android settings and turn off battery optimization for the Telex RDC app.

Appear on Top

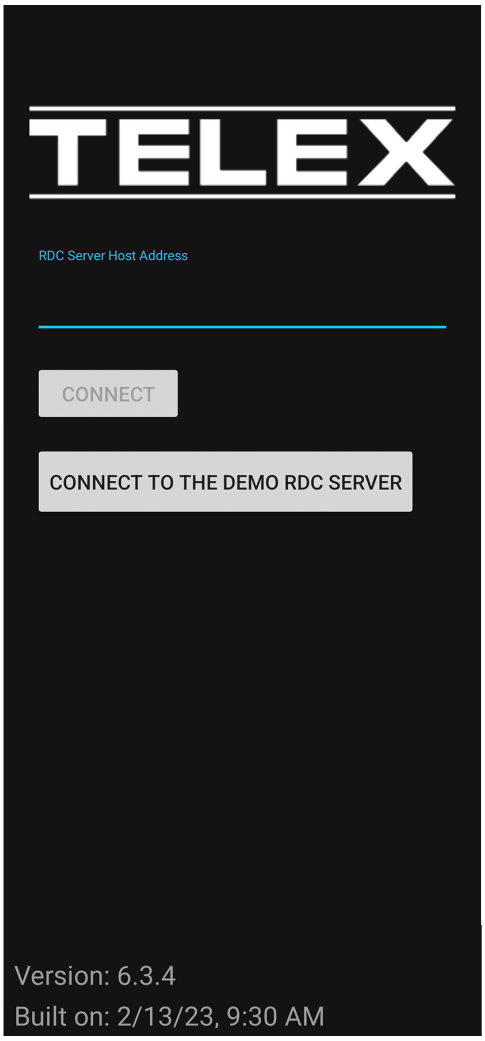
The second optimization option available in this menu is the Appear On Top option. The Appear on Top option allows the Telex RDC app to display itself even if you are in the middle of something else. Tap the OPEN MENU option and enable the Appear On Top option for the Telex RDC app.

Background Notification

The third optimization option is the Background Notification option. The Telex RDC app is obligated to notify you that it is operating in the background. You can hide the notification by tapping the OPEN MENU button and disabling the show notifications option. You will continue to receive other notifications created by the app.

1.2 iOS App Installation

1.2.1 Server Host Address



Install the Telex RDC Client App from the Apple App Store. When prompted, enter the IP address or Host Name for the installed Telex RDC Server given by your System Administrator and select ‘Connect’.

When the IP address or Host Name is blank, the ‘Connect to demo Telex RDC server’ can also be selected. The demo Telex RDC server allows the functionality of one or more Telex RDC Client Apps to be explored but without a connected Radio or C-Soft Console.

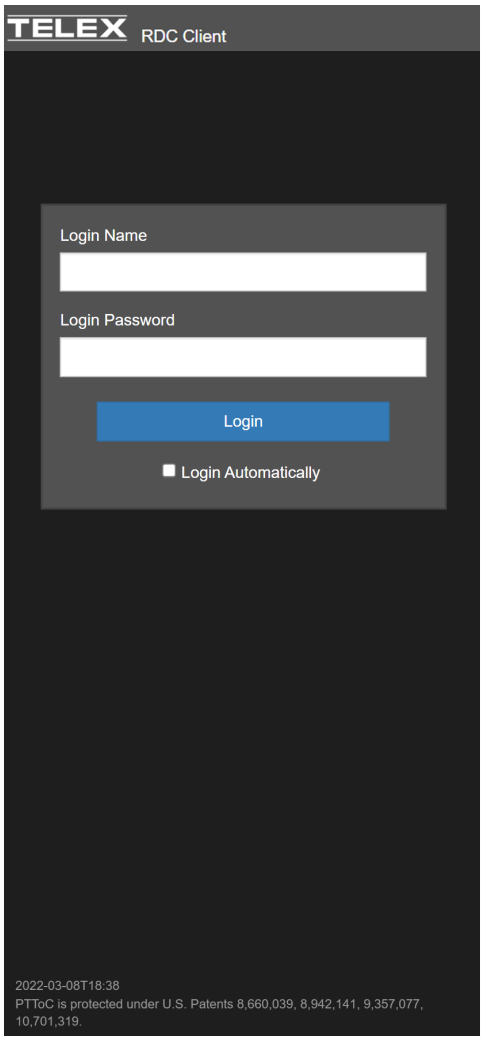
1.2.2 Battery Utilization

Due to restrictions in Apple iOS, the Telex RDC App cannot run in the background on iOS like it can on the Android operating system. Based on criteria beyond the Telex RDC application's control, iOS optimizes battery usage by suspending background

applications without warning, Therefore, the Telex RDC iOS App must always run in the foreground, whether it is active and on screen or inactive and off screen, and maintain a stable audio and data connection to the server. This means that the Telex RDC iOS App will consume noticeably more battery power than the Telex RDC Android App.

1.3 Usage

1.3.1 Logging In



Log in with the default credentials or the credentials you configured in the System Administration. The default users have a Login Name of user01 to user30 and no password. Once connected to the server the App will remain connected whenever there is an available network connection even if the User Interface closed by swiping up. To disconnect from the server the user must select the Logout button from the User Interface.

1.3.2 Group Tab

Telex RDC includes 3 main tabs: Groups, Users, and Recent Calls. The group tab displays a series of buttons called "Selectors." The leftmost text is the Group Name and the rightmost text is the name of the last user to speak on the channel. Selectors will turn white when there is audio on the channel.

Tap the right side of the selector to listen. A green speaker icon will appear to indicate that you are listening to the channel. As long as you are logged in and have the selector listen enabled you will continue to hear audio even if the app is closed and/or the display is off.

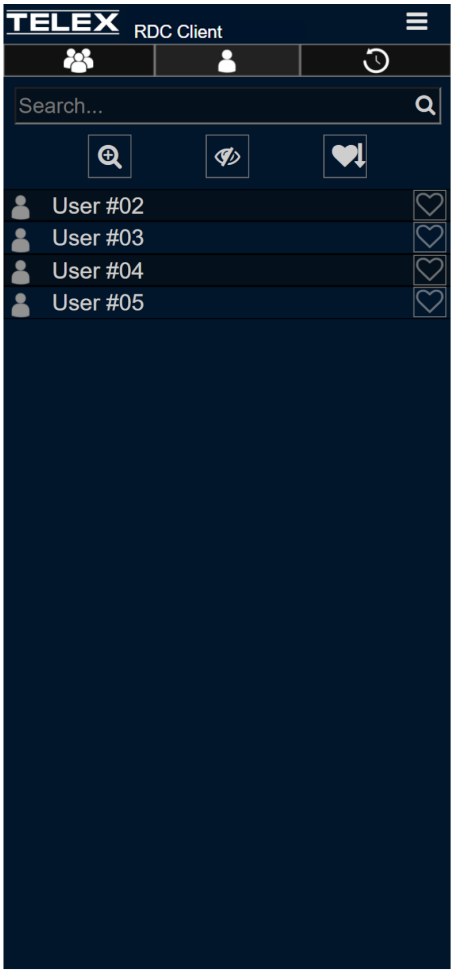
Tap the left side of the selector to enable talking on the channel. A blue microphone icon will appear to indicate that you have enabled talking on the channel. This also enables listening to the channel. Press the red microphone button at the bottom of the screen to talk. If no one on the channel is speaking you will hear a "go-ahead" tone otherwise you will hear a "busy" tone.

Emergency Mode

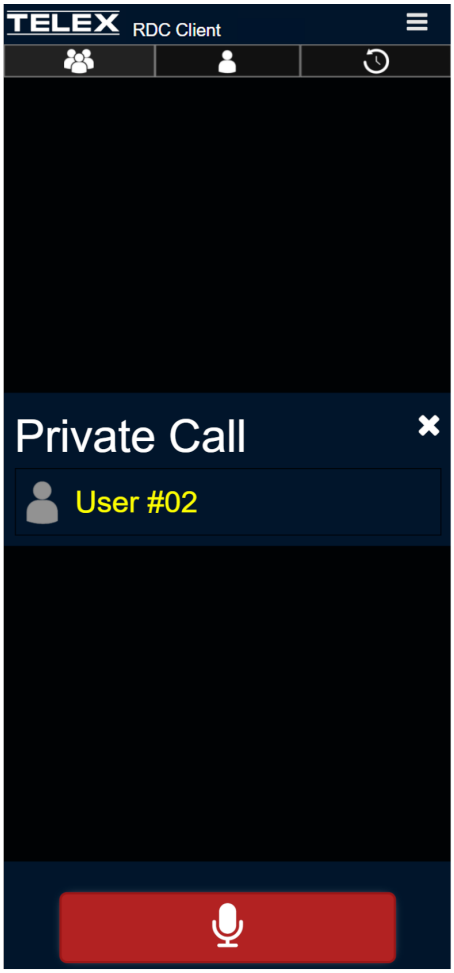
Emergency Mode is activated by pressing and holding the red Emergency Mode button in the top right corner. When Emergency Mode is activated it will declare an emergency on the channel which will result in emergency tones being played on all devices that have this selector assigned as well as on the Radios and the C-Soft Dispatch Console. The Emergency can only be cleared by the console operator.

Press and hold the red exclamation point button at the top of the screen to enable Emergency Mode. Tap the button to disable Emergency Mode.

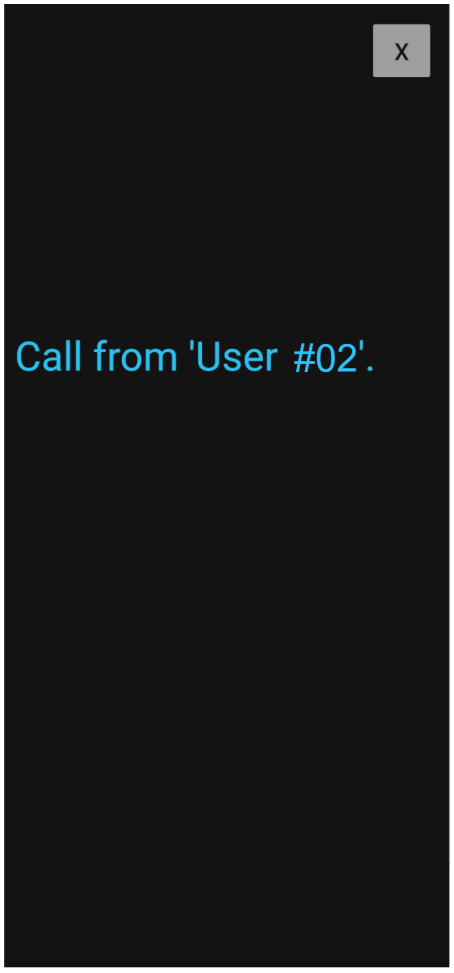
1.3.3 User Tab



Main Screen



Call Screen 1



Call Screen 2

The User tab allows you to make a Private Call with an individual user.

Making a call
Tap the name of the user you wish to make a Private Call to. Press the red talk button to speak to the callee. Once the talk button is pressed the callee will see a screen listing the caller's name.

Receiving a call
Note: Once the User Interface is put into the background it will close after 1 minute.

When receiving a Private call, when the User Interface is open, the Appear On Top option is enabled, and the screen is off, the Call Screen 1 is shown at which point the Private Call can be answered with the PTT.

When receiving a Private call, when the User Interface is closed, and the screen is off, Call Screen 2 is shown at which point the Private Call can be answered with the PTT.

When receiving a Private Call, when the User Interface is closed, and the screen is on, an Android notification message will be received. When a Private Call is received, the PTT will be temporarily re-assigned to allow responding to the Private Call. The temporary assignment of the Private Call will end after 10 seconds of inactivity which will be indicated by a notification tone. When the User Interface is not visible (either in the background or closed) and a Private Call is not active, the PTT button will activate whatever Group Selector is selected.

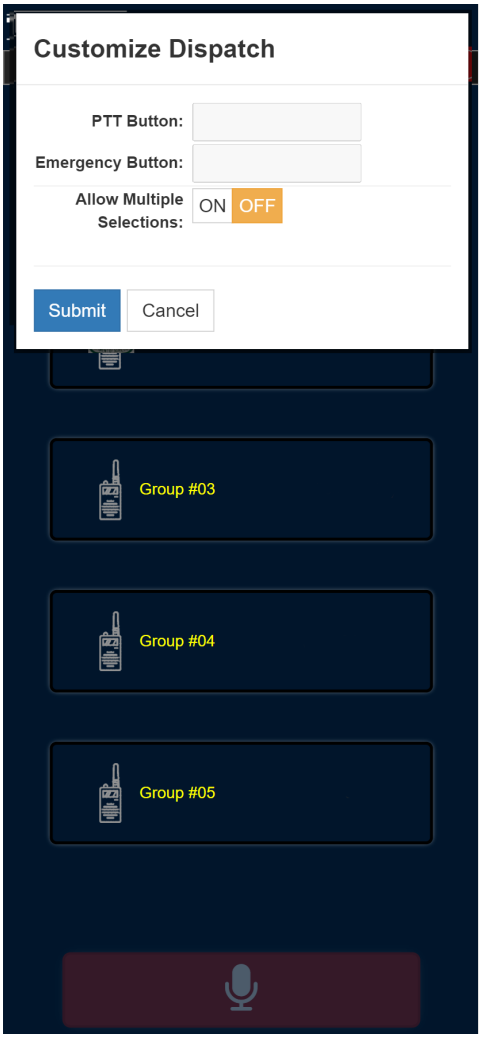
Other Functionality

Use the search bar at the top of the screen to search for individual users. Tapping the magnifying glass button increases/decreases the size of the user list. The eye button shows/hides offline users. The rightmost button (displaying a heart in the image above) allows you to sort by favorites, most recent call, or alphabetically. Tap the heart button to the right of a user's name to favorite them.

1.3.4 Recent Calls Tab

The Recent Calls Tab displays a list of the incoming/outgoing Private Calls. An arrow pointing to the right indicates an outbound call while an arrow pointing to the left indicates an inbound call. A red arrow indicates a missed call and a green arrow indicates a completed call. Press the Clear Log button to clear the list of recent calls.

1.3.5 Physical PTT and Emergency Button Assignment



On supported devices such as the Samsung Galaxy XCover it is possible to use the physical PTT and emergency buttons with Telex RDC. To enable this functionality tap the three bars at the top right of the screen and then select Customize. Tap the PTT button field and then press the physical PTT button. You will see the title of the button appear in the field. Follow the same process for the emergency button and then press submit.

2. Administrator Guide

2.1 Product Part Numbers

Followings are the part numbers for the RDC product.

Part Number	Description
F.01U.394.128	RDC System license
F.01U.413.775	RDC 5 devices increment license
F.01U.394.129	RDC 10 devices increment license
F.01U.394.130	RDC 2 groups increment license
F.01U.413.776	Annual software update subscription, Year 2 and higher

NOTE: Customers can download the RDC System Server application here to evaluate. Upon the installation of the Server application, customers will have access to 2 users and 1 group for a 30 day trial period.

2.2 Server Installation

2.2.1 Hardware Requirements

Operating System Requirements

The Telex RDC Server can be installed on virtually any modern Windows based operating system however Windows 10 Professional x64 or Windows Server 2019 x64 are highly recommended.

Memory Requirements

The memory requirement for the Telex RDC Server are very minimal and system size does not realistically need to be considered. It is recommended to use 8GB of memory with any modern OS which will also provide sufficient resources for operation of the Server.

Storage Requirements

The storage requirements for Telex RDC Server in the standard configuration are not substantial but some incremental storage space is required for Activity/Debug Logs. In the standard configuration, a minimum of a 128GB SSD is recommended although a 256GB SSD is preferred. An SSD is specified only for reliability.

2.2.2 Network Requirements

Bandwidth Requirements

The network bandwidth requirements must be carefully analyzed to ensure proper bandwidth is available at any point where multiple clients will share the same physical connection point. The most obvious connection point where this is critical is at the server where bandwidth requirements will be the sum of the requirements of every possible client. The least obvious connection point where this is also important occurs when multiple remote clients in one physical location need to access the server in another physical location as the bandwidth requirements for the connection between these two points will be the sum of the requirements for all remote clients.

To determine the bandwidth requirements it is necessary first to determine the network bandwidth utilization per client connection, which is indicated below for the various audio sample rates that can be configured.

Telex RDC:

Audio Sample Rate	Data Rate (Kbps)
48 KHz	200

To determine server bandwidth requirements, first determine maximum potential bandwidth utilization by multiplying the number of clients (users and devices interfaced) by the Data Rate associated with appropriate Audio Sample Rate for the configured Audio Time Slice per packet. The product is the bandwidth required if every client were to receive audio simultaneously (maximum download bandwidth requirement) and also the bandwidth required if every client were to send audio simultaneously (maximum upload bandwidth requirement). In a typical system, the maximum download bandwidth requirement must be allocated for, as several system functions can require simultaneous audio transmission to all clients. The maximum upload bandwidth requirement however will realistically never be achieved as it is not feasible that all audio sources in a system would be active simultaneously since the result would be inaudible. As such the upload bandwidth to be allocated must be made based on the estimation of the number of simultaneous active audio sources noting that inactive audio sources will have no bandwidth requirements.

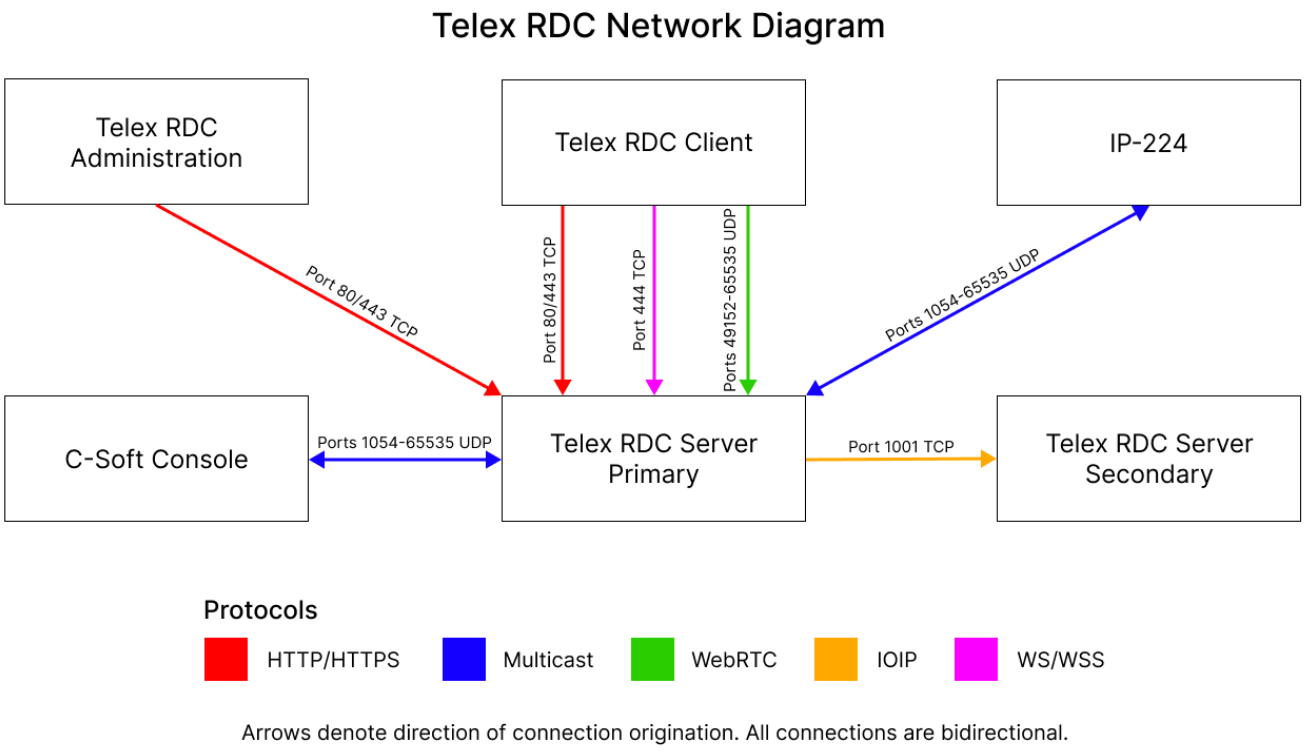
Firewall Requirements

Telex RDC requires certain ports to be traversable through firewalls to allow the various components to connect. Factors such as the network location of the hardware and of the RDC clients that will connect to the Server as well as where those connections originate will need to be considered. For the initial configuration, it is recommended to completely disable the Windows Firewall. The diagram and the chart below indicate which ports are required for all components.

The IP-224, the C-Soft Console and the Server Secondary Server will generally coexist on the same private network segment as the Server Primary as as such there may not be any firewalls between.

The RDC clients are most likely to exist in the public network outside of the private network. In such case there will be a firewall to traverse. By default, the clients establish their initial connection to the server on the standard HTTP/HTTPS ports of 80/443. Note that the HTTP port is optional as it sole purpose is to redirect any HTTP request to an HTTPS request. In addition to the standard HTTPS port, a default WSS port of 444 is also required to complete the connection. As forwarding the standard HTTP/HTTPS ports may not be possible, it may be required to change the default HTTP/HTTPS ports in the RDC

Administration → System Settings dialog. Note that the WSS port will always be 1 greater than the HTTPS port. If the HTTPS ports is changed, all clients must then append the new port number to the Server Host Name (eg 100.100.100.100:8443).



Port or Port Range	Protocol	Description
80	TCP (HTTP)	RDC Administration and Telex RDC App data (Unsecure)
443	TCP (HTTPS)	RDC Administration and Telex RDC App data (Secure)
444	TCP (WSS)	Telex RDC App Signaling data (Secure)
1001	TCP (IOIP)	Telex RDC Server Failover data
49152 to 65535	UDP (WebRTC)	Telex RDC App WebRTC Audio (see ‘WebRTC Audio Connection’ section)
1054 to 65535	UDP (Multicast)	Connection to C-Soft Console
1054 to 65535	UDP (Multicast)	Connection to IP-224

The C-Soft Console and IP-224 use the UDP multicast address range 224.0.0.0 to 239.255.255.255.

2.2.3 WebRTC Audio Connection

When the client logs into the server, the client and the server work together determine the network path for the audio connection. If the client and server are both located on the same private network, the audio connection is straight forward and a connection is made directly between the client and server. If the server is located on a private network

and the client is on the public Internet or the client is on separate private network that is also connected to the public internet, the audio connection is more complex as the connection must be established via the firewall(s) of the private network(s). In 80% of network installations, this is all handled automatically and transparently such that the audio connection is routed directly to and through the firewall(s) of the private network(s) without further considerations necessary. However, in 20% of the network installations, typically on highly secure corporate networks using Symmetric NATs, the firewall restrictions are such that the audio connection cannot be routed directly to and through the firewall of the private network. In this situation, the audio connection must be routed through a relay server located in the public Internet. This relay server is referred to as a “TURN” server which stands for ‘Traversal Using Relays around NAT’. If a TURN server is required, please refer to the ‘TURN Server Provisioning’ section for setup and configuration information. If provisioning a TURN server is not feasible, a TURN server can be provided as a service by a 3rd party partner. Using a TURN server is completely secure as all WebRTC audio packets must be encrypted using TLS (Transport Layer Security) by definition and can only be decrypted by the intended recipient.

2.2.4 Software Installation

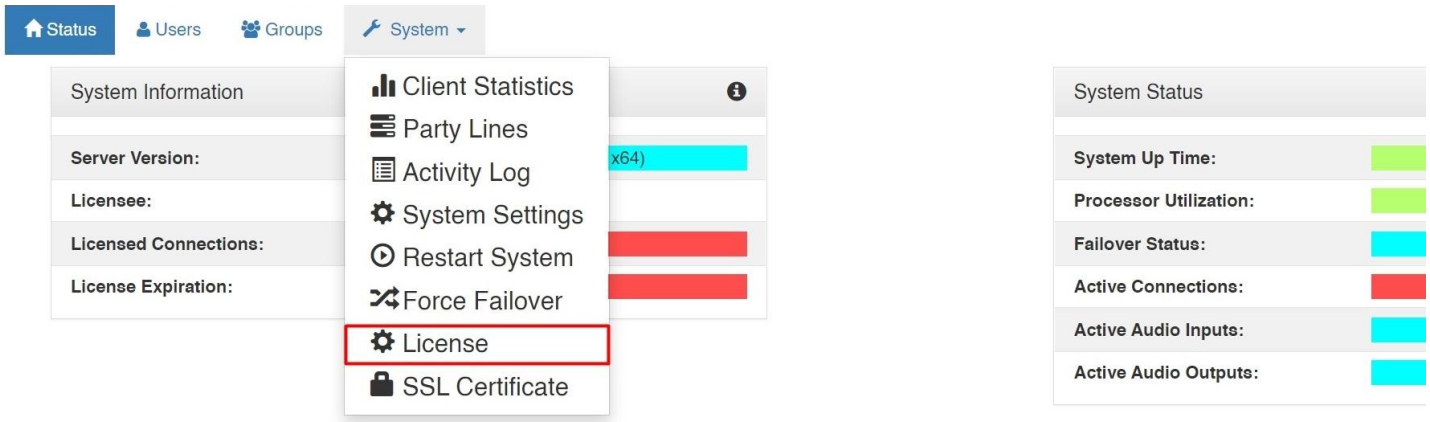
Download Telex RDC Server from our downloads page and unzip the installer.

Run the installer and follow the prompts. You will need to accept Telex License Agreement to install the software. During the installation process you will be asked if you want to install the Telex RDC Server to run as a service or application. Servers should run Telex RDC as a service.

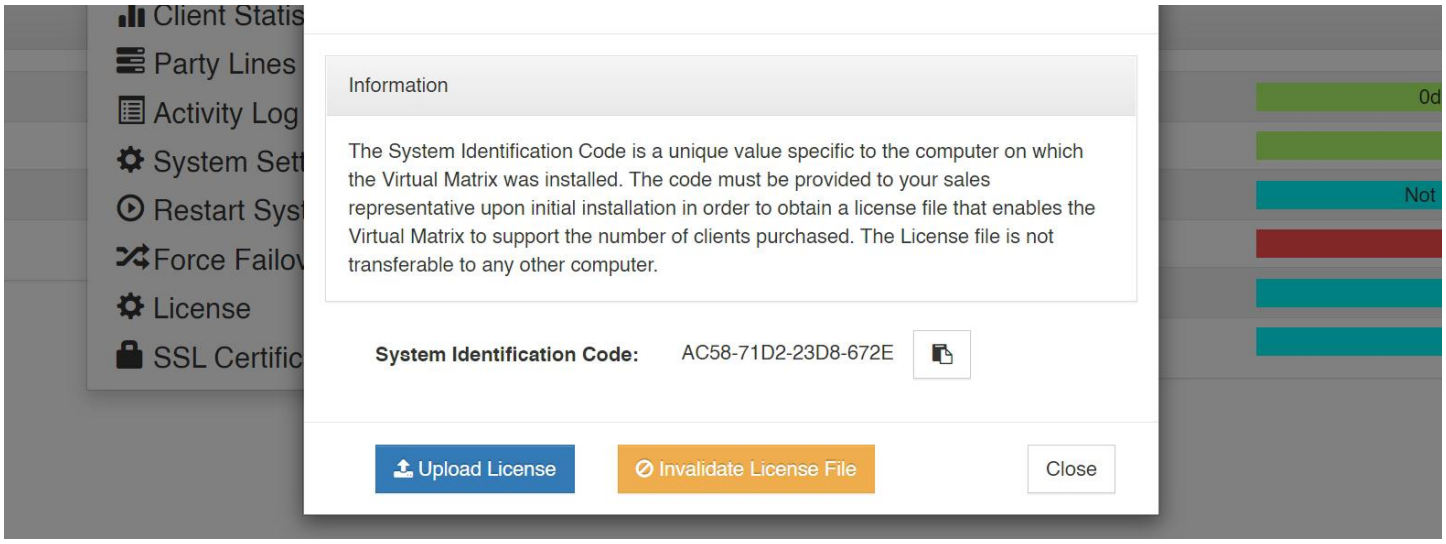
2.2.5 Licensing

To license your Telex RDC System you need to acquire a valid license file from Telex. To do so you must provide Telex with your unique ‘System Identification Code’ generated automatically when you install the Telex RDC Server. The ‘System Identification Code’ is a unique value specific to the computer on which the Server was installed and is not transferable to any other computer. If the server you are running the Telex RDC Server on has dual network cards make sure the primary NIC to be used is select as the Primary Server IP Address in the System Settings before sending the system identification code as it is dependent on the network card being used.

To generate a license for a new Telex RDC Server installation:



1) Log into the RDC Administration and select License from the System tab at the top of the screen.



2) Make a note of the displayed System Identification Code.

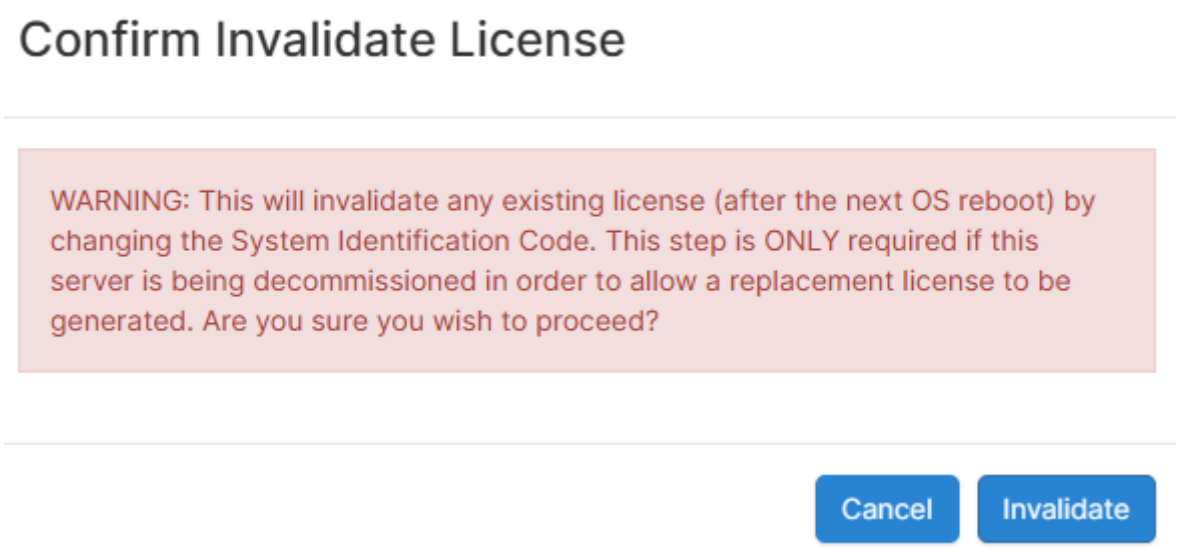
3) Send the System Identification Code to your Telex RDC sales representative who will use that code to generate the license.

4) Upon receiving the license from your Telex RDC sales representative, click 'Upload License' and chose the provided license file.

To transfer a license from an existing Telex RDC Server installation to a new computer in the case of computer upgrade or replacement:

1) Log into the RDC Administration and select License from the System tab at the top of the screen.

2) Make a note of the displayed existing System Identification Code.



3) Click 'Invalidate License' and after reading the invalidation WARNING dialog, click 'Invalidate'.

4) Make a note of the displayed Invalidation Code.

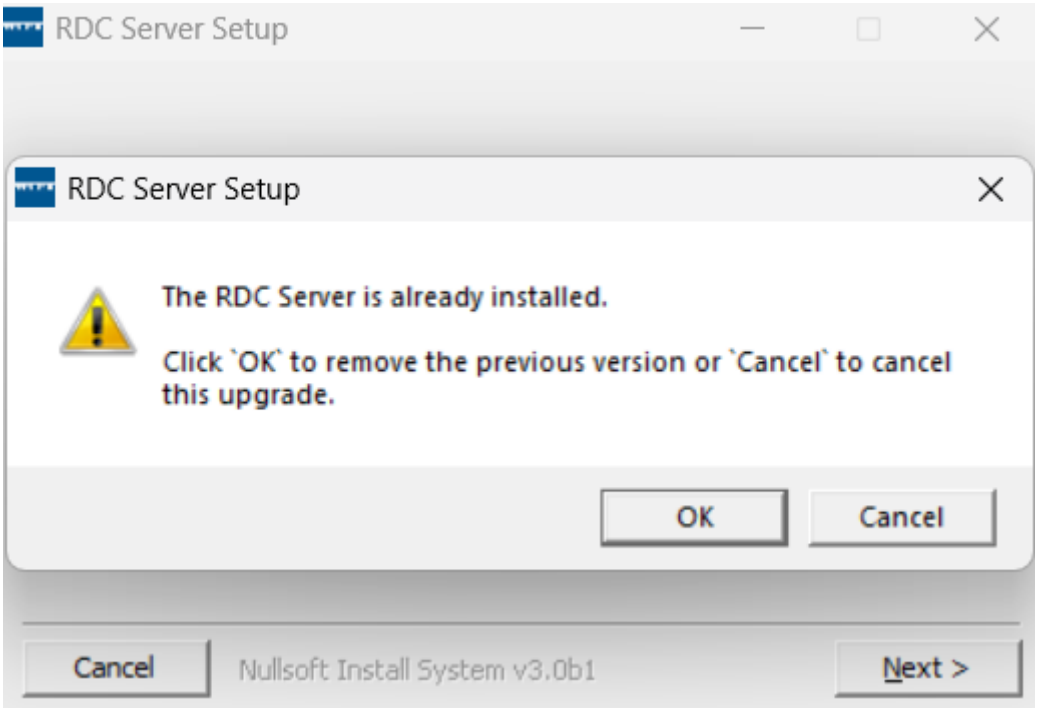
5) Send both the System Identification Code and the Invalidation Code to your Telex RDC sales representative.

2.3 RDC Server Upgrade Instructions

Note: Upgrading your server version will not erase any existing settings or configuration.

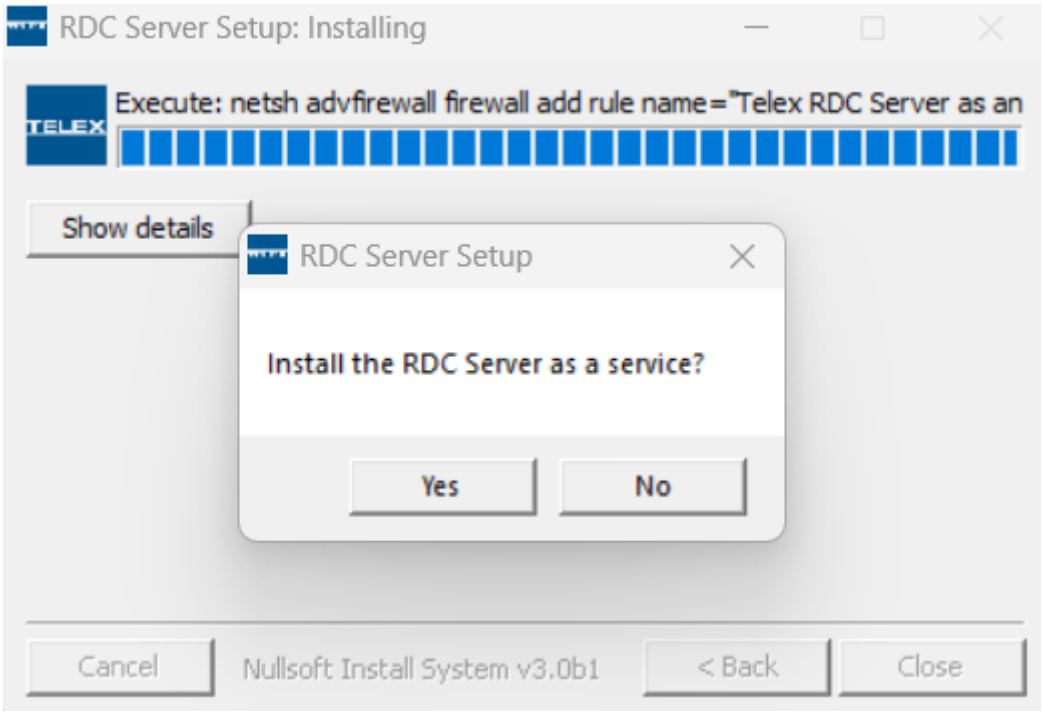
To upgrade RDC Server:

1. Using Windows Services (Task Manager → Services), stop the RDC Server Services for the hosting machine.
2. In Windows Explorer, navigate to `C:\Program Files\Telex`.
3. Copy the folder named **RDC Server**.
4. Paste the folder to the desktop.
   This is a backup of the previous system.
5. Download the current version of RDC Server.



6. Browse to and double-click the downloaded file.
   The executable first uninstalls the older version, and then prompts to proceed with the installation of the new version.
7. Click **OK**.
   The uninstall begins.
8. When the uninstall is done, click **Close**.
   The License Agreement screen appears.
9. Click **I Agree** when prompted.

10. Click **Next** when prompted.
    The installation starts.



11. Towards the end of the installation, a pop-up window appears asking if you wish to run the RDC Server as a service.
12. Once the install is complete, a web browser appears with the RDC Administration screen.
13. Log into your system.
14. Verify the latest version is running.

2.4 TURN Server Provisioning

The open-source TURN server called Coturn is highly recommended as the TURN server to be installed, if a TURN server is required, although likely any TURN server can be used. Following are the requirements and setup instructions for the Coturn TURN server.

2.4.1 Minimum Server Requirements

Operating System: Linux (recommend Ubuntu 18.3 or higher)
CPU Requirements: 2 vCPUs
RAM: 2 GB
DISK: 10 GB
Network bandwidth required per client: 100 Kbps (aka 1000 clients per 100 Mbps of bandwidth)
Approximate Clients per vCPU: 100

2.4.2 Software Installation

Once the cloud-based server has been provisioned, access the server via SSH (Secure Shell). To install the server, perform the following steps:

Install the Coturn Software
1. Run `sudo apt-get update`.
2. Run `sudo apt-get upgrade`.
3. Run `sudo apt-get install coturn`.

Download and Install the Configuration File
4. Preserve the default Coturn configuration file by running `mv /etc/turnserver.conf /etc/turnserver.conf.original`.
5. Download the preconfigured ‘turnserver.conf’ configuration here.

By default, the Coturn server will be accessible on the default TURN port # of 3478 with a Username of ‘telex’ and Password of ‘RDC’. If a different port #, Username or Password is desired, these items can be changed in this configuration file.

6. Using the SCP (Secure Copy) protocol of SSH, or any other applicable method, copy the pre-configured ‘turnserver.conf’ configuration file to the /etc directory.

Start the Server

7. Run `systemctl start coturn` to start the server.

Connect the Coturn Server to the RDC Server

8. To have the RDC server use the newly provisioned TURN server, login to the RDC Administration and from the System → System Settings dialog, change the ICE Server Host Name to 'turn:<TURN_SERVER_HOST_NAME>:<TURN_SERVER_PORT_NUMBER>’ and configure the ICE Server User Name and ICE Server Password as appropriate.

2.5 Logging In

If you are using the Telex RDC Administration from the same machine Telex RDC is installed on:
After Telex RDC Server is installed on the machine, a shortcut will be placed on the desktop called ‘Telex RDC Administration.’ Click on the shortcut. A browser window will appear. The Telex RDC Administration application can also be accessed by typing ‘localhost’ into the URL box and pressing enter.

If you are using the Telex RDC Administration from a different machine:
Open a browser window and type the IP address or domain name of the machine running Telex RDC into the URL box and press enter.

The default master ‘Login Name’ and ‘Login Password’ are both ‘admin’. The credentials can be changed after logging in.

2.6 Status

System Information fields are color-coded. Red indicates a problem; Yellow a potential problem; and Green normal operations. Blue fields are informational. The ‘System Information’ area in the upper, left-hand side of the System Administration main window displays the name of the licensee, the number of clients licensed, and expiration date. ‘License Expiration’ will typically display ‘---’ which means a system has been purchased and a perpetual license has been granted. Demo, trial, and rental systems will display a numerical value in days reflecting the limited duration for which a license has been granted.

System Status
System Status fields are color-coded. Red indicates a problem, Yellow a condition that needs attention, and Green normal operations. Blue fields are informational.

The ‘System Status’ on the right side of the System Administration main window displays general system metrics.

System Up Time: Displays how long the Telex RDC Server has been running in days, hours, and minutes.

Processor Utilization: Displays CPU utilization of the server or PC hosting the Telex RDC Server.

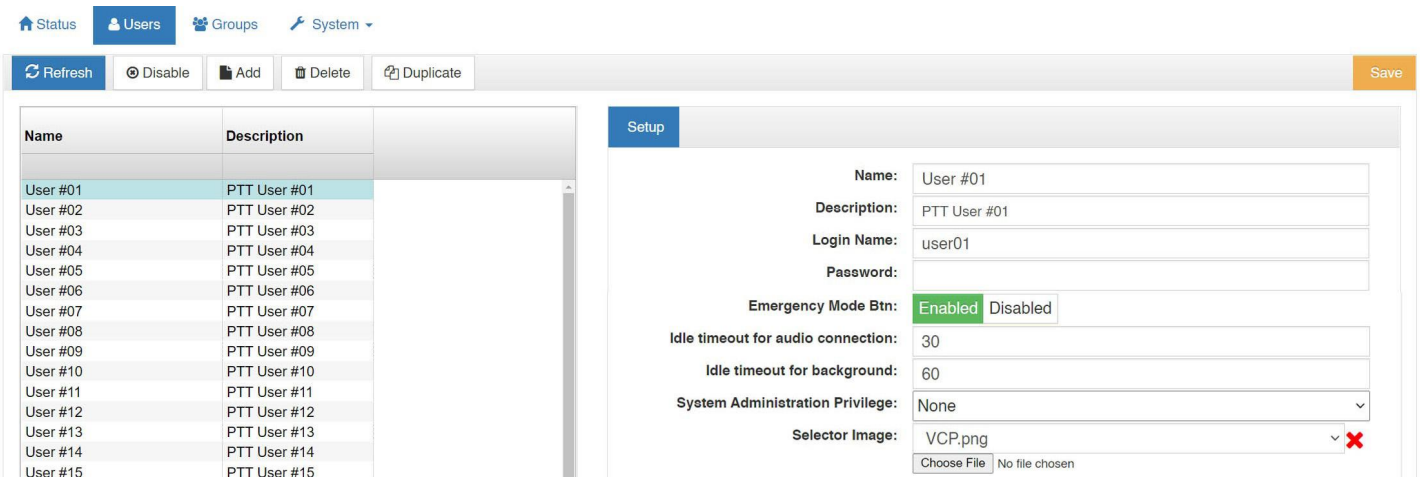
Failover Status: Displays the operational status of the Primary and Secondary servers when Failover is licensed and configured.

Active Connections: Displays how many clients are connected to the Server at any given moment out of how many clients are configured.

Active Audio Inputs: Displays how many active audio channels are being streamed from clients into the Server at any given time.

Active Audio Outputs: Displays how many active audio channels are being streamed out of the Server to clients at any given time.

2.7 Users



The Users tab allows you to configure Telex RDC Client credentials and settings. The system is preconfigured with 30 users.

Name: The alphanumeric identifier that will display on the Selector shown on all Clients.

Login Name: The name assigned to a user which is used to login a Client.

Password: The password assigned to a user which is used to login a Client.

Emergency Mode Btn: Enables/Disables the Emergency Mode button that appears on the Client.

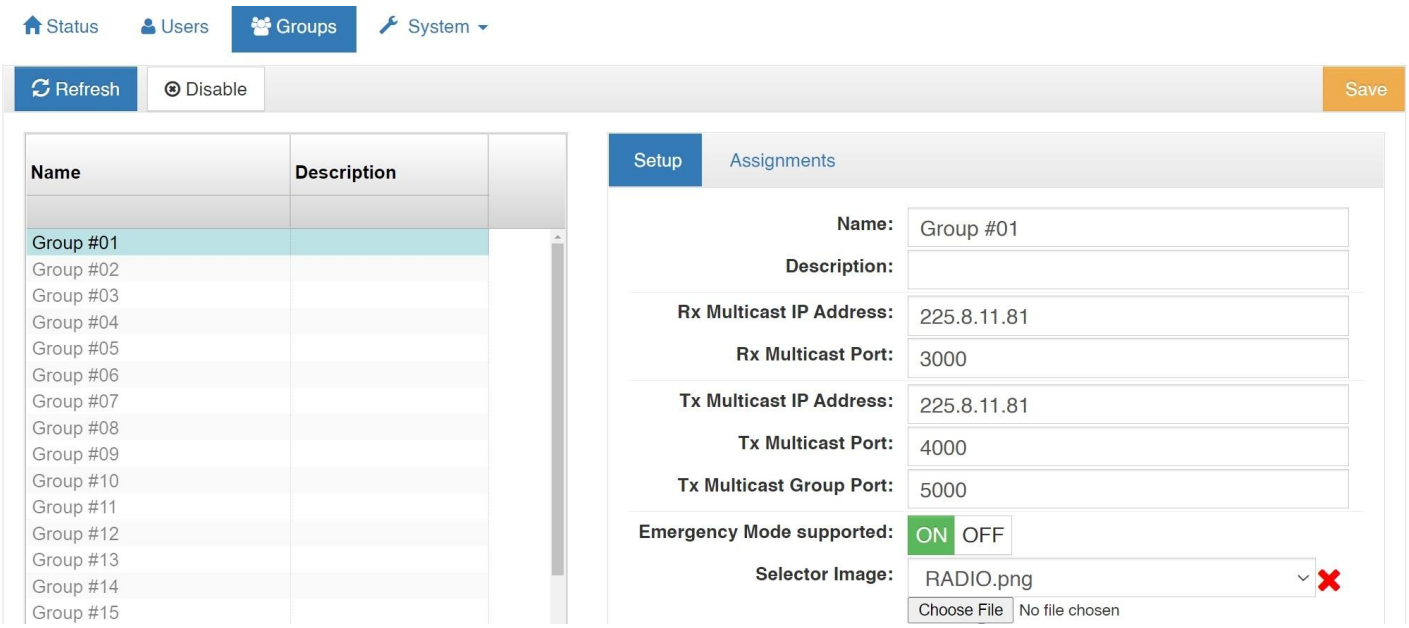
Idle Timeout for Audio Connection: The number of seconds that the server will wait before it attempts to reestablish the audio websocket connection.

Idle Timeout for Background: The number of seconds that the server will wait before it attempts to wake the application from sleep mode. This setting is only applicable to Android devices.

System Administration Privilege: Choose whether this client can access the System Administration. Master privileges gives the user full control and Standard privileges will give the user limited control.

Selector Image: The image that will be displayed on the selector for this user.

2.8 Groups



The Groups menu allows you to set up User talk Groups. The system comes with 20 preconfigured Groups.

Name: The alphanumeric identifier that appears on the Client.

Description: The description given to identify the client that is used exclusively in the System Administration application.

Rx Multicast IP Address: The Multicast IP address for Talk-Group receive audio used between C-Soft, IP-224 and RDC.

Rx Multicast IP Port: The Multicast IP port for Talk-Group receive audio used between C-Soft, IP-224 and RDC.

Tx Multicast IP Address: The Multicast IP address for Talk-Group transmit audio used between C-Soft, IP-224 and RDC.

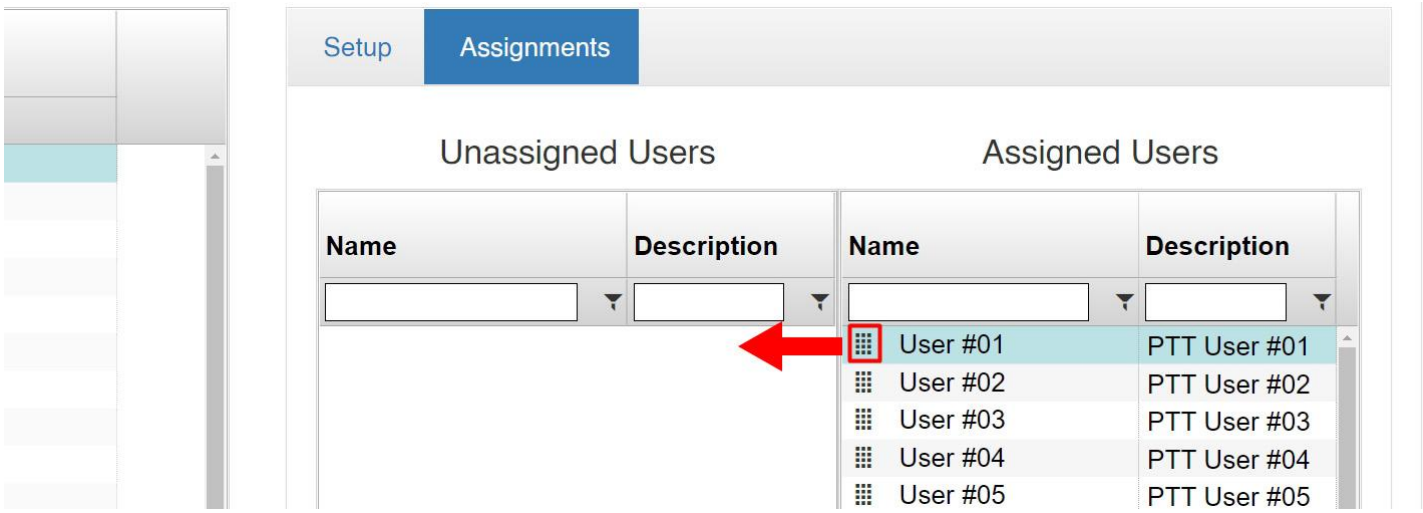
Tx Multicast IP Port: The Multicast IP port for Talk-Group transmit audio used between C-Soft, IP-224 and RDC.

Tx Multicast Group Port: The Multicast IP port on which the IP-224 receives radio transmit audio from RDC. This number will need to be configured into the IP-224 TX Group Port field.

Emergency Mode supported: Designates whether the group supports activation of the Emergency Mode.

Selector Image: The image that will appear on the groups's selector.

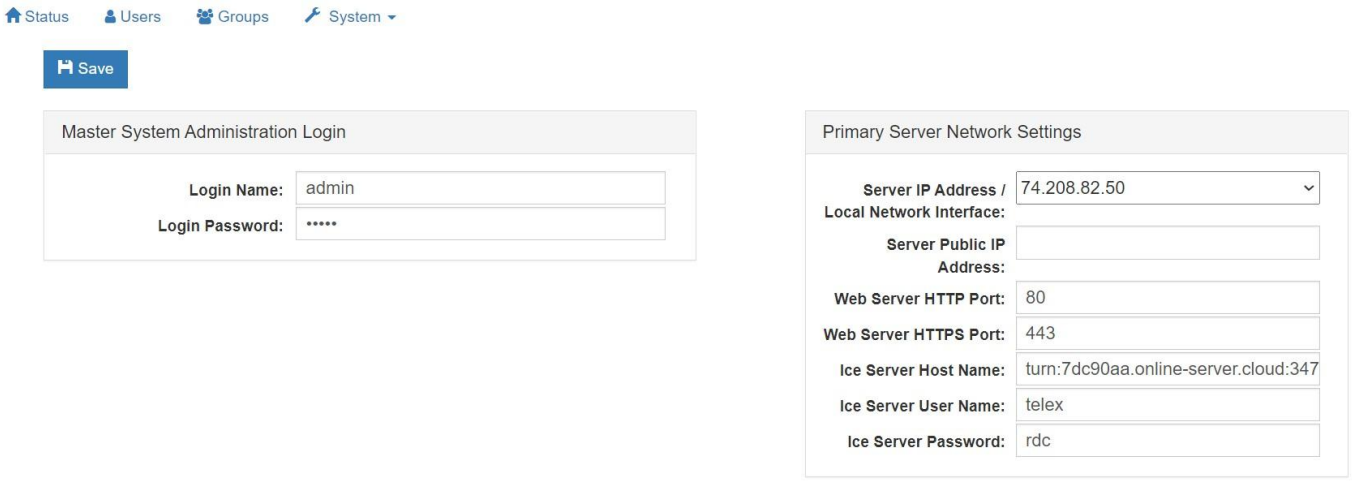
Assigning/Unassigning Users to/from the Group



Select the Assignments tab and then drag the User's handle to the Assigned Users list of the Unassigned Users list. Alternatively, double click the User to move them to the opposite list. Click the Save button to save your changes.

2.9 System

2.9.1 System Settings



Master System Administrator Login : Displays and allows you to edit the master system administrator login name and login password.

Primary Server Network Settings
Server IP Address / Local Network Interface: The IP address of the server hosting the Server.

Server Public IP Address: The public IP address that is used to route data to the Server's IP address within the LAN. This is only used when Network Address Translation (NAT) is being used on your LAN.

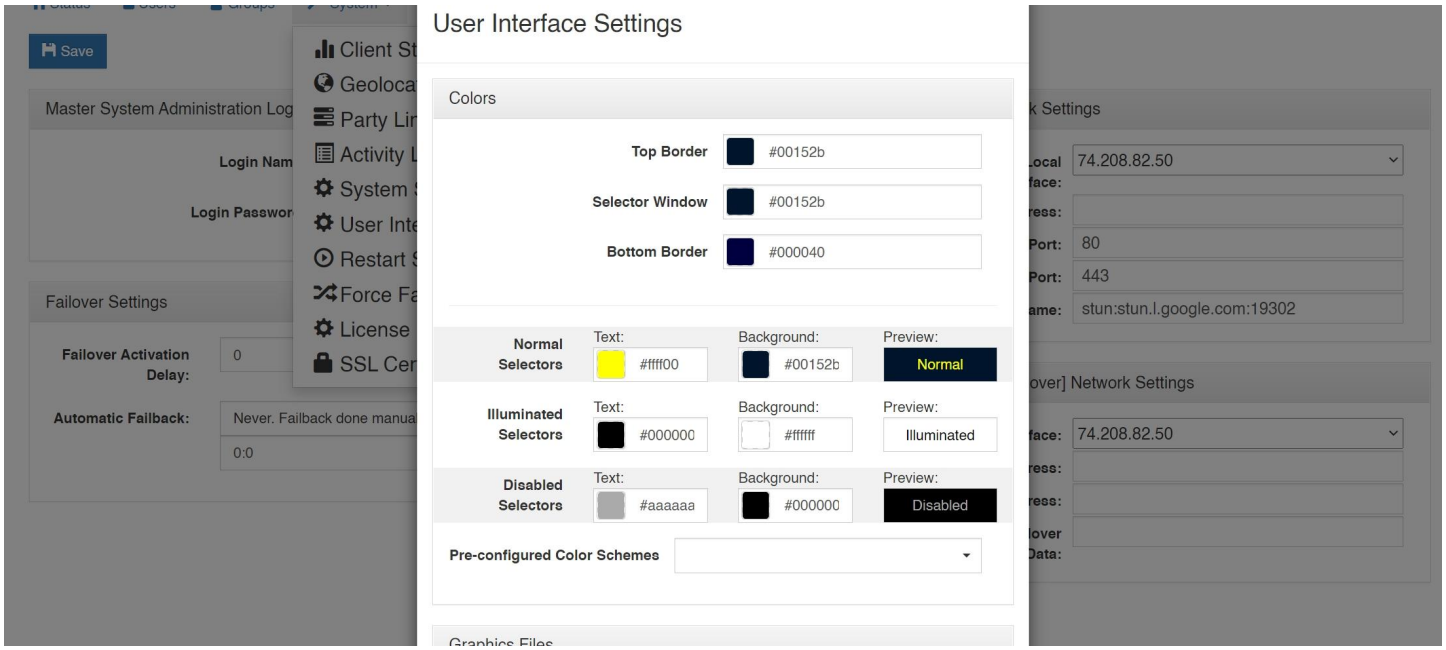
Secondary (Failover) Server Network Settings
If you wish to set up a failover server for a second Server, and have purchased 'Redundancy', enter the relevant values. In an instance of a hardware or connectivity failure client applications will reconnect to the failover server. Refer to Section 6 of the Telex RDC Server User Guide for a detailed description of the failover capability.

Server IP Address: The IP address of the machine hosting the Telex RDC Server.

Failover Settings (visible only if the server is licensed for this feature)
Failover Activation Delay: Set the amount of time to delay the failover from coming online in place of the Primary Server.

Automatic Failback: Define when to restore the Primary Server. Choose the setting that best fits your procedures.

2.9.2 User Interface Settings



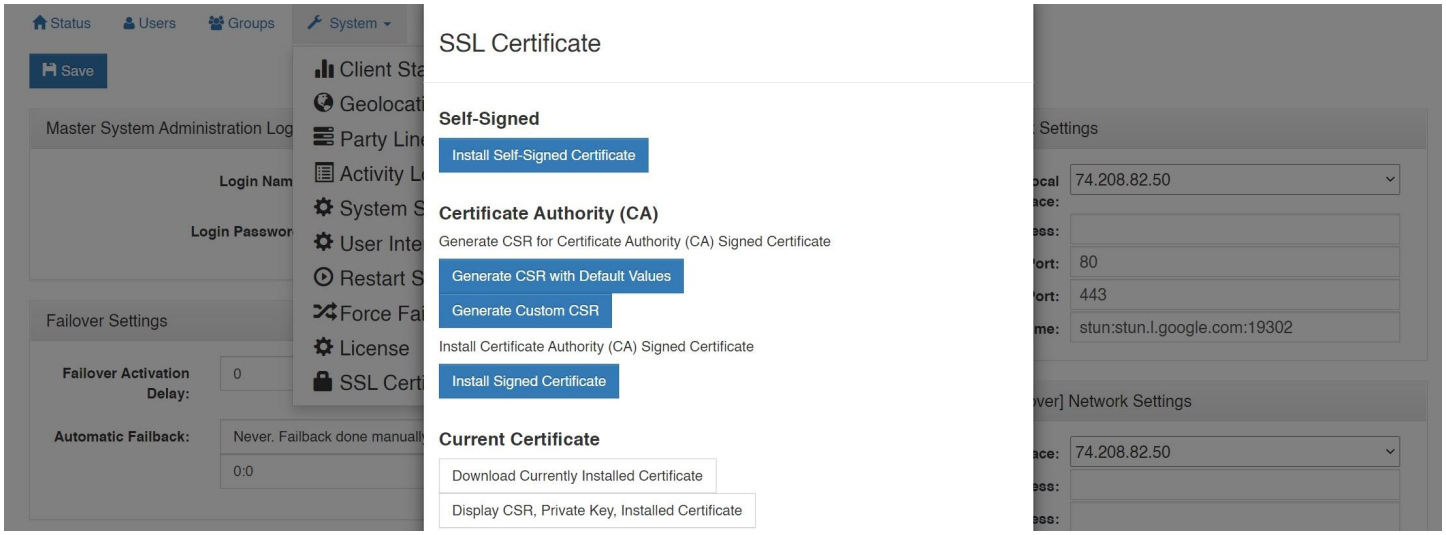
This allows customizations of the VCP GUI such as the Colors (Background and Text), Selector Spacing, and 24-bit PNG graphic files that can be uploaded such as a logo.

Restart System: This feature restarts the system. A warning message will first appear noting that selecting this feature will temporarily render the system inoperable and asking if you wish to proceed. This feature is only available to the system administrator logged in with the master username and password.

Force Failover: Forces the Primary to relinquish control to Secondary Server.

Force Failback: Forces the Secondary to relinquish control to Primary Server.

2.9.3 Certificates



Telex RDC Server generates its own self-signed certificate upon initial launch. All data transmitted between the Telex RDC Server and the System Administration as well as the Telex RDC app is encrypted. However, browsers will display a warning because a self-signed certificate is being used. It is possible to install a certificate signed by a Certificate Authority in which case no browser warning will be displayed.

Install Self-Signed Certificate: Generates and installs a self-signed certificate onto the Telex RDC server.

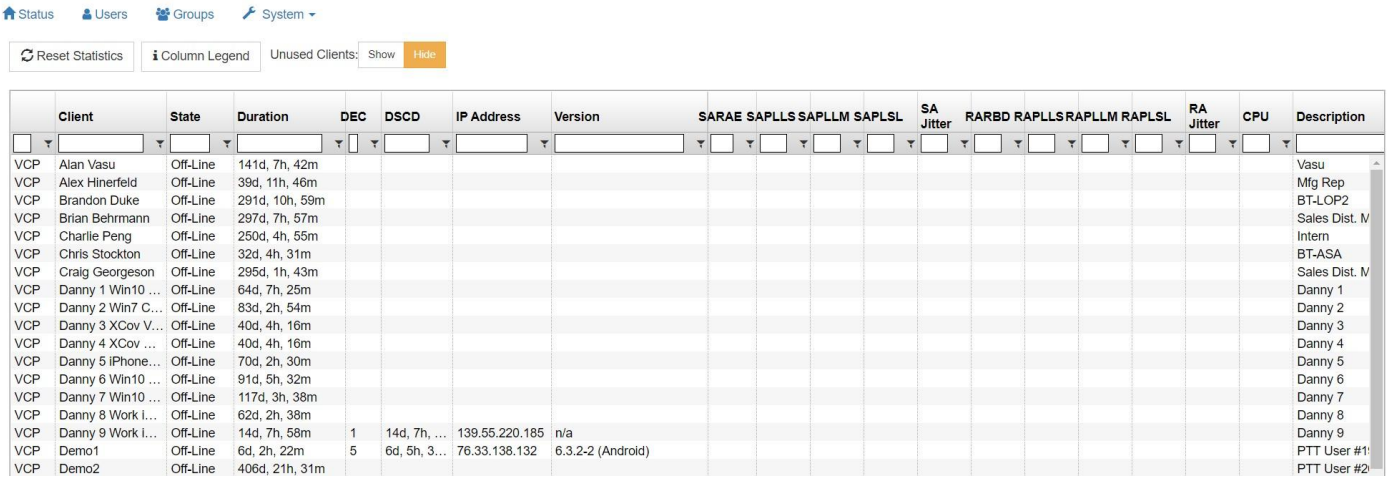
Generate CSR with Default Values: Prompts the user for the Domain Name(s) with which to generate a CSR to send to a Certificate Authority.

Generate Custom CSR: Prompts the user for Domain name(s), Organization Name, County Name, and State/Province. These values are used to generate a CSR to send to a Certificate Authority.

Install Signed Certificate: Installs a certificate generated by a certificate authority.

2.10 System

2.10.1 Client Statistics



	Client	State	Duration	DEC	DSCD	IP Address	Version	SARAE	SAPLLS	SAPLLM	SAPLSL	SA Jitter	RARBD	RAPLLS	RAPLLM	RAPLSL	RA Jitter	CPU	Description
VCP	Alan Vasu	Off-Line	141d, 7h, 42m																Vasu
VCP	Alex Hinerfeld	Off-Line	39d, 11h, 46m																Mfg Rep
VCP	Brandon Duke	Off-Line	291d, 10h, 59m																BT-LOP2
VCP	Brian Behrmann	Off-Line	297d, 7h, 57m																Sales Dist. M
VCP	Charlie Peng	Off-Line	250d, 4h, 55m																Intern
VCP	Chris Stockton	Off-Line	32d, 4h, 31m																BT-ASA
VCP	Craig Georgeson	Off-Line	295d, 1h, 43m																Sales Dist. M
VCP	Danny 1 Win10 …	Off-Line	64d, 7h, 25m																Danny 1
VCP	Danny 2 Win7 C…	Off-Line	83d, 2h, 54m																Danny 2
VCP	Danny 3 XCov V…	Off-Line	40d, 4h, 16m																Danny 3
VCP	Danny 4 XCov …	Off-Line	40d, 4h, 16m																Danny 4
VCP	Danny 5 iPhone…	Off-Line	70d, 2h, 30m																Danny 5
VCP	Danny 6 Win10 …	Off-Line	91d, 5h, 32m																Danny 6
VCP	Danny 7 Win10 …	Off-Line	117d, 3h, 38m																Danny 7
VCP	Danny 8 Work i…	Off-Line	62d, 2h, 38m																Danny 8
VCP	Danny 9 Work i…	Off-Line	14d, 7h, 58m	1	14d, 7h, …	139.55.220.185	n/a												Danny 9
VCP	Demo1	Off-Line	6d, 2h, 22m	5	6d, 5h, 3…	76.33.138.132	6.3.2-2 (Android)												PTT User #1
VCP	Demo2	Off-Line	406d, 21h, 31m																PTT User #2

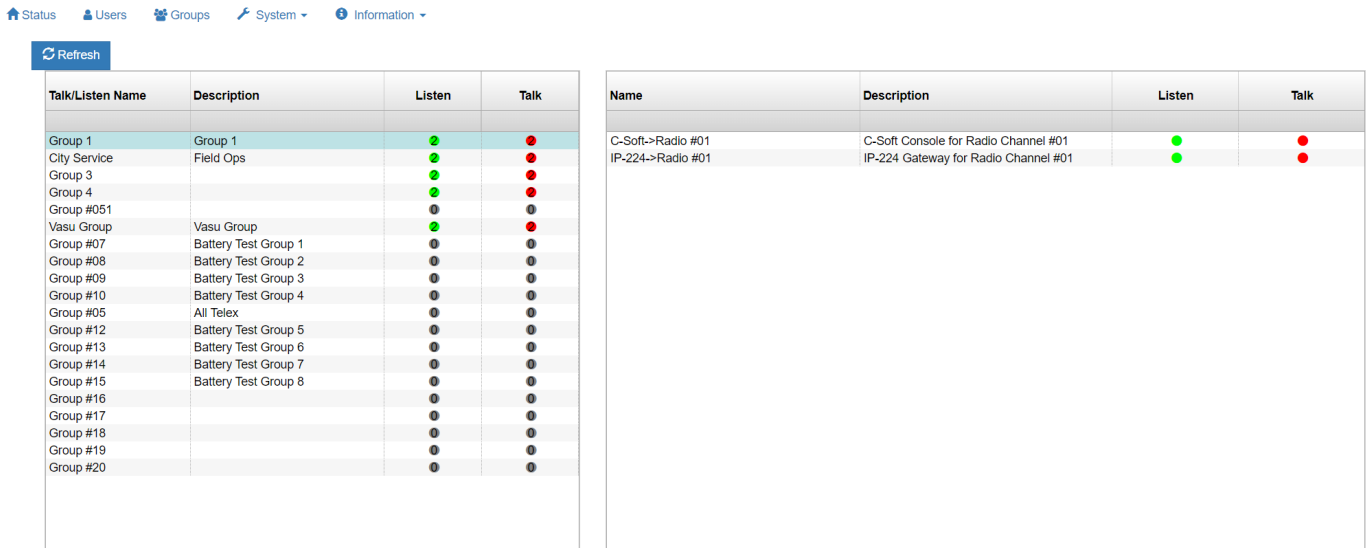
Client Statistics: Displays individual send and receive audio and packet loss statistics for all client connections.

Click the ‘Reset Statistics’ button in the upper, left-hand corner to reset all client statistics or highlight a user or device and then click ‘Reset Statistics’ to reset the statistics of an individual user or device.

Select ‘Show Unused Clients’ to display users and devices programmed for your system but have never been connected.

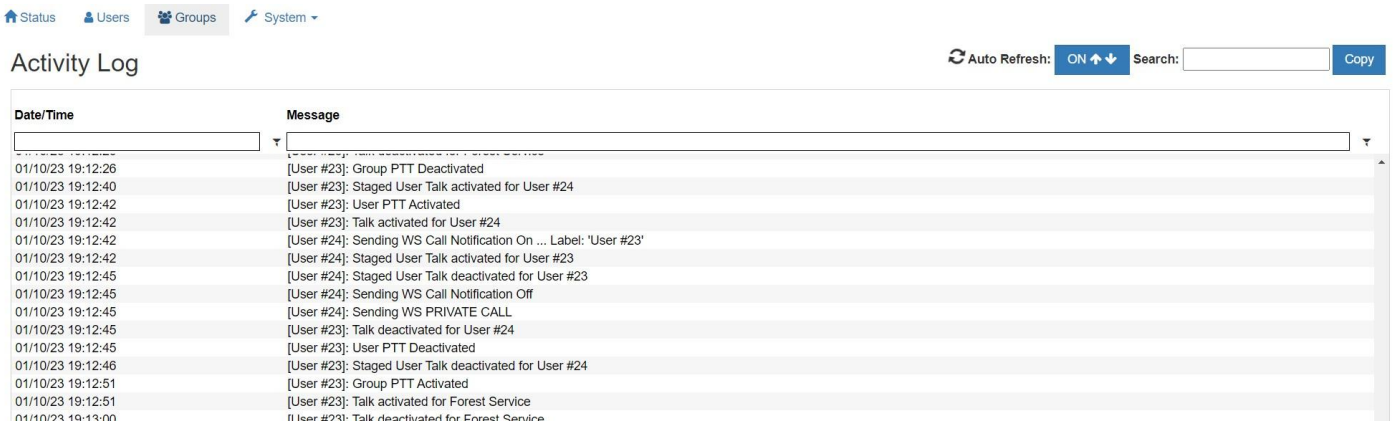
Click the ‘Column Legend’ button in the upper, left-hand side of the ‘Client Statistics’ page to display the legend.

2.10.2 Group Status



The Group Status page allows administrators to monitor who is talking and listening on a given group selected on the left pane.

2.10.3 Activity Log



During system operation the logging feature displays a time-stamped entries for general system activity including each client connection/disconnection and selector activations/ deactivations.

3. Failover Capability

In any mission critical communications system it is imperative to have built in redundancy. Telex RDC supports this function with a Failover capability. Failover by definition is the ability to automatically switch over from a primary working server to a secondary backup server should there be any catastrophic failure in operation of the primary server or its associated network.

3.1 Implementation

In the primary server, the IP address of the secondary server is configured. When the primary server starts, a connection to the secondary server is immediately established. Through this connection the primary server shares its licensing information to the secondary server. Additionally, the primary server conveys any operational changes to the system configuration to secondary server in real time so that the system configurations remain synchronized. This connection will remain active as long as both servers are running. If this connection is lost, the secondary server will immediately assume it is an active server allowing Telex RDC clients to connect. However in some cases even if the connection is not lost, the complexities of some network failures may still warrant the secondary server becoming the active server. When any Telex RDC client logs into the primary server, the secondary server IP address is automatically provided to it. In the event that communications with the primary server is lost, the client will automatically attempt to connect to the secondary server. If the secondary server is available and active, the Telex RDC client will log into the secondary server.

Once the secondary server becomes the active server, switching back to the primary server generally will require a manual authorization as the condition that caused the failover would need to be properly evaluated to ensure there is no possibility for reoccurrence of that event which would unnecessarily disrupt active communications. The manual switchover can be controlled through the System Administration application.

For failover to work seamlessly, all Telex RDC clients must be using a security certificate for which the issuing Certificate Authority is trusted. If the certificate is not signed by a public Certificate Authority, as is the case with the default Bosch self-signed certificates, then the Bosch Certificate Authority (CA) certificate must be installed on all Telex RDC clients to allow the Telex RDC client to trust Bosch self-signed certificates. The process to

do so is slightly different for each OS and browser. For all clients, the Bosch CA certificate can be downloaded from the menu available on the Login dialog. For Android and iOS, on screen instructions will detail the steps necessary to install the certificate. For the Windows OS, the certificate will specifically need to be installed into the store for “Trusted Root Certificate Authorities”. For the FireFox browser on the Windows OS, one additional step must be taken to enable the use of the Windows Certificate store which can be done by entering “about:config” in the FireFox browser bar, searching for the “security.enterprise_roots.enabled” option and setting this value to ‘true’.

Notice for FireFox Users: It has been observed that after a failover/failback the user may intermittently not be able to receive audio as a result of a FireFox specific implementation restriction. A logout/login will resolve the issue.

Notice for Android Users: It has been observed that after a failover/failback, the user interface, if open, will intermittently not reconnect to the active server but instead display a page showing “Webpage not found”. Returning to the Host Address dialog and re-connecting to the server will resolve the issue.

3.2 Failover Criteria

In normal operations, the primary server is always the active server. In general as long as the communications link between the primary and secondary server is connected, the primary server will remain as the active server. When a server is not the active server, logins will not be allowed. There are many different scenarios that can result in a failover event. The most common are as follows:

Communication link between primary and secondary servers lost due to primary server failure:
In this simplest scenario, the secondary server would recognize the loss of the primary server and immediately become the active server. All clients would also recognize the loss of the primary server and would immediately reconnect to the secondary server.

Communication link between primary and secondary servers lost due to failure of network infrastructure:
In this scenario, the secondary server would recognize the loss of the primary server and immediately become the active server. Since the primary server is still running, it too would also still consider itself to be the active server. However, if the network failure also

resulted in the simultaneous loss of the majority of connected Telex RDC clients the primary server will deactivate itself forcing all remaining clients to connect to the secondary server.

Communication link between primary and secondary servers is not lost but partial failure of network infrastructure:
In this scenario, the partial network failure may result in the loss of a large portion of the Telex RDC clients. In this case the primary server will inform the secondary server to activate allowing connections to be made. If the secondary server reports the client connection were established the primary server will deactivate itself forcing all remaining clients to connect to the secondary server.

3.3 Summary

The Telex RDC Failover support is an integral part of any mission critical communications solution. While its operation will never be visible to the end user, it availability in the case of an unforeseen catastrophic primary server failure will quickly restore communications capability.

4. Contact Information

Sales
E-mail: TelexDispatch@keenfinity-group.com
Phone: (800) 752-7560
Fax: (402) 467-3279

Customer Service Repair
E-mail: repair@keenfinity-group.com
Phone: (800) 553-5992

Technical Support
E-mail: TelexDispatchtechsupport@keenfinity-group.com
Web: www.telex.com

5. Open Source Software Licenses

Telex RDC Open-Source Libraries with Respective Licensing.

5.1 Server

Boost
Licensed for use under the Boost Custom License.

Casablanca
Licensed for use under a MIT License.

Crypto++
Licensed for use under the Crypto++ Custom License.

G711 Codec
Licensed for use under a MIT License.

jRTPlib
Licensed for use under a MIT License.

jThread
Licensed for use under a MIT License.

OpenSSL
Licensed for use under the OpenSSL Custom License.

Opus Codec
Licensed for use under a BSD License

RabbitCode
Licensed for use under a BSD-2 License.

Resizeable
Licensed for use under a CPOL License.

Speex
Licensed for use under a BSD Variant License.

WebRTC
Licensed for use under a BSD-3 License.

WebSockett++
Licensed for use under a BSD-3 License.

WT Web Toolkit
Licensed for use under a GNU General Public (GPL) License.

5.2 Client (iOS App)

RealHTTP
Licensed for use under a MIT License.

SwiftyJSON
Licensed for use under a MIT License.

WebRTC
Licensed for use under a BSD-3 License.

5.3 Client (Android App)

Android Jetpack
Licensed for use under an Apache 2.0 License.

Facebook Flipper
Licensed for use under a MIT License.

google-webrtc
Licensed for use under a BSD Variant License.

kotlin-semver
Licensed for use under a MIT License.

kotlinx-coroutines
Licensed for use under an Apache 2.0 License.

nv-websocket-client
Licensed for use under an Apache 2.0 License.

Permission-util
Licensed for use under an Apache 2.0 License.

rxkotlin
Licensed for use under an Apache 2.0 License.

sslcontext-kickstart
Licensed for use under an Apache 2.0 License.

5.4 Client (Web)

ag-grid
Licensed for use under a MIT License.

angular-bootstrap
Licensed for use under a MIT License.

angular-minicolors
Licensed for use under a MIT License.

angular-slider
Licensed for use under a MIT License.

angular-touch
Licensed for use under a MITLicense.

angular-ui-router
Licensed for use under a MIT License.

angularjs
Licensed for use under a MIT License.

blob-polyfill
Licensed for use under a MIT License.

bluebird
Licensed for use under a MIT License.

bootstrap
Licensed for use under a MITLicense.

dragula
Licensed for use under a MIT License.

font-awesome fonts
Licensed for use under a SIL-OFL License.

FontAwesome (Code)
Licensed for use under a MIT License.

GoldenLayout
Licensed for use under a MIT License.

hammerjs
Licensed for use under a MIT License.

jquery
Licensed for use under a MIT License.

jquery-minicolors
Licensed for use under a MIT License.

jsonlint
Licensed for use under a MIT License.

kurento-client
Licensed for use under an Apache 2.0 License.

kurento-utils
Licensed for use under an Apache 2.0 License.

Leaflet
Licensed for use under a BSD-2 License.

leaflet-popup-angular
Licensed for use under a MIT License.

Leaflet.awesome-markers
Licensed for use under a MIT License.

Leaflet.markercluster
Licensed for use under a MIT License.

ng-file-upload
Licensed for use under a MIT License.

preventPullRefresh
Licensed for use under a MIT License.

Promise.finally polyfill
Licensed for use under a MIT License.

ui-select
Licensed for use under a MIT License.

URI
Licensed for use under a MIT License.

virtual-keyboard
Licensed for use under a MIT License.

web-audio-touch-unlock
Licensed for use under a MIT License.

webrtc-adapter
Licensed for use under a BSD-3 License.

x-frame-bypass
Licensed for use under an Apache 2.0 License.

6. Downloads

Telex RDC Server:
Download Telex RDC Server v130 for Windows

Telex RDC Client:
Download Telex RDC Client for Android (AAB)
Download Telex RDC Client for Android (Google Play)
Download Telex RDC Client for iOS (App Store)