## Contents

**About LogMeIn Rescue** ............................................................................................................. 5  
Technician Console – At a Glance ................................................................................................. 5  
Administration Center – At a Glance .......................................................................................... 5  
Security in LogMeIn Rescue ........................................................................................................ 6  
How to Set Up LastPass Authenticator for Rescue Two-Step Verification ............................... 6  
About Rescue in a Multilingual Environment ........................................................................... 7  
How to Set Technician Console Language ............................................................................... 8  
How to Set Language for the Technician Console for Collaborators ....................................... 8  
About Customer-side Language Settings .................................................................................... 8  

**Technician Console Fundamentals** ....................................................................................... 9  
LogMeIn Rescue System Requirements ...................................................................................... 9  
Launching the Technician Console in a Browser ......................................................................... 9  
Technician Console Desktop App for Windows and Mac ............................................................... 9  
How to Install the Desktop App .................................................................................................. 10  
How to Run the Desktop App ...................................................................................................... 10  
How to Set Up One-Click Login to the Desktop App .................................................................. 10  
About Technician Console Permissions ...................................................................................... 10  
Managing Technician Status ...................................................................................................... 11  
Setting up the Technician Console ............................................................................................ 11  
How to Change Technician Console Color .................................................................................. 11  
How to Set Sound Alerts ........................................................................................................... 11  
How to Set Session-end and Log-off Prompts ......................................................................... 12  
How to Set Rescue to Automatically Start Sessions .................................................................... 12  
How to Enable Spell Check ........................................................................................................ 12  
Managing Sessions ................................................................................................................... 13  
About the Session Toolbar ......................................................................................................... 13  
Using the Queue tabs to Locate Sessions .................................................................................. 15  
Using the Session List to View Sessions .................................................................................... 15  
How to Edit Fields on the Session List ...................................................................................... 15  
How to Switch Between Multiple Active Sessions ..................................................................... 16  
How to Put a Session on Hold .................................................................................................... 17  
How to Transfer a Session ......................................................................................................... 17  
Communicating with Customers ................................................................................................. 18  
About the Technician Console Chat Panel .................................................................................. 18  
About Predefined Replies and URLs ........................................................................................... 21  
How to Send a File to a Customer .............................................................................................. 22  
How to Send a Customer Survey .............................................................................................. 23  
Documenting your Sessions ....................................................................................................... 23  
How to View Session History (Log and Notes) ......................................................................... 24  
How to Take Notes During a Session .......................................................................................... 24  
Monitoring Technicians ............................................................................................................ 24  
How to View a Technician's Desktop .......................................................................................... 24  
How to Join a Monitored Technician's Session ......................................................................... 25  

**Supporting Desktop Devices** ................................................................................................. 26  
Connecting to PCs and Macs ..................................................................................................... 26  
How to Start a PC/Mac Session via Link and Messaging Tool ...................................................... 26  
How to Start a PC/Mac Session via PIN Code ............................................................................. 27  
How to Start a PC/Mac Session via Email .................................................................................... 27
About LogMeIn Rescue

LogMeIn Rescue is used to provide instant remote support to customers and employees. With Rescue, you can gain control of a remote PC, Mac, or smartphone over the web in seconds, without the need to pre-install software.

- **Increase first call resolution.** Multi-session handling, Instant chat, technician collaboration and more help reduce escalations to level 2 support and solve more issues on the first call.
- **Decrease average call handle times.** Advanced diagnostic, collaboration and reporting tools accelerate problem identification and resolution.
- **Reduce costly device returns.** Diagnostic tools, device history and remote device configuration help technicians resolve more issues remotely and reduce unnecessary returns.

To purchase subscriptions or sign up for a free trial or demo, go to the LogMeIn Rescue website at [https://www.logmeinrescue.com/](https://www.logmeinrescue.com/).

Technician Console – At a Glance

Technicians provide remote support using the LogMeIn Rescue Technician Console. Technicians can choose to run the Technician Console in a supported browser or as a desktop application.

Key features:
- Direct connection to the Customer via PIN code or emailed link
- Desktop View and Remote Control, including Whiteboard
- Detailed Session History & Notes
- Chat Interface with Predefined Replies, URL Push, and File Transfer
- Detailed System Diagnostics, including Reboot & Reconnect
- Collaboration with internal or external technicians
- Rescue Lens

**Note:** A limited version of the Technician Console is used by unlicensed technicians during an external collaboration session.

Administration Center – At a Glance

Administrators use the LogMeIn Rescue Administration Center to configure LogMeIn Rescue for use by support organizations of any size.

The online interface is used by administrators to create and assign permissions for other administrators and Technician Groups. Administrators can also create support channels – web-based links that automatically connect customers to technicians.

The Administration Center allows administrators to:
- Create Technician Groups and assign group permissions
- Assign support channels to specific Technician Groups

Copyright © 2018 LogMeIn, Inc.
• Enable and view reports of technician performance
• Enable and view reports of customer satisfaction levels
• And more. See the LogMeIn Rescue Administrator's Guide for details.

Security in LogMeIn Rescue

For detailed information, see the LogMeIn Rescue Architecture Whitepaper.

How to Set Up LastPass Authenticator for Rescue Two-Step Verification

Master Administrators can require you to use two-step verification when logging in to Rescue. This section describes how you can set up the LastPass authenticator app to verify your identity during two-step verification.

1. Upon entering your LogMeIn Rescue credentials at the Rescue website or in the Rescue Desktop Technician Console, you are prompted to set up an additional way to verify your account. Click Set up.
   The Set up two-step verification page is displayed.
2. On the Set up two-step verification page, click Set up two-step verification.
   The Protect your account page is displayed.
3. On the Protect your account page, click Set up mobile app.
   The Set up mobile app page is displayed.

   Tip: If you already have the LastPass Authenticator mobile app, click Next.

4. Download the LastPass Authenticator app, and click Next.
5. Launch LastPass Authenticator on your device, and scan the QR code, as follows:
   a) On the LastPass Authenticator app, tap the + (plus) sign.
   b) Physically hold your device in front of the Rescue website to scan the code.
   A message is displayed confirming that your device has been paired to your LogMeIn Rescue account. Tap to dismiss the message.
6. Returning to the Protect your account page, you must now set up the text message backup method to be used when your primary method is unavailable.
   a) Click Set up text message.
      The Set up backup text messages page is displayed.
   b) Enter the phone number to which login codes should be sent, and click Next. A code is sent to your phone in a text message.
   c) On your phone, open the text message from LogMeIn Rescue.
   d) Enter the code from the text message on the Verify phone number page.
   e) Click Finish text setup.
      You are taken back to the Protect your account page.
7. Click Activate at the bottom of the page to actually turn on two-step verification. The Your changes have been saved page is displayed.
8. Click Done.
   You can now log in to your Rescue account or the Rescue Desktop Technician Console using two-step verification.
About Rescue in a Multilingual Environment

Supported Languages

The LogMeIn Rescue web site, Technician Console, Administration Center, Command Center, Mobile BlackBerry Applet, and the www.LogMeIn123.com PIN code entry form are available in the following languages:

<table>
<thead>
<tr>
<th>Language Code</th>
<th>Language</th>
</tr>
</thead>
<tbody>
<tr>
<td>de</td>
<td>German</td>
</tr>
<tr>
<td>en</td>
<td>English</td>
</tr>
<tr>
<td>es</td>
<td>Spanish</td>
</tr>
<tr>
<td>fr</td>
<td>French</td>
</tr>
<tr>
<td>it</td>
<td>Italian</td>
</tr>
<tr>
<td>ja</td>
<td>Japanese</td>
</tr>
<tr>
<td>ko</td>
<td>Korean</td>
</tr>
<tr>
<td>nl</td>
<td>Dutch</td>
</tr>
<tr>
<td>pt-br</td>
<td>Portuguese (Brazilian)</td>
</tr>
<tr>
<td>th</td>
<td>Thai</td>
</tr>
<tr>
<td>zh</td>
<td>Chinese</td>
</tr>
<tr>
<td>zh-TW</td>
<td>Chinese (Taiwan)</td>
</tr>
</tbody>
</table>

The Rescue Applet for PC and Mac, mobile apps, Calling Card, and Instant Chat interface are available in the following languages:

<table>
<thead>
<tr>
<th>Language Code</th>
<th>Language</th>
</tr>
</thead>
<tbody>
<tr>
<td>ar</td>
<td>Arabic</td>
</tr>
<tr>
<td>bg</td>
<td>Bulgarian</td>
</tr>
<tr>
<td>cz</td>
<td>Czech</td>
</tr>
<tr>
<td>da</td>
<td>Danish</td>
</tr>
<tr>
<td>de</td>
<td>German</td>
</tr>
<tr>
<td>el</td>
<td>Greek</td>
</tr>
<tr>
<td>en</td>
<td>English</td>
</tr>
<tr>
<td>es</td>
<td>Spanish</td>
</tr>
<tr>
<td>fi</td>
<td>Finnish</td>
</tr>
<tr>
<td>fr</td>
<td>French</td>
</tr>
<tr>
<td>he</td>
<td>Hebrew</td>
</tr>
<tr>
<td>hr</td>
<td>Croatian</td>
</tr>
<tr>
<td>hu</td>
<td>Hungarian</td>
</tr>
<tr>
<td>it</td>
<td>Italian</td>
</tr>
<tr>
<td>ja</td>
<td>Japanese</td>
</tr>
<tr>
<td>ko</td>
<td>Korean</td>
</tr>
<tr>
<td>nl</td>
<td>Dutch</td>
</tr>
<tr>
<td>no</td>
<td>Norwegian</td>
</tr>
<tr>
<td>pl</td>
<td>Polish</td>
</tr>
<tr>
<td>pt</td>
<td>Portuguese</td>
</tr>
<tr>
<td>pt-BR</td>
<td>Portuguese (Brazilian)</td>
</tr>
<tr>
<td>ru</td>
<td>Russian</td>
</tr>
<tr>
<td>sk</td>
<td>Slovak</td>
</tr>
<tr>
<td>sv</td>
<td>Swedish</td>
</tr>
<tr>
<td>th</td>
<td>Thai</td>
</tr>
<tr>
<td>tr</td>
<td>Turkish</td>
</tr>
<tr>
<td>zh</td>
<td>Chinese</td>
</tr>
<tr>
<td>zh-TW</td>
<td>Chinese (Taiwan)</td>
</tr>
</tbody>
</table>

The Android app is available in these additional languages: es-AR, et, fa, in, lt, lv, my, sl, sr, uk, vi

Tip: To resolve problems with keyboard layout during remote control, see How to Use Local and Remote Keyboard Layouts (Keyboard Synchronization) on page 49.
Tip: For self-hosted Instant Chat, you can add or remove languages to meet your organization’s requirements. See How to Customize Instant Chat Language Files in the LogMeIn Rescue Customization and Integration Guide.

How to Set Technician Console Language

The browser-based version of the Technician Console will use the language that is active on the Rescue Login page, Administration Center, or My Account page when you launch the Technician Console. The desktop app will use the language selected at the time of installation.

For example, if you are viewing the Rescue Login page in Spanish when you launch the Technician Console, then the Technician Console will open in Spanish.

- To change the active language used by the browser-based console:
  a) Exit the Technician Console.
  b) Change the active language on the Login page or My Account page.
  c) Re-launch the Technician Console in your browser.

- To change the language used by the desktop app, uninstall and reinstall the desktop app. Be sure to choose the desired language during installation.

How to Set Language for the Technician Console for Collaborators

The language used by the Technician Console for Collaborators is determined as follows:

- If the external technician is invited via link, the Collaborator version of the Technician Console will use the same language as the inviting technician.
- If the external technician is invited via PIN code, then the collaborating technician is able to select from available languages on the PIN code entry page (for example, LogMeIn123.com). Available languages are the same as for the regular Technician Console.

About Customer-side Language Settings

The LogMeIn Rescue Applet, Instant Chat, and Calling Card will run in the language selected as the active language on the customer’s computer.

If the Applet is not available in the customer’s language, the English version will be used.

The Instant Chat panel has a language selector, while the Applet and Calling Card do not.

The Mobile Applet will automatically detect the target smartphone’s language setting and run in that language. If the Applet is not available in the customer’s language, the English version will be used.

Tip: In Windows, language is set using the Control Panel > Regional and Language Settings > Language tab.

Example

Assume you are a UK-based technician using Rescue in English. You make contact with a customer in Germany. Your customer is using a German version of Windows, but she has changed her Regional and Language Settings to Turkish. She will see the Applet in Turkish.
Technician Console Fundamentals

LogMeIn Rescue System Requirements
Visit help.logmein.com for up-to-date system requirements.

Launching the Technician Console in a Browser
The first time a technician logs on at the LogMeIn Rescue website from a particular PC, a small software client is offered for download and installation.

A Technician Console client MSI installer is also available in case the automatic download and install does not succeed.

Restriction: On a Mac, the Technician Console cannot be run in a browser.

Technicians can also run the Technician Console as a desktop application. See Technician Console Desktop App for Windows and Mac on page 9.

Technician Console Desktop App for Windows and Mac
Technician Console as a desktop application is available for technicians both on Windows and Mac computers.

The desktop app offers the same set of features as the browser-based version. The only difference is that it runs as a standalone executable, which means it can be launched with a single click – no browser required.

Restrictions and limitations for the Technician Console for Mac
The following Technician Console features are not available on Mac:
- Technician screen sharing
- Screen recording with MSVC codec (falls back to MRLE codec)
- Monitoring the desktop of a technician running the Technician Console for Mac
- Integrated content portal (ICP)
- Connect On LAN
- Single Sign-on (SSO) login
- Lens audio

Note: Files saved/exported during a session are available at Users/[username]/Library/Application Support/LogMeIn-Rescue/Bottles/logmeinrescue/drive_c/users/crossover/My Documents
How to Install the Desktop App

On Windows

• **Option 1.** Click this link to *download and install the desktop app*
• **Option 2.** Log in to your account at the LogMeIn Rescue website and go to the **My Account** page. Click the link to download the desktop app.

On a Mac

1. Click this link to *download the Technician Console for Mac app.*
2. In the Downloads box, double-click *LogMeInRescueTechnicianConsoleMAC.dmg.*
3. Follow instructions to drag the LogMeIn Rescue icon to your Applications folder. The application is now installed on your computer.

How to Run the Desktop App

On Windows

Launch the application via the Windows Start button, a desktop shortcut, or any other preferred method. You may be prompted to log in to your Rescue account. Use the same email and password combination you use to log in at the LogMeIn Rescue website.

**Tip:** Rescue technicians with a Single Sign-On (SSO) ID can also start the Rescue Desktop Technician Console using any supported SSO authentication method.

On a Mac

Launch the application via **Launchpad** or **Finder > Applications.**

Use the same email and password combination you use to log in at the LogMeIn Rescue website.

**Remember:** Technician Console for Mac will use the language set as the preferred language of the Mac OS X.

How to Set Up One-Click Login to the Desktop App

You can tell Rescue to remember your user name and password when you log in to the desktop app.

About Technician Console Permissions

The exact features you can use and actions you can take in the LogMeIn Rescue Technician Console may depend on permissions granted by a Rescue administrator, a collaborating technician, and potentially a customer during a session.

Check with a Rescue Administrator or lead collaborating technician if you experience permission-related problems.
Managing Technician Status

Status is communicated in the log and illustrated by an icon displayed next to the technician’s name in the Console Status area at the upper left of the Technician Console.

**Online**

![Online icon]

An online technician can accept any session allowed for his Technician Group.

**Away**

![Away icon]

A technician can set his own status to Away by clicking the Online icon. The Away icon will flash while the technician is in Away status. Click the flashing Away icon to switch back to Online.

Sessions cannot be transferred to an Away technician, but an Away technician can see all sessions in his queue and pick up new sessions.

Administrators can set technician status to automatically switch to Away after a given period of system-level inactivity.

**Busy**

![Busy icon]

A technician cannot set his own status to Busy. This is an automatic setting controlled by the Rescue administrator. Administrators can set technician status to automatically switch to Busy once a technician reaches a given number of active sessions.

Sessions cannot be transferred to a Busy technician, but a Busy technician can see all sessions in his queue and pick up new sessions.

Setting up the Technician Console

**How to Change Technician Console Color**

Go to Options > Color Scheme to choose from the available color schemes.

All functionality is the same for all the color schemes.

**How to Set Sound Alerts**

Set the Technician Console to play sounds when particular events occur.
The sounds are standard bells and beeps and cannot be customized.

1. On the Technician Console Options menu, select Configure Sound Alerts. The Sound Alerts dialog box is displayed.
2. You can set the following options:
   - Play a sound when the Technician Console is minimized and a new session enters a private or channel queue
   - Play a sound when the Technician Console is open and a new session enters a private or channel queue
   - Play a sound when a customer intentionally disconnects
   - Play a sound when the network connection is temporarily lost
   - Play a sound when a customer refuses a permission request
   - Play a sound when a session changes status to Urgent
   - Play a sound when new chat text arrives while the Technician Console is minimized or not in focus
   - Play a sound when new chat text arrives when the chat box is not in focus
   - Play a sound when a customer sends a file
   
   A sound will play when each selected event occurs.
3. Click OK to apply your settings.

How to Set Session-end and Log-off Prompts
Set the Technician Console to ask you to confirm each time you end a customer session or log off from the Technician Console.

1. In the Technician Console, select Options. The Options menu opens.
2. You can set the following options:
   - Select Prompt Before Ending Session if you want to be asked to confirm each time you close a customer session
   - Select Prompt before Closing Console if you want to be asked to confirm each time you log off or close the Technician Console

How to Set Rescue to Automatically Start Sessions
You can set all PIN Code and Link sessions to go directly from Connecting status to Active without having to select Start on the Session Toolbar.

- Select Options > Auto-start Incoming Private Sessions.

Tip: If this option is disabled, your Rescue administrator may have set the default behavior in the Administration Center (Administration Center > Settings > Technician Console > Auto-start incoming private sessions).

How to Enable Spell Check
Enable spell check to automatically check the spelling of all text you enter in the Rescue Chat panel.

- To enable spell check, select Tools > Spell Check > Download [language] Dictionary.
The active spelling dictionary will appear with a checkmark next to the language name.

Select Turn Off to deactivate the spell check.

Managing Sessions

About the Session Toolbar
Use the Session Toolbar to take action on sessions in your Session List.

New Session

Use the New Session button to start a new Private Session.
This option is only available if the agent’s Technician Group has permission to start Private Sessions.

Unattended Access

Click Computers to open a list of computers on the Unattended Accessible tab for which Unattended Access has been enabled. See Working with Unattended Computers on page 31.

Only computers which you have the right to access are shown.

Unattended Access Over LAN

Click Computers to open a list of computers on the Connect On LAN tab that are accessible over your local network.

Note: In case of Technician Console for Mac, the Connect On LAN feature is not available.

You must have the login credentials for connecting to a computer on your network.

Monitor technician

Administrators with a technician seat can click Monitor technician to view the desktop of technicians in their organization.
For details, see How to View a Technician’s Desktop on page 24.

**Start**

Click **Start** to activate a selected session.

If the **Start** button is inactive (grayed out), you may have reached the maximum number of active sessions allowed by your administrator.

See also How to Set Rescue to Automatically Start Sessions on page 12.

**End**

Click **End** to terminate a selected session. The connection to the customer will be closed.

**Hold**

Click **Hold** to place a session on Hold.

**Transfer**

Select any session in the queue and click **Transfer** to transfer a session to an available technician.

This option is available if the agent’s Technician Group has permission to transfer sessions.

**Screen Sharing**

Click the **Screen Sharing** button to initiate screen sharing with a customer.

This option is available if the agent’s Technician Group has permission to use the Screen Sharing feature.

**Invite Technician (Collaborate)**

Click **Invite Technician** to initiate Technician Collaboration.
This option is only available if the agent's Technician Group has permission to send collaboration invitations.

Using the Queue tabs to Locate Sessions

Use the Queue tabs to locate accessible sessions.

Select a queue to change the sessions displayed in the Session List.

- **All**: Select the All queue to show all sessions from all queues.
- **Private Queue**: Select the Private Queue to show Private Sessions of any status.
- **Channel Queue**: Select the Channel Queue to show Channel Sessions of any status.
- **Active Sessions**: Select the Active Sessions queue to show only sessions with Active status.
- **Monitored**: Administrators can select the Monitored queue to show technicians being monitored. This tab is not visible to technicians.

Using the Session List to View Sessions

The Session List (also sometimes referred to simply as the "queue") displays all sessions for the selected queue.

- To take action on a listed session, select the session and click the appropriate Session Control
- To copy various session details for use in other programs, right click on a session and select **Copy to Clipboard**
- You can customize Session List columns by right-clicking any column and selecting columns from the resulting menu
- You can edit any Custom Field (as defined in the Administration Center) directly from the Session List for any Active session.

Colors, sounds and visual effects

Various colors, sounds and visual effects are used to highlight sessions at different times.

- A session being established is shown in gray
- A newly added session flashes blue for a few seconds
- A waiting session or an active session is shown in black
- An urgent session flashes orange

If the Technician Console is minimized when a session is added to a queue, the minimized window in the task bar will flash.

💡 Tip: The exact timing of the various warnings is set in the Administration Center.

How to Edit Fields on the Session List

You can edit any Custom Field (as defined in the Administration Center) directly from the Session List for any Active session.
The agent's Technician Group must have permission to use the **Inline Editing of Queue** feature.

1. For any Active session, hold your mouse over any field. Any field that turns yellow can be edited. The entire field must be visible. Scroll to show the entire field before trying to make changes.

2. Click the field. The field becomes editable.

3. Type your changes.

4. Exit the field. The new value is shown in the **Name** field, the Chat Panel title, and on the Session tab title.

**How to Switch Between Multiple Active Sessions**

Use the Active Session tabs to switch between up to ten concurrent sessions.
• Click on the session you want to work with. You will be able to support the customer using the Technician Console tabs and workspace.

Caution: For Private Sessions, the name shown on the Session tab is the name you enter in the Generate New Session dialog box when you create the session. If you do not enter a name or other identifier when you create a session, then the Active Session tab for that session will be labeled “Customer”.

• Other options for switching sessions:
  • Click the Chat panel belonging to the target customer’s session
  • Click the target session in the Session List

Note: The time shown on the Active Session tab is the elapsed time for the current session status.

Tip: You can maintain ten active sessions at a time. Since On Hold sessions do not count as Active, the hold feature gives you flexibility when managing multiple sessions.

How to Put a Session on Hold

The agent’s Technician Group must have permission to hold sessions.

A session can remain On Hold for 14 days.

1. On the Session List, select the session you want to place on hold.
2. Click the **Hold** button.

The session remains in your Session List with the status On Hold.

Tip: The session timer will show the Time On Hold, as well as the cumulative Total Time of the session.

Any active remote control sessions will close when you place a customer On Hold. To restore the session, select it and click **Start**.

Note: You can maintain ten active sessions at any time. Since On Hold sessions do not count as Active, the hold feature gives you flexibility when managing multiple sessions.

How to Transfer a Session

The agent’s Technician Group must have permission to transfer sessions.

1. Select any session in the Session List and click **Transfer**. The **Transfer Session** window is displayed.
2. In the **Enter Comment** field, enter useful information for the technician to whom you are transferring the session.
3. Use the **Search** box to help locate the organization member to whom you want to transfer the session. You can select any organization member shown in bold.
Note: The list of organization members visible in the Transfer Session window depends on a permission granted by a Rescue Administrator.

4. Select the technician to whom you want to transfer the session.
5. Click OK.
   The session appears in the selected technician's Session List as incoming and in your own as Outgoing.

   **Tip:** To cancel the transfer, click Start while the session is Outgoing.

6. The receiving technician selects the session and clicks Start to activate.
   The session is removed from your Session List.
   The transfer is complete.

### Communicating with Customers

**About the Technician Console Chat Panel**

Use the Chat panel to communicate with customers during active sessions.

Unless you are in Collaboration mode, chat sessions are limited to two participants: the technician and the customer.

The Chat panel consists of the following elements.

#### Session controls

1. Click the tab of any session you want to work with.
2. Click a down arrow to minimize a session.
3. Click an X to close a session.
4. Click a right arrow to restore a minimized chat session.

#### Screen Share button

1. Click the **Share Screen** icon to share your screen with a customer.
Click the **Invite Technician** icon to collaborate with other technicians.

This option is available if the agent’s Technician Group has permission to use the Collaboration feature and at least one other technician is online and available.

This option is available if the agent’s Technician Group has permission to use the Enable/Disable Chat feature.

The Log area shows the chat conversation and also other activities, such as status changes and connection messages.

**Text Input box**
Use the Text Input box to type messages and view input before you send it to the customer. If you do not see the Text Input box, chat may be disabled for your account (check with your administrator for more information).

**View Chat Panel in Fullscreen Mode**

When viewing the customer’s computer in fullscreen mode, click the **Show chat window** button to see the Chat panel without toggling between windows.

**Send File button**

Click the **Send File** button to send a single file to the customer. This option is not available during Instant Chat in chat-only mode.

**Push URL button**

Allows you to push a URL to the customer. Type the URL into the text input field and then send it to the customer by clicking URL. For Applet-based sessions, the website automatically opens on the customer’s machine. For Instant Chat in Chat-only mode, the customer must click a link. See *About Predefined Replies and URLs* on page 21.
Predefined Replies

Allows you to choose from a list of frequently used messages and URLs. See About Predefined Replies and URLs on page 21.

About Predefined Replies and URLs

A Predefined Reply or URL is a string of text or a URL that a technician can send to a customer. Predefined replies and URLs help you save time and keystrokes. FTP addresses can also be sent using the Push URL function.

How to Send a Predefined Reply

You can send a predefined reply to a customer at any time during an active session.

1. On the Chat console, click the Predefined Reply button.
   
   A menu is displayed showing all available predefined replies.

2. Select the predefined reply you want to send to the customer. The text of the selected reply appears in the Chat box.

3. Optional: edit the text.

4. Press Enter or click the Send button. The reply is sent to the customer.

How to Send a Predefined URL

You can send a predefined URL to a customer at any time during an active session.

The agent’s Technician Group must have permission to send URLs.

1. On the Chat console, click the Push URL button.

   A menu is displayed showing all available predefined URLs.

2. Select the predefined URL you want to send to the customer. The text of the selected reply appears in the Chat box.

3. Optional: edit the text.

4. Press Enter or click the Send button. The URL opens in the customer’s default browser.

How to Add an Individual Predefined Reply or URL

1. From the Tools menu, select Manage Predefined Replies. The Manage Predefined Replies tab is displayed in the Technician Console workspace.

2. On the Predefined Replies or Predefined URLs tab, click Add New. The Add New Predefined Reply form is displayed.

3. Give the reply or URL a short Name.
4. Type the text of the reply or the URL in the **Content** box.
   All content is text only. Formatting is not available.

   ![Note] You can also enter an FTP address.

5. Click **Save**.

   You can send the predefined replies and URLs via the Chat panel.

**How to Export Predefined Replies and URLs**

An administrator or technician can create a set of standard replies and URLs and then export them to an XML file. Other technicians will then be able to import the replies and URLs into their own Technician Console.

1. Create a set of predefined replies and URLs.
2. From the **Tools** menu, select **Manage Predefined Replies**.
   The Manage Predefined Replies tab is displayed in the Technician Console workspace.
3. On the Manage Predefined Replies tab, click the **Import/Export** tab.
4. Click **Export**.
   The **Save As** dialog box is displayed with **replies.xml** in the **File name** field.
5. Choose a location where you would like to save **replies.xml**.
   You should choose a location accessible to other members of your organization.

   ![Remember] Files saved/exported during a session are available at
   Users/[username]/Library/Application
   Support/LogMeIn-Rescue/Bottles/logmeinrescue/drive_c/users/crossover/My
   Documents

6. Click **Save**
   Your replies and URLs are saved as an XML file.

**How to Import Predefined Replies and URLs**

An administrator or other technician must first create and export an xml file containing the predefined replies and URLs.

1. From the **Tools** menu, select **Manage Predefined Replies**.
   The Manage Predefined Replies tab is displayed in the Technician Console workspace.
2. On the Manage Predefined Replies tab, click the **Import/Export** tab.
3. Click **Import**.
   The **Open** dialog box is displayed.
4. Locate the xml file and click **Open**.
   The replies are added to your list of predefined replies.

   You can send any of the imported predefined replies via the Chat panel.

**How to Send a File to a Customer**

Follow this procedure to send a single file to a customer via LogMeIn Rescue.
The customer must be running the Rescue Applet or Calling Card. This option is not available during Instant Chat in chat-only mode.

The agent’s Technician Group must have permission to send files.

You can only send one file at a time.

1. On the Chat console, click the Send File button.

   The Open dialog box is displayed.

2. Select the file you want to send to the customer and click Open.
   The customer is prompted to save the file.

3. Ask the customer to choose a location and click Save.
   The file is saved to the customer's chosen location.

   An MD5 fingerprint is generated and communicated to both the technician and the customer in the log.

**How to Send a Customer Survey**

A Rescue Administrator must activate Customer Survey at the Technician Group or Channel level for this feature to be available.

- **Automatic Deployment at Session End**
  - For all Applet-based sessions, the customer survey automatically opens in a browser window at session end.
  - For Instant Chat sessions in Chat-only mode, the customer is prompted to open the survey when the technician ends the session.

    Sample Message: "0:00 AM [Technician Name] would like you to complete a brief Customer Survey. Open Customer Survey"

    The customer must click the link to open the survey.

- **Manual Push During Session**
  - At any time during an active session, right-click a session in the Session List and select Push Customer Survey. For Applet-based sessions, the customer survey automatically opens in a browser window. For Instant Chat sessions in Chat-only mode, the customer is prompted to open the survey.

**Documenting your Sessions**

See also:

- *How to Record Sessions* on page 49
- *How to Make a Screen Capture During Remote Control* on page 50
- *How to Send a Customer Survey* on page 23
How to View Session History (Log and Notes)

Use the History & Notes tab to view the session log and any notes made during past sessions with the current in-session device.

Note: When supporting an iOS device, the History & Notes tab is not available.

1. During an Active session, click the History & Notes tab.
   The History tab has two sub-tabs: History and Add/Edit Notes. On the History sub-tab, a list of past sessions with the current in-session device is displayed.
2. To view the session log, click View in the Logfile column.
3. To view notes made during a session, click View in the Notes column.

How to Take Notes During a Session

You can take notes during a session and save the notes along with the session log in the session history.

Note: When supporting an iOS device, the History & Notes tab is not available.

1. During an Active session, click the History & Notes tab.
   The History tab has two sub-tabs: History and Add/Edit Notes.
2. Click the Add/Edit Notes tab.
3. Type your note on the Add/Edit Notes tab.
4. Click Save to save your note.
   Any technician will be able to view the note on the History tab during the next session with the same device.

Monitoring Technicians

How to View a Technician's Desktop

Administrators can view the desktop of technicians in their organization from within the LogMeIn Rescue Technician Console.

Requirements:
- A Master Administrator or Administrator with both an administrator and a technician license can use this feature
- Both the administrator and the monitored technician must be running a Technician Monitoring enabled version of the Technician Console
- A Master Administrator can monitor any technician in an organization
- An Administrator can monitor any technician in a Technician Group to which he has administrative rights

Restriction: Monitoring the desktop of a technician running the Technician Console for Mac is not supported.
1. On the Technician Console Session toolbar, click the Monitoring button.

The Monitor Technician dialog box is displayed.

2. In the Monitor Technician dialog box, select the technician you want to monitor.

   Note: The list of technicians visible in the Monitor Technician dialog box depends on a permission granted by a Rescue Administrator.

   Optional: In a large organization, use the Filter field to locate technicians.

3. Click OK.

   A connection is made to the technician's computer and a new Session tab appears in the Technician Console workspace showing the technician's name.

4. You must authenticate yourself to the technician's computer. On the Session tab showing the technician's name, select an authentication method.

   • Select Use current credentials to send the Windows credentials you used to log on to your current Windows session. You must be a Windows administrator or otherwise have user rights on the target machine.

   • Select Add username and password to use a different combination with valid user rights on the target machine.

      Tip: If the domain name is needed in the Username field, the acceptable formats are username@domain and domain\username.

   • Select Request Authorization to ask the technician for permission to monitor his desktop.

5. Click Launch Monitoring.

   The technician's desktop is displayed on the Session tab in your Technician Console workspace.

   Note: The technician will be notified if the Notify technician when monitoring desktop option is selected in the LogMeIn Rescue Administration Center on the Global Settings tab.

How to Join a Monitored Technician's Session

Using the Technician Console, Administrators can invite themselves to join a monitored technician's session as a Collaborating Technician.

This procedure assumes that you are already monitoring a technician.

1. On the Technician Console workspace, select the Session tab for the monitored technician. The Session tab has two sub-tabs: Desktop and Active Sessions.

2. Select the Active Sessions sub-tab.

   A list of the technician's current sessions is displayed.

3. Select the session you want to join.

4. Click Join Session.

   You join the session as a Collaborating Technician. See also About Collaborating Technician Capabilities on page 43.
Supporting Desktop Devices

Connecting to PCs and Macs

LogMeIn Rescue connection methods are defined as either Private or Channel.

- A Private connection is made when the technician initiates a remote session with a customer (the direction is from the technician to the customer). PIN code, Link, and SMS are all Private connection methods.
- A Channel connection is made when a customer initiates contact with a technician through a channel link or form, or using the Rescue Calling Card (the direction is from the customer to the technician).

See also:

- Connecting to On-LAN Computers on page 30
- Working with Unattended Computers on page 31

How to Start a PC/Mac Session via Link and Messaging Tool

Follow this procedure to connect to a customer using a link that you send to a customer using a messaging service or related tool.

The agent's Technician Group must have permission to start Private Sessions.

The agent's Technician Group must have permission to use the Link connection method.

1. On the Session toolbar, click **New Session**. The **Create New Session** window is displayed.
2. Type the customer's name or other identifier in the **Name** field. You will use this name to identify the session on the Active Session tab and in the Session List.
3. Select the **Link** tab.
4. Click **Copy Link to Clipboard**. The link is copied to your clipboard.
5. Paste the link into your messaging tool and send it to your customer.
6. Ask your customer to open the message and click the link or paste it to his browser. The customer sees a dialog box asking him to download the Rescue Applet.
7. Tell the customer to download the Applet. The download should take about 15 to 30 seconds.

   **Note:** The download procedure may vary depending on the customer's operating system and browser.

8. Once the download is complete, ask the customer to click **Run** to execute the Applet. Once the Applet is installed, the customer status will change from Connecting to Waiting.
9. Pick up the session by selecting it in the Session list and clicking **Start**. Customer Status will change to **Active**.

You can now use the Technician Console to deliver remote support.
How to Start a PC/Mac Session via PIN Code

Follow this procedure to connect to a customer using a PIN code.

The agent's Technician Group must have permission to start Private Sessions.

The agent's Technician Group must have permission to use the PIN Code connection method.

1. On the Session toolbar, click New Session.
   The Create New Session window is displayed.
2. Type the customer's name or other identifier in the Name field.
   You will use this name to identify the session on the Active Session tab and in the Session List.
3. Select the PIN Code tab.
4. Click Create PIN Code.
   Rescue generates a 6-digit PIN code and displays it in the Generate New Session window and in the Session Log.
5. Ask the customer to go to the PIN code entry site.
6. The customer enters the PIN and clicks Connect to technician.
   The customer will see a dialog box asking him to download the Rescue Applet.
7. Tell the customer to download the Applet.
   The download should take about 15 to 30 seconds.
   Note: The download procedure may vary depending on the customer's operating system and browser.
8. Once the download is complete, ask the customer to click Run to execute the Applet.
   Once the Applet is installed, the customer status will change from Connecting to Waiting.
9. Pick up the session by selecting it in the Session list and clicking Start.
   Customer Status will change to Active.

You can now use the Technician Console to deliver remote support.

How to Start a PC/Mac Session via Email

Follow this procedure to connect to a customer using a link sent via email.

The agent's Technician Group must have permission to start Private Sessions.

The agent's Technician Group must have permission to use the email connection method.

1. On the Session toolbar, click New Session.
   The Create New Session window is displayed.
2. Type the customer's name or other identifier in the Name field.
   You will use this name to identify the session on the Active Session tab and in the Session List.
3. Select the Email tab.
4. Choose how you want to send the email to the customer:
   - To use your own email client and account, choose Send email via my default email client on this computer.
To allow Rescue to send the email, choose **Send email on my behalf via the LogMeIn Rescue servers** and enter a valid email address in the **To** field.

Additional, technicians with the mobile add-on can select **This email is for a mobile device** if the customer is using a smartphone. (If you know the customer’s platform, you can choose to manually set **Device Platform** using the drop-down list on the Create New Session dialog box. Manual detection may be necessary if local browser settings prevent automatic detection.)

5. Click **Email Link**.
   The email is generated (and sent if you chose to send the mail via the Rescue system).

6. Ask your customer to open the message and click the link or paste it to his browser.
   The customer sees a dialog box asking him to download the Rescue Applet.

7. Tell the customer to download the Applet.
   The download should take about 15 to 30 seconds.

   **Note:** The download procedure may vary depending on the customer's operating system and browser.

8. Once the download is complete, ask the customer to click **Run** to execute the Applet.
   Once the Applet is installed, the customer status will change from Connecting to Waiting.

9. Pick up the session by selecting it in the Session list and clicking **Start**.
   Customer Status will change to Active.

You can now use the Technician Console to deliver remote support.

---

### Sample Email Containing a Connection Link

The default text of the Connection email is set in the Administration Center on the **Settings** tab.

From: Technician's Name, Your Organization  
Sent: Monday, December 31, 2010 3:36 PM  
To: Customer's Name  
Subject: Connection email link

Please click the link below to request a live support session:


Best Regards,  
Support Team

---

### About the Channel Form Connection Method

Channel Form is useful if you offer web-based support to your customers.

This method allows you to host both a link on your website/Intranet as well as a questionnaire which your customers have to complete.

#### Process Overview: Channel Form

- A Rescue Administrator assigns any of the ten available channels in the Administration Center to a Technician Group
- A Rescue Administrator develops the custom web form and defines the custom fields
- A Rescue Administrator makes the Channel Form available on an Internet or Intranet site
A customer opens the Channel Form, enters all required information, and submits the form.
The support session is assigned to the Channel Queue of the Technician Group(s) associated with the
channel.
Any online technician in an assigned Technician Group can activate the support session.

Benefits of the Channel Form Method
- Pre-qualify your users with various customizable conditions: error codes, user ID, problem type
- Collect contact information from your end users; such as phone numbers or email addresses
- Integrates into online functions such as user authentication or automated qualification of the user's
  request via a simple HTML code element
- Allows the best tracking of the user and the problem in the Rescue database

Points to consider:
- Customers may try to connect 24 hours a day, so Rescue Administrators must use 'No Technician
  Available' settings to deal with connections made outside of business hours
- When customers are initiating session requests, Rescue Administrators must use dynamic channel
  and team re-routing to control traffic during peak hours
- Web developer and/or graphic design resources may be required for customization and integration

About the Calling Card Connection Method
The LogMeIn Rescue Calling Card allows for both Channel and Private connections.

When your customers need support, they simply click the Calling Card icon to open your branded Calling
Card Applet.

Unlike other connection methods, the Calling Card needs to be installed on the customer's PC before
it can be used. It exists as a desktop shortcut or Quick Launch icon, which the customer clicks to launch
the pre-installed Calling Card Applet.

The Calling Card can be downloaded as an MSI installer from your website, or it can be silently deployed
by technicians during the first Rescue session with the customer, using the Technician Console.

The Calling Card can be customized in appearance; including text, logos, images, and color schemes.
For advanced Calling Card customization options, see the Customization and Integration Guide.

Important: Calling Card is not available if the customer is using a Mac.

Note: The LogMeIn123 app available through the Microsoft Store offers a limited set of the Calling
Card functionalities for Windows 10S. For detailed information, see the related Release Notes.

Process Overview: Calling Card
- A Rescue Administrator generates Calling Card Installers for channels in the Administration Center
- A Rescue Administrator allows Calling Card deployment for Technician Groups
- A Rescue Administrator associates Calling Card Installers with Technician Groups
- Optional: Rescue Administrators may customize the Calling Card's appearance
- Customers download the Calling Card application or it is deployed by technicians via the Technician
  Console
- A customer opens the Calling Card and connects to your organization using a PIN provided by a
  specific technician or via the channel associated with the Calling Card
- The support session is assigned to the individual technician who provided the PIN, or to the Channel
  Queue of the Technician Group(s) associated with the channel
The individual technician or any online technician in an assigned Technician Group can activate the support session.

**Benefits of Calling Card Connection**
- Once the Calling Card is installed, it offers an easy, one-click, no-download connection
- Branding allows you to extend your corporate appearance right to the customer’s desktop
- The layout can be dynamically changed, for example to announce special offers and marketing messages
- Each Calling Card is linked to a channel

Points to consider:
- Customers may try to connect 24 hours a day, so Rescue Administrators must use ‘No Technician Available’ settings to deal with connections made outside of business hours
- When customers are initiating session requests, Rescue Administrators must use dynamic channel and team re-routing to control traffic during peak hours
- Web developer and/or graphic design resources may be required for customization and integration

**Connecting to On-LAN Computers**

**How to Connect to a Computer on a Local Area Network**
Access computers on your Local Area Network and provide support and maintenance without end-user interaction.

The agent's Technician Group must have **Connect On LAN** permission.

**Restriction:** The Connect On LAN feature is not available for Technician Console for Mac.

1. On the Session Toolbar, click the **Computers** icon.

   The **Computers** list is displayed.

2. On the **Computers** list, click the **Connect On LAN** tab to see a list of accessible computers.

3. Filter computers by name or IP address.

   **Tip:** You can search and connect at any time. You do not need to wait for the entire list of computers to load.

4. Select the computer you want to access and click **Connect**.

   **Important:** If you do not have Administrator rights, you are prompted to enter the login credentials of the computer you want to access.
The session appears in the Technician Console in **Connecting** status. The applet launches on the remote computer and the session starts. The customer does not have to grant access to the computer, so you can manage it without customer interaction.

### Technical Information for Advanced Users

- **Required Windows settings:**
  - File and Printer sharing must be allowed on the customer's firewall.
  - Both the technician and customer computer must use a compatible NTLM authentication method: Control Panel > [System and Security in Win7] > Administrative Tools > Local Security Policy > Local Policies > Security Options > Network security: LAN Manager authentication level (for example, set both to Send NTLMv2 response only).
  - Remote Registry service must not be disabled on the remote computer. Go to Control Panel > Administrative Tools > Services, right-click Remote Registry and click Properties. Set Startup type to Automatic or Manual.
  - NetBIOS uses ports 135, 137, 138, 139
  - Windows uses NTLM authentication to acquire administrator rights. This authentication uses randomly allocated TCP ports: 1024-65535, or 49152-65535 on Vista and Windows Server 2008. Communication through these ports must be allowed by firewalls.

### Working with Unattended Computers

#### About Unattended Access

Unattended access allows a technician to connect to a remote computer when no user is present.

Technicians are often unable to resolve an issue during a single Rescue session; the job may be too big, or the customer may need his computer. The technician and customer could theoretically arrange a time for a second session, but it is more practical for the technician to continue work later – at a time more convenient for all – even when the customer is not present.

#### How to Request Unattended Access to a Customer's Computer

Unattended access allows a technician to connect to a remote computer when no user is present.

Requirements:

- The agent's Technician Group must have permission to use unattended access
- Unattended access requests cannot be sent during the following session types: Instant Chat in Chat-only mode, Mobile Applet

1. During an Active session, click the **Unattended Access** tab.
2. Under **Credentials required**, you may be given the choice between the following options (depending on the authentication settings made in the Administration Center):
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>At connection</strong></td>
<td>Require valid administrator credentials at the start of every unattended session</td>
</tr>
<tr>
<td><strong>At setup</strong></td>
<td>Use credentials entered by the customer during unattended setup</td>
</tr>
</tbody>
</table>

3. Set the duration of unattended access in terms of days, a specific date range, indefinitely, and for a specific daily time range.

*Note:* When the customer's computer is in a different time zone, you can choose to set unattended access according to either local (technician) or customer time.

*Important:* The duration of unattended access is limited to two weeks when you authenticate using customer credentials.

4. Click **Request Unattended Access** to submit the request to the customer.

   The customer must approve the request.
   • When the technician is required to enter valid Administrator credentials at the start of every unattended session, the customer simply clicks **OK** to approve the request.
   • When the technician is allowed to use customer credentials, the customer is prompted to enter his Windows user name and password.

Once unattended access is active, the session can be ended.

**How to Start an Unattended Session**

Unattended access allows a technician to connect to a remote computer when no user is present.

Requirements:
• The agent's Technician Group must have permission to use unattended access
• The customer's computer must be powered on and not in sleep mode for the technician to be able to launch an unattended session

1. On the Session Toolbar, click the **Computers** icon.

   The **Computers** list is displayed.

2. Select a computer from the list.

3. Click **Connect**.

4. You must enter valid Administrator credentials unless you are using credentials entered by the customer during setup of unattended access.

You can now use the Technician Console to deliver remote support.

**How to Manage Accessible Unattended Computers**

Use the Unattended Accessible Computers dialog box to manage unattended computers under your control.

1. On the Session Toolbar, click the **Computers** icon.
The Computers list is displayed.

2. On the Computers list, click the Unattended Accessible tab to see a list of computers that you can access while they are unattended.

3. Manage your accessible computers:
   - Type in the Filter box to locate a computer by name
   - Use the Show box to filter computers by status
   - Select a computer and click Delete to disable unattended access
   
   **Note:** Delete is inactive when other technicians can access the selected computer.

4. Click Close.
   Changes are saved.

**Understanding the Customer Experience**

Customers experience Rescue remote support through one of the following tools.

- Rescue Applet
- Instant Chat
- Rescue Calling Card
- Rescue+Mobile Applet

We have also created an illustrated *Step-by-Step Connection Guide for LogMeIn Rescue* that you can share with customers who need help during the connection process.

**The Customer Experience: Rescue Applet**

The customer is asked to install this small executable file to his computer when a technician initiates a normal session.
Figure 1: Standard Rescue Applet interface

Customer capabilities using the Applet:

• Chat with the technician(s)
• View a detailed session log
• Allow or deny the technician the right to perform certain actions
• Send individual files to a technician
• Change the display font size
• Revoke permissions, such as remote control or file management, from the technician by clicking the large X in the upper-left corner
• End a session by clicking the small X in the upper-right corner

Note: The Applet automatically removes itself at session conclusion.

The Customer Experience: Instant Chat

Instant Chat allows a support technician to engage in a two-way chat session with a customer without forcing the customer to download any software.
With Instant Chat you lose no functionality, but rather gain the flexibility to use the Rescue Applet or not.

**Tip:** To open a remote session or troubleshoot the customer's device, prompt the customer to download the Rescue Applet.

Customers have the following capabilities using the Instant Chat interface in chat-only mode:

- Chat with the technician(s)
- View a detailed session log
- Allow or deny the technician the right to perform certain actions (install the Applet, start remote control)
- End a session by clicking the large X at upper left
- Change the display language using the Language Selector
- Change the display font size

For detailed information on Instant Chat setup and customization, see the LogMeIn Rescue *Customization and Integration Guide*.

**How to Launch the Rescue Applet during Instant Chat**

During an Instant Chat session, the Chat-Only Mode dialog box informs the technician that advanced Rescue tools can only be activated if the customer is running the Rescue Applet.

1. In the Chat-Only Mode dialog box, click **Prompt for Download**.
The customer receives a message asking him to download the Rescue Applet by clicking a link in the chat box.

2. The customer clicks the link and installs the Applet.
   The Instant Chat interface now acts as the full Rescue Applet.

Once the Applet is running, the technician can start remote control and perform all activities he is normally able to perform using the Rescue Applet.

The Customer Experience: Calling Card

It's helpful to understand the customer's experience during a Calling Card session.

Before the session begins, the customer can choose a connection method using the Connect menu (PIN code or a Channel). The customer can also change Proxy Settings by clicking Settings menu.

Figure 3: Standard Rescue Calling Card interface, before connection

The customer has the following capabilities during a Calling Card session:

• Chat with the technician(s)
• View a detailed session log
• Allow or deny the technician the right to perform certain actions
• Send individual files to a technician (or to the Lead Technician during a Collaboration Session)
• Change the display font size
• End Remote Control by clicking the large X at upper left
• End a session by clicking the small X at upper right
• View a brief Help file
Sharing your Screen with Customers

How to Share your Screen with a Customer

Give a customer view-only access to your desktop with a single click.

Requirements:
- The customer must be running the Rescue Applet or Calling Card
- Technician Screen Sharing will not function during Instant Chat until the customer has downloaded the Rescue Applet
- Technician Screen Sharing will not function when the technician is using the Technician Console for Mac.
- The customer must be running a supported Windows operating system (Screen Sharing is currently not compatible with Mac)
- Allow screen sharing with customers must be enabled at the Technician Group level in the Administration Center

1. During an active session, click the Screen Sharing button on the Chat panel or on the Session toolbar.

The customer will see your desktop in a new window.

Important: If the customer's desktop is being displayed on your screen, the customer will see a confusing "mirror effect" during Technician Screen Sharing. To prevent confusion, do not share your desktop during remote control.
2. To end Technician Screen Sharing and continue the support session, click the **Screen Sharing** button again.

![Screen Sharing button](image)

The customer can end Technician Screen Sharing by closing the screen sharing window. The session will remain active.

**Tip:** You can also share your screen with a customer when you are participating in a Collaboration session as a Collaborating Technician.

### About Customer Controls During Technician Screen Sharing

Technicians should be aware of the following controls available to customers during a Technician Screen Sharing session.

- **Full Screen**
  The customer clicks Full Screen to open the technician desktop to cover the entire customer desktop area.

- **Options**
  The customer clicks Options to change color settings and viewing options.

- **Multiple Monitors**
  When the technician is using more than one monitor, the customer clicks the Monitors button to switch between available monitors.

- **Zoom**
  The customer clicks the zoom option to get a more or less detailed view of the technician desktop.

- **Magnifying Glass**
  The customer clicks the Magnifying Glass to activate a box that he can drag around the technician’s desktop to show a small area of the screen in high resolution.

- **End Screen Sharing**
  The customer clicks **End** to stop screen sharing. The End button is only available for the customer in Full Screen mode.

### Collaborating with Other Technicians

### About Technician Collaboration

#### How to Invite an Internal Technician to Collaborate

With Technician Collaboration, multiple technicians can simultaneously support a single customer. Technicians can improve problem resolution by inviting online and available technicians from their Rescue organization to an Active session.

**Requirements:**

- The customer must be running the Rescue Applet, Calling Card
- The session must be Active
- **Send collaboration invitations** must be enabled at the Technician Group level in the Administration Center

1. On the Session List, select the Active session to which you want to invite another technician.
2. On the Session toolbar, click the **Invite Technician** button.
The **Invite Technician** dialog box is displayed.

3. In the **Invite Technician** dialog box, select the technician you want to invite.

   **Note:** The list of technicians visible in the **Invite Technician** dialog box depends on a permission granted by a Rescue Administrator.

   **Remember:** Technician Collaboration is not designed to be used as a meeting tool. To achieve optimal performance, limit participation to four or five technicians. Performance will be impacted by the speed and power of the customer’s device.

4. In the **Set Permissions** section, select the permissions you want to grant to the Collaborating Technician.

   **Note:** All existing Technician Group permissions are applied unless otherwise specified by the Lead Technician, either at the time of invitation or during the session.

5. In the **Comment** box, type a message to the Collaborating Technician.

6. Click **OK**.

   A Collaboration invitation is sent to the selected technician.

   The Collaborating Technician sees the Invitation in his Session List.

---

**How to Invite an External Technician to Collaborate**

With Technician Collaboration, multiple technicians can simultaneously support a single customer. Technicians can improve problem resolution by inviting online and available technicians from outside their Rescue organization to an Active session.

**Requirements:**
- The customer must be running the Rescue Applet, Calling Card
- The session must be Active
- **Invite external technicians** must be enabled at the Technician Group level in the Administration Center
- The external technician must be running a supported Windows operating system: Microsoft Windows 7, 8, 8.1, 10, Vista (all including 64-bit)

1. On the Session List, select the Active session to which you want to invite another technician.

2. On the Session toolbar, click the **Invite Technician** button.

   The **Invite Technician** dialog box is displayed.

3. In the **Invite Technician** dialog box, select the **External** tab.

4. Choose from the available invitation options, as determined by settings made in the Administration Center.

   - Invite unlisted technician
   - Invite approved technician
Remember: Technician Collaboration is not designed to be used as a meeting tool. To achieve optimal performance, limit participation to four or five technicians. Performance will be impacted by the speed and power of the customer's device.

5. In the Set Permissions section, select the permissions you want to grant to the Collaborating Technician.

6. In the Comment box, type a message to the Collaborating Technician.

7. Click OK.
   The Invitation to External Technician is displayed.

8. Choose from the available connection methods, as determined by settings made in the Administration Center.
   - PIN Code
   - Email
   - Link

9. The procedure for sending the invitation to an external technician is similar to the procedure for starting a new session. You must send the PIN Code, email, or link to the external technicians.

To join, the external technician accepts the invitation and downloads the Technician Console – Collaboration version. The session's status changes to Collaborating once the external technician joins.

**Can sessions be transferred to an external technician?** Technicians cannot transfer sessions to an external technician. To receive a transferred session, a technician must be part of your Rescue organization and logged in with a valid Rescue subscription.

### How to Join a Collaboration Session

With Technician Collaboration, multiple technicians can simultaneously support a single customer. Technicians can improve problem resolution by inviting online and available technicians from inside or outside their Rescue organization to an Active session.

Collaboration is by invitation only.

This procedure assumes you have been invited by a Lead Technician from within your own organization. Administrators can invite themselves using the Technician Monitoring feature. See [Monitoring Technicians](#) on page 24.

1. You see a session on your Session List with the status Invitation. Select the session.

2. On the Session toolbar, click Start to accept the invitation and join the session.

   The session appears as Collaborating in the Session List.

3. You can now participate in the session.
   The Lead Technician has ultimate control over your permissions during the session. See [About Collaborating Technician Capabilities](#) on page 43.

4. To leave the session, click the X on the Collaboration Panel (at the top of the Chat panel).
   The session does not end; the Lead Technician remains Active.

### About Lead Technician Capabilities During Collaboration

During a Collaboration Session, the Lead Technician can perform the following actions.
Hand-off Lead Technician status  
This is only available for collaborating technicians within your Rescue organization. External collaborating technicians cannot become lead technician. In the example below, Chris Jones hands off the Lead status to Sam Russel.

Cancel a hand-off  
This is only available for collaborating technicians within your Rescue organization. External collaborating technicians cannot become lead technician. In the example below, Chris Jones cancels handing off the Lead status to Sam Russel.

Remove a Collaborating Technician from a session  
Click the X next to a collaborating technician's name.

Change permissions  
Click a collaborating technician's name to change permissions.
Share their own screen with the customer
Only available if this feature is enabled at the Technician Group level in the Administration Center.

Invite additional technicians
The lead technician can invite additional internal or external technicians, depending on permissions set in the Administration Center.

Enable/Disable Chat
Only available if this feature is enabled at the Technician Group level in the Administration Center.
Chat privately with Collaborating Technicians

The customer will not see the communications. Collaborative chat is available even when chat with the customer is disabled at the Technician Group level.

Place the session on hold

When the lead technician places the session on hold, the session goes on hold for all participants.

Only available if this feature is enabled at the Technician Group level in the Administration Center.

End the session

The session ends for all participants.

About Collaborating Technician Capabilities

During a Collaboration Session, a Collaborating Technician can perform the following actions:

Accept an invitation to take over the Lead Technician role

Once the Lead role is accepted, the technician assumes all of the capabilities of a Lead Technician.

Chat privately with Collaborating Technicians

The customer will not see the communications. Collaborative chat is available even when chat with the customer is disabled at the Technician Group level.

Leave the Collaboration Session

The session does not end. Others will be able to continue to support the customer.

Place a session on Hold, but only for himself

Others will be able to continue to support the customer.
The customer will not see the communications. Collaborative chat is available even when chat with the customer is disabled at the Technician Group level.

**Transfer the session**
Only available if this feature is enabled at the Technician Group level in the Administration Center.

**Screen sharing**
Only available if this feature is enabled at the Technician Group level in the Administration Center.

**Restriction:** A Collaborating Technician cannot receive files sent by a customer using the Applet Send File feature.

## Controlling a Customer's Computer

### How to Remote Control a Customer's Computer
Use Remote Control to operate the customer's device.

**Requirements:**
- The agent's Technician Group must have permission to launch remote control sessions.
- The session must be Active.
- During Instant Chat, remote control can only be started once the customer has downloaded the Rescue Applet.

1. On the Technician Console **Customer Desktop** tab, click **Launch Remote Control Session**. The customer is prompted to accept or decline your request to control his computer.
2. Ask the customer to accept the request. Remote control begins.
3. Use the Remote Control toolbar to manage the remote session. All other Workspace tabs remain available.
4. To end remote control, click the red X on the Remote Control toolbar. Remote control ends, but the session remains active.

**Caution:** Transferring the session or placing it on Hold will end remote control.

### How to View a Customer's Desktop without Taking Control
Use Desktop Viewing to view a customer’s desktop without taking control of the device.

**Requirements:**
- The agent's Technician Group must have permission to launch desktop viewing
- During Instant Chat, desktop viewing can only be started once the customer has downloaded the Rescue Applet
- The session must be Active

1. On the Technician Console **Customer Desktop** tab, click **Launch Desktop Viewing Session**. If the customer is prompted to accept or decline your request, ask them to accept.
2. Use the Remote Control toolbar to manage the session. During desktop viewing, some toolbar options are disabled. All other Workspace tabs remain available.
3. To end desktop viewing, click the red X on the Remote Control toolbar. Desktop viewing ends, but the session remains active.

About Customer User Rights During Remote Control

When you access a customer's computer, you inherit the customer's user rights. As a result, you may encounter support scenarios where the user of the remote device does not have the rights you need to fully support the machine.

To overcome this problem, you can run the Rescue Applet as a Windows System Service Local System account or Mac OS X daemon.

The following table helps clarify when this feature is useful.

<table>
<thead>
<tr>
<th>Customer's Operating System</th>
<th>Customer's Rights</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows 7, Vista, Server 2008</td>
<td>Administrator, with User Account Control (UAC) activated</td>
</tr>
<tr>
<td>Windows 7, Vista, Server 2008</td>
<td>Non-administrator</td>
</tr>
<tr>
<td>Windows NT-based</td>
<td>Administrator, but you want to switch users without losing the active session</td>
</tr>
<tr>
<td>Windows NT-based</td>
<td>Non-administrator</td>
</tr>
<tr>
<td>Mac OS X</td>
<td>Administrator, but you want to switch users without losing the active session.</td>
</tr>
<tr>
<td>Mac OS X</td>
<td>Non-administrator</td>
</tr>
</tbody>
</table>

How to Restart the Rescue Applet as a Windows System Service or Mac Daemon

To log on as a different Windows or Mac user, you must restart the Applet as a Windows System Service or Mac OS X daemon.

You must be in an Active session with a customer lacking Administrator rights on the host. You must be able to enter Administrator credentials.

1. On the Technician Console workspace, select the Customer Desktop tab (this is the tab you use to launch remote control and desktop viewing).
2. In the Username and Password fields, enter valid Administrator credentials for the remote device.
   **Tip:** If the domain name is needed in the Username field, the acceptable formats are username@domain and domain\username.
3. Click Restart Applet as Windows System Service (or Mac OS X daemon).
   The chat log will indicate when the customer applet has started as a Windows system service (or Mac OS X daemon) and is reconnected.
4. Launch remote control.
5. Log-off the current user or switch between users without losing your connection to the machine.
   **Tip:** To activate the login dialog box during a remote control session, press the Ctrl-Alt-Insert keyboard shortcut or click the Ctrl-Alt-Del button on the Remote Control toolbar.
Note: Rescue ensures that the technician will be logged out at the end of any session in which a technician restarts the Applet as a Windows System Service. The customer will be forced to log back in to his original limited-rights account at the end of the support session, thus eliminating potential security risks.

How to View the Customer's Computer in Fullscreen Mode

In Fullscreen Mode the customer's display covers the technician's entire display. Fullscreen mode gives you the most realistic "as if you were there" experience.

- On the Remote Control toolbar, click the Fullscreen button.

Fullscreen

The LogMeIn interface is minimized and the host computer's display appears on your entire screen. Only the Remote Control toolbar remains visible.

- To exit fullscreen mode, click the Fullscreen button again.

Tip: To keep the toolbar visible, click the Pin icon on the Fullscreen version of the Remote Control toolbar.

Tip: To see the Chat Panel without having to toggle between windows, click the Show chat window button.

How to View a Remote Control Session in a Secondary (Tear-Away) Window

By detaching a Remote Control session, you can view the customer's computer in a secondary window outside of the main Technician Console workspace.

- On the Remote Control toolbar, click the Tear Away button next to the Customer Desktop tab.

Customer Desktop  File Manager

The customer’s screen is detached from the Technician Console and appears in a new window. You can move this window to your secondary display.

- Another way to detach the session is to drag-and-drop the Customer Desktop tab.
- To return the session to the Technician Console, click the Attach button next to the Customer Desktop tab or on the detached window itself.
To always launch remote control sessions in a separate window, select Options > Launch Tear-Away Session Windows.

**How to Change Screen Size During Remote Control**

View the customer’s display in a way that you find comfortable.

1. On the Remote Control toolbar, click the View Settings button.
2. Select the appropriate setting.
   - **Actual size** – Select Actual Size to show the host display exactly as it appears to the host-side user. When using this option you may need to scroll to see the entire screen.
   - **Fit to Window** – Select Fit to Window to make the entire host display visible on the client display without the need to scroll.
   - **Stretch to Window** – When in Full Screen Mode, use this option to stretch the host display to fill the entire client display even if the host is set to a lower resolution than your own.

Your selection is applied immediately.

**Tip:** To change the actual screen resolution of the host display, edit the host Desktop Properties (Windows) or System Preferences (Mac).

**How to Change the Color Quality of the Customer’s Screen**

Select a lower setting to optimize the amount of information transferred during remote control, or select a higher setting to improve the quality of the image.

1. On the Remote Control toolbar, click the View Settings button.
   The Color Quality options are displayed.
2. Select the appropriate setting.

   **Tip:** Choose Automatically adjust color settings to allow LogMeIn to detect the optimal setting.

   - **Very Low** – (grayscale) This is best if you are using a slow connection, such as a dial-up modem
   - **Low** – This setting offers excellent performance with acceptable color quality
   - **Medium** – This setting offers a good balance between performance and color quality
   - **High** – This setting offers excellent color reproduction, but potentially slower performance
   - **Auto** – Choose Auto to allow LogMeIn Rescue to detect the optimal setting

Your selection is applied immediately.

**How to Magnify a Section of the Customer’s Screen**

The Magnifying Glass feature opens a box that you move on the customer’s screen to view a small area in high resolution without otherwise adjusting your resolution.

The Magnifying Glass is available when screen resolution is less than 100%.
1. On the Remote Control toolbar, click the **Magnifying Glass** button. The magnifying glass is activated.
2. Drag the box. Any area within the box is displayed in high resolution.
3. Click the **Magnifying Glass** button again to deactivate the magnifying glass.

### How to Open the Windows Task Manager on the Customer's Computer (Ctrl-Alt-Del)

During a remote session, the Ctrl-Alt-Del key combination entered on the technician's computer will only be registered by the client.

This feature is not available during Desktop Viewing.

- On the Remote Control toolbar, click the **Task Manager** button. The Windows Task Manager opens on the customer's computer.

### How to Copy and Paste Between Devices (Clipboard Synchronization)

Use Clipboard Synchronization to save time and avoid errors by directly copying and pasting information between devices during remote control.

This feature is not available during Desktop Viewing.

**Note:** If the customer is using a BlackBerry smartphone, clipboard synchronization will not function.

- On the Remote Control toolbar, select **Clipboard Synchronization On**. Anything copied on either device is available to be pasted to the other.
- To enable clipboard synchronization for all sessions, select **Options > Clipboard Synchronization Enabled**.
How to Use Local and Remote Keyboard Layouts (Keyboard Synchronization)

Use Keyboard Synchronization to ensure that the text you type appears according to the selected keyboard’s layout.

This feature is not available during Desktop Viewing.

1. On the Remote Control toolbar, click **Keyboard Synchronization**.
2. Select **Local** or **Remote** depending on which computer’s keyboard layout you want to use.

How to Draw on the Customer’s Screen

Use the Whiteboard to activate a pencil tool that you can use to draw freehand images on the customer’s screen.

1. On the Remote Control toolbar, click the **Whiteboard** icon and select **Whiteboard On**.
   The pencil tool is activated.

   ![Note](https://via.placeholder.com/150)
   **Note:** You cannot control the host while Whiteboard is enabled.

2. Draw on the host screen.
   The pencil tool leaves a red line on the customer’s screen. All drawings appear on both the Technician Console and the customer’s computer.
3. To erase drawings, click the **Whiteboard** button and select **Erase Drawings** or **Whiteboard Off**.

How to Use the Laser Pointer

The Laser Pointer is a small red dot that the client-side user moves around the host screen to highlight features for the host-side user.

1. On the Remote Control toolbar, click the **Laser Pointer** button and select **Laser Pointer On**.
   To the host-side user, the laser pointer appears as a simple red dot.

   ![Note](https://via.placeholder.com/150)
   **Note:** You cannot control the host while Laser Pointer is enabled.

2. To exit, click **Laser Pointer** again and select **Laser Pointer Off**.

How to Record Sessions

Follow this procedure to make a recording of all on-screen activity during a Remote Control or Desktop Viewing session.

The agent’s Technician Group must have permission to record sessions.

1. During Remote Control or Desktop Viewing, click the **Screen Recording** icon on the Remote Control toolbar.
2. Select **Start Screen Recording**. If you have not yet done so, you will be asked to choose a folder where screen recordings will be saved.

   **Note:** The customer is prompted during a remote control session when the technician starts screen recording. This prompt is displayed even if the customer previously granted the technician permission to access his computer.

3. Recording begins. All activity on the customer's screen will be recorded.

4. To stop recording, click the **Screen Recording** button again and select **Stop Screen Recording**. Screen recording is ended. The session does not end.

   The recording is saved to the assigned location.

   **Tip:** To set the folder where you want to save the recording file, select **Options > Screen Recording Folder**...

   **Note:** Recording file format is set in the LogMeIn Rescue Administration Center on the Settings tab. If files are saved to the LogMeIn proprietary .rcrec format, then you will need to convert them to .avi using the **LogMeIn Rescue AVI Converter** tool on a Windows PC.

### How to Make a Screen Capture During Remote Control

Create a screen capture of the customer's desktop. You can only capture the entire customer display. You cannot select a specific area to capture.

**Remember:** The technician's Technician Group must have permission to make screen captures.

- Click the screen capture icon on the Remote Control toolbar.

### Using File Manager

#### How to Manage Files on a Customer's Device

Use the File Manager to easily and securely transfer files between your computer and the customer's device.

Requirements:

- The agent's Technician Group must have permission to launch File Manager
- During Instant Chat, File Manager can only be started once the customer has downloaded the Rescue Applet
• The session must be Active

1. On the Technician Console File Manager tab, click Launch File Manager Session. The customer is prompted to accept or decline your request to control his computer.

2. Ask the customer to accept the request. The File Manager session begins.

3. Use the File Manager toolbar to work with the customer’s files and folders. All other Workspace tabs remain available.

4. To end the File Manager session, click the red X on the File Manager toolbar. The File Manager session closes, but the session remains active.

Caution: Transferring the session or placing it on Hold will end the File Manager session.

How to Navigate and Sort Files using File Manager

Navigate and Sort options are accessed via a drop-down menu on the File Manager toolbar. Shortcut keys are available for each item.

Note: The host computer’s files are displayed in the right frame, the client computer’s in the left. Use the Tab key to switch between the two frames.

<table>
<thead>
<tr>
<th>Option</th>
<th>Shortcut</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Refresh</td>
<td>F5</td>
<td>Refreshes the folders on both the client and host computer.</td>
</tr>
<tr>
<td>Up</td>
<td>Backspace</td>
<td>Moves up to the parent directory.</td>
</tr>
<tr>
<td>Drive list</td>
<td>Ctrl+Backspace</td>
<td>Displays the available root drives on the selected computer.</td>
</tr>
<tr>
<td>Select left drive</td>
<td>Alt+F1</td>
<td>Click to select the disk drive you want to view in the left pane of the File Manager window.</td>
</tr>
<tr>
<td>Select right drive</td>
<td>Alt+F2</td>
<td>Click to select the disk drive you want to view in the right pane of the File Manager window.</td>
</tr>
<tr>
<td>Go to folder...</td>
<td>Ctrl+G</td>
<td>Click this item to open a box where you can type the name of a specific folder or directory you want to view.</td>
</tr>
<tr>
<td>Sort by Name</td>
<td>Ctrl+1</td>
<td>Sort the directory contents by file name.</td>
</tr>
<tr>
<td>Sort by Type</td>
<td>Ctrl+2</td>
<td>Sort the directory contents by file type.</td>
</tr>
<tr>
<td>Sort by Size</td>
<td>Ctrl+3</td>
<td>Sort the directory contents by file size.</td>
</tr>
<tr>
<td>Sort by Date</td>
<td>Ctrl+4</td>
<td>Sort the directory contents by the date files were last modified.</td>
</tr>
<tr>
<td>Show...</td>
<td></td>
<td>Select Show folders for all users, Show hidden files, and/or Show system files in any combination.</td>
</tr>
</tbody>
</table>

Tip: Click to change between the local and the remote disk drives on the left/right pane of the File Manager window (the shortcut is Alt+1 and Alt+2).
How to Transfer Files Between Computers using File Manager

Transferring files between computers is as easy as selecting files and dragging them to the appropriate folder. Otherwise, use the appropriate options on the File Manager toolbar.

<table>
<thead>
<tr>
<th>Option</th>
<th>Icon</th>
<th>Shortcut</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Copy</td>
<td></td>
<td>Ctrl+C</td>
<td>Copy the selected file or folder from the existing location to the selected new location. The copied file or folder is now in both locations.</td>
</tr>
<tr>
<td>Move</td>
<td></td>
<td>Ctrl+X</td>
<td>Cut a file or folder from the existing location and move it to the new location. The moved file or folder is now only in the new location.</td>
</tr>
<tr>
<td>Synchronize</td>
<td></td>
<td>Ctrl+S</td>
<td>Update the current folders to the client and host so that their contents are the same. Files and folders that exist only on one side are copied normally. If both folders contain one or more files that are different on the client and host, the newer version will be copied. The folders must be open, not simply selected.</td>
</tr>
<tr>
<td>Replicate</td>
<td></td>
<td>Ctrl+R</td>
<td>Files and folders that do not exist in the destination folder are copied normally. Files that already exist in the destination folder will be transferred from the source folder. If a destination folder contains a file or a folder that does not exist in the source it will be deleted. This is very useful if you update the Source folder and want to push those changes to the Destination.</td>
</tr>
</tbody>
</table>
How to Edit Files using File Manager

Edit options are accessed on the File Manager toolbar or by right clicking on a file. Shortcut keys are available for each option.

<table>
<thead>
<tr>
<th>Option</th>
<th>Icon</th>
<th>Shortcut</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create Folder</td>
<td></td>
<td>Ctrl+N</td>
<td>Create a new folder in the selected location</td>
</tr>
<tr>
<td>Rename</td>
<td></td>
<td>F2</td>
<td>Rename a selected file or folder</td>
</tr>
<tr>
<td>Delete</td>
<td></td>
<td>Delete key</td>
<td>Delete a selected file or folder</td>
</tr>
</tbody>
</table>

How to Select Files using File Manager

File selection options are accessed on the File Manager toolbar. Shortcut keys are available for each option.

<table>
<thead>
<tr>
<th>Option</th>
<th>Icon</th>
<th>Shortcut description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select files</td>
<td></td>
<td>+ (on the numeric keypad)</td>
<td>Opens a dialog box you can use to select multiple files</td>
</tr>
<tr>
<td>Unselect files</td>
<td></td>
<td>- (on the numeric keypad)</td>
<td>Opens a dialog box you can use to clear selected files</td>
</tr>
<tr>
<td>Select all</td>
<td></td>
<td>Ctrl+A</td>
<td>Selects all files in the current location</td>
</tr>
<tr>
<td>Select none</td>
<td></td>
<td>Ctrl+- (on the numeric keypad)</td>
<td>Clears all selections in the current location</td>
</tr>
<tr>
<td>Invert selection</td>
<td></td>
<td>* (on the numeric keypad)</td>
<td>Change the current selection status to its opposite (any selected item becomes cleared and any unselected items becomes selected)</td>
</tr>
</tbody>
</table>

Working with System Information

From the System Info tab you can examine various aspects of the customer’s device, but cannot make any changes.

About System Information – Dashboard

The System Info Dashboard tab provides a snapshot of the current status of the customer’s device.

During an active session, click Request Information to retrieve data from the customer’s device.

The following view-only information is available.

- **System Information**
  - Gives details of the customer’s Operating System, BIOS, when the device was last booted, and which user is logged in.

- **CPU Information**
  - Gives details of the make, type and speed of the host’s central processing unit.

Copyright © 2018 LogMeIn, Inc.
<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Memory Information</td>
<td>Provides a complete breakdown of the host's memory size and usage.</td>
</tr>
<tr>
<td>Disk Drives</td>
<td>Gives the amount of used and free space on each disk drive on the customer's device.</td>
</tr>
<tr>
<td>Processes (top 5)</td>
<td>Gives the names of the five processes that are using most CPU time, the percentage of CPU time they are using, and their memory usage.</td>
</tr>
<tr>
<td>Events (top 5)</td>
<td>Gives the five most recent Events from the Application Event Log and System Event Log that have a status other than Information. This is the same information you can see with Administrative Tools/Event Viewer within Windows.</td>
</tr>
<tr>
<td>Scheduled Tasks (last 5)</td>
<td>Gives a list of the five most recently executed scheduled tasks, as run with Windows Scheduled Tasks feature.</td>
</tr>
</tbody>
</table>

**About System Information – Processes**

System Info > Processes gives information about running processes, similar to Windows Task Manager > Processes.

During an active session, click Request Process Information to retrieve data from the customer's device.

**About System Information – Services**

System Info > Services gives information about registered services, similar to Windows Administrative Tools > Services.

During an active session, click Request Services Information to retrieve data from the customer's device.

**About System Information – Applications**

System Info > Applications gives information about installed programs, similar to Windows Control Panel > Add/Remove Programs.

During an active session, click Request Application Information to retrieve data from the customer's device.

**About System Information – Interactive User**

System Info > Interactive User gives details of the account the customer used to log in to his device. This includes information about the user, the group to which the user belongs, and the user's privileges.

During an active session, click Request Interactive User Information to retrieve data from the customer's device.

**About System Information – Drivers**

System Info > Drivers gives driver details similar to Windows Control Panel > System > Hardware > Device Manager (when examining the properties of individual devices).

During an active session, click Request Driver Information to retrieve data from the customer's device.

**About System Information – Startup**

System Info > Startup gives details of applications and processes started when the device starts.
This includes applications and processes started from entries in the registry and those started because they are in a defined ‘startup’ folder (for example, c:\documents and settings\all users\start menu\programs\startup).

During an active session, click **Request Startup Information** to retrieve data from the customer’s device.

**About System Information – Event Viewer**

**System Info > Event Viewer** offers an event viewer much like that found in Windows (Control Panel > Administrative Tools > Event Viewer).

Recent application, security, and system events are shown in a tabbed interface, and can be sorted according to name, date, source, event, user and computer.

During an active session, click **Request Event Viewer Information** to retrieve data from the customer’s device.

**Rebooting a Customer’s Device**

Click the **Reboot** tab to access options for restarting a customer’s device during a remote session.

**Note:** Only available if this feature is enabled at the Technician Group level in the Administration Center.

<table>
<thead>
<tr>
<th>Reboot Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Normal Reboot and Reconnect</td>
<td>All applications on the customer’s device are closed down in an orderly manner and the device is restarted. The customer will have to enter any hardware or other passwords, after which the support session is resumed. During this process the session status is shown as Rebooting.</td>
</tr>
<tr>
<td>Safe Reboot and Reconnect</td>
<td>Use this option to restart the customer's computer in safe-mode with networking enabled. Safe-mode is a special way for Windows to load when there is a system-critical problem that interferes with the normal operation of Windows.</td>
</tr>
<tr>
<td>Emergency Reboot and Reconnect</td>
<td>This option does not allow applications and other processes to terminate gracefully; the customer may lose unsaved data. Windows will, however, shut down properly and flush all outstanding file operations to disk.</td>
</tr>
<tr>
<td>Request Windows Credentials</td>
<td>To allow you to reboot a device while the customer is not present at his machine, the customer can be asked to enter his login credentials. This information remains on the customer’s device, is encrypted, and cannot be accessed or seen.</td>
</tr>
</tbody>
</table>

*Caution:* This option should be used with care. The customer will need to enter any hardware or other passwords, after which the support session is resumed.
### Reboot Option

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Restriction:</strong> If the customer device has a BIOS password configured, or any other hardware-related security mechanism, Unattended Boot Mode cannot work.</td>
</tr>
</tbody>
</table>

---

## Working with Scripts

### How to Create and Edit Scripts

An unlimited number of scripts and resource files can be specified in the Technician Console. LogMeIn Rescue will transfer and execute the script inside the Rescue temp folder on the host computer.

**Script deployment** must be enabled at the Technician Group level in the Administration Center.

1. In the Console Status area, select **Tools > Manage Scripts**. The Manage Scripts page is displayed.
2. Click **Add New**.
3. Name the new script in the **Script name** field.
4. Next to the **Script file** field, click **Browse** to locate the pre-written script.
   - The script file must be present on your computer.
5. Use the **Resource file** field to attach any other file needed to run or support the script.
   - A resource file is any file that you send to a customer via the script. For example, if the script sends a ZIP file to the customer, the ZIP file is the resource file.
   - The resource file must be present on your computer.
6. To make the script run automatically when a session starts, select **Execute when Applet starts**.
7. Select the operating system(s) on which the script will run.
8. Click **Save**.
   - Scripts will be listed in the Local Scripts section on the Scripts tab and will be available for deployment during an active session.

Click **Import** or **Export** to import/export script definitions from/to an XML file.

Click the up and down arrows to the left of a numbered script to change the order in which scripts will execute.

**Remember:** Only those scripts will run automatically that have the **Execute when Applet starts** box selected.

Tip: Sample scripts are available in the **LogMeIn Community Script Repository**.

Tip: You can find your most frequently used scripts more easily by making them favorites. Click the star icon next to the script you want to make favorite.

The script appears on your **Favorite Scripts** list.
You can have maximum five scripts on your Favorite Scripts list.

**How to Deploy a Script**

Follow this procedure to deploy a script during an active session.

**Script deployment** must be enabled at the Technician Group level in the Administration Center.

1. Click the **Scripts** tab.
   
   A list of available scripts is displayed.

2. Select the script you want to deploy.

3. Click **Deploy**.
   
   The script is deployed.

**Remember:** Running an embedded script manually requires the **Run embedded script** permission to be set in the Administration Center.

Embedded scripts are configured by Administrators in the Administration Center.

**Deploying the Rescue Calling Card**

**How to Deploy the Calling Card to a Customer's Computer**

Install the Calling Card on the customer's PC from the Technician Console.

Requirements:

- The agent's Technician Group must have permission to deploy the Calling Card
- A Rescue Administrator must have already applied a Calling Card to the agent's Technician Group
- The session must be Active
- The Calling Card cannot be deployed to a Mac

1. Click the **Calling Card** tab.

2. Select one of the following options:

   - Select **Launch Calling Card immediately after installation** if you want the Calling Card application to run once it has been successfully installed on the customer's computer
• Select **Launch Calling Card every time the remote device is started** to set the Calling Card application to open each time the target device is started.

  **Tip:** Customers can clear this setting on the Settings > General tab of the Calling Card.

3. Click **Install Calling Card.**
   The Calling Card installer is deployed and executed. The customer may be prompted to give you permission to deploy the installer. If so, ask the customer to accept the deployment.

   Once installation is complete, the customer will be able to initiate sessions via the Calling Card.
Supporting Mobile Devices

About LogMeIn Rescue+Mobile

With LogMeIn Rescue+Mobile, remote support technicians can quickly connect to and troubleshoot today’s most popular smartphones as if the device were in their own hands. The product supports Apple iOS, Android, and BlackBerry devices.

The Rescue+Mobile add-on can help you cut costs, save time, increase first call resolution, and show users how to use their smartphone or tablet.

What You Get

- Remote control over most leading smartphone platforms
- Proven helpdesk technology
- Reduced support costs
- Increased customer satisfaction
- Accelerated adoption of new services
- Increased first-call resolution and a decrease in “no trouble found” device returns
- The ability to solve difficult issues for your highly valued customers
- Shorter support lines at your retail outlets

About Click2Fix

The Click2Fix tab gives technicians a set of tools for analyzing and resolving the most commonly encountered issues faced by mobile customers.

The agent’s Technician Group must have permission to use Click2Fix for mobile.

The Click2Fix tab opens by default for each session with a mobile device.

<table>
<thead>
<tr>
<th>Widget</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Info and Alert Bar</td>
<td>The blue <strong>Info Bar</strong> shows basic device info (manufacturer, device model, phone number). The red <strong>Alert Bar</strong> highlights important issues or action items. For example, battery information, flagged applications, or out-of-date firmware. <strong>Detect flagged apps</strong>: Upon connection to an Android or BlackBerry, the Technician Console will automatically check for unwanted or missing apps according to parameters set in an XML uploaded by an administrator. <strong>Detect out-of-date firmware</strong>: Upon connection to an Android or BlackBerry, the Technician Console will automatically check a device’s firmware according to OS properties defined in a file uploaded by an administrator. The file can also contain a URL to current firmware.</td>
</tr>
<tr>
<td>Widget</td>
<td>Notes</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Mobile Network with APN settings transfer</td>
<td>View mobile network info. For Android, BlackBerry and iOS, you can also click <strong>Network setup</strong> to send predefined APN settings to the customer’s device. Available settings are set by an administrator.</td>
</tr>
</tbody>
</table>
| System                                      | For Android, BlackBerry, and iOS, you can view basic information about the customer’s device. Exact information may vary by platform and device. For example:  
  - System version  
  - Baseband number  
  - Build number  
  - Internal storage  
  - SD Card  
  - IMEI |
| Web Shortcuts                               | For Android, BlackBerry, and iOS, you can push icons that give the customer access to web content from their home screen. Available shortcuts are set by an administrator. |
| Battery                                     | For Android, BlackBerry, and iOS, you can view battery details. For Android and BlackBerry, push settings that help optimize battery usage on the customer’s device. Settings can include the following:  
  - Switch off Wi-Fi  
  - Switch off Bluetooth  
  - Switch off GPS  
  - Change brightness settings  
  - Change display timeout settings |
| Connections                                 | For Android, BlackBerry, and iOS, you can view a device’s Bluetooth, GPS, and Wi-Fi connections. For Android and BlackBerry, you can also manage a device’s Bluetooth, GPS, Wi-Fi connections. |
| Device View                                 | View the screen of supported devices (also known as Remote View). Zoom in to draw on the screen. This is also where remote control can be launched for supported devices. |
| QuickNav                                    | For Android, you can jump to specific destination on the customer’s mobile device. |
| Direct URL                                  | For Android, BlackBerry, and iOS, you can send customers predefined or custom URLs, which automatically open on the device. |
| Email                                       | For Android, you can view configuration information about the email accounts configured in the default email app of the customer’s device. You can also add new accounts. For iOS, you can add new email accounts to the default email app of the customer’s device. |
For Android, you can view and manage missing or unwanted (flagged) applications.

For Android, you can view processes and applications running on the device, and see how much memory they are using. You can also kill selected processes and running applications.

Remember: The exact features you can use and actions you can take depend on permissions granted by a Rescue administrator. If a specific widget is inactive (grayed-out), you may not have permission to use it.

Connecting to a Mobile Device

How to Start a Mobile Session by SMS

1. On the Session toolbar, click New Session. The Create New Session window is displayed.
2. Type the customer’s name or other identifier in the Name field. You will use this name to identify the session on the Active Session tab and in the Session List.
3. Click Send SMS. If you know the customer’s platform, you can choose to manually set Device Platform using the drop-down list on the Create New Session dialog box. Manual detection may be necessary if local browser settings prevent automatic detection. A confirmation box appears detailing the phone number and the PIN code that has been sent to the customer in an SMS (text) message.
4. The customer opens the SMS message. The customer clicks to download the applet if not already installed.

Note: The download procedure may vary depending on the customer’s operating system.

5. Pick up the session by selecting it in the Session list and clicking Start. Customer Status will change to Active.

How to Start a Mobile Session via PIN Code

Follow this procedure to connect to a customer using a PIN code.

1. On the Session toolbar, click New Session. The Create New Session window is displayed.
2. Type the customer’s name or other identifier in the Name field. You will use this name to identify the session on the Active Session tab and in the Session List.
3. Click Send SMS. If you know the customer’s platform, you can choose to manually set Device Platform using the drop-down list on the Create New Session dialog box. Manual detection may be necessary if local browser settings prevent automatic detection. A confirmation box appears detailing the phone number and the PIN code that has been sent to the customer in an SMS (text) message.
4. The customer opens the SMS message. The customer clicks to download the applet if not already installed.

Note: The download procedure may vary depending on the customer’s operating system.

5. Pick up the session by selecting it in the Session list and clicking Start. Customer Status will change to Active.

How to Start a Mobile Session via PIN Code

Follow this procedure to connect to a customer using a PIN code.

1. On the Session toolbar, click New Session. The Create New Session window is displayed.
2. Type the customer’s name or other identifier in the Name field. You will use this name to identify the session on the Active Session tab and in the Session List.
3. Click Send SMS. If you know the customer’s platform, you can choose to manually set Device Platform using the drop-down list on the Create New Session dialog box. Manual detection may be necessary if local browser settings prevent automatic detection. A confirmation box appears detailing the phone number and the PIN code that has been sent to the customer in an SMS (text) message.
4. The customer opens the SMS message. The customer clicks to download the applet if not already installed.

Note: The download procedure may vary depending on the customer’s operating system.

5. Pick up the session by selecting it in the Session list and clicking Start. Customer Status will change to Active.
1. On the Session toolbar, click **New Session**.
The *Create New Session* window is displayed.

2. Type the customer’s name or other identifier in the **Name** field.
You will use this name to identify the session on the Active Session tab and in the Session List.

3. Select the **PIN Code** tab.

4. Click **Create PIN Code**.
Rescue generates a 6-digit PIN code and displays it in the *Create New Session* window and in the Session Log.

5. Ask the customer to go to the PIN code entry site:
   - On devices running the Rescue+Mobile app, the user launches the app to view the PIN entry screen
   - On devices without a Rescue+Mobile app, the PIN code entry site is *oty.com* or *rescuemobile.com*

6. The customer enters the PIN.
The customer clicks to download the applet if not already installed.

   ![Note:](image)
   The download procedure may vary depending on the customer’s operating system.

7. Pick up the session by selecting it in the Session list and clicking **Start**.
Customer Status will change to Active.

You can now use the Technician Console to deliver remote support.

**How to Start a Mobile Session via Link and Messaging Tool**

Follow this procedure to connect to a customer’s mobile device using a link that you send to a customer using a messaging service or related tool.

The agent must have an active Rescue+Mobile add-on licence.
The agent’s Technician Group must have permission to start Private Sessions.
The agent’s Technician Group must have permission to use the Link connection method.

1. On the Session toolbar, click **New Session**.
The *Create New Session* window is displayed.

2. Type the customer’s name or other identifier in the **Name** field.
You will use this name to identify the session on the Active Session tab and in the Session List.

3. Select the **Link** tab.

4. Click **Copy Link to Clipboard**.
The link is copied to your clipboard.

5. Paste the link into your messaging tool and send it to your customer.

6. The customer clicks the link in the message.
The customer clicks to download the applet if not already installed.

   ![Note:](image)
   The download procedure may vary depending on the customer’s operating system.

7. Once the download is complete, ask the customer to click **Run** to execute the Applet.
Once the Applet is installed, the customer status will change from Connecting to Waiting.

8. Pick up the session by selecting it in the Session list and clicking **Start**.
Customer Status will change to Active.

You can now use the Technician Console to deliver remote support.
**The Customer Experience: Mobile Applet**

What can a customer using a smartphone do during a session?

- Chat
- View a detailed session log
- Allow or deny the technician the right to perform certain actions
- Send individual files to a technician
- Cancel a file transfer
- End Remote Control
- End Display Sharing
- Pause Display Sharing (on Android and BlackBerry)
- Pause Display Viewing (on Android and BlackBerry)
- End a session

**Note:** An iPhone user can chat and allow or deny an email configuration file sent by the technician during an Instant Chat session.

**Controlling a Mobile Device**

**Launch Remote Control from Click2Fix**

The agent must have an active Rescue+Mobile add-on licence.

The agent’s Technician Group must have permission to use Click2Fix for mobile.

The agent’s Technician Group must have permission to launch remote control sessions.

The session must be Active.

**What devices can be controlled?**

- Due to Android OS security restrictions, Remote Control is available only on Android 2.3+ devices from Samsung, HTC, Motorola, Huawei, Sony, Vertu, Kazam, LG, and some Lenovo and Positivo devices.
- Technicians are able to view the screen of any Android 5.0+ device without taking control (known as Remote View).

1. On the **Click2Fix** tab under **Device view**, click **Switch to remote control in a new window** to open a tear-away window.
   A new window opens showing the customer’s device.
2. Chat with the customer and remote control the device.
   - Use your computer keyboard as normal
   - Use your mouse to control the mobile device’s keypad

The following features are available when you remote control a mobile device:

<table>
<thead>
<tr>
<th>Feature</th>
<th>Android</th>
<th>BlackBerry</th>
<th>Apple iOS</th>
</tr>
</thead>
<tbody>
<tr>
<td>White Board</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Laser Pointer</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Remote Control from Customer Display

The agent’s Technician Group must have permission to use the Classic display for mobile.

What devices can be controlled?

• Due to Android OS security restrictions, Remote Control is available only on Android 2.3+ devices from Samsung, HTC, Motorola, Huawei, Sony, Vertu, Kazam, LG, and some Lenovo and Positivo devices.
• Technicians are able to view the screen of any Android 5.0+ device without taking control (known as Remote View).

1. On the Customer Display tab, click Launch Remote Control Session to activate remote control.
   If available, you will see a simulation of the customer’s device. Otherwise, you will see the generic simulation.
2. Chat with the customer and remote control the device.
   • Use your computer keyboard as normal
   • Use your mouse to control the mobile device’s keypad

The following features are available when you remote control a mobile device:

<table>
<thead>
<tr>
<th></th>
<th>Android</th>
<th>BlackBerry</th>
<th>Apple iOS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Screen Capture</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Screen Recording</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

3. Click End on the Session toolbar to end the session.

Remote Viewing (without remote control)

With Remote View, Technicians can view the screen of a customer's Android 5.0+ device without taking control.

• On the Click2Fix or Customer Display tab under Device view, click the play button ("view the customer's device").
  The screen of the customer's device is shown in the Device View section.

QuickNav: Jump to Specific Destinations on a Mobile Device

Click2Fix offers the QuickNav widget, which enables technicians to jump to specific settings or destinations on the customer's device.

The agent's Technician Group must have permission to use Click2Fix for mobile.

The session must be Active.
• On the Click2Fix tab under QuickNav, click the destination you want to open on the customer's device.

Don't see the one that you want? Click More...to get a list of all the available destination items.

💡 Tip: Pin your favorite items to the widget.

The selected destination opens on the customer's device.

---

### QuickNav Examples

**With remote control.** You are controlling the customer's device and want to change privacy settings. Instead of clicking through to privacy settings, you click the QuickNav Privacy destination item. You will see that the "Privacy settings" destination opens on the customer's device.

**Without remote control.** You want to guide the customer to privacy settings on their mobile device. Rather than coach the customer through all the steps to reach privacy settings, you click the QuickNav Privacy destination item. On the customer's device, the "Privacy settings" destination opens. Now you can coach the customer to change the required setting.

---

### Managing Settings on a Mobile Device

#### Managing Settings on a Mobile Device Using Click2Fix

Specialized widgets on the Click2Fix tab provide technicians with a quick and easy solution for managing settings on the customer's mobile device.

The agent's Technician Group must have permission to use Click2Fix for mobile.

The session must be Active.

**How to Push APN Settings to a Mobile Device**

This feature is only available when settings are defined in the Administration Center.

1. Click the Click2Fix tab.
   
   The Click2Fix widgets appear.

2. In the Mobile Network widget, click Network Setup
   
   The list of available pre-defined APN settings appears.

3. Choose the desired predefined APN, and click Push.
   
   The selected APN settings are transferred to the customer's mobile device.

**How to Push Web Shortcut Icons**

With the Web Shortcuts widget, a technician can push a web shortcut icon to the customer's device giving them quick and easy access to frequently used sites.

This feature is only available when settings are defined in the Administration Center.

1. Click the Click2Fix tab.
   
   The Click2Fix widgets appear.

2. In the Web Shortcuts widget, click Start.
The list of available predefined web shortcuts appears.
3. Choose the desired predefined web shortcut, and click Push.
   The selected web shortcut icon is pushed and installed to the customer's device.

**How to Push Direct URLs**
Technicians can send customers predefined or custom URLs, which automatically open in their mobile's default browser.

**How to Send a Custom URL**
1. Click the Click2Fix tab.
   The Click2Fix widgets appear.
2. Under Direct URL widget, type your custom URL in the enter URL here window.
3. Click Send custom URL.
   The custom URL automatically opens in the default browser of the customer’s device.

**How to Send a Predefined URL**
1. Click the Click2Fix tab.
   The Click2Fix widgets appear.
2. Under Direct URL, click Select other predefined URL....
   A list of predefined URLs appears.
3. Select the desired URL, and click Send.
   **Tip:** If the URL you want to push is on the list under Recently sent, then just select the URL, and click Send.
   The selected predefined URL automatically opens in the default browser of the customer’s device.

**How to Push Battery Optimization Settings**
For Android and BlackBerry, technicians can push settings that help optimize battery usage on the customer’s device.

1. Click the Click2Fix tab.
   The Click2Fix widgets appear.
2. In the Battery widget, click Optimize battery use.
   The Optimize battery use window is displayed.
3. Choose from the available actions and click Apply settings.
   - Switch off Wi-Fi
   - Switch off Bluetooth
   - Switch off GPS
   - Change Display brightness settings
   - Set Display timeout

**How to Push Quick Connection Settings**
Technicians can toggle on and off Bluetooth, GPS and Wi-Fi connection settings of Android and Blackberry devices.
1. Click the Click2Fix tab.
The Click2Fix widgets appear.

2. Under **Connections**, click the connection method that you want to toggle on or off. The selected connection method is toggled on/off on the customer's device.

### How to Manage Missing and Unwanted Applications

This feature is only active when the App Checker list has been uploaded in the Administration Center at **Global Settings** > **Mobile device settings** > **App Checker List Upload**.

1. Click the **Click2Fix** tab.
   The Click2Fix widgets appear.
2. In the **Applications** widget, click **Show all applications**.
   The **Applications** window is displayed.

![Applications Window](image)

3. Choose from the following options.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Uninstall an Unwanted Application</strong></td>
<td>This feature is only active when the App Checker list has been uploaded in the Administration Center at <strong>Global Settings</strong> &gt; <strong>Mobile device settings</strong> &gt; <strong>App Checker List Upload</strong>.</td>
</tr>
<tr>
<td></td>
<td>1. Click <strong>Flagged</strong>. Flagged applications on the device are displayed on a list.</td>
</tr>
<tr>
<td></td>
<td>2. Select the flagged application you want to uninstall, and click <strong>Uninstall application</strong>.</td>
</tr>
</tbody>
</table>

Note: Pre-deployed applications cannot be uninstalled from a device. In this case, the **Uninstall updates** button is displayed. This removes the latest update of the concerned application.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Send URL for Missing Application</strong></td>
<td>1. In the Applications window, click <strong>Missing</strong>.</td>
</tr>
<tr>
<td></td>
<td>Missing applications on the device are displayed on a list.</td>
</tr>
<tr>
<td></td>
<td>2. Select the missing application with which you want to provide help to your customer, and click <strong>Send URL</strong>.</td>
</tr>
<tr>
<td></td>
<td>The URL predefined for this application in the LogMeIn Rescue Administration Center is pushed to the customer’s device.</td>
</tr>
<tr>
<td><strong>Tip:</strong></td>
<td>For example, you can push the URL of the app in Google Play to make it easier for the customer to install the missing app.</td>
</tr>
</tbody>
</table>

**How to Kill Processes and Running Applications**

Technicians can kill selected applications and processes to free up device memory for improved performance.

1. Click the **Click2Fix** tab.  
The Click2Fix widgets appear.

2. In the **Processes** widget, click **Show all processes**.  
The **Processes** window is displayed showing all processes and running applications on the device.

3. Depending on whether you want to kill a process or a running application, click **Processes** or **Running applications**.

4. Select the process or application you want to kill, and click **Kill selected**.  
The selected process or application is terminated on the customer’s device.

**Fastpath:** On the opening widget screen, technicians can view those five processes and running applications that use the most memory. All a technician has to do to kill any of these is the following:

1. On the opening widget screen, select the process or application you want to kill.
2. Click **Kill selected**.

**Tip:** You can customize the information displayed in the **Processes** window. To select what information is displayed, on the **Processes** window right-click the header row of the table, and select the categories you want to see.

**How to Add a New Email Account**

Technicians can add new email accounts to the default email app of the customer’s mobile device.

1. Click the **Click2Fix** tab.  
The Click2Fix widgets appear.

2. In the **Email** widget, click **Add new IMAP/POP3 account**.  
The **Add new email** window is displayed.
3. Fill in the fields.
4. Click **Apply**
   At the bottom of the window, the **Settings transferred** notification is displayed. The new email account has been successfully configured on the customer's device.

   **Fastpath:** To speed up configuration, in the Email field type the email address belonging to the account you want to add. Click **Retrieve domain-specific settings**. For major email providers, the Email widget will automatically fill in configuration fields. All you have to submit is the password(s) belonging to the email account.

### Pushing Settings to a Mobile Device from Device Configuration

Use the **Device Configuration** tab to change settings on the customer's mobile device.

The agent must have an active Rescue+Mobile add-on licence.

The agent's Technician Group must have permission to configure mobile device settings.

For Android and iOS, additional permissions are required on the Administration Center **Settings** tab under **Mobile Device Configuration**.

The session must be Active.

1. On the Technician Console, select the **Device Configuration** tab.
   The available settings are displayed.
2. Choose from the available settings.

<table>
<thead>
<tr>
<th>Platform</th>
<th>Available Tabs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Android</td>
<td>• Wi-Fi settings</td>
</tr>
<tr>
<td></td>
<td>• APN settings</td>
</tr>
</tbody>
</table>
### Available Tabs

<table>
<thead>
<tr>
<th>Platform</th>
<th>Available Tabs</th>
</tr>
</thead>
</table>
| iOS        | • Email settings  
            | • Exchange ActiveSync settings  
            | • Access Point settings  
            | • Passcode settings  
            | • Restrictions settings  
            | • Web Clips settings  
            | • Wi-Fi settings                                               |
| BlackBerry | • Email settings                                               |

3. Click **Request Settings** to view the settings available on the customer's device.

   🚨 **Important:** Wi-Fi must be enabled.

   The settings are displayed.

4. Click **Push Settings**.

   📢 **Remember:** Wi-Fi must be enabled.

   For most operating systems, the settings are applied on the customer's device immediately after being pushed.

   🚨 **Important:** Customer's on iOS may be prompted to install a Profile.

---

### Managing Files on a Mobile Device

Use the File Manager to easily and securely transfer files between your computer and the customer's device.

**Supported platforms:**

- Android
- BlackBerry
- Not available for iOS

**Other requirements:**

- The agent's Technician Group must have permission to launch File Manager.
- The session must be Active.

1. On the Technician Console **File Manager** tab, click **Launch File Manager Session**.

   The customer may be prompted to accept or decline your request to control his device. If so, ask the customer to accept the request.

   The File Manager session begins.

2. Use the File Manager toolbar to work with the customer's files and folders.
   All other Workspace tabs remain available.

3. To end the File Manager session, click the red ✗ on the File Manager toolbar.
The File Manager session closes, but the session remains active.

Note: You can move and delete files with the File Manager from the device's SD card, but not from its memory. From the device's memory, you can only copy files to your local drive.

Working with Mobile Device System Information

Working with Mobile System Info via Click2Fix

Viewing Mobile System Info via Click2Fix

The Click2Fix tab gives technicians a convenient tool for analyzing various aspects of the customer's device. With specialized widgets, technicians can retrieve specific data from the mobile device.

The agent's Technician Group must have permission to use Click2Fix for mobile.

The session must be Active.

Info Bar and Alert Bar

Immediately upon starting a session, technicians get some of the most important information about the mobile device.

The blue Info Bar shows basic device information. For example:
- Manufacturer
- Device model
- Phone number

The red Alert Bar highlights important issues or action items. For example:
- Battery information (power level, temperature)
- Flagged and Missing applications
- Out-of-date or rooted firmware

Battery warnings are triggered by the following hardcoded settings:

- **Battery Power "Very Low"** < 20%
- **Battery Temperature "Overheating"** > 55 degrees Celsius

App Checker

Upon starting a session with an Android or BlackBerry device, the Technician Console checks for apps according to parameters set in an XML file uploaded in the Administration Center.

Firmware Checker

Upon starting a session with an Android, BlackBerry and iOS device, the Technician Console automatically checks the firmware of the device according to OS properties defined in a file uploaded in the Administration Center. The file can also contain a URL to current firmware.
Mobile Network Information

For Android, BlackBerry and iOS devices, technicians can view network information from the customer’s device. Depending on platform, these may include:

• Home Operator
• Roaming Operator
• Connection Type
• Signal Strength

Signal Strength is determined by the following hardcoded settings:

<table>
<thead>
<tr>
<th>Level</th>
<th>dBm Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>-90 dBm</td>
</tr>
<tr>
<td>Medium</td>
<td>-100 ... -91 dBm</td>
</tr>
<tr>
<td>Low</td>
<td>-110 ... -101 dBm</td>
</tr>
<tr>
<td>Very Low</td>
<td>-111 dBm and lower</td>
</tr>
</tbody>
</table>

System Information

For Android, BlackBerry and iOS devices, technicians can view basic system information from the customer's device. Depending on platform, these may include:

• System version
• Baseband number
• Build number
• Memory
• Internal storage
• SD Card
• IMEI

Connection Information

Technicians can view connection status for Bluetooth, GPS and Wi-Fi.

Battery Status Information

For Android, BlackBerry and iOS devices, technicians can view basic battery details.

Processes Information

Technicians can view processes and applications running on an Android device, and see how much memory they are using.

Applications Information

This feature is only active when the App Checker list has been uploaded in the Administration Center at Global Settings > Mobile device settings > App Checker List Upload.

Upon connection to an Android device, the Technician Console will check for missing or unwanted (flagged) apps according to parameters set in an XML file uploaded in the Administration Center.

Email Information

Technicians can view configuration information about the email accounts configured in the default email app of the customer’s mobile device.
The email accounts configured in the default email app are listed on the widget. Click the eye icon next to the account for which you want to view the configuration parameters.

**Working with Mobile System Info on the System Info Tab**

**How to View General System Information for a Mobile Device**

The agent's Technician Group must have permission to view system information.

The session must be Active.

1. On the **System Info** tab, click **Dashboard**.
   The system info Dashboard is displayed.
2. Click **Request Information** to retrieve data from the customer's device.
   The customer may be prompted to accept or decline your request.
3. The following view-only information is available, depending on the customer's operating system.

<table>
<thead>
<tr>
<th></th>
<th>Android</th>
<th>BlackBerry</th>
<th>Apple iOS</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Information</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>OS</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Default Browser Path</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Device model</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Device screen</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Device PIN</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Locale and Time Zone</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**How to View CPU Information for a Mobile Device**

The agent's Technician Group must have permission to view system information.

The session must be Active.

1. On the **System Info** tab, click **Dashboard**.
   The system info Dashboard is displayed.
2. Click **Request Information** to retrieve data from the customer's device.
   The customer may be prompted to accept or decline your request.
3. The following view-only information is available, depending on the customer's operating system.

<table>
<thead>
<tr>
<th></th>
<th>Android</th>
<th>BlackBerry</th>
<th>Apple iOS</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU Information</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**How to View Memory Information for a Mobile Device**

The agent's Technician Group must have permission to view system information.

The session must be Active.

1. On the **System Info** tab, click **Dashboard**.
The system info Dashboard is displayed.
2. Click **Request Information** to retrieve data from the customer's device.
   The customer may be prompted to accept or decline your request.
3. The following view-only information is available, depending on the customer's operating system.

<table>
<thead>
<tr>
<th></th>
<th>Android</th>
<th>BlackBerry</th>
<th>Apple iOS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Memory Information</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**How to View Wireless and Network Information for a Mobile Device**

The agent's Technician Group must have permission to view system information.
The session must be Active.

1. On the **System Info** tab, click **Dashboard**.
The system info Dashboard is displayed.
2. Click **Request Information** to retrieve data from the customer's device.
The customer may be prompted to accept or decline your request.
3. The following view-only information is available, depending on the customer's operating system.

<table>
<thead>
<tr>
<th></th>
<th>Android</th>
<th>BlackBerry</th>
<th>Apple iOS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wireless and Network Information</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Radio Manufacturer</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Phone number</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Serial/IMEI number</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Subscriber number</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Current operator</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Network connect type (GSM/CDMA)</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Signal Strength</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**How to View Battery and Power Consumption Information for a Mobile Device**

The agent's Technician Group must have permission to view system information.
The session must be Active.

1. On the **System Info** tab, click **Dashboard**.
The system info Dashboard is displayed.
2. Click **Request Information** to retrieve data from the customer's device.
The customer may be prompted to accept or decline your request.
3. The following view-only information is available, depending on the customer's operating system.

<table>
<thead>
<tr>
<th></th>
<th>Android</th>
<th>BlackBerry</th>
<th>Apple iOS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Battery Information</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Power source</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
### How to View Storage/Disk Drive Information for a Mobile Device

The agent's Technician Group must have permission to view system information.

The session must be Active.

1. On the **System Info** tab, click **Dashboard**.
   The system info Dashboard is displayed.
2. Click **Request Information** to retrieve data from the customer's device.
   The customer may be prompted to accept or decline your request.
3. The following view-only information is available, depending on the customer's operating system.

<table>
<thead>
<tr>
<th></th>
<th>Android</th>
<th>BlackBerry</th>
<th>Apple iOS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Storage / Disk Drive</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### How to View the Top 5 Processes for a Mobile Device

The agent's Technician Group must have permission to view system information.

The session must be Active.

1. On the **System Info** tab, click **Dashboard**.
   The system info Dashboard is displayed.
2. Click **Request Information** to retrieve data from the customer's device.
   The customer may be prompted to accept or decline your request.
3. The following view-only information is available, depending on the customer's operating system.

<table>
<thead>
<tr>
<th></th>
<th>Android</th>
<th>BlackBerry</th>
<th>Apple iOS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top 5 Processes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### How to View System Processes Running on a Mobile Device

The agent's Technician Group must have permission to view system information.

The session must be Active.
Supported platforms:
• Android
• BlackBerry
• iOS

1. On the System info tab click Processes.
2. To retrieve data from the customer's device, click Request Process Information.
   The customer may be prompted to accept or decline your request.

All processes running on the device are displayed.

**How to Terminate a Process for a Mobile Device**

The agent's Technician Group must have permission to view system information. The session must be Active.

Supported platforms:
• Android

1. On the System info tab, click Processes.
2. To terminate a selected process on the customer’s device click End Process.

The selected process is terminated on the customer's device.

**How to View Services Registered on a Mobile Device**

The agent's Technician Group must have permission to view system information. The session must be Active.

Supported platforms:
• Android
• BlackBerry (Service Books)
• Not available for iOS

1. On the System info tab, click Services.
2. To retrieve data from the customer's device, click Request Services Information.
   The customer may be prompted to accept or decline your request.

All services registered on the device are displayed.

**How to View Applications Installed on a Mobile Device**

The agent's Technician Group must have permission to view system information. The session must be Active.

Supported platforms:
• Android
• BlackBerry (Service Books)
• Not available for iOS

1. On the System info tab, click Applications.
2. To retrieve data from the customer's device, click Request Application Information.
   The customer may be prompted to accept or decline your request.
All applications installed on the device are displayed.

**How to Launch an Application for a Mobile Device**
The agent's Technician Group must have permission to view system information. The session must be Active.
Supported platforms:
- Android

1. On the System info tab, click Applications.
2. To launch an application on the customer's device, click Launch Application.

The application is running on the customer's device.

**How to Uninstall an Application from a Mobile Device**
The agent's Technician Group must have permission to view system information. The session must be Active.
Supported platforms:
- Android

1. On the System info tab, click Applications.
2. To uninstall an application from the customer's device, click Uninstall Application.

The application is uninstalled from the customer's device.

**How to View Recent Events from a Mobile Device - Logcat**
View application, security, and system events.
The agent's Technician Group must have permission to view system information. The session must be Active.
Supported platforms:
- Android

1. On the System info tab, click Logcat.
2. To view recent events on the customer's device, click Request Logcat.

Logcat opens. Recent application, security, and system events are shown in a tabbed interface, and can be sorted according to name, date, source, event, user and computer.

**Supporting Android Devices**
This section summarizes how Rescue+Mobile can be used to support Android devices.

**Remember:** The actual set of features available to a technician is set at the group level in the Administrator Center.

**What devices can be controlled?**
Due to Android OS security restrictions, Remote Control is available only on Android 2.3+ devices from Samsung, HTC, Motorola, Huawei, Sony, Vertu, Kazam, LG, and some Lenovo and Positivo devices. Technicians are able to view the screen of any Android 5.0+ device without taking control (known as Remote View).

**Rescue+Mobile App for Android**

The customer must have the Rescue+Mobile app for Android. The app can be downloaded from Google Play or by following a link sent by the technician during connection.

**Connection Methods**

- SMS
- PIN Code
- Link and Messaging Tool
- Email

**Tip:** For detailed information concerning the process of starting a remote support session on Android devices, see [LogMeIn Rescue Step-by-Step Connection Guide](#).

**Click2Fix Tab**

The Click2Fix tab gives technicians a set of tools for analyzing and resolving the most commonly encountered issues faced by mobile customers.

The following widgets are available for Rescue sessions with Android devices:

<table>
<thead>
<tr>
<th>Widget</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Info and Alert Bar</strong></td>
<td>View basic device info and highlighted issues or action items.</td>
</tr>
<tr>
<td><strong>Mobile Network</strong></td>
<td>View mobile network information. Push predefined APN settings.</td>
</tr>
<tr>
<td><strong>System</strong></td>
<td>View basic information about the customer's device (System Version, Baseband number, Build number, IMEI, etc.).</td>
</tr>
<tr>
<td><strong>Web Shortcuts</strong></td>
<td>Push icons that give the customer access to web content from their home screen.</td>
</tr>
<tr>
<td><strong>Battery</strong></td>
<td>View battery details and push settings that help optimize battery utilization.</td>
</tr>
<tr>
<td><strong>Connections</strong></td>
<td>View and manage a device’s Bluetooth, GPS, and Wi-Fi connections.</td>
</tr>
<tr>
<td><strong>Direct URL</strong></td>
<td>Send customers predefined or custom URLs, which open in their default browser.</td>
</tr>
<tr>
<td><strong>Device View</strong></td>
<td>View a simulation of the customer’s device. With supported devices, technicians can also start a remote control session.</td>
</tr>
<tr>
<td><strong>QuickNav</strong></td>
<td>Jump to specific destination on the customer’s mobile device.</td>
</tr>
<tr>
<td><strong>Processes</strong></td>
<td>View processes and applications running on an Android device, and see how much memory they are using. Kill selected processes and running applications.</td>
</tr>
<tr>
<td><strong>Applications</strong></td>
<td>View and manage missing or unwanted (flagged) applications.</td>
</tr>
<tr>
<td><strong>Email</strong></td>
<td>View configuration information about the email accounts configured in the default email app of the customer’s device. Add new accounts.</td>
</tr>
</tbody>
</table>
Customer Display Tab

**Launch Remote Control Session**
View and control the customer's device. Depending on permissions, the following features may also be available when controlling an Android:
- Chat
- White Board
- Laser Pointer
- Screen Capture
- Screen Recording

**Launch Display Viewing Session**
View the customer's device. Depending on permissions, the following features may also be available when controlling an Android:
- White Board
- Laser Pointer

System Info Tab

**Dashboard**
The Dashboard tab provides access to the following information:
- System Information (OS, Baseband number, Build number, Device model, etc.)
- Memory Information
- Wireless and Network Information
- Battery and Power Consumption Information
- Storage Information

**Processes**
View and terminate processes running on the customer's device.

**Services**
View services registered on the customer's device.

**Applications**
View all applications installed on the customer's device; launch and uninstall applications.

**Logcat**
View recent events of the customer's device.

File Manager tab
Transfer files between customer and technician.

History and Notes tab

**Add/Edit Notes**
Take notes during a session and save them.

**History and Notes Capabilities**
View the session log and any notes made during the active or past sessions with the current in-session device.

Supporting iOS Devices
This section summarizes how Rescue+Mobile can be used to support iOS devices (iPhone, iPad, iPod touch).
**Remember:** The actual set of features available to a technician is set at the group level in the Administrator Center.

**Rescue+Mobile App for iOS**

For a full-featured experience, the customer's device should be running the Rescue+Mobile app for iOS, which the customer must download from the App Store. When the customer has the Rescue app for iOS, Rescue+Mobile technicians can push configuration settings and view system info. Otherwise, the session can be run in Safari using Instant Chat, which only allows the technician to push configuration settings.

**Connection Methods**

- SMS
- PIN Code
- Link and Messaging Tool
- Email

**Tip:** For detailed information concerning the process of starting a remote support session on iOS devices, see *LogMeIn Rescue Step-by-Step Connection Guide*.

**Click2Fix Tab**

The Click2Fix tab gives technicians a set of tools for analyzing and resolving the most commonly encountered issues faced by mobile customers. The following widgets are available for Rescue sessions with an iOS device with the app:

- **Info and Alert Bar** - View basic device info and highlighted issues or action items.
- **System** - View basic information about the customer's device.
- **Web Shortcuts** - Push icons that give the customer access to web content from their home screen.
- **Battery** - View battery details.
- **Connections** - View a device's Bluetooth, GPS, and Wi-Fi connections.
- **Direct URL** - Send customers predefined or custom URLs, which open automatically.
- **Processes** - View how much of the available memory is used by running processes and applications.
- **Email** - Add new email accounts to the default email app.

**Customer Display Tab**

**Launch Remote Control Session** - View and control the customer's device. Depending on permissions, the following features may also be available when controlling an iOS:

- Chat
- White Board
- Laser Pointer

LogMeIn Rescue Technician Console User Guide
Launch Display Viewing Session
View the customer's device. Depending on permissions, the following features may also be available when viewing an iOS:
- White Board
- Laser Pointer

System Info Tab
The Dashboard tab provides access to the following information:
- System Information (OS, Device model, Device screen)
- Memory Information
- Wireless and Network Information
- Battery and Power Consumption Information
- Storage Information
- Process (Top 5 per CPU)

Processes
View processes running on the customer's device.

Device Configuration Tab
- Email settings
- Exchange ActiveSync settings
- Access Point settings
- Passcode settings
- Restrictions settings
- Web Clips settings
- Wi-Fi settings

History and Notes Capabilities
Add/Edit Notes
Take notes during a session and save them.

History and Notes Capabilities
View the session log and any notes made during the active or past sessions with the current in-session device.

Supporting BlackBerry Devices
Depending on permissions set in the Administrator Center, the following features are available when connected to a BlackBerry device:
- System Info tab
- History & Notes tab
- Device Configuration tab (email configuration)
- Hot Keys
- Chat
- Customer Terms of Service (Admin)
- Click2Fix tab
How to Set BlackBerry Device Permissions

In some cases, the Mobile Applet will function only after your customer has granted appropriate Application Permissions to the Applet. Ask your customer to follow these instructions.

Note: Some customers may not be able to modify settings due to a centrally administered BlackBerry IT Policy.

1. Depending on the BlackBerry OS your device runs, do one of the following:
   - On devices running OS5 or earlier, in the device options, click Applications. If you cannot find the Applications menu, click Advanced Options > Applications.
   - On devices running OS6 or later, tap Option > Device > Application Management.

2. Highlight the LogMeIn Rescue application.

3. Press the Menu key and then select Edit Permissions.

4. Set the following permissions to Allow.
   - Connections > Carrier Internet, Company Network, Wi-Fi
   - Interactions > Interprocess Communication, Device Settings Modification, Module Management, Keystroke Injection, Screen Capturing, Security Timer Reset
   - User Data > Files, Key Store

Note: You may only see Connections, Interactions, and User Data as permissions.

Tip: If a customer experiences problems with permissions, he can access permission settings during the Applet download process by selecting Set application permissions before starting the download. Rescue generally sets all required permissions automatically, so this feature should only be used as part of your troubleshooting efforts.
Wireless Applet Deployment to BlackBerry smartphones

For details, see the Knowledge Base article How do I configure LogMeIn Rescue+Mobile over BlackBerry Enterprise Server (BES)?

How to Uninstall the Applet from a BlackBerry

Your customers can follow this procedure to uninstall the Mobile Applet from a BlackBerry device.

On devices running BlackBerry OS5 or earlier, do the following:

1. From the Home menu, open the Options screen.
2. Select > Advanced Options > Applications > LogMeIn Rescue > Delete > Delete Confirm

Note: You may have Advanced Options and Applications on the same level in the Options screen.

Reboot may be required.

On devices running BlackBerry OS6 or later, do the following:

1. On the Home screen, tap and hold LogMeIn Rescue.
2. Tap Delete.

About Advanced BlackBerry Connection Settings

Your BlackBerry customers can access advanced Connection Settings from the PIN Entry screen. This feature is useful for troubleshooting connection issues with BES, Wi-Fi, and APN (if there is an APN setting available in the network).

For each type of connection, the following options can be set:

Disabled The Applet will not try to use this connection
| **Enabled** | The Applet will try to use this connection |
| **Forced** | The Applet tries to use this connection first (only one option at a time can be set to Forced) |

For APN, the customer can enter service provider APN settings for the Direct TCP internet connection.
Providing Support via Rescue Lens

Rescue Lens is LogMeIn's video-enabled support solution with integrated VoIP. With Rescue Lens, support technicians are able to use the camera of a customer's mobile device to provide a secure, live camera feed to the Technician Console, thus allowing them to see the actual situation the customer is facing and help them solve complex set-up, configuration or troubleshooting issues.

Restriction: Lens audio is not available for Technician Console for Mac.

Starting a Rescue Lens Session

Starting a Rescue Lens Session by PIN Code

Follow this procedure to connect to a customer using a PIN code.

Technician Starts the Session

Required permissions:

- The agent's Technician Group must have permission to start Rescue Lens sessions.
- The agent's Technician Group must have permission to start Private Sessions.
- The agent's Technician Group must have permission to use the PIN code connection method.

1. Log in to the Technician Console.
2. On the Session toolbar, click New Session.

The Create New Session window is displayed.
3. Select **Rescue Lens** as session type.
4. Type the customer's name or identifier in the **Name** field.  
   This name is shown on the Active Session tab and Session List.
5. Select the **PIN Code** tab.
6. Click **Create PIN Code**.  
   A 6-digit PIN code is generated and displayed in the **Create New Session** window and in the Session Log.

   **Restriction:** A technician can handle only one active Lens session at a time.

**Customer Launches the Rescue Lens App**
Once you have a PIN, make sure the customer has the app. They will enter the PIN in the app.

1. Ask the customer to launch the Rescue Lens app, available on Google Play or the App Store.

   The customer may see a tutorial. They can tap **Skip** or **OK**.
2. The customer is prompted to grant access to the device camera and microphone. Ask them to tap **OK**.
3. Ask the customer to enter the PIN.  
   At this point the camera image may already be displayed on the customer’s mobile device, but nothing is streamed to the Technician Console.
4. Ask the customer to accept the End-User License Agreement.

**Technician Supports the Customer**
The session appears in the Technician Console once the customer has launched the Rescue Lens app, entered a valid PIN, and accepted the End-User License Agreement.

Pick up the session by selecting it in the Session list and clicking **Start**.

The Rescue Lens support session starts; a live video feed is streamed from the camera of the customer’s device to the technician. Lens audio enables the customer and technician to communicate via a VoIP connection.
**Restriction:** Lens audio is not available for Technician Console for Mac.

---

Starting a Rescue Lens Session by SMS

Follow this procedure to connect to a customer using an SMS containing a PIN code.

**Technician Starts the Session**

**Required permissions:**

- The agent's Technician Group must have permission to start Rescue Lens sessions.
- The agent's Technician Group must have permission to start Private Sessions.
- The agent's Technician Group must have permission to use the SMS connection method.

1. Log in to the Technician Console.
2. On the Session toolbar, click **New Session**.
   
   The **Create New Session** window is displayed.
3. Select **Rescue Lens** as session type.

4. Type the customer’s name or identifier in the **Name** field. This name is shown on the Active Session tab and Session List.

5. Select the **SMS** tab.

6. Type the customer’s phone number into the **To:** field. The SMS containing the PIN code will be sent to this phone number.

7. Click **Send SMS**. A 6-digit PIN code is generated and sent to the customer in an SMS. The code is also displayed in the **Create New Session** window.

   **Restriction:** A technician can handle only one active Lens session at a time.

### Customer Launches the Rescue Lens App

1. Ask the customer to open the SMS message, and click the link to launch the Rescue Lens app.

   **Note:** If the Rescue Lens app is not already installed on the customer’s device, they are redirected to Google Play or the App Store to install the app first.

   **Note:** The download procedure may vary depending on the customer’s operating system.

   The customer may see a tutorial. They can tap **Skip** or **OK**.

2. The customer is prompted to grant access to the device camera and microphone. Ask them to tap **OK**.
At this point the camera image may already be displayed on the customer's mobile device, but nothing is streamed to the Technician Console.

3. Ask the customer to accept the End-User License Agreement.

**Technician Supports the Customer**

The session appears in the Technician Console once the customer has launched the Rescue Lens app, and accepted the End-User License Agreement.

Pick up the session by selecting it in the Session list and clicking **Start**.

The Rescue Lens support session starts; a live video feed is streamed from the camera of the customer's device to the technician. Lens audio enables the customer and technician to communicate via a VoIP connection.

*Restriction:* Lens audio is not available for Technician Console for Mac.
Starting a Rescue Lens Session by Email

Follow this procedure to connect to a customer using an Email containing a PIN code.

Technician Starts the Session

Required permissions:

- The agent's Technician Group must have permission to start Rescue Lens sessions.
- The agent's Technician Group must have permission to start Private Sessions.
- The agent's Technician Group must have permission to use the Email connection method.

1. Log in to the Technician Console.
2. On the Session toolbar, click **New Session**.
   
   The **Create New Session** window is displayed.
3. Select **Rescue Lens** as session type.

4. Type the customer's name or identifier in the **Name** field. This name is shown on the Active Session tab and Session List.

5. Select the **Email** tab.

6. Choose how you want to send the email to the customer:
   - To use your own email client and account, choose **Send email via my default email client on this computer**.
   - To allow Rescue to send the email, choose **Send email on my behalf via the LogMeIn Rescue servers** and enter a valid email address in the **To** field.

7. Click **Email Link**.
   A 6-digit PIN code is generated and sent to the customer in an Email.

**Restriction**: A technician can handle only one active Lens session at a time.

**Customer Launches the Rescue Lens App**

1. Ask the customer to open the Email, and click the link to launch the Rescue Lens app.

**Note**: If the Rescue Lens app is not already installed on the customer's device, they are redirected to Google Play or the App Store to install the app first.

**Note**: The download procedure may vary depending on the customer's operating system.
The customer may see a tutorial. They can tap **Skip** or **OK**.

2. The customer is prompted to grant access to the device camera and microphone. Ask them to tap **OK**.
   At this point the camera image may already be displayed on the customer’s mobile device, but nothing is streamed to the Technician Console.
3. Ask the customer to accept the End-User License Agreement.

**Technician Supports the Customer**

The session appears in the Technician Console once the customer has launched the Rescue Lens app, and accepted the End-User License Agreement.

Pick up the session by selecting it in the Session list and clicking **Start**.

The Rescue Lens support session starts; a live video feed is streamed from the camera of the customer’s device to the technician. Lens audio enables the customer and technician to communicate via a VoIP connection.

**Restriction**: Lens audio is not available for Technician Console for Mac.
Starting a Rescue Lens Session by Link and Messaging Tool

Follow this procedure to connect to a customer using a link that you send to a customer using a messaging service or related tool.

**Technician Starts the Session**

**Required permissions:**

- The agent's Technician Group must have permission to start Rescue Lens sessions.
- The agent's Technician Group must have permission to start Private Sessions.
- The agent's Technician Group must have permission to use the Link connection method.

1. Log in to the Technician Console.
2. On the Session toolbar, click **New Session**.

   The **Create New Session** window is displayed.
3. Select **Rescue Lens** as session type.
4. Type the customer’s name or identifier in the **Name** field. This name is shown on the Active Session tab and Session List.
5. Select the **Link** tab.
6. Click **Copy link to clipboard**. A session-specific link containing the PIN code is copied to your clipboard. The link is also displayed in the **Create New Session** window.
7. Paste the link into your messaging tool and send it to your customer.

**Restriction:** A technician can handle only one active Lens session at a time.

**Customer Launches the Rescue Lens App**

1. Ask the customer to open the message and click the link or paste it into their browser to launch the Rescue Lens app.

**Note:** If the Rescue Lens app is not already installed on the customer’s device, they are redirected to Google Play or the App Store to install the app first.

The customer may see a tutorial. They can tap **Skip** or **OK**.

2. The customer is prompted to grant access to the device camera and microphone. Ask them to tap **OK**. At this point the camera image may already be displayed on the customer’s mobile device, but nothing is streamed to the Technician Console.
3. Ask the customer to accept the End-User License Agreement.
**Technician Supports the Customer**

The session appears in the Technician Console once the customer has launched the Rescue Lens app, and accepted the End-User License Agreement.

Pick up the session by selecting it in the Session list and clicking **Start**.

The Rescue Lens support session starts; a live video feed is streamed from the camera of the customer's device to the technician. Lens audio enables the customer and technician to communicate via a VoIP connection.

**Restriction:** Lens audio is not available for Technician Console for Mac.
Managing a Rescue Lens Session

What Can the Technician Do?

During a Rescue Lens session, the technician can perform the following actions:

Remember: The actual set of features available to a technician is set at the group level in the Administration Center.

End session

Hold session

When the technician places a session on hold, the camera stream is paused on the customer's side and the session goes to On Hold status in the Technician Console.

Transfer session

You can transfer a Rescue Lens session only to another technician who has permission to use Rescue Lens.

Mute/Unmute microphone and speaker

For Lens sessions using audio, the technician can mute/unmute the audio connection at any time during the session.

Restriction: Lens audio is not available for Technician Console for Mac.

Chat

The technician can chat with the customer and send predefined URLs.

Whiteboard

Draw on the streamed image to highlight particular areas or objects. For example, you can highlight a part that needs to be removed or a switch that needs attention.

Multi-object tracking ensures that whiteboard annotations stay attached to the drawn-upon image. For example, if the customer moves their camera away from a circled part, the circle stays "attached" to the part and moves with it, thus ensuring that the correct part remains highlighted.

To start drawing on the streamed image, click Whiteboard On.
To clear the streamed image from drawings, click **Erase Drawings**.
Whiteboard functionality is not supported on iPhone 4 devices.

**Freeze**

Freeze the camera stream for both technician and customer. This allows you to draw on a stable background to better communicate to the customer.

**Screen recording**

Technicians can make a recording of all on-screen activity during a Rescue Lens session by clicking the **Screen Recording** icon on the Rescue Lens toolbar.
The agent's Technician Group must have permission to record sessions.

Rescue Lens session recordings are always saved to .mkv format and should be played back using **VLC media player**.

**Screen capture**

Technicians can create screen captures during a Rescue Lens session.

**Configure View Settings**

Technicians can select from the following options to specify zoom settings of the video stream:
- Actual Size
Manage Video Quality

During a Lens session started from the Rescue Technician Console, Rescue Lens automatically adjusts the quality of the video stream to suit the quality of service provided by the carrier network. The support technician can, however, also change the video quality manually at any point during the session.

Rescue Lens uses three video stream quality presets.

<table>
<thead>
<tr>
<th>Preset Value</th>
<th>Resolution for Android</th>
<th>Resolution for iOS</th>
<th>Frame Rate</th>
<th>Activating Chat Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>Actual Screen Size</td>
<td>640*480</td>
<td>18 FPS</td>
<td>!_videoquality high</td>
</tr>
<tr>
<td>Medium</td>
<td>352<em>288 320</em>244 (Nexus 4)</td>
<td>480*360</td>
<td>15 FPS</td>
<td>!_videoquality medium</td>
</tr>
<tr>
<td>Low</td>
<td>352<em>288 320</em>244 (Nexus 4)</td>
<td>480*360</td>
<td>5 FPS</td>
<td>!_videoquality low</td>
</tr>
</tbody>
</table>

The default setting for each session is the High preset value. When the network cannot transfer the necessary volume of traffic, Lens temporarily decreases the video quality to a lower preset value. The technician can also change the video quality manually at any point during the session by typing the corresponding command in the Chat field.

**Tip:** Examples for the need to decrease video quality:
- To limit the bandwidth consumed by the video stream
- To support video streaming on networks having a bandwidth lower than 400 kbps
- In case of slow cellular networks, the automatic network adaptation may produce slow adaptation, or may stop streaming. To ensure quicker adaptation, use the medium or low preset values

**Restriction:** Technician Collaboration is not available for Rescue Lens sessions.

**Important:** To support mobile devices using advanced Rescue+Mobile support tools (remote control, diagnostic and troubleshooting tools, etc.), the technician must have an active Rescue+Mobile add-on license.
What Can the Customer Do?

During a Rescue Lens session, the customer can perform the following actions.

**Figure 5: Lens as experienced by the customer**

- **Chat**
  - The customer can chat with the technician. The customer can extend and minimize the chat dialogue on the screen of the mobile device by swiping up or down.

- **Disconnect**
  - The customer can **Disconnect** at any time during the session.

- **Pause streaming**
  - The customer can **Pause streaming** at any time during the session. When the customer taps **Pause streaming**, only the camera stream is stopped, the support session stays Active in the Technician Console.
  - The camera stream is also paused when the Rescue Lens goes to the background.

- **Mute/Unmute audio**
  - For Lens sessions using audio, the customer can mute their microphone.
    
    **Important**: The Lens audio connection is automatically muted in case of an incoming call to the customer’s device.

- **Turn on flashlight**
  - When working in a dark environment, the customer can tap this button to activate their device's flashlight.
    
    **Restriction**: On Android devices, flashlight is only available during an active camera stream.
## Appendix - Session statuses in the Rescue Technician Console

The following table describes the possible statuses that are displayed in the Status column of the session queue in the Rescue Technician Console.

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
<th>Previous status</th>
<th>Next status</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Active</strong></td>
<td>Session is picked up either by a technician, or automatically by the Technician Console (if it was an incoming private session).</td>
<td>• Waiting • Incoming • Outgoing • On Hold</td>
<td>• Closed • Closed by technician • Incoming • Outgoing • Timed out • Closed by waiting customer • Aborted • Rebooting • On Hold • Reconnecting • Offline • Collaborating</td>
</tr>
<tr>
<td><strong>Closed (by active customer)</strong></td>
<td>The customer closed the session.</td>
<td>• Active • On Hold • Incoming • Outgoing</td>
<td>Closed by technician</td>
</tr>
<tr>
<td><strong>Removed from TC queue (after closed by technician)</strong></td>
<td>• The technician clicked Close session on the already closed session. • The technician closed a timed out session after the Admin-defined idle timeout was exceeded (as defined in Administration Center &gt; Technician Group &gt; Settings tab &gt; Time-outs) • The technician closed an active session</td>
<td>• Active • Closed • Timed out</td>
<td>none</td>
</tr>
<tr>
<td><strong>Closed by waiting customer</strong></td>
<td>The technician did not pick up the session and the customer closed the session.</td>
<td>• Waiting</td>
<td>none</td>
</tr>
<tr>
<td><strong>Collaborating</strong></td>
<td>The technician invited another technician to collaborate in the session and the invited technician already accepted the invitation.</td>
<td>• Active • On Hold • Rebooting</td>
<td>• Active • Closed • On Hold • Rebooting</td>
</tr>
<tr>
<td>Status</td>
<td>Description</td>
<td>Previous status</td>
<td>Next status</td>
</tr>
<tr>
<td>-------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Connecting</td>
<td>The applet starts downloading after a PIN code is generated or the customer initiates a session on a channel.</td>
<td>PIN code generated or channel connection is initiated</td>
<td>Waiting</td>
</tr>
<tr>
<td>Incoming</td>
<td>Session has been transferred but not yet picked up by the intended recipient. This is the status that the intended recipient can see.</td>
<td>Waiting, Active, On Hold</td>
<td>Active, Timed out, Closed by waiting customer, Closed, Reconnecting, Rebooting</td>
</tr>
<tr>
<td>Invitation</td>
<td>The technician was invited to collaborate in a session but has not yet accepted the invitation.</td>
<td>none</td>
<td>Collaborating, Removed from TC queue</td>
</tr>
<tr>
<td>Offline</td>
<td>Rebooting or reconnecting fails for more than five minutes. Even if reconnecting fails and the session goes to Offline status, the Technician Console tries to reconnect to the customer's computer.</td>
<td>Rebooting, Reconnecting</td>
<td>Waiting, Incoming or Outgoing if the session was in Incoming or Outgoing status before the customer's device tried to reboot or reconnect, On Hold if it was in On Hold status, Active, Timed out, Closed, Closed by technician</td>
</tr>
<tr>
<td>On Hold</td>
<td>The session was put on hold.</td>
<td>Active, Incoming, Outgoing, Reconnecting, Rebooting, Offline, Collaborating</td>
<td>Active, Timed out, Closed, Outgoing, Rebooting, Reconnecting, Collaborating</td>
</tr>
<tr>
<td>Outgoing</td>
<td>Technician A has transferred a session, but it has not yet been picked up by Technician B.</td>
<td>See Incoming status.</td>
<td>See Incoming status.</td>
</tr>
<tr>
<td>Rebooting</td>
<td>The technician reboots the customer's device.</td>
<td>Active, Incoming, Outgoing, On Hold</td>
<td>Waiting, Incoming or Outgoing if the session was in Incoming or Outgoing status</td>
</tr>
</tbody>
</table>
### Session status changes in the Rescue Technician Console

The following table describes how a session can get from a certain status to another one.

<table>
<thead>
<tr>
<th>Start status</th>
<th>End status</th>
<th>How to get there</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connecting</td>
<td>Waiting</td>
<td>Customer downloads and starts the Applet.</td>
</tr>
<tr>
<td>Connecting</td>
<td>Removed from TC queue</td>
<td>1. Technician creates a PIN code but does not run the Applet or accepts the T&amp;C.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Tip:</strong> You can define the T&amp;C in Administration Center &gt; Technician Group &gt; Settings tab &gt; Customer Applet.</td>
</tr>
<tr>
<td>Start status</td>
<td>End status</td>
<td>How to get there</td>
</tr>
<tr>
<td>--------------</td>
<td>------------</td>
<td>------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Technician lets the connecting session time out (for example, after one minute, or as defined in Administration Center &gt; Technician Group &gt; Settings tab &gt; Time-outs).</td>
</tr>
<tr>
<td>Waiting</td>
<td>Active</td>
<td>1. Technician creates a PIN code and shares that with the customer by any connection method. 2. Customer downloads the Applet. 3. Technician starts a session in the Technician Console.</td>
</tr>
<tr>
<td>Waiting</td>
<td>Outgoing</td>
<td>Technician transfers the session from Technician Console session queue.</td>
</tr>
<tr>
<td>Waiting</td>
<td>Removed from TC queue</td>
<td>1. Customer downloads the Applet. 2. Technician lets the connecting session time out (as defined in Administration Center &gt; Technician Group &gt; Settings tab &gt; Time-outs).</td>
</tr>
<tr>
<td>Waiting</td>
<td>Reconnecting</td>
<td>1. Customer downloads the Applet. 2. LAN gets disabled on customer's side. Session will be in Reconnecting status in one minute.</td>
</tr>
<tr>
<td>Waiting</td>
<td>Rebooting</td>
<td>Technician initiates a reboot on the customer’s computer while the session is in Waiting status in the Technician Console queue.</td>
</tr>
<tr>
<td>Active</td>
<td>Closed</td>
<td>1. Customer downloads the Applet. 2. Technician starts a session in the Technician Console. 3. The Applet is closed on the customer side.</td>
</tr>
</tbody>
</table>
| Active       | Timed Out  | 1. Admin sets **Active session idle timeout** in the Administration Center. (For example, to one minute.) 2. Customer downloads the Applet. 3. Technician starts a session in the Technician Console.  
Technician Console should not be in focus until Active session idle timeout is reached. Certain processes will prevent time out, including the following: an open remote control, screen sharing, or file manager session; a pending file transfer; an open save dialog; or a pending Calling Card deployment. |
<p>| Active       | Removed from TC queue | Technician closes an active session by clicking <strong>End session</strong>. |</p>
<table>
<thead>
<tr>
<th>Start status</th>
<th>End status</th>
<th>How to get there</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active</td>
<td>Rebooting</td>
<td>Technician initiates a reboot from Technician Console or asks the customer to reboot his computer.</td>
</tr>
<tr>
<td>Active</td>
<td>Reconnecting</td>
<td>Technician disables LAN connection on the Customer's side or Customer's computer loses network connection.</td>
</tr>
</tbody>
</table>
| Active       | Collaborating| 1. Technician A invites Technician B to a session to collaborate.  
2. Technician A gives lead status to Technician B.  
3. Technician B gives lead status back to Technician A.  
In this case, the status of Technician B changes from Active to Collaborating. |
| Active       | On Hold     | Technician clicks **Hold session** on an active session. |
| Active       | Outgoing    | Technician clicks **Transfer session** on an active session. |
| On Hold      | Active      | 1. Technician places the session on hold.  
2. Technician clicks **Start session**. |
| On Hold      | Outgoing    | 1. Technician places the session on hold.  
2. Technician clicks **Transfer session**. |
| On Hold      | Rebooting   | 1. Technician places the session on hold.  
2. Customer reboots his computer. |
| On Hold      | Collaborating| 1. Technician accepts a collaboration invitation by clicking **Start session**.  
2. Technician places the collaboration session on hold by clicking **Hold session**.  
3. Technician clicks **Start session** to start the session again. |
| On Hold      | Closed      | 1. Technician places the session on hold.  
2. Customer closes the Applet. |
| On Hold      | Reconnecting| 1. Technician places the session on hold.  
2. LAN gets disabled on customer's side. |
| Reconnecting | Active      | 1. Technician initiates a session.  
2. Technician clicks **Start session** to start it.  
3. LAN gets disabled on customer's side.  
4. LAN is enabled. |
<table>
<thead>
<tr>
<th>Start status</th>
<th>End status</th>
<th>How to get there</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reconnecting</td>
<td>On Hold</td>
<td>1. Technician places the session on hold.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. LAN gets disabled on customer's side.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. LAN is enabled.</td>
</tr>
<tr>
<td>Reconnecting</td>
<td>Timed Out</td>
<td>1. Admin sets <em>Active session idle timeout</em> in the Administration Center. (For example, to one minute.)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. LAN gets disabled on customer's side.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. <em>Active session idle timeout</em> expires.</td>
</tr>
<tr>
<td>Reconnecting</td>
<td><em>Removed from TC queue</em></td>
<td>1. LAN gets disabled on customer's side.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Technician clicks <em>End session</em>.</td>
</tr>
<tr>
<td>Reconnecting</td>
<td>Waiting</td>
<td>1. Customer downloads the Applet but the Technician does not start the session.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. LAN gets disabled on customer's side.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. LAN is enabled.</td>
</tr>
<tr>
<td>Reconnecting</td>
<td>Incoming</td>
<td>1. Technician transfers a session.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. LAN gets disabled on customer's side.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. LAN is enabled.</td>
</tr>
<tr>
<td>Reconnecting</td>
<td>Offline</td>
<td>1. LAN gets disabled on customer's side.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Technician waits more than five minutes.</td>
</tr>
<tr>
<td>Offline</td>
<td>Active</td>
<td>1. LAN gets disabled on customer's side.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Technician waits more than five minutes.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. LAN is enabled.</td>
</tr>
<tr>
<td>Offline</td>
<td>Timed Out</td>
<td>1. Admin sets active session timeout to at least eight minutes in the Administration Center.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. LAN gets disabled on customer's side.</td>
</tr>
<tr>
<td>Offline</td>
<td><em>Removed from TC queue</em></td>
<td>Technician selects a session in Offline status and clicks <em>End session</em>.</td>
</tr>
<tr>
<td>Offline</td>
<td>On Hold</td>
<td>1. Technician places the session on hold.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. LAN gets disabled on customer's side.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Technician waits more than five minutes.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. LAN is enabled.</td>
</tr>
<tr>
<td>Start status</td>
<td>End status</td>
<td>How to get there</td>
</tr>
<tr>
<td>-------------</td>
<td>--------------------</td>
<td>----------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Offline     | Waiting            | 1. Customer downloads and starts the Applet but the Technician does not start it in the Technician Console.  
2. LAN gets disabled on customer's side.  
3. Technician waits more than five minutes.  
4. LAN is enabled. |
| Incoming    | Outgoing           | 1. Technician starts a session in the Technician Console.  
2. Technician clicks **Transfer session** and selects a technician group or channel. |
| Incoming    | Reconnecting       | 1. Technician transfers a session.  
2. LAN gets disabled on customer's side. |
| Incoming    | Rebooting          | 1. Technician transfers a session.  
2. Customer's computer is rebooted. |
| Incoming    | Removed from TC queue | 1. Technician transfers a session.  
2. Close the Applet or pick up the outgoing session in the original Technician Console. |
| Incoming    | Active             | Technician picks up an incoming session. |
| Outgoing    | Active             | 1. Technician A transfers a session to Technician B.  
2. Technician A clicks **Start session** on the Outgoing session.  
In this case, the session is removed from the TC queue of Technician B, who did not pick up the incoming session. |
| Outgoing    | Incoming           | 1. Technician A transfers a session to Technician B.  
2. Technician B transfers the incoming session back to Technician A. |
| Outgoing    | Rebooting          | 1. Technician transfers a session.  
2. Technician reboots the customer's computer. |
| Outgoing    | Closed             | 1. Technician transfers a session.  
2. Customer closes the Applet. |
| Outgoing    | Removed from TC queue | 1. Technician A transfers a session to Technician B.  
2. Technician B picks up the session. |
<table>
<thead>
<tr>
<th>Start status</th>
<th>End status</th>
<th>How to get there</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>In this case, the session is removed from the TC queue of Technician A.</td>
</tr>
</tbody>
</table>
| Invitation   | Collaborating          | 1. Technician starts a session in the Technician Console.  
2. Technician clicks **Invite technician**.  
3. The invited technician click **Start session**.                                           |
| Invitation   | Removed from TC queue  | 1. Technician starts a session in the Technician Console.  
2. Technician clicks **Invite technician**.  
3. Technician clicks **Remove technician**.                                                    |
| Collaborating | Rebooting              | 1. Technician starts a session in the Technician Console.  
2. Technician A invites Technician B to a session to collaborate.  
3. Technician B accepts the invitation.  
4. Technician B reboots the customer's computer from the Technician Console or from the customer's side. |
| Collaborating | Removed from TC queue  | 1. Admin sets **Active session idle timeout** in the Administration Center. (For example, to one minute.)  
2. Technician removes focus from the Technician Console while collaborating.                  |
| Collaborating | Closed                 | 1. Technician starts a session in the Technician Console.  
2. Technician A invites Technician B to a session to collaborate.  
3. Technician A close the session as the lead technician or the Customer closes the session. |
| Collaborating | On Hold                | Technician clicks **Hold session** while collaborating.                                                                                           |
| Collaborating | Removed from TC queue  | 1. Technician A invites Technician B to a session to collaborate.  
2. Technician A clicks **Remove technician** to remove Technician B.  
In this case, the session is removed from the TC queue of Technician B.                       |
<p>| Collaborating | Active                 | 1. Technician A invites Technician B to a session to collaborate.                                                                               |</p>
<table>
<thead>
<tr>
<th>Start status</th>
<th>End status</th>
<th>How to get there</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>2. Technician A hands-off lead status to Technician B.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Technician B accepts the lead status by clicking the <strong>Accept lead status</strong> blinking green button above his chatlog.</td>
</tr>
<tr>
<td>Rebooting</td>
<td>Active</td>
<td>Either the Technician or the customer reboots the customer's computer.</td>
</tr>
<tr>
<td>Rebooting</td>
<td>Closed</td>
<td>1. Technician A invites Technician B to a session to collaborate.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. One of the Technicians reboots the customer's computer.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Technician with the lead closes the session during reboot.</td>
</tr>
<tr>
<td>Rebooting</td>
<td>Removed from TC queue</td>
<td>1. Technician A invites Technician B to a session to collaborate.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Technician A (with the lead) reboots the customer's computer.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Technician A removes the collaborating Technician B during reboot.</td>
</tr>
<tr>
<td>Rebooting</td>
<td>Outgoing</td>
<td>1. Technician initiates a session.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Technician clicks <strong>Transfer session</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Technician reboots the customer’s computer after the session acquires Outgoing status.</td>
</tr>
<tr>
<td>Rebooting</td>
<td>On Hold</td>
<td>1. Technician starts a session in the Technician Console.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Technician places the session on hold.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Reboot the customer's computer from the Applet side.</td>
</tr>
<tr>
<td>Rebooting</td>
<td>Incoming</td>
<td>1. Technician starts a session in the Technician Console.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Technician clicks <strong>Transfer session</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Customer reboots the his computer.</td>
</tr>
<tr>
<td>Rebooting</td>
<td>Collaborating</td>
<td>1. Technician A starts a session.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Technician A clicks <strong>Invite technician</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Technician B accepts the invitation.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. Technician B reboots the customer’s computer.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>After reboot, Technician B’s status changes from Rebooting to Collaborating.</td>
</tr>
</tbody>
</table>
## Session status changes during technician monitoring

The following table describes how a session changes its status while a technician is monitoring another technician.

<table>
<thead>
<tr>
<th>Start status</th>
<th>End status</th>
<th>Action to take</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connecting</td>
<td>Waiting</td>
<td>1. Technician A clicks <strong>Monitoring technician</strong> and selects Technician B.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Technician A clicks <strong>OK</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The session is only in Waiting status for a brief moment.</td>
</tr>
</tbody>
</table>

### Table 1: Session status changes during technician monitoring

<table>
<thead>
<tr>
<th>Start status</th>
<th>End status</th>
<th>How to get there</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rebooting</td>
<td>Waiting</td>
<td>1. Technician initiates a session but does not start it.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Customer restarts his computer.</td>
</tr>
<tr>
<td>Closed</td>
<td>Removed from TC queue</td>
<td>1. Technician starts a session in the Technician Console.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Customer closes the session.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Technician clicks <strong>End session</strong> in the Technician Console.</td>
</tr>
<tr>
<td>Timed Out</td>
<td>Timed Out</td>
<td>1. Admin sets <strong>Active session idle timeout</strong> in the Administration Center.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(For example, to one minute.)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Technician initiates a session.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Technician moves focus from the Technician Console so that the session times out.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. Technician leaves the Timed Out session in the Technician Console queue and wait at least three minutes.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The session remains in Timed Out status and does not disappear from the queue.</td>
</tr>
<tr>
<td>Timed Out</td>
<td>Removed from TC queue</td>
<td>1. Admin sets <strong>Active session idle timeout</strong> in the Administration Center.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(For example, to one minute.)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Technician initiates a session.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Technician moves focus from the Technician Console so that the session times out.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. Technician clicks <strong>End session</strong>.</td>
</tr>
<tr>
<td>Start status</td>
<td>End status</td>
<td>Action to take</td>
</tr>
<tr>
<td>--------------</td>
<td>--------------------------</td>
<td>-------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Waiting</td>
<td>Active</td>
<td>1. Technician A clicks <strong>Monitoring technician</strong> and selects Technician B.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Technician A clicks <strong>OK</strong>.</td>
</tr>
<tr>
<td>Active</td>
<td>Closed</td>
<td>1. Technician A clicks <strong>Monitoring technician</strong> and selects Technician B.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Technician A clicks <strong>OK</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Technician B logs out or closes his Technician Console.</td>
</tr>
<tr>
<td>Active</td>
<td>Removed from TC queue</td>
<td>1. Technician A clicks <strong>Monitoring technician</strong> and selects Technician B.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Technician A clicks <strong>OK</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Technician A clicks <strong>End session</strong>.</td>
</tr>
<tr>
<td>Closed</td>
<td>Removed from TC queue</td>
<td>Technician A clicks <strong>End session</strong> while monitoring Technician B.</td>
</tr>
</tbody>
</table>
Legal Notice

PUBLISHED BY
LogMeIn, Inc.
320 Summer Street Suite 100
Boston, MA 02210

All rights reserved. No part of the contents of this document may be reproduced or transmitted in any form or by any means without the written permission of the publisher.

LogMeIn® Central™, LogMeIn Hamachi®, join.me®, LogMeIn Pro®, LogMeIn Rescue® or LogMeIn® Rescue+Mobile™, along with their related software, including the Network Console™, and the other denoted terms in this publication are the trademarks and service marks of LogMeIn, Inc., and may be registered in the U.S. Patent and Trademark Office and in other countries. All other trademarks and registered trademarks are property of their respective owners.

This publication may contain the trademarks and service marks of third parties and such trademarks and service marks are the property of their respective owners. These marks may be registered and/or used in the U.S. and other countries around the world. These third party marks include, but are not limited to, Blackberry, Windows, Apple, iPhone, iPod Touch, iTunes App Store and related trademarks, names and logos. These third party marks are the property of Research In Motion Limited, Microsoft Corporation, and Apple, Inc., respectively, and are registered and/or used in the U.S. and other countries around the world.

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS AND SERVICES IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS AND SERVICES. THE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT AND SERVICES ARE SET FORTH IN THE LOGMEIN TERMS AND CONDITIONS AND ARE INCORPORATED HEREIN BY THIS REFERENCE.
Index

A
access network computers 30
Administration Center
   overview 5
App Store 85, 87, 90, 93
attach remote control window 46
audio 96
Authenticator app 6
automatically start sessions 12

B
BlackBerry 81
   application permissions 82
   connection settings 83
   uninstall the applet 83
   wireless deployment 83

C
Calling Card
   deploying to the customer 57
   the customer's experience 36
chat
   about the chat panel 18
Chat 96
Click2Fix 59
clipboard synchronization 48, 49
collaborating with other technicians 38
collaboration 41, 43
   about 38
   invite external technician 39
   invite internal technician 38
   join session 40
color
   color codes and warnings for sessions 15
   quality during remote control 47
   Technician Console interface 11
confirmations
   when closing the Technician Console 12
   when ending a session 12
connect to customers 26, 61, 63
connecting
   to an unattended computer 32
   via Calling Card 29
   via Channel 28
   via email 27
   via messaging tool 26, 62
   via PIN code 27, 61
copy and paste between computers 48, 49
copying files from one computer to another 52
ctrl+alt+del 48
customer experience 33
customizing
   custom field contents 15
   session list columns 15
   sound alerts 12

D
desktop viewing 44
detach remote control window 46
display size during remote control 47
draw during remote control 49

E
Email 90
email connection method
   step-by-step 27
End session 96

F
file manager 50
File Manager
   open files for editing 53
   select files 53
   sort files 51
files
   copying 52
   moving 52
   replicating 52
   synchronizing 52
Flashlight 96
Freeze 96
fullscreen 46

G
Google Play 85, 87, 90, 93

H
hold 17
Hold session 96

I
inline editing of queue 15
installation
   Technician Console client 9
Instant Chat
   launch the Applet from Instant Chat 35
Instant Chat (continued)
   the customer's experience 34
   iPhone 79

L
languages
   customer-side settings 8
   set Technician Console language 8
   supported 7
laser pointer 49
LastPass 6
Link 93
LogMeIn123 29

M
Mac OS X daemon 45
magnify screen during remote control 47
manage files 50
managing a Rescue Lens session 96
Messaging tool 93
messaging tool connection method
   step-by-step 26, 62
microphone 85, 87, 90, 93
mobile
   QuickNav 64
mobile add-on
   overview 59
monitoring technicians
   step-by-step 24
moving files from one computer to another 52
Multi-object tracking 96
mute 96

N
network computers
   access 30

P
Pause streaming 96
permissions 41, 43
   about technician permissions 10
PIN code 85
PIN code connection method
   step-by-step 27, 61
placing a session on hold 17
predefined replies 21
predefined replies and URLs 21
   export 22
   import 22
predefined URLs 21
   add 21
purchase subscriptions 5

Q
QR code 6
queue
   about 15

R
reboot 55
record sessions 49
remote control 44
remote control
   user rights 45
Rescue Applet
   supported languages 7
   the customer's experience 33
resolution 46

S
screen capture
   during remote control 50
Screen recording 96
screen sharing
   customer controls 38
screen size 47
scripts 56
   deploy 57
   edit and create 56
security
   overview 6
Security 6
sending a customer survey 23
sending a file to a customer 22
session
   history 24
   join 25
   logs 24
   notes 24
session controls 13
sharing your screen with customers
   step-by-step 37
SMS 87
SMS connection method
   step-by-step 61
sound alerts 12
Start a Rescue Lens Session 85, 87, 90, 93
supporting mobile phones 59
switching between sessions 16
sync clipboard 48, 49
system information 53
   applications 54
   dashboard 53
   drivers 54
   interactive user 54
   processes 54
   services 54, 55
   startup 54
unattended access (continued)
   start a session 32
unmute 96

V

video quality 96

W

warnings
   color codes and warnings for sessions 15
whiteboard 49
Whiteboard 96
Windows System Service 45
Windows Task Manager 48