Contents

About LogMeIn Rescue..........................................................................................................................6

LogMeIn Rescue Components..............................................................................................................6

Administration Center – At a Glance..................................................................................................6

Technician Console – At a Glance....................................................................................................6

Command Center – At a Glance......................................................................................................7

About LogMeIn Rescue+Mobile......................................................................................................7

LogMeIn Rescue System Requirements..........................................................................................8

Technician Desktop Device System Requirements.........................................................................8

Customer Desktop Device System Requirements..............................................................................9

Customer Mobile Device System Requirements................................................................................9

About Rescue in a Multilingual Environment................................................................................10

How to Set Administration Center Language................................................................................11

How to Set Technician Console Language......................................................................................12

How to Set Language for the Technician Console for Collaborators..............................................12

About Customer-side Language Settings........................................................................................12

Security in LogMeIn Rescue.............................................................................................................13

Securing your LogMeIn Rescue Account..........................................................................................13

Customer Data Retention..................................................................................................................13

Customer IP Address Retention Policy............................................................................................13

Customer Session Data Removal......................................................................................................13

Setting up Your Organization..........................................................................................................15

About the Organization Tree..............................................................................................................15

How to Add a Master Administrator..................................................................................................15

How to Add an Administrator............................................................................................................16

How to Create an Administrator Group............................................................................................17

How to Create a Technician Group and Assign Permissions............................................................18

Hiding Disabled Features..................................................................................................................20

About Chat Permissions....................................................................................................................21

How to Add Technicians...................................................................................................................22

How to Add a Technician...................................................................................................................22

How to Import Technicians from a File.............................................................................................22

How to Synchronize Rescue Technician Groups with Active Directory User Groups....................23

How to Set Global Password Policies...............................................................................................25

How to Enforce Two-Step Verification.............................................................................................25

How to Reset Two-Step Verification..................................................................................................26

How to Set Hierarchy Visibility in Technician Console.................................................................27

How to Restrict Access Based on IP Address..................................................................................28

Grant/Deny Access to All Components............................................................................................28

Grant/Deny Access to Technician Console......................................................................................29

Setting up Channels.........................................................................................................................31

About Channels.................................................................................................................................31

How to Assign a Channel to a Technician Group.............................................................................31

How to Make a Channel Available for Use.......................................................................................31

How to Remove an Individual Technician from a Channel.............................................................32

How to Test a Channel......................................................................................................................32

Setting up the Applet.........................................................................................................................34

How to Set the Default Applet (Standard or Instant Chat).............................................................34

How to Set Windows System Service Behavior...............................................................................34
Generating Reports .......................................................................................................................... 94
  How to Generate a Report.................................................................................................................... 94
  Customer Survey Report (List All)...................................................................................................... 95
  Customer Survey Report (Summary).................................................................................................. 95
  Customer Survey Issuance Report (List All).................................................................................... 96
  Customer Survey Issuance Report (Summary).................................................................................. 97
  Performance Report (List All)............................................................................................................ 97
  Performance Report (Summary)........................................................................................................... 98
  Login Report (List All)...................................................................................................................... 99
  Login Report (Summary).................................................................................................................... 100
  Session Report (List All).................................................................................................................. 100
  Session Report (Summary) ................................................................................................................. 103
  Chatlog Report........................................................................................................................................ 104
    How to Delete Chatlogs.................................................................................................................... 105
  Collaboration Chat Log Report.......................................................................................................... 106
  Custom Fields Report.......................................................................................................................... 107
  Missed Sessions Report (List All)..................................................................................................... 108
  Missed Sessions Report (Summary)................................................................................................... 109
  Transferred Sessions Report.............................................................................................................. 109
  Transferred Sessions - Extended Report........................................................................................... 110
  Technician Survey Report (List All).................................................................................................. 111
  Failed Sessions Report (List All).................................................................................................... 111
  Failed Sessions Report (Summary).................................................................................................... 112
  Failed Sessions - Extended................................................................................................................. 113
  External Technician Chatlog Report.................................................................................................. 113
  Audit Report (List All)....................................................................................................................... 114
  Rebooting/Reconnecting Report ...................................................................................................... 116
  Technician Status Report.................................................................................................................... 117
  Administrator Status Report.............................................................................................................. 118

Integration and API .......................................................................................................................... 120
  Setting up Single Sign-On Authentication.......................................................................................... 120
  Generate API Token............................................................................................................................ 122
  Sending Session Data to a URL (Post-to-URL).................................................................................. 123
    About Post-to-URL............................................................................................................................. 123
    How to Post Session Data to a URL.................................................................................................. 125
    How to Hide Post Session URLs...................................................................................................... 126
  Integrating Rescue with Other (CRM) Systems.................................................................................. 126
  API Reference........................................................................................................................................ 126

Legal Notice........................................................................................................................................... 127
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/.

LogMeIn Rescue Components

**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.

**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

For details, see the LogMeIn Rescue Technician Console User Guide.

**Note:** A limited version of the Technician Console is used by unlicensed technicians during an external collaboration session.
Command Center – At a Glance

The Command Center is a LogMeIn Rescue component that gives you a powerful tool for monitoring key performance indicators in your support organization. Use it to generate and analyze performance data to determine usage patterns, optimize resource allocation and identify problem areas in your organization.

Requirements:

• A LogMeIn Rescue account
• A Rescue organization already built in the Administration Center
• A supported browser
  • Internet Explorer 8 or higher
  • The latest version Firefox, Chrome, Safari

Here is a quick look at how it works:

1. Launch the Command Center.
   Log in to your Rescue account. Click Command Center on the My Account page or in the Administration Center.

2. Choose a unit.
   Choose any Channel or Technician Group assigned to you, or a custom unit based on labels.

   You will see various performance and capacity related information about the chosen unit (such as capacity, waiting time, handling time, session count).

4. Receive alerts.
   Based on your alert settings, you get visual notification if the performance of the selected unit is out of the specified range.

For more information, see Monitoring Performance Data: The Command Center on page 56.

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

See also Setting up Rescue+Mobile on page 39.

LogMeIn Rescue System Requirements

Important: Make sure you are using up to date, officially supported third-party technology together with LogMeIn Rescue. LogMeIn Rescue is designed for use with third-party products and services (browser, OS, etc.) that are officially supported by their respective vendors and well-maintained by the end user (latest patches and updates installed). Learn more

Technician Desktop Device System Requirements

Any computer running the LogMeIn Rescue Technician Console must meet the following system requirements.

Requirement for using the standalone version of Technician Console:
• Microsoft Windows Vista and above
• Apple Macintosh OS X 10.7 (Lion) and above for Technician Console for Mac desktop application
• A working Internet connection (ISDN or faster if performing remote control or remote viewing)
• Up to 100MB of memory plus 20MB per remote control session
• Up to 30MB of storage space plus 20MB for all smartphone simulations

Requirements for the browser-based Technician Console:
• Microsoft Windows Vista and above
• Microsoft Server 2008 and above (including 64 bit versions)
• Internet Explorer 7 and above with support for 128-bit or 256-bit encryption
• Firefox under version 43
• Chrome and MS Edge are not supported
• A working Internet connection (ISDN or faster if performing remote control or remote viewing)
• Up to 100MB of memory plus 20MB per remote control session
• Up to 30MB of storage space plus 20MB for all smartphone simulations

Requirements for using the Collaboration version of the Technician Console:
• Microsoft Windows Vista and above
• A working Internet connection (ISDN or faster if performing remote control or remote viewing)
• Up to 100MB of memory plus 20MB per remote control session
• Up to 30MB of storage space plus 20MB for all smartphone simulations

Requirements for using the Rescue Lens Technician Console:
• Internet connection with minimum 800 kbit/sec bandwidth
• From both the support technician's and the customer's network, the following web resources need to be accessible:
  • *.logmeinrescue.com domain group
Note: For Rescue-enterprise customers the *.logmeinrescue-enterprise.com domain group applies.

- For networks explicitly filtering outbound destination ports and protocols, the following ports are used on the Rescue side:
  - 15000 (UDP traffic) or 443 (TCP traffic) for Rescue Lens media sessions
  
  Example: rescuemedia[XX-XX].logmeinrescue-enterprise.com:443

Customer Desktop Device System Requirements

Technicians using LogMeIn Rescue can provide remote support to computers meeting the following system requirements:

- Microsoft Windows Vista and above
- Microsoft Server 2008 and above (including 64 bit versions)
- Apple Macintosh OS X 10.4 (Tiger) and above

Note: Rescue Applet over Mac Instant Chat supports only MAC OS X 10.6 (Snow Leopard) and above.

- For optimal performance, the customer should be connected to the Internet via a broadband connection (T1, cable modem, ISDN, or DSL); 28K dial-up is also supported
- 100MB, plus an additional 20MB of memory for each remote control session (Technician Collaboration can cause simultaneous remote control sessions on the customer device)

Choosing how to handle sessions when an unsupported OS is detected

It may happen that customers using an unsupported operating system try to start a Rescue session. Administrators have two options available in the Administration Center on the Global Settings tab under Unsupported customer OS > If an unsupported OS is detected:

- Start Instant Chat session – Place the customer in an Instant Chat session.
- Do not start session – Show the customer a message explaining that they cannot start a session because they are using an unsupported browser.

Customer Mobile Device System Requirements

Requirements for Using the Rescue+Mobile App

Android Requirements:

- Android 4.4 and above (Android 5.0 or above recommended)
- Dual-core CPU (Quad-core CPU recommended)
- 1 GByte RAM (2 GByte recommended)
- 20 MByte free space
- Internet connection with minimum 400 kbit/sec bandwidth (4G/LTE or equivalent WiFi recommended)

Requirements for Remote Control Advanced:

For Remote Control Advanced features, certain devices also require an add-on application from Google Play.

- Samsung devices powered by KNOX
• The following devices running Android 4.4 and above:
  • LG
  • HTC
  • Honeywell Mobility Edge
  • Huawei
  • select Positivo devices

iOS Requirements:
• iOS 11 and above
• 20 MByte free space
• Internet connection with minimum 400 kbit/sec bandwidth (4G/LTE or equivalent WiFi recommended)

Restriction: Advanced Remote Control is not available for iOS devices.

Requirements for Using the Rescue Lens Mobile App

Rescue Lens Android Requirements:
• Android 4.4 or above (Android 5.0 or above recommended)
• Dual-core CPU (Quad-core CPU recommended)
• 1 GByte RAM (2 GByte recommended)
• 25 MByte free space
• Camera with autofocus and resolution 640*480
• Internet connection with minimum 400 kbit/sec bandwidth (4G/LTE or equivalent WiFi recommended)

Rescue Lens iOS Requirements:
• iOS 11 or above
• 20 MByte free space
• Internet connection with minimum 400 kbit/sec bandwidth (4G/LTE or equivalent WiFi recommended)

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>de – German</th>
<th>ko – Korean</th>
</tr>
</thead>
<tbody>
<tr>
<td>en – English</td>
<td>nl – Dutch</td>
</tr>
<tr>
<td>es – Spanish</td>
<td>pt-br – Portuguese (Brazilian)</td>
</tr>
<tr>
<td>fr – French</td>
<td>th – Thai</td>
</tr>
<tr>
<td>it – Italian</td>
<td>zh – Chinese</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>zh-TW</td>
<td>Chinese (Taiwan)</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>en</td>
<td>English</td>
</tr>
<tr>
<td>ro</td>
<td>Romanian</td>
</tr>
<tr>
<td>es</td>
<td>Spanish</td>
</tr>
<tr>
<td>ru</td>
<td>Russian</td>
</tr>
<tr>
<td>fi</td>
<td>Finnish</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>hu</td>
<td>Hungarian</td>
</tr>
<tr>
<td>zh-TW</td>
<td>Chinese (Taiwan)</td>
</tr>
<tr>
<td>ja</td>
<td>Japanese</td>
</tr>
<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>
</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)" in the LogMeIn Rescue Technician Console User Guide.

**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 Administration Center Language

To change the language used by the Administration Center, use the language drop-down list on any Administration Center page. You can change Administration Center language at any time.

### About Language Selection for Custom Fields and the Organization Tree

The default language used by the Administration Center Organization Tree, channel names, and Custom Fields on the Global Settings tab is set according to the language used at the time when you register for a LogMeIn Rescue account. This feature protects your Custom Fields and Organization Tree entity names from unwanted changes.

For example, if you register for a LogMeIn Rescue account using the German registration form, then the Organization Tree and custom fields will show in German until they are manually edited. The language selector will not change the language displayed in the Organization Tree or custom fields.
Code samples are always in English.

**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.
Security in LogMeIn Rescue

For detailed information, see the LogMeIn Rescue Architecture Whitepaper.

Securing your LogMeIn Rescue Account

Master Administrators can set Rescue to send notifications by email when selected events occur. Log in to your LogMeIn Rescue account and go to My Account. On the left side of the page, click Notifications.

- Successful login attempt
- Unsuccessful login attempt
- Contact information modified
- Billing information modified
- Password changed
- Administrator information changed
- Administrator(s) deleted
- Technician information change
- Technician(s) deleted

Customer Data Retention

Customer IP Address Retention Policy

By default, Rescue stores the IP address of each customer involved in a session. If you are concerned about protecting the privacy of your customers, you can choose not to save or report this data.

1. Select the Global Settings tab.
2. Under Customer IP Address Retention Policy, select Do not store customer IP address.
3. Click Save changes.

While this option is selected, Rescue does not store any information about customer IP address. As a result, the Session (List All) report returns no data in the Customer IP column.

**Remember:** This option does not work retroactively. It has no impact on IP address information already saved by Rescue. No historical data is deleted when you activate this option.

Customer Session Data Removal

Administrators can delete personal customer data collected from sessions conducted within Technician Groups to which they are assigned. Master Administrators can delete personal customer data in the whole support organization.

1. On the Organization Tree, select the organizational unit for which you want to generate a report.
2. Select the Reports tab.
3. Select the **Session Report** report type using the **Report Area** drop-down box.

4. Specify details and generate the report as indicated in section **How to Generate a Report** on page 94.
   
   When the report is generated, each row represents a unique session.

5. Select the row that contains customer data you want to delete.

6. Click the **trash can icon** at the end of the row to delete all customer data related to the selected session.

   **Note:** Customer data is deleted within 30 days from the moment of queuing it for deletion.

   **Caution:** Pending deletions cannot be revoked.
Setting up Your Organization

About the Organization Tree

The Organization Tree is where you configure Rescue to match your support organization. It is displayed in the left panel of the Administration Center interface.

Once you have set up your organization, the Organization Tree offers a clear representation of your structure and makes it easy to select existing organization members and channels, and to make changes with a simple drag-and-drop motion.

Tip: To achieve optimal performance, close all items on the Organization Tree that you are not currently using. This is particularly important for very large accounts.

Expand/Collapse branches Branches can be expanded/collapsed by clicking +/-

Search Enter text in the search field to search for a group, technician, or any other unit in your organization.

Drag-and-Drop Certain items of the Organization Tree can be dragged and dropped items within the tree. For example, Administrators can be assigned to a Technician Group by dragging them into the group. Technicians and Technician Groups can also be easily moved and assigned using the drag-and-drop facility.

Right-click menu Right-click any item in the tree brings to open a shortcut menu. The available selections in the menu change depending on your user role and the item you are clicking.

Dynamic relationship with the Workspace Selecting an item on the organization tree opens the relevant form in the Workspace (the right pane).

How to Add a Master Administrator

Master Administrators have complete control over all areas of the Administration Center. They are the only users with access to the Global Settings tab.

This option is only available to Master Administrators.

1. Right-click Master Administrators on the Organization Tree.
2. Click Create Master Administrator.
   A new Master Administrator is added to the Organization Tree.
3. Make sure the user you want to work with is selected on the Organization Tree and click the Organization tab.
   The Configuration page is displayed.
4. Edit the following options:
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The user’s name as it will be displayed on the Organization Tree and in the Technician Console, if licensed.</td>
</tr>
<tr>
<td>Email</td>
<td>The email address the user will use to log in to LogMeIn Rescue.</td>
</tr>
<tr>
<td>Single Sign-On ID</td>
<td>The identification number the user will use to log on if Single Sign-on is active.</td>
</tr>
<tr>
<td>Description</td>
<td>This is for your own reference.</td>
</tr>
<tr>
<td>New password</td>
<td>The password the user will use to log in to LogMeIn Rescue.</td>
</tr>
<tr>
<td><strong>Note:</strong> To require the user to change this password when they first log in, make sure the Admin password changes force user to change password at next logon option is selected under the Password policies section of the Global Settings tab.</td>
<td></td>
</tr>
<tr>
<td>Minimum password strength</td>
<td>The minimum required password strength as set on the Global Settings tab under Password Policies.</td>
</tr>
</tbody>
</table>

5. Under Status, select **Enabled** to activate the user.
6. Click **Save changes**.

**How to Add an Administrator**

Administrators manage technicians and Technician Groups, generate reports, and more. This option is only available to Master Administrators.

Administrator Characteristics:
- Maintains all assigned technicians and Technician Groups
- Disables any technicians and Technician Groups if necessary
- Generates reports
- Configures support channels for assigned Technician Groups
- Can be assigned to multiple Technician Groups
- Can perform all functions of a technician (if licensed)

1. Right-click the location in the organization where you want to add the new Administrator and click **Create administrator**.
   - To add the new administrator at the Administrators root-level, right-click **Administrators** on the Organization Tree
   - To add the new administrator as a member of an existing Administrator Group, right-click the chosen group on the Organization Tree

   A new administrator is added to the Organization Tree at the chosen location.
2. Make sure the user you want to work with is selected on the Organization Tree and click the **Organization** tab.
   The Configuration page is displayed.
3. Edit the following options:
### Option | Description
--- | ---
Name | The user’s name as it will be displayed on the Organization Tree and in the Technician Console, if licensed.
Email | The email address the user will use to log in to LogMeIn Rescue.
Single Sign-On ID | The identification number the user will use to log on if Single Sign-on is active.
Description | This is for your own reference.
New password | The password the user will use to log in to LogMeIn Rescue.

**Note:** To require the user to change this password when they first log in, make sure the Admin password changes force user to change password at next logon option is selected under the Password policies section of the Global Settings tab.

| Minimum password strength | The minimum required password strength as set on the Global Settings tab under Password Policies. |

4. Under **Status**, select **Enabled** to activate the user.
5. Click **Save changes**.

**Tip:** To assign the user to a group (or groups), drag the user's icon to a target group.

### How to Create an Administrator Group

An Administrator can belong to one Administrator Group at any time. You can include Administrator Groups within Administrator Groups.

This option is only available to Master Administrators.

1. Right-click the location in the organization where you want to add the new Administrator Group and click **Create group**.
   - To add the new Administrator Group at the Administrators root-level, right-click **Administrators** on the Organization Tree
   - To add the new Administrator Group as a sub-group of an existing Administrator Group, right-click the chosen group on the Organization Tree

   A new Administrator Group is added to the Organization Tree at the chosen location.

2. Enter a **Group name** and **Description**.
3. Under **Status**, select **Enabled** to activate the group.
4. Set group permissions.

| Option | Description |
--- | ---|
Standard administrator rights | When **Standard administrator rights** is selected, group members can administer technicians and access both the Administration Center and the Command Center. |
When **Restricted administrator rights** is selected, at least one sub-option must be selected:

- Select **Grant access to Command Center** to allow group members to access the Command Center.
- Select **Grant access to Administration Center > Reports** to allow group members to access only the Reports tab in the Administration Center. No other tabs are visible.

5. Click **Save changes**.

### How to Create a Technician Group and Assign Permissions

Master Administrators can create Technician Groups anywhere in the organization, while administrators can only create groups under Technician Groups to which they are assigned. Master Administrators can lock permissions so they cannot be changed by an Administrator.

1. Right-click the location in the organization where you want to add the new Technician Group and click **Create group**.

   - To add the new Technician Group at the Technician Group root-level, right-click **Technicians** on the Organization Tree
   - To add the new Technician Group as a sub-group of an existing Technician Group, right-click the chosen group on the Organization Tree

   A new Technician Group is added to the Organization Tree at the chosen location.

2. Enter a **Group name** and **Description**.

3. Under **Status**, select **Enabled** to activate the group.

4. Set group permissions.

<table>
<thead>
<tr>
<th>Permission</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Chat</strong></td>
<td>Enables chat at session start. See <em>About Chat Permissions</em> on page 21.</td>
</tr>
<tr>
<td><strong>Allow chat enable/disable by Technician</strong></td>
<td>Allows group members to enable or disable chat. See <em>About Chat Permissions</em> on page 21.</td>
</tr>
<tr>
<td><strong>Launch remote control</strong></td>
<td>Allow group members to initiate a remote control session during any active session.</td>
</tr>
<tr>
<td><strong>Launch desktop viewing</strong></td>
<td>Allow group members to initiate a Desktop Viewing Session during any active session.</td>
</tr>
<tr>
<td><strong>Send files</strong></td>
<td>Allow group members to send files to a customer during any active session.</td>
</tr>
<tr>
<td><strong>Receive files</strong></td>
<td>Allow group members to receive files from a customer during any active session.</td>
</tr>
<tr>
<td>Permission</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Access File Manager tab</strong></td>
<td>Allow group members to access the File Manager tab in the Rescue Technician Console during any active session.</td>
</tr>
<tr>
<td><strong>Send URLs</strong></td>
<td>Allow group members to send a URL that will open on the customer's device during any active session.</td>
</tr>
<tr>
<td><strong>View system information</strong></td>
<td>Allow group members to view the customer's system information during an active desktop or mobile session. Not applicable to Click2Fix.</td>
</tr>
<tr>
<td><strong>Reboot</strong></td>
<td>Allow group members to reboot the customer's device during an active session.</td>
</tr>
<tr>
<td><strong>Record sessions</strong></td>
<td>Allow group members to make a screen recording of any session.</td>
</tr>
<tr>
<td><strong>Start private sessions</strong></td>
<td>Allow group members to start a session using a private method (PIN Code, Link, SMS with Rescue+Mobile, Calling Card).</td>
</tr>
<tr>
<td><strong>Use single prompt for all permissions</strong></td>
<td>Customers will be asked only once to grant the technician permission to perform remote actions. Otherwise, the customer will be prompted each time the technician attempts an action.</td>
</tr>
<tr>
<td><strong>Transfer sessions</strong></td>
<td>Allow group members to transfer a session to a valid member of the organization. You have the following options:</td>
</tr>
<tr>
<td><strong>Hold sessions</strong></td>
<td>Allow group members to place sessions on hold.</td>
</tr>
<tr>
<td><strong>Request Windows credentials</strong></td>
<td>Allow group members to request a customer’s Windows credentials during an active session.</td>
</tr>
<tr>
<td><strong>Allow clipboard synchronization</strong></td>
<td>Allow group members to synchronize the customer’s clipboard to their own. Anything copied on one machine is automatically available to be pasted on the other.</td>
</tr>
<tr>
<td><strong>Deploy the Calling Card</strong></td>
<td>Allow group members to deploy the Calling Card Applet to the customer’s desktop.</td>
</tr>
<tr>
<td><strong>Allow screen sharing with customers</strong></td>
<td>Allow group members to be able to share their desktop with customers.</td>
</tr>
</tbody>
</table>

**Note:** The actual capability to send/receive files depends on the Send files and Receive files permissions; therefore, when the Access File Manager tab permission is denied, group members may still be able to send/receive files.

When the Manage files permission is selected, group members will be allowed to manage a customer's files during any active session.

When the only with customer consent is selected, group members will only be allowed to record a customer's screen with the customer's consent. Customers will always be prompted to grant the technician permission, even when Use single prompt for all permissions is enabled.

Customers will be asked only once to grant the technician permission to perform remote actions. Otherwise, the customer will be prompted each time the technician attempts an action.

- to any technician allows technicians to transfer sessions to any other technician in the organization.
- to specific technician groups or channels allows technicians to transfer sessions to selected Technician Groups and channels.
<table>
<thead>
<tr>
<th>Permission</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Send collaboration invitations</strong></td>
<td>Allow group members to be able to invite other technicians to an active session. You have the following options:</td>
</tr>
<tr>
<td></td>
<td>• <strong>to any technician</strong> allows technicians to invite any other technician in the organization.</td>
</tr>
<tr>
<td></td>
<td>• <strong>to specific technician groups</strong> allows technicians to invite members of the selected Technician Groups.</td>
</tr>
<tr>
<td><strong>Invite external technicians</strong></td>
<td>Allow group members to collaborate on a session with individuals who are external to your Rescue organization. External technicians do not need to have a Rescue subscription of their own. That is, they are not configured as users in your Rescue account. You have the following options:</td>
</tr>
<tr>
<td></td>
<td>• <strong>anyone can be invited</strong> allows technicians to send an invitation to any email address.</td>
</tr>
<tr>
<td></td>
<td>• <strong>only approved</strong> allows technicians to invite only approved individuals who have been added to External Technician Groups.</td>
</tr>
<tr>
<td><strong>Inline editing of Queue</strong></td>
<td>Allow group members to edit Custom Fields during a session.</td>
</tr>
<tr>
<td><strong>Script deployment</strong></td>
<td>Allow group members to deploy scripts to the customer’s system.</td>
</tr>
<tr>
<td><strong>Run embedded scripts</strong></td>
<td>Allow group members to manually run embedded scripts by clicking the <strong>Run Script</strong> button on the Technician Console <strong>Reboot</strong> tab.</td>
</tr>
<tr>
<td><strong>Unattended access</strong></td>
<td>Unattended access allows a technician to connect to a remote computer when no user is present. Allow group members to request permission to be able to access the customer's computer when the customer is not present and to start unattended sessions.</td>
</tr>
<tr>
<td><strong>Connect On LAN</strong></td>
<td>Allow group members to connect to unattended computers on the local area network. No customer interaction required.</td>
</tr>
<tr>
<td><strong>Configure mobile device settings</strong></td>
<td>Allow group members to manage mobile device settings using the Device Configuration tab in the Technician Console. Not applicable to Click2Fix.</td>
</tr>
<tr>
<td><strong>Click2Fix for mobile</strong></td>
<td>When selected, all sessions with a mobile device will default to the Click2Fix tab.</td>
</tr>
<tr>
<td><strong>Classic display for mobile</strong></td>
<td>For mobile sessions, activate the legacy Customer Display tab.</td>
</tr>
<tr>
<td><strong>Rescue Lens</strong></td>
<td>Allow group members to start Rescue Lens sessions. With Rescue Lens, customers can use their mobile device to stream live video to a technician.</td>
</tr>
<tr>
<td><strong>Screen capture</strong></td>
<td>Allow group members to capture images of the customer's screen during a session.</td>
</tr>
</tbody>
</table>

5. Click **Save changes**.

**Hiding Disabled Features**
To ensure that technicians can focus on the right tools for the job, the Technician Console hides certain tabs and buttons when a technician does not have permission to use the associated feature.
<table>
<thead>
<tr>
<th>To hide this...</th>
<th>Deny this permission on the Organization tab...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Launch Remote Control Session button on Customer Desktop tab</td>
<td>Launch remote control</td>
</tr>
<tr>
<td>Launch Desktop Viewing button on Customer Desktop tab</td>
<td>Launch desktop viewing</td>
</tr>
<tr>
<td>File Manager tab</td>
<td>Access File Manager tab or Send files, Receive files, and Manage files</td>
</tr>
<tr>
<td>System Info tab</td>
<td>View system information</td>
</tr>
<tr>
<td>Reboot tab</td>
<td>Reboot</td>
</tr>
<tr>
<td>Calling Card tab</td>
<td>Deploy the Calling Card</td>
</tr>
<tr>
<td>Scripts tab</td>
<td>Script deployment and Run embedded scripts</td>
</tr>
<tr>
<td>Unattended Access tab</td>
<td>Unattended Access</td>
</tr>
<tr>
<td>Device Configuration tab</td>
<td>Configure mobile device settings</td>
</tr>
<tr>
<td>Customer Display tab for mobile sessions</td>
<td>Classic display for mobile</td>
</tr>
<tr>
<td>Click2Fix tab for mobile sessions</td>
<td>Click2Fix for mobile</td>
</tr>
</tbody>
</table>

**About Chat Permissions**

An administrator sets a Technician Group's permission to use the Enable/Disable Chat feature on the Organization tab.

- **Chat**
  - Select only **Chat** to enable Chat at session start.

- **Chat** and **Allow chat enable/disable by technician**
  - Select **Chat** plus **Allow chat enable/disable by technician** to enable Chat at session start and allow technicians to toggle Chat during the session.

- **Allow chat enable/disable by technician**
  - Select only **Allow chat enable/disable by technician** to disable Chat at session start, but allow technicians to toggle Chat during the session.

- **Chat** and **Allow chat enable/disable by technician**
  - When neither option is selected, Chat is disabled at session start, and technicians are not allowed to toggle Chat during the session.

**Note:** The above settings apply to sessions started by running the Rescue Applet. Chat is always enabled for Instant Chat sessions.
How to Add Technicians

Master Administrators can add technicians to any Technician Group in the organization, while Administrators can only add technicians to groups to which they are assigned.

How to Add a Technician

Technician permissions are inherited from the Technician Group.

1. Right-click the Technician Group to which you want to add the technician and click Create technician.
2. Make sure the user you want to work with is selected on the Organization Tree and click the Organization tab.
   The Configuration page is displayed.
3. Edit the following options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The user’s name as it will be displayed on the Organization Tree and in the Technician Console, if licensed.</td>
</tr>
<tr>
<td>Nickname</td>
<td>The user’s name as it will be displayed to the customer during a session. Example: [10:46 AM] Chat session established with Nickname.</td>
</tr>
<tr>
<td>Email</td>
<td>The email address the user will use to log in to LogMeIn Rescue.</td>
</tr>
<tr>
<td>Single Sign-On ID</td>
<td>The identification number the user will use to log on if Single Sign-on is active.</td>
</tr>
<tr>
<td>Description</td>
<td>This is for your own reference.</td>
</tr>
<tr>
<td>New password</td>
<td>The password the user will use to log in to LogMeIn Rescue.</td>
</tr>
</tbody>
</table>

Note: To require the user to change this password when they first log in, make sure the Admin password changes force user to change password at next logon option is selected under the Password policies section of the Global Settings tab.

4. Under Status, select Enabled to activate the user.
5. Click Save changes.

Tip: To move a technician to another group, select a technician on the Organization Tree and drag it to the desired Technician Group or use the Move to Technician Group drop-down list on the Configuration page.

How to Import Technicians from a File

Master Administrators can import technicians “in bulk” by uploading a CSV or JSON file.

Note: During the below procedure, you will be required define a password for each technician that you import. As a best practice, before you perform the import, we recommend that you enable
a setting that will require the technician to change this initial password when they first log in. To do so, make sure the Admin password changes force user to change password at next logon option is selected under the Password policies section of the Global Settings tab in the Rescue Administration Center.


   Note: For detailed information about requirements related to the CSV or JSON files, you can download example files from the Import technicians page.

   To change the delimiter used in the example file, follow the below instructions.
   - Windows
   - Mac

2. Select the Technician Group to which you want to import technicians by starting to type the name of the group in the Search technician group... field.

   Fastpath: If the uploaded file contains valid Technician Group IDs for each line, you may leave this field empty.

3. Click Upload file to choose the CSV or JSON file from your source.
4. Click Start import.

   Import starts. When the process ends, the Import Summary is displayed listing all the successful or failed import items.

   Note: The CSV or JSON file must meet the following requirements.
   - All column headers are required and MUST remain in their original order in the file.
   - The following fields are required and each row must contain data as part of the import:
     - Name
     - Email address
     - Password
     - (technician is) Enabled
     - (has) Standard License
     - (has) Mobile License
   - If you set all users to be imported into the same Technician Group (by selecting a global group), you can leave the Tech Group ID column blank.

   Remember: The column header must remain in the original order.
   - If you select a global Tech Group, Tech Group IDs in the file will be ignored during the import.
   - Each import file is limited to a maximum of 500 users.

How to Synchronize Rescue Technician Groups with Active Directory User Groups

Master Account Holders can import Active Directory users as Rescue technicians into their organization. Key user data in Rescue will be automatically updated when those change in Active Directory.

1. Generate a service token and default password for new users in the Admin Center.
   a) Select the Global Settings tab.
b) To generate a service token, click **Generate and Copy** under **Active Directory Synchronization**. A service token is generated and copied to your clipboard.

c) Define the default password you want your new technicians to use for their first login.

**Note:** Users are required to change this password upon their first login.

2. Download and extract the server application.

a) In the Rescue Administration Center, under **Active Directory Synchronization**, click **Download** to download the service installer.

The service installer is downloaded to your computer in a zip file.

b) Extract the zip file to a folder.

3. Run the server application, and configure synchronization behavior.

**Important:** You need privileges to run the application as a system service. The computer running the application must be connected to Active Directory with sufficient permissions to access and query all Active Directory groups and users.

a) Submit the following credentials:

- Master Account Holder Rescue credentials
- Email
- Password
- The service token you previously generated on the **Global Settings** tab of the Admin Center.

b) Click **Next** to run **ADService.exe**.

**Note:** The application runs in Admin mode.

c) Enter the Active Directory domain from which you want to import users, and click **Next**.

d) Select the source and destination groups.

- The Active Directory group from which you want to import users/data.
- The Rescue Technician Group to which you want to add users/data.

The service application is installed as a windows service provisioning users belonging to the selected Active Directory group to the selected Rescue Technician Groups.

The following user data is synchronized from Active Directory to Rescue both during initial provisioning of users and subsequently upon changes in Active Directory:

- Name
- Email
- Status

**Restriction:** It is not possible to delete a technician from the Rescue Admin Center by using the Active Directory synchronization service. When a user is deleted or moved in Active Directory, the corresponding Rescue technician is disabled.

**Note:** If a technician is moved to another Rescue Technician Group, subsequent synchronization will only update the user’s status, but will not move the user back to its initial synchronization group.
Note: If a user is disabled, deleted, or moved in Active Directory, the technician's mobile license is freed up, and becomes available for other members of the Rescue organization.

Tip: If the synchronization service fails, you can get an error log by clicking Active Directory Logger at the bottom of the Active Directory Synchronization section on the Global Settings tab of the Admin Center.

How to Set Global Password Policies

Master Administrators can set password policies that apply to all users in the Rescue organization.

1. Select the Global Settings tab.
2. Under Password Policies, select from the following options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum password strength</td>
<td>Specify the minimum password strength that must be met by all members of the organization.</td>
</tr>
<tr>
<td></td>
<td>No password may be less than 8 characters in length. Passwords comprise four character types: lowercase (&quot;abc&quot;); uppercase (&quot;ABC&quot;); numeric (&quot;123&quot;); and special (&quot;%#&amp;&quot;).</td>
</tr>
<tr>
<td></td>
<td>Three password strengths can be assigned:</td>
</tr>
<tr>
<td></td>
<td>• Good: 3 character types, but some repeat characters, i.e. &quot;Sampla12&quot;</td>
</tr>
<tr>
<td></td>
<td>• Strong: 3 character types, no repeat characters, i.e. &quot;Sample12&quot;; or 4 character types, but some repeat characters, i.e. &quot;Sampla1%&quot;</td>
</tr>
<tr>
<td></td>
<td>• Excellent: 4 character types, no repeat characters, i.e. &quot;Sample1%&quot;</td>
</tr>
<tr>
<td>Maximum password age</td>
<td>Specify the maximum number of days that a password remains valid (0 = no limit).</td>
</tr>
<tr>
<td>Notification before password expires</td>
<td>Notify users that their password is due to expire in this many days (0 = no notification).</td>
</tr>
<tr>
<td>Admin password changes force user to change password at next logon</td>
<td>Force a user to change his password when next logging in to his account if his Rescue password has been changed. After logging in with the new password created by the administrator, the user will be prompted to create his own new password.</td>
</tr>
</tbody>
</table>

3. Click Save Changes.
   The settings are applied to all users in your Rescue organization.

How to Enforce Two-Step Verification

Master Administrators can add a second layer of protection to their Rescue account by forcing members of their organization to use two-step verification for logging in to Rescue.

1. Select the Global Settings tab.
2. Under **Two-step verification**, select the members of your organization who you want to use two-step verification when logging in to the Rescue website and Desktop Technician Console and when changing their password in either component.

![Two-step verification](image)

**Important:** Administrators with both an administrator and a technician license will be required to use two-step verification if settings apply to them either as an Administrator, or as an affected technician.

If **Members of selected Technician Group(s)** is selected under **Technicians**, make sure to select the **Enforce two-step verification** checkbox on the **Settings** tab for the desired Technician Group(s).

3. Click **Save Changes**. The settings are applied to the selected users in your Rescue organization.

### How to Reset Two-Step Verification

Resetting two-step verification is necessary when a member of the Rescue organization required to use two-step verification needs to reinstall the LastPass Authenticator app.

Examples when reinstalling the Authenticator app is necessary:

- The user loses their mobile device on which the Authenticator app is installed.
- The user starts using a new mobile device and has to install another instance of the Authenticator app.
- The Authenticator app fails, and there is no other way of fixing the issue.

**Important:** Master Administrators can reset two-step verification for any organization member for whom the feature is enabled, while Administrators can only reset two-step verification for members of the Technician Groups they are assigned to.

1. Select the **Organization** tab.
2. On the Organization Tree, select the member for whom you want to reset two-step verification.
3. Click **Force two-step verification reset**.
   The selected member will have to set up the LastPass Authenticator for their Rescue account upon their next login attempt.

### How to Set Hierarchy Visibility in Technician Console

The Hierarchy Visibility feature allows Master Administrators to simplify the organizational hierarchy displayed to Rescue users when transferring sessions, inviting other technicians, or choosing a technician to monitor.

1. Select the **Global Settings** tab.
2. Under **Hierarchy Visibility in Technician Console**, select from the following options:
   
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Compact View</strong></td>
<td>Technicians see only those organization entities that are relevant targets for their given action (transferring a session, inviting a technician, or monitoring a technician).</td>
</tr>
<tr>
<td></td>
<td><strong>Compact View</strong> displays an aggregated view of channels (only one instance of each channel displayed).</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The Monitoring Technician feature is available for Administrators with a technician seat.</td>
</tr>
<tr>
<td><strong>Extended View</strong></td>
<td>Transfer session, Invite technician, and Monitor technician windows display the full Organization Tree. Channels are displayed for each organization entity they are assigned to.</td>
</tr>
</tbody>
</table>
3. Click **Save Changes**.
   The settings are applied to all users in your Rescue organization.

# How to Restrict Access Based on IP Address

Use the IP Restriction feature to grant or deny access to Rescue according to specified IP address ranges.

## Grant/Deny Access to All Components

By default, Rescue users can access all Rescue components from any IP address. You can grant or deny access to all Rescue components, including the Rescue Administration Center and Technician Console, according to specified IP address ranges.

1. Select the **Global Settings** tab.
2. Under **IP restrictions (Global)**, complete the **Add new exception** fields to *allow* access to all Rescue components from all IP addresses except those specified.
3. To deny access to all Rescue Components from all IP addresses except those specified, select Denied access and enter the appropriate Network ID.

Users of the Rescue account will be able to access Rescue components only from the address set as an exception.

**Grant/Deny Access to Technician Console**

By default, technicians can access the Technician Console from any IP address. You can grant or deny access to the Technician Console according to specified IP address ranges.

These settings have no impact on external collaborating technicians.

1. On the Organization Tree, select the Technician Group you want to work with.
2. Select the Settings tab.
3. Under IP restrictions (Technician Console), complete the Add new exception fields to allow access to the Technician Console from all IP addresses except those specified.

**Remember:** If a technician cannot access the Technician Console, make sure they have also been granted access to all Rescue components under Global Settings > IP restrictions (Global)

4. To deny access to the Technician Console from all IP addresses except those specified, select Denied access and enter the appropriate Network ID.
Users in the Technician Group will be able to access the Technician Console only from the address set as an exception.

**Remember:** If a technician cannot access the Technician Console, make sure they have been granted access to all Rescue components under **Global Settings > IP restrictions (Global)**

5. Save your changes.
Setting up Channels

About Channels

Customers use channels to initiate Rescue support sessions by clicking a URL embedded in your website or via the Calling Card.

Incoming sessions are added to the queue for all members of any Technician Group which is assigned to a channel. Any incoming channel session will be displayed to all technicians in a group until it is picked up or times out.

Rescue provides ten channels for flexible session routing.

How to Assign a Channel to a Technician Group

Channels can be assigned to a Technician Group by a Master Administrator or by an Administrator responsible for that Technician Group.

By default, the channels are named "Channel 1", "Channel 2", and so on. You cannot create new channels; only rename.

1. On the Organization Tree, select the Technician Group to which you want to assign a channel.
2. Select the Channels tab.
3. On the Channels tab, click the checkbox next to the channel(s) you want to assign to the selected Technician Group.

The assignment is applied immediately in the Administration Center. Any technician who is logged in to the Technician Console must log off and log in again before the change is applied.

How to Make a Channel Available for Use

Master Administrators can configure channel details and integrate a channel link or form code into your support site.

1. On the Organization Tree, select the channel you want to work with.
2. Select the Channels tab. The Channel Configuration page is displayed.
3. Enter a Channel name.
   This will be seen in both the Administration Center and Technician Console.
4. Enter a Description (optional). This is for your own reference.
5. Copy the appropriate channel link or code for your preferred channel type.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Channel link</td>
<td>This method allows you to build a simple link into your website/intranet. Customers click the link to establish a support session.</td>
</tr>
</tbody>
</table>
### How to Remove an Individual Technician from a Channel

Technicians and channels are assigned to Technician Groups. By default, each technician can work with sessions in any channel assigned to his Technician Group. To deny an individual technician access to a channel, follow this procedure.

1. On the Organization Tree, select the technician that you want to remove from a channel.
2. Select the Channels tab.
   The Channels tab shows a list of channels assigned to the selected technician.
3. On the Channels tab, clear the checkmark next to the Assigned to... box for each restricted Channel.
   The assignment is applied immediately in the Administration Center. Any technician who is logged in to the Technician Console must log off and log in again before the change is applied.

**Example: Deny an individual technician access to a channel**

This feature is useful if you use product- or platform-based channels and have technicians who may not be ready to support certain products or platforms.

Assume that you have assigned the Windows channel and Mac channel to Technician Group 1. All technicians in Technician Group 1 except for the technician named "Sample Technician" have the skills to handle Mac issues. In this case, you can remove "Sample Technician's" access to the Mac channel. "Sample Technician" will see sessions arriving to the Windows channel, but not the Mac channel. Once "Sample Technician" has the skills to handle Mac sessions, you can re-assign him to the Mac channel.

### How to Test a Channel

Test a channel to make sure it is working properly.

1. On the Organization Tree, select the channel you want to test.
2. Select the Channels tab.
3. Click Test channel (Standard) or Test channel (Instant Chat) as appropriate.
   Download and run the Applet when prompted.
4. Select the Sessions tab.
If the channel is working properly, the test session will appear in the appropriate queue.
Setting up the Applet

How to Set the Default Applet (Standard or Instant Chat)

Choose to run either the Rescue Applet or Instant Chat at the start of any session with a PC or Mac.

**Note:** Instant Chat runs by default for all sessions with PalmPre devices. No settings are required.

1. On the Organization Tree, select the channel or Technician Group you want to work with.
2. Select the Settings tab.
3. Go to the Customer Applet section.
4. Choose a Running Mode:
   - Choose Use Instant Chat to activate all sessions for the selected channel or group as Instant Chat sessions in Chat-only mode.
   - Choose Standard to activate all sessions for the selected channel or group as standard Rescue Applet sessions.
5. For the standard Rescue Applet, you can select the following options:
   - Select Display Customer Applet download page to show customers a standard web page that explains how to download the Applet.
   - Select Use ActiveX Customer Applet if you want to install an ActiveX component on the customer device that will download and automatically run the Applet. Use this feature to overcome restrictions related to direct downloading of .exe files and to reduce the number of steps required to establish a connection.
     **Restriction:** This method does not work for customers using Internet Explorer 11 and above, as these browsers do not allow .exe files to be run from an ActiveX control.
6. Save your changes.
   - Click Save Changes to apply the settings to the current channel or Technician Group
   - Click Save settings to all channels/groups to apply the same settings to all channels or Technician Groups in your organization

How to Set Windows System Service Behavior

By default, the Rescue Applet is started as a normal application. You can set Rescue to launch the Applet as a Windows System Service whenever the customer has Windows administrative rights.

1. On the Organization Tree, select the channel or Technician Group you want to work with.
2. Select the Settings tab.
3. Under **Customer Applet**, go to **Automatically start as Windows System Service** and select the appropriate options:
   - **Select if customer has administrative rights** to launch the Applet as a Windows System Service whenever the customer has Windows administrative rights.
   - **Select and UAC is enabled** to launch the Applet as a Windows System Service when the customer has administrative rights but is running an operating system with UAC enabled.

4. Save your changes.

   - **Click** Save Changes to apply the settings to the current channel or Technician Group
   - **Click** Save settings to all channels/groups to apply the same settings to all channels or Technician Groups in your organization

**Tip**: If the customer does not have administrative rights, or is running a Mac, then the technician can manually restart the Applet as described in the “How to Restart the Rescue Applet as Windows System Service or Mac Daemon” section of Technician Console User Guide.

---

**How to Set Mouse and Keyboard Data Entry Priority for Remote Control**

During a Remote Control session, the technician and customer may simultaneously use their mouse or keyboard. Select the user whose actions should be processed first.

1. On the Organization Tree, select the **Technician Group** you want to work with.
2. Select the **Settings** tab.
3. Under **Customer Applet**, go to **Priority over mouse and keyboard actions during remote control** and select the user whose actions should be processed first: **Technician** or **Customer**.
4. Save your changes.

---

**How to Show Estimated Length of Waiting to Customers**

Show your customers the amount of time they can expect to wait before a technician will be able to activate their session.

**For a Technician Group**

For private sessions, you can show the estimated waiting time. Rescue calculates the estimated waiting time based on the average pick-up time for the last ten sessions of a specific technician. The time is displayed in the Applet, Calling Card, or Instant Chat.

1. On the Organization Tree, select the **Technician Group** you want to work with.
2. Select the **Settings** tab.
3. Under **Customer Applet**, select **Display estimated waiting time**.
4. Save your changes.

   - **Click** Save Changes to apply the settings to the current channel or Technician Group
   - **Click** Save settings to all channels/groups to apply the same settings to all channels or Technician Groups in your organization
For a Channel

For channel sessions, you can choose to show customers either the estimated waiting time or their position in the queue of waiting customers. For estimated waiting time, Rescue calculates the average pick-up time of the last ten sessions of a channel. The time or position in queue is displayed in the Applet, Calling Card, or Instant Chat.

1. On the Organization Tree, select the channel you want to work with.
2. Select the Settings tab.
3. Choose what you want Rescue to show to waiting customers.
   - For Rescue to show the estimated waiting time, under Customer Applet > Message to waiting customers:, select Estimated waiting time.
   - For Rescue to show the customer’s position in the queue, under Customer Applet > Message to waiting customers:, select Queue position.
4. Save your changes.
   - Click Save Changes to apply the settings to the current channel or Technician Group
   - Click Save settings to all channels/groups to apply the same settings to all channels or Technician Groups in your organization

How to Customize Applet Appearance

An Administrator can customize the appearance of the Applet by inserting a custom logo and icon.

1. On the Organization Tree, select the channel or Technician Group you want to work with.
2. Select the Settings tab.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application name</td>
<td>Enter text to be displayed at the top of the Customer Applet, Mobile Applet, and Instant Chat.</td>
</tr>
<tr>
<td>Logo</td>
<td>Upload the logo for the selected channel or Technician Group to use. The logo will be shown in the top-right corner of the standard Applet, Mobile Applet, and Instant Chat. Download the template to see a sample that conforms to all format requirements.</td>
</tr>
<tr>
<td>Icon</td>
<td>Upload the icon you want to use. The icon will be shown in the top-left corner of the Customer Applet and Instant Chat. Download the template to see a sample that conforms to all format requirements.</td>
</tr>
</tbody>
</table>

Note: The name of your organization will appear on the Applet as entered in the Organization field of the My Account > Modify Contact Information.
How to Set up Custom Terms and Conditions

Show customers a customized Terms and Conditions after they have downloaded the Applet, but before the technician can begin to provide service (while the session is in Connecting status).

1. On the Organization Tree, select the channel or Technician Group you want to work with.
2. Select the Settings tab.
3. Under Customer Applet, go to Terms and Conditions and select from the following options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use Terms and Conditions</td>
<td>Select <em>Use Terms and Conditions</em> to show customers a customized Terms and Conditions after they have downloaded the Applet or Mobile Applet, but before the technician can begin to provide service (while the session is in Connecting status).</td>
</tr>
<tr>
<td></td>
<td><strong>Tip:</strong> To give customers enough time to read the Terms and Conditions, increase the time allowed before connecting sessions will time out (on the Settings tab under Time-outs).</td>
</tr>
<tr>
<td>Terms and Conditions</td>
<td>Type or insert your Terms and Conditions text in the Terms and Conditions box that customers using computers or mobile devices will see. Plain text only. No formatting. No character limit.</td>
</tr>
<tr>
<td>Force scrolling to bottom</td>
<td>Select <em>Force scrolling to bottom</em> to force customers to scroll through the entire Terms and Conditions before the Accept button on the Applet or Mobile Applet is activated.</td>
</tr>
</tbody>
</table>

4. Save your changes.
   - Click **Save Changes** to apply the settings to the current channel or Technician Group
   - Click **Save settings to all channels/groups** to apply the same settings to all channels or Technician Groups in your organization

**How does it work?** A session remains in Connecting status while the customer is reading the Terms and Conditions. Once the customer accepts the Terms and Conditions, the Applet chat window will appear and the connection to the technician will be made. The session appears as Waiting in the technician's queue. If the customer declines the Terms and Conditions, the Applet closes and is deleted immediately.

How to Disable the Pause/Break Key

Disable the Pause/Break key as a hotkey that customers press to revoke all permissions and end the current action, even when the Rescue Applet is not in focus.

1. On the Organization Tree, select the channel or Technician Group you want to work with.
2. Select the Settings tab.
4. Save your changes.
• Click **Save Changes** to apply the settings to the current channel or Technician Group
• Click **Save settings to all channels/groups** to apply the same settings to all channels or Technician Groups in your organization

The Pause/Break key is disabled as a Rescue hotkey. Customers will be forced to click the red X on the Applet toolbar to revoke permissions and end the current action.

---

**Sample use of Pause/Break key**

The technician starts to control the customer's desktop. The customer realizes that confidential information is exposed on his desktop. The customer presses the Pause/Break key to immediately end remote control even though the Rescue Applet is not in focus on his desktop. Remote control ends; the session continues.

---

**How to Prompt the Customer for Permissions at Session Start**

Force the Rescue Applet to display a permission dialog before any other session activity occurs. Otherwise, customers are prompted when the technician first attempts a remote action, such as when launching remote control or requesting system information.

1. On the Organization Tree, select the **channel** or **Technician Group** you want to work with.
2. Select the **Settings** tab.
3. Under **Customer Applet**, select **Prompt customer for permissions > One time when session starts**.
4. Save your changes.
   - Click **Save Changes** to apply the settings to the current channel or Technician Group
   - Click **Save settings to all channels/groups** to apply the same settings to all channels or Technician Groups in your organization

Once downloaded, the Applet will immediately display a dialog prompting the customer to grant overall permission that remains valid for the life of the session.

**Important**: If the customer denies permission upon startup, he will be prompted again for permission when the technician next attempts a remote action. If the customer accepts the first request, no further requests are made.
Setting up Rescue+Mobile

How to Purchase the Rescue+Mobile Add-on

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

How to Enable Technicians to Support Mobile devices

You must activate the Rescue+Mobile add-on for each technician for whom you have purchased a subscription.

1. Log in to your Rescue account and open the Administration Center.
2. On the Organization Tree, select the technician for whom you want to activate the mobile add-on.
3. Select the Organization tab.
4. Under Licenses, select Mobile.
   Upon next login, the user will be able to support smartphones.

For further control over the exact functionality available to technicians, set any of the numerous mobile-related permissions on the Organization tab or Settings tab for a Technician Group.

See also:
• How to Create a Technician Group and Assign Permissions on page 18
• Setting up Click2Fix on page 39
• How to Set Mobile Device Configuration Permissions on page 42

Setting up Click2Fix

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

• To allow members of a technician group to see the Click2Fix tab, make sure the following permission is enabled in the Administration Center at the group level on the Organization tab:
  • Click2Fix for mobile (enabled by default)

• To allow technicians to use all Click2Fix widgets, select these additional options:
  • Launch remote control
  • Launch desktop viewing
  • Upload lists of applications to check for upon session start (App Checklist)
  • Upload a file containing firmware requirements and update URLs (Firmware Data)
  • Create and assign packages of access point settings (APN) that technicians can push to customers
• Upload and assign lists of Web Shortcuts that technicians can push to customers

Setting up Rescue to Check for Unwanted or Missing Apps (App Checklist)
Upload a list of applications that Rescue will look for upon connection to an Android or BlackBerry device.

1. Select the Global Settings tab.
2. Under Mobile device settings > App Checker List Upload, click Browse and select the file containing the list of applications you would like technicians to be able to check for.

   **Important:** Download the template XML file to ensure that you follow the proper format.

3. Click Upload.
   The selected file is uploaded.
4. Click Save Changes.
   The data is made available on Click2Fix.

How does this work for the technician? In the Technician Console, the Click2Fix alert bar will notify the technician when an unwanted or missing app is detected.

Setting up Rescue to Check for Firmware Issues
Upload a file that Rescue uses to identify when a device’s firmware is not current. The file contains OS properties and can include a link to current firmware.

1. Select the Global Settings tab.
2. Under Mobile device settings > Firmware Data Upload, click Browse and select the file containing firmware requirements and URLs directing customers to current firmware versions.

   **Important:** Download the template XML file to ensure that you follow the proper format.

3. Click Upload.
   The selected file is uploaded.
4. Click Save Changes.
   The data is made available on Click2Fix.

How does this work for the technician? In the Technician Console, the Click2Fix alert bar will notify the technician when a difference is detected between the firmware on the customer’s device and properties defined in the uploaded file.

Setting up Access Point Presets
Upload and assign packages of APN settings that technicians can push to the customer’s device.

1. Upload APN packages. Here’s how:
   a) Select the Global Settings tab.
   b) Under Mobile device settings > Access Point Presets, click New.
   c) Enter values for mandatory fields and any other optional settings:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Point Name (APN)</td>
<td>The short name of the carrier’s network. (required)</td>
</tr>
</tbody>
</table>
### Option Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preset name</td>
<td>The name as it will be seen by the technician in the Technician Console. (required)</td>
</tr>
<tr>
<td>Proxy Server</td>
<td>The IP address of the carrier’s proxy server that the customer’s device connects to.</td>
</tr>
<tr>
<td>Proxy Server Port</td>
<td>The port that the customer’s device uses to communicate with the proxy server.</td>
</tr>
<tr>
<td>Username</td>
<td>The username to access the carrier’s proxy server.</td>
</tr>
<tr>
<td>Password</td>
<td>The password to access the carrier’s proxy server.</td>
</tr>
<tr>
<td>Server</td>
<td>The IP address of the carrier’s WAP server.</td>
</tr>
<tr>
<td>MMSC</td>
<td>The URL of the carrier’s MMS (Multimedia Messaging Service) server.</td>
</tr>
<tr>
<td>MMS Proxy</td>
<td>The IP address and port of the carrier’s MMS server.</td>
</tr>
<tr>
<td>MCC</td>
<td>Mobile Country Code (required)</td>
</tr>
<tr>
<td>MNC</td>
<td>Mobile Network Code (required)</td>
</tr>
<tr>
<td>Type</td>
<td>The type of the carrier’s network. Generally internet, mms, or default.</td>
</tr>
</tbody>
</table>

- **Important:** Use `http://` or `https://` format.

### How does this work for the technician?
In the Technician Console, technicians use the Click2Fix **Mobile Network > Network setup** widget to push settings to customers.

### Setting up Web Shortcuts

Upload a list of Web Shortcuts and assign them to technician groups. Technicians can push shortcuts to a customer’s home screen from the Click2Fix tab, thereby giving customers access to frequently used sites.

1. **Upload the Web Shortcuts that you want technicians to be able to push.** Here's how:
   - Select the **Global Settings** tab.
   - Under **Mobile device settings > Web Shortcuts**, click **New**.
   - In the **Icon Label** field, name the icon. This name is seen by technicians before push, and by customers after push.
   - Enter the **URL** that you want technicians to be able to send.

   **Important:** Use `http://` or `https://` format.

   - **Important:** Use `http://` or `https://` format.

   - **Important:** Use `http://` or `https://` format.

- **Important:** Use `http://` or `https://` format.

   e) **Upload the Icon** that you want technicians to be able to send. This icon is seen by technicians before push, and by customers after push.
**Important:** Icon requirements:
- .png format
- Same width and height
- Maximum 512 pixel width and height

**Important:** Do not forget to click **Upload**.

f) Click **Apply** and **Save Changes**.

2. Once you have uploaded Web Shortcuts, you must make them available to technician groups. Here’s how:
   a) Select a technician group.
   b) Select the **Settings** tab.
   c) Under **Web Shortcut Availability**, select shortcuts from the right panel and click **Add** to make them available to the group.
   d) Save your changes.

**How does this work for the technician?** In the Technician Console, technicians use the **Click2Fix Web Shortcuts** widget to push Web Shortcuts to customers.

---

**How to Set Mobile Device Configuration Permissions**

Set the device configurations that technicians can manage during sessions with a mobile device.

These settings only apply to agents with a Rescue+Mobile license who are members of a Technician Group with permission to **Configure mobile device settings**.

1. On the Organization Tree, select the **Technician Group** you want to work with.
2. Select the **Settings** tab.
3. Under **Mobile Device Configuration**, select the features that technicians will be allowed to use while working with the Device Configuration tab in the Technician Console. These settings do not apply to the Click2Fix tab.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email (IMAP/POP)</td>
<td>Allow technicians to change email settings on an iOS device.</td>
</tr>
<tr>
<td>Exchange ActiveSync</td>
<td>Allow technicians to change Exchange ActiveSync settings on an iOS device.</td>
</tr>
<tr>
<td>Access Point (APN)</td>
<td>Allow technicians to change APN settings on an Android or iOS device.</td>
</tr>
<tr>
<td>Passcode</td>
<td>Allow technicians to change Passcode settings on an iOS device.</td>
</tr>
<tr>
<td>Restrictions</td>
<td>Allow technicians to change Restrictions on an iOS device.</td>
</tr>
<tr>
<td>Web Clips</td>
<td>Allow technicians to push Web Clips to an iOS device.</td>
</tr>
<tr>
<td>Wi-Fi</td>
<td>Allow technicians to change Wi-Fi settings on an Android or iOS device.</td>
</tr>
</tbody>
</table>
4. Save your changes.

How to Customize the Session Invitation SMS

Customize the SMS message sent to mobile devices when the technician invites a customer to a Rescue session.

1. On the Organization Tree, select the **Technician Group** you want to work with.
2. Select the **Settings** tab.
3. Under **Session invitation SMS customization**, enter customized values:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Text above URL</td>
<td>The text shown above the applet download URL.</td>
</tr>
<tr>
<td><strong>URL</strong></td>
<td>The URL that the recipient clicks to download the applet.</td>
</tr>
</tbody>
</table>

**Note:** This field is not editable.

| Text below URL    | The text shown below the applet download URL. It must contain the parameter for the applet identification number: $PINCODE$
|-------------------|-----------------------------------------------------------------------------|

4. Save your changes.

How to Customize Mobile Applet Appearance

Administrators can change the logo displayed to customers who are using a BlackBerry device.

1. On the Organization Tree, select the **channel** or **Technician Group** you want to work with.
2. Select the **Settings** tab.
3. Under **Customer Applet**, upload the logo to be used by the selected channel or Technician Group.
   The file must be a 78x32 bitmap (bmp) of no more than 8192 bytes.

**Tip:** Download the logo template to see a sample logo that conforms to all format requirements.

How to Set Mobile Applet Options (Display Custom Terms of Service)

Use these settings to control when you want your customers to see the Custom Terms of Service.

1. On the Organization Tree, select the Technician Group you want to work with.
2. Select the **Settings** tab.
3. Under **Mobile Applet**, set when you want your customers to see the Custom Terms of Service:
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display Custom Terms of Service</td>
<td>Use this feature to push your organization’s Terms of Service to your customers. Enter the URL where your Custom Terms of Service is stored. Select <strong>first time only</strong> if you want your customers to see the Custom Terms of Service the first time they use your service, but not on subsequent occasions. Select <strong>every time</strong> if you want your customers to see the Custom Terms of Service each time they use your service.</td>
</tr>
</tbody>
</table>

4. Save your changes.
   - Click **Save changes** to apply settings to the current Technician Group.
   - Click **Save settings to all groups** to apply the same settings to all Technician Groups in your organization.

**Google Play Link for Android Sessions**

When connecting to an Android device, technicians can send customers a Google Play link in the session invitation SMS.

For example, a company called "ACME Support" directs all of their customers to download the "Rescue Mobile for ACME Support" application. They do this through the SMS link rather than verbally directing the customer to Google Play to search for the app.

**Fastpath:** Administrators set the custom link at **Global Settings > Custom Google Play URL**.

**How does it work?** When the customer opens the session invitation SMS, they do not see an actual Google Play link, but rather a standard Rescue session link `http://rescuemobile.com/xxxxxx` where `xxxxxx` is the session PIN code. The Rescue service matches the PIN code to the technician and redirects the customer to the Google Play link defined in the Administration Center.
Setting up Rescue Lens

Allowing Technicians to Use Rescue Lens

Allow group members to start Rescue Lens sessions. With Rescue Lens, customers can use their mobile device to stream live video to a technician.

1. Log in to the LogMeIn Rescue Administration Center.
2. On the Organization Tree, select the Technician Group you want to work with.
3. Select the Organization tab.
5. Click Save Changes.

Enabling Rescue Lens Audio

You can set Lens sessions to launch with an active VoIP connection between technician and customer that remains open throughout the session but can be muted by either party.

1. Log in to the LogMeIn Rescue Administration Center.
2. On the Organization Tree, select the Technician Group you want to work with.
3. Select the Settings tab.
4. Under Rescue Lens, select Enable audio:
   For the selected Technician Group, all Lens sessions are launched with an active VoIP connection between technician and customer.
5. Save your changes.
   • Click Save changes to apply settings to the current Technician Group
   • Click Save changes to subgroups to apply the settings to the current Technician Group and all of its subgroups
   • Click Save settings to all groups to apply the same settings to all Technician Groups in your organization
Controlling How Sessions are Started and Managed

How to Set Connection Methods Available to Technicians

Choose which connection methods to make available to technicians on the Technician Console Create New Session dialog box.

1. On the Organization Tree, select the Technician Group you want to work with.
2. Select the Settings tab.
3. Under Connection Method, select the connection methods you want to allow.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PIN Code</td>
<td>Allow technicians to use the PIN Code connection method. Enter the URL of the site that customers use to enter the session PIN. The value will be shown to technicians on the PIN Code tab of the Create New Session dialog box.</td>
</tr>
<tr>
<td>Allow email via default client</td>
<td>Allow technicians to use the email connection method and to send the email via their default email client.</td>
</tr>
<tr>
<td>Allow email via Rescue servers</td>
<td>Allow technicians to use the email connection method and to send the email via LogMeIn Rescue servers.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Reply-to address (optional)</td>
<td>Specify the email address to which replies to a session connection email are sent. To use the email address of the technician who sent the session connection email, leave this field blank.</td>
</tr>
<tr>
<td><strong>Restriction:</strong></td>
<td>Applies only to emails sent via Rescue servers!</td>
</tr>
<tr>
<td>Connection email subject</td>
<td>The default subject line of all session connection emails. A technician can change the subject line in his email client.</td>
</tr>
<tr>
<td>Connection email text</td>
<td>The default introductory text of all session connection emails. A technician can change the text in his email client.</td>
</tr>
<tr>
<td>Link</td>
<td>Allow technicians to use the Link connection method.</td>
</tr>
<tr>
<td>SMS</td>
<td>Allows technicians to use the SMS connection method to start private sessions:</td>
</tr>
<tr>
<td></td>
<td>• For Rescue Lens sessions, available to all technicians with Rescue Lens permission</td>
</tr>
<tr>
<td></td>
<td>• For Rescue+Mobile sessions, available to technicians with a Rescue+Mobile license</td>
</tr>
</tbody>
</table>

4. Save your changes.

### How to Set Private Sessions to Start Automatically

Administrators can set all PIN Code, Link, and SMS sessions to go directly from Connecting status to Active. Technicians will be unable to change the **Auto-start Incoming Private Sessions** option in the Technician Console.

1. On the Organization Tree, select the **Technician Group** you want to work with.
2. Select the **Settings** tab.
3. Under **Technician Console**, select **Auto-start incoming private sessions**.
4. Save your changes.
How to Set Channel Sessions to Transfer Automatically

Reduce customer waiting time for channel-based sessions by automatically transferring waiting sessions to another channel. Set the amount of time to wait before initiating a transfer to the selected receiving channel. The actual transfer may take up to an additional 90 seconds to complete.

1. On the Organization Tree, select the channel you want to work with.
2. Select the Settings tab.
3. Under Session management, go to Auto-transfer waiting sessions.
4. Set the amount of time (in minutes) to wait before initiating a transfer to the selected receiving channel.
5. Click Save changes.

Note: You cannot save this setting to all channels.

From the technician perspective, the status of any automatically transferred session will be shown as Outgoing in the original channel queue and Incoming in the receiving queue.

How to Set Channel Sessions to Start Automatically

Reduce customer waiting time for channel-based sessions by automatically activating sessions at the least busy technician (defined as the technician with the fewest active sessions or the longest idle time upon session arrival).

1. On the Organization Tree, select the channel you want to work with.
2. Select the Settings tab.
3. Under Session management, select the Auto-start waiting sessions box.
   Sessions will only be started automatically when the technician is handling a number of sessions under the threshold defined in the ...less than X active sessions drop-down list.

Tip: Select a value of 10 to start sessions automatically regardless of the number of active sessions a technician is handling.

4. Click Save changes.

Note: You cannot save this setting to all channels.

How to Defer Auto-start for Channel Sessions

Exempt group members from being auto-assigned waiting sessions for a configurable period of time after logging in to the Technician Console.

Remember: This setting only applies when Auto-start waiting sessions is enabled.
1. On the Organization Tree, select the **Technician Group** you want to work with.
2. Select the **Settings** tab.
3. Under **Technician Console > Defer auto-start after login by** set the length of time for which you want the selected group members to be exempted from being assigned waiting channel sessions.
   
   **Note:** A value of 0 means no deferment.

4. Save your changes.

### How to Prevent Technicians from Transferring Sessions to Unmanned Channels

An Administrator can ensure technicians can only transfer sessions to a channel with available technicians. This feature helps you avoid long customer waiting times due to transfer to an unmanned channel.

1. On the Organization Tree, select the **channel** you want to work with.
2. Select the **Settings** tab.
3. Under **Session management**, select the **Incoming transfer restriction** box.
4. Save your changes.

   - Click **Save Changes** to apply the setting to the current channel.
   - Click **Save settings to all channels** to apply the setting to all channels in your organization.

### How to Exempt a Technician from Channel Session Auto-start

An Administrator can override the auto-start waiting session option for individual technicians.

The use of this feature is recommended for supervisors who should be exempt from "round-robin" session routing. For example, let's say you have an Administrator who logs in as a technician in order to monitor technicians by using the Technician Console monitoring feature. You do not want the Administrator to be interrupted by new sessions, so you select the **Never auto-start waiting channel sessions** option.

1. On the Organization Tree, select the technician who should be exempt from channel session routing.
2. Select the **Organization** tab.
3. Select **Never auto-start waiting channel sessions**.
4. Click **Save changes**.

### How to Schedule Working Hours and "No Technician Available" Behavior for a Channel

Apply working hours to a channel and set the default behavior in response to requests that arrive when no technician is available.

1. On the Organization Tree, select the **channel** you want to work with.
2. Select the Settings tab.
3. Under No technician available and Scheduling, choose the Start Time and End Time for your working day.
4. Choose the Time Zone to be associated with the selected working hours.
5. Clear the box next to each day that should not be a working day.
6. Set up the default behavior in response to sessions that arrive during working hours when no technician is available and during non-working hours.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Keep sessions alive</td>
<td>Choose Keep sessions alive if you want all sessions to remain in a queue even if no technicians are online and available.</td>
</tr>
<tr>
<td>Notify technicians of pending sessions via email</td>
<td>Select Notify technicians of pending sessions via email if you want to send an email to the relevant technicians when an incoming support request is received, but no technician is logged in. An email message from <a href="mailto:alerts@LogMeInRescue.com">alerts@LogMeInRescue.com</a> will be sent to all the technicians who could handle this support request.</td>
</tr>
<tr>
<td>Abort sessions and show this webpage to the customer</td>
<td>Choose Abort sessions and show this webpage to the customer if you want to display a specific web page to the customer when no technician is available. Enter the URL of the web page to be displayed in the corresponding box.</td>
</tr>
</tbody>
</table>

7. Save your changes.
   - Click Save Changes to activate the form for the current Channel.
   - Click Save settings to all channels to apply the same settings to all Channels in your organization.

---

How to Set No Technician Available Behavior for Private Sessions

Set the default behavior in response to requests that arrive when no technician is available.

1. On the Organization Tree, select the Technician Group you want to work with.
2. Select the Settings tab.
3. Under No technician available, select from the following options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Keep sessions alive</td>
<td>Choose Keep sessions alive if you want all sessions to remain in a queue even if no technicians are online and available.</td>
</tr>
<tr>
<td>Notify technicians of pending sessions via email</td>
<td>Select Notify technicians of pending sessions via email if you want to send an email to the relevant technicians when an incoming support request is received, but no technician is logged in. An email message from <a href="mailto:alerts@LogMeInRescue.com">alerts@LogMeInRescue.com</a> will be sent to all the technicians who could handle this support request.</td>
</tr>
<tr>
<td>Abort sessions and show this webpage to the customer</td>
<td>Choose Abort sessions and show this webpage to the customer if you want to display a specific web page to the customer when no technician is available. Enter the URL of the web page to be displayed in the corresponding box.</td>
</tr>
</tbody>
</table>
How to Set Time-outs and Warnings

1. On the Organization Tree, select the channel or Technician Group you want to work with.
2. Select the Settings tab.
3. Under Time-outs, select from the following options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Private code validity period</td>
<td>The length of time a PIN Code or Link remains valid. If a customer attempts to start a session after this period has expired, he receives a message saying that the PIN Code or Link has expired.</td>
</tr>
<tr>
<td>Connecting sessions will time out</td>
<td>The length of time a connecting session remains valid. The session will be removed from the Technician Console queue after the specified time is exceeded.</td>
</tr>
<tr>
<td>Waiting sessions will time out</td>
<td>The number of minutes after which a waiting session (a session in a queue that has not yet been picked up) is dropped from a technician's queue. The session is displayed in red before being removed. The period can be between 1 and 999 minutes. A value of 0 means sessions will never time out.</td>
</tr>
<tr>
<td>Active session idle time-out</td>
<td>The number of minutes after which an Active session will be ended if no action is taken by the technician or customer. 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. The period can be any length between 1 and 999 minutes. A value of 0 means an active session will never time out. On Hold sessions will never time out.</td>
</tr>
<tr>
<td>Time-out alarms</td>
<td>Use predefined colors to highlight Time-out and Waiting session alarms. The connection and/or wait times can be specified in seconds, including multiple alarms to escalate waiting sessions in the Technician Console.</td>
</tr>
</tbody>
</table>

4. Save your changes.

- Click Save Changes to apply the settings to the current channel or Technician Group
- Click Save settings to all channels/groups to apply the same settings to all channels or Technician Groups in your organization
Managing Sessions: Start, Transfer, Close, Hold

Administrators use the Sessions tab to manage LogMeIn Rescue support sessions. A session can be started, transferred, closed, or put on hold directly from the Sessions tab.

How to View Session Information

Administrators use the Sessions tab to manage LogMeIn Rescue support sessions. A session can be started, transferred, closed, or put on hold directly from the Sessions tab.

1. On the Organization Tree, select the Technician Group, channel, or technician for which you want to view session information.
2. Select the Session tab.

   Sessions are displayed for the selected Technician Group, channel or technician. You can see a simple snapshot of active and waiting sessions, including the name of the technician(s) handling sessions, session start times, and whether the sessions are Channel or Private.

   Tip: To view session information for another Technician Group, Channel, or Technician simply select a new item on the Organization Tree and the Session tab will be updated.

How to Start a Session from the Administration Center

Sessions can be manually started directly from the Administration Center Sessions tab.

1. In the Administration Center, select the appropriate session from the list on the Session tab and click Start.
   The Session Start dialog box is displayed.
2. Select the technician for which you want to start the session.
   You are prompted to confirm your selection.
3. Click OK to start the session.
   The session appears in the session list of the technician for whom it was started.

   Tip: You may need to click Refresh to see the change.

How to Transfer Sessions

Sessions can be manually transferred directly from the Administration Center Sessions tab.

Remember: You can only transfer mobile sessions to a technician with a valid Rescue + Mobile subscription.

1. Select the appropriate session from the session list on the Session tab and click Transfer.
The Transfer dialog box is displayed.

2. Type a description in the **Comment** box (for example, a reason for the transfer or a brief summary of the case).

3. Select the technician, Technician Group or channel to which you want to transfer the session. You are prompted to confirm your selection.

4. Click **OK** to execute the transfer.

   The session appears in the session list of the Technician, Technician Group, or Channel to which it was transferred.

   **Tip:** You may need to click **Refresh** to see the change.

The original technician will see the session as Transferred in their Technician Console queue. Any comment that the administrator added during the transfer will also be visible in the **Transferred by** box.
Monitoring a Technician's Desktop

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.

Remember: Technician Monitoring is initiated in the Technician Console, not the Administration Center.

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.

How to Set up Technician Monitoring Options

Set up authentication requirements for administrators attempting to monitor a technician's desktop. Control how technicians will be notified when they are being monitored.

1. Select the Global Settings tab.
2. Under Technician monitoring, select from the following options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Credentials required for authentication</td>
<td>Select this option to allow monitoring only by users with an administrative account on the monitored technician's computer. Select any user to allow monitoring by users with any user account type on the monitored technician's computer.</td>
</tr>
<tr>
<td>Notify technician when monitoring desktop</td>
<td>Select this option if you want monitored technicians to receive notification when they are being monitored. When notification is switched off, technicians will be shown a message listing users who are permitted to monitor their desktop without providing notification.</td>
</tr>
</tbody>
</table>

3. Click Save Changes.
   The settings are applied to all administrators in your Rescue organization.
Monitoring Performance Data: The Command Center

The Command Center is a LogMeIn Rescue component that gives you a powerful tool for monitoring key performance indicators in your support organization. Use it to generate and analyze performance data to determine usage patterns, optimize resource allocation and identify problem areas in your organization.

Requirements:
- A LogMeIn Rescue account
- A Rescue organization already built in the Administration Center
- A supported browser
  - Internet Explorer 8 or higher
  - The latest version Firefox, Chrome, Safari

To have a quick look at how the Command Center works, see Command Center – At a Glance on page 7.

How to Monitor Performance Data for a Channel

1. In the Command Center, open the drop-down menu and select the unit you want to monitor.

   **Remember:** Master Account Holders and Master Administrators can access data from their whole Organization Tree. Administrators can only access data concerning the Technician Group they are assigned to.

   Data for the selected Channel is displayed in two sections: **Overview** and **Table**.

   **Tip:** Don't see the data you expected? You can set the starting time of the data collection period. See How to Set Monitoring Data Collection Time Period on page 64.

   **Caution:** The browser Back button quits the Command Center. To navigate to previous levels in the hierarchy, use the breadcrumb.

2. Review data in the **Overview** section.

   This is aggregated data about the selected Channel as a collective entity including all of its Technician Groups.
   - Status (Technicians)
   - Capacity (Total, Available, Used). Both private and channel sessions are considered.
   - Missed session count
   - Closed session count
   - Running session count
   - Waiting session count
   - Incoming session count
   - Outgoing session count
   - Wait time average
• Wait time max
• Handling time average
• Handling time max

Tip: For definitions, see Command Center Terms and Definitions on page 64.

3. Review data in the Table section.
   • Under the Technicians tab, data pertain to technicians belonging to the selected Channel.
     • Status
     • Name
     • Technician Group
     • Wait time average
     • Wait time maximum
     • Handling time average
     • Handling time maximum
     • Available capacity
     • Total capacity
     • Closed session count
     • Active session count from the selected Channel
     • Active session count from other Channel(s)
     • Private session count
   • Under the Sessions tab, you can view data for individual channel sessions handled by technicians belonging to the selected channel.
     • Technician
     • Wait time
     • First chat time
     • Handling time
     • Wrap time
     • Session status
     • Custom column (as defined under Settings)
     • Channel
     • Session ID
     • Chat monitor

Tip: For definitions, see Command Center Terms and Definitions on page 64.

How to Monitor Performance Data for a Technician Group

1. In the Command Center, open the drop-down menu and select the unit you want to monitor.

Remember: Master Account Holders and Master Administrators can access data from their whole Organization Tree. Administrators can only access data concerning the Technician Group they are assigned to.
Data for the selected Technician Group is displayed in two sections: **Overview** and **Table**.

**Tip:** Don't see the data you expected? You can set the starting time of the data collection period. See *How to Set Monitoring Data Collection Time Period* on page 64.

**Caution:** The browser **Back** button quits the Command Center. To navigate to previous levels in the hierarchy, use the breadcrumb.

2. Review data in the **Overview** section.
   
   This is aggregated data about the selected Technician Group as a collective entity of all the technicians that belong to it.

   **Important:** Sub-groups of the selected Technician Group are excluded from calculation.

   - Status (Technicians)
   - Capacity (Total, Available, Used)
   - Missed session count
   - Closed session count
   - Running session count
   - Waiting session count
   - Incoming session count
   - Outgoing session count
   - Wait time average
   - Wait time max
   - Handling time average
   - Handling time max

   **Tip:** For definitions, see *Command Center Terms and Definitions* on page 64.

3. Review data in the **Table** section.

   - Under the **Technicians** tab, data pertain to technicians belonging to the selected Technician Group.
     - Status
     - Name
     - Wait time average
     - Wait time maximum
     - Handling time average
     - Handling time maximum
     - Available capacity
     - Total capacity
     - Closed session count
     - Channel session count
     - Private session count
   
   - Under the **Sessions** tab, you can view data for individual channel sessions handled by technicians belonging to the selected channel.
     - Technician
     - Wait time
How to Monitor Performance Data for a Technician

Technicians cannot be accessed directly, but rather through a Technician Group or Channel to which they belong.

1. In the Command Center, use the drop-down menu to choose the unit that includes the technician who you want to monitor.

2. In the Table section under the Technicians tab, find the technician's row and click it. Monitoring data for the selected technician is displayed in two sections: Overview and Table.

   Tip: Don't see the data you expected? You can set the starting time of the data collection period. See How to Set Monitoring Data Collection Time Period on page 64.

3. Review data in the Overview section.
   Data pertain to the selected technician.

   Tip: For definitions, see Command Center Terms and Definitions on page 64.

4. Review data in the Table section.
   Under the Sessions tab, you can view detailed data about each channel and private session handled by the selected technician.

   • Technician
   • Wait time
   • First chat time
   • Handling time
   • Wrap time
   • Session status
   • Custom column (as defined under Settings)
   • Channel
   • Transferring from/to
   • Session ID
   • Chat monitor

   Tip: For definitions, see Command Center Terms and Definitions on page 64.
How to Monitor Performance Data Based on Custom Attributes (Labels)

What is a Label?

A label collects all Technician Groups and/or Channels that have been tagged with it, so that organization units can be monitored as an arbitrary group. This helps administrators to monitor their organization along any lines relevant to their operation. By applying labels, Command Center monitoring is no longer restricted to a single organizational unit.

![Figure 1: Labels in the Command Center](image)

Organization units can be assigned more than one label. For example, if a support organization has five Technician Groups (TG1, TG2, TG3, TG4 and TG5), and these work in two geographical areas, an Administrator can create labels such as "Central Europe" (TG1, TG2 and TG3 belong here in this example) and "USA East Coast" (TG4 and TG5 belong here in this example). Also, in this example, this organization supports two departments; therefore, the Administrator will also create two corresponding labels "Finance" (for TG1, TG3 and TG4 in this example) and "Legal" (for TG2 and TG5 in this example). This means that, for example, Technician Group 2 has both label "Central Europe" and label "Legal".

<table>
<thead>
<tr>
<th>Technician Group</th>
<th>Labels</th>
</tr>
</thead>
<tbody>
<tr>
<td>TG1</td>
<td>Central Europe, Finance</td>
</tr>
<tr>
<td>TG2</td>
<td>Central Europe, Legal</td>
</tr>
<tr>
<td>TG3</td>
<td>Central Europe, Finance</td>
</tr>
<tr>
<td>TG4</td>
<td>USA East Coast, Finance</td>
</tr>
<tr>
<td>TG5</td>
<td>USA East Coast, Legal</td>
</tr>
</tbody>
</table>

How to Add Labels

This option is available to Master Administrators and Master Account Holders.

1. In the Administration Center, go to the Global Settings tab.
2. Under Labels, click Manage Labels.
   - The Add/Remove Labels page is displayed.
3. Click the gear icon.
   - The Add new labels option is displayed.
4. Under Add new labels, name the new label and click Add.
   - The new label is displayed.
Tip: Repeat this step for each label you want to add.

5. Click Done.

Remember: Don't forget to assign labels to Channels or Technician Groups. See How to Assign Labels on page 61.

How to Assign Labels

Master Administrators and Master Account Holders can assign labels to any Technician Group or Channel in their organization tree. Administrators can assign labels to the Technician Group that they are assigned to.

1. In the LogMeIn Rescue Administration Center on the Organization Tree, select the Technician Group or Channel to which you want to assign the label.
2. Select the Organization tab.
3. Under Assigned labels, select a label.
4. Click Add.
   The selected label is displayed next to Labels
5. Click Save Changes.

How to Monitor Performance Data According to a Label

Monitoring according to labels is only available if labels have been added and assigned.

1. In the Command Center, select a label from the Label List or from the drop-down menu.

   Data related to the selected label is displayed in two sections: Overview and Table.

   Remember: Master Account Holders and Master Administrators can access data from their whole Organization Tree. Administrators can only access data concerning the Technician Group they are assigned to.

   Tip: Don't see the data you expected? You can set the starting time of the data collection period. See How to Set Monitoring Data Collection Time Period on page 64.

   Caution: The browser Back button quits the Command Center. To navigate to previous levels in the hierarchy, use the breadcrumb.

2. Review data in the Overview section:
This is aggregated data about the selected Label as a collective entity of all the elements assigned to it.

- Status (Technicians)
- Capacity (Total, Available, Used)
- Missed session count
- Closed session count
- Running session count
- Waiting session count
- Incoming session count
- Outgoing session count
- Wait time average
- Wait time max
- Handling time average
- Handling time max

Tip: For definitions, see *Command Center Terms and Definitions* on page 64.

3. Review data under **Table**:
   Data is for all Technician Groups and all Channels assigned to the selected Label.
   - Under the **Channels** tab, data pertain to Channel(s) assigned to the selected Label.
   - Under the **Technician Groups** tab, data pertain to the Technician Group(s) assigned to the selected Label.
   - Under the **Sessions** tab, you can view data for individual sessions handled by technicians belonging to Technician Groups and Channels assigned to the selected Label.
     - Technician
     - Wait time
     - First chat time
     - Handling time
     - Wrap time
     - Session status
     - Custom column (as defined under Settings)
     - Channel
     - Session ID
     - Chat monitor

Tip: For definitions, see *Command Center Terms and Definitions* on page 64.

**How to Monitor Technician Chatlog**

Administrators can monitor chat sessions in the Rescue Command Center.

1. Under the **Sessions tab** in the **Table** section of the Command Center, select the session you want to monitor.
2. Click the **CHAT MONITOR** icon to see the full chatlog of the selected session.
The chat conversation is displayed in a new window. All information normally included in a chatlog is displayed, such as status changes and connection messages.

**Tip:** In case of active sessions, the Chat Monitor window displays the live chatlog in real time.

### How to Set Command Center Alert Thresholds

Command Center alerts give you visual notification if the performance of the selected unit is out of the specified range. Configure the values that trigger alerts.

There are two kinds of alerts: **Warning** (yellow) and **Alert** (red). When triggered, these alerts make the background of the corresponding Table panel cell yellow (for Warnings) or red (for Alerts).

**Important:**

Configuring alerts is optional. However, when you configure both an Alert value and a Warning value for a cell, the following applies:

- For Wait Time Max, Handling Time Max, and Handling Time Avg, the **Alert value** must be higher than the **Warning** value. This is because lower Wait and Handling time values are more desirable, and an Alert is stronger than a Warning.

1. In the Command Center, click the gear icon in the upper right corner. The **Settings** page is displayed.
2. Set alert levels for any of the following fields:
   - Wait Time Max
   - Handling Time Max
   - Handling Time Avg

### How to Restrict Administrators to Command Center Monitoring Function

A Master Administrator or a Master Account Holder can restrict an Administrator Group's role to Command Center monitoring only.

If this feature is activated for an Administrator Group, members will not be able to access the Administration Center.

**Tip:** This feature is recommended for Administrators whose role is exclusively to monitor Technician Groups to which they are assigned.
1. In the Administration Center on the Organization Tree, select the Administrator Group that should be restricted to Command Center monitoring only.
2. Select the Organization tab.
3. Select Access Command Center only.
4. Click Save Changes.

Customizing the Command Center

How to Set Monitoring Data Collection Time Period
Set the starting time from which Command Center should collect data.

1. In the Command Center, click the gear icon in the upper right corner. The Settings page is displayed.
2. Use the slider to set the time from which you want to start collecting data.
3. Click Apply to save your changes.

In this example, a monitoring agent's shift starts at 4pm, so he is only interested in data reported starting from 4pm and wants to ignore data before that time.

How to Set Value of Custom Column on Sessions Tab
When viewing detailed information about sessions, you can choose which Custom Field is reported as a column on the Session tab.

1. In the Command Center, click the gear icon in the upper right corner. The Settings page is displayed.
2. Under Custom column on Session tab, select a field. These are the Custom Fields set in the Administration Center under Global Settings > Custom fields.
3. Click Apply to save your changes.

The chosen field is shown as a column on the Sessions tab in the Table section of the Command Center.

Command Center Terms and Definitions
For information on general LogMeIn Rescue terms and definitions, see "Appendix - Session statuses in the Rescue Technician Console" in LogMeIn Rescue Technician Console User Guide.
<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Available capacity</strong></td>
<td>Total capacity minus active sessions of technicians belonging to the unit being monitored.</td>
</tr>
<tr>
<td><strong>Capacity</strong></td>
<td>The number of sessions a technician can handle. Configurable in Rescue Administration Center (value: 1-10).</td>
</tr>
<tr>
<td><strong>Total capacity</strong></td>
<td>Total capacity is the sum of the capacity of all the technicians who belong to the organizational unit that is being monitored. For example, for a Technician Group the sum of all the online technicians in the group is calculated. For a label, the calculation considers all Technician Groups assigned to the given label, plus all Technician Groups belonging to the Channels assigned to the label, excluding any technicians whose assignment to a given channel has been revoked.</td>
</tr>
<tr>
<td><strong>Used</strong></td>
<td>Total capacity minus Available capacity.</td>
</tr>
<tr>
<td><strong>Running</strong></td>
<td>The number of sessions of the given type (private or channel) that have been picked up and are in a status that allows a technician to work with them in the Technician Console.</td>
</tr>
<tr>
<td><strong>Waiting</strong></td>
<td>The number of sessions of the given type (private or channel) in waiting status in the Technician Console.</td>
</tr>
<tr>
<td><strong>Incoming</strong></td>
<td>The number of sessions of the given type (private or channel) being transferred to the unit being viewed.</td>
</tr>
<tr>
<td><strong>Outgoing</strong></td>
<td>The number of sessions of the given type (private or channel) being transferred from the unit being viewed.</td>
</tr>
<tr>
<td><strong>Missed</strong></td>
<td>Sessions that reached Waiting status, but did not become Active. This includes: • Sessions closed by customer before Pickup • Sessions that timed out after Waiting time</td>
</tr>
<tr>
<td><strong>Remember:</strong></td>
<td>Waiting session timeout is configurable in the Administration Center. For information, see &quot;How to Set Time-outs and Warnings&quot; in LogMeIn Rescue Administration Center User Guide.</td>
</tr>
<tr>
<td><strong>Closed</strong></td>
<td>Sessions that were picked up, and then closed.</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>Only those sessions are calculated that were closed after the starting time configured in Settings &gt; Reset time. (For details, see section How to Set Monitoring Data Collection Time Period on page 64).</td>
</tr>
<tr>
<td><strong>Wait time</strong></td>
<td>The length of time the session is in Waiting status. (Pickup time minus Start time)</td>
</tr>
<tr>
<td><strong>Wait time average</strong></td>
<td>Average of waiting time calculating sessions in Waiting state.</td>
</tr>
<tr>
<td><strong>Wait time max</strong></td>
<td>The longest waiting time calculating sessions in Waiting state.</td>
</tr>
<tr>
<td><strong>Handling time</strong></td>
<td>1. If the session has been picked up and closed: Close time minus Pickup time 2. If the session has been picked up but has not been closed: Current time minus Pickup time 3. If the session has neither been picked up nor closed: 0</td>
</tr>
</tbody>
</table>
Handling time average
Average of handling time for all the sessions.

Handling time max
The length of the session with the longest handling time.

Command Center Error Messages

The selected view is not available. Select an option below.
This error message is displayed in either of the following cases:
• An Administrator tries to monitor an organizational entity for which he has no authorization.
• An Administrator tries to monitor an organizational entity that no longer exists.

Note: The Command Center remembers the view last used by the Administrator. If his authorization for the given organizational entity has been revoked, or the organizational entity has been deleted since his last using/refreshing the Command Center, this error message is displayed.

Authorization has been denied for this request.
This error message is displayed in either of the following cases:
• An Administrator tries to refresh the Command Center, but he has already been logged out of his LogMeIn Rescue account.

Note: For example, an Administrator is working in the Rescue Command Center, and he is also logged in to the Rescue Administration Center at the same time. If he logs out from the Administration Center, or his Rescue account login expires, he will receive this error message in the Command Center.

• An Administrator tries to refresh the Command Center, but his right to access the Command Center has been revoked.
Managing 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.

Rescue Administrators use the Administration Center to assign unattended computers to groups or technicians, or to disable unattended access.

See the Technician Console User Guide for step-by-step instructions on how to enable unattended access.

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

Setting up Unattended Access on Multiple Computers (Access Wizard)

By using the Access Wizard, Rescue customers can conveniently mass-deploy the Unattended Access service to multiple devices. Once the installer is deployed, Rescue Administrators can manage the machines associated with each MSI they created.

Topics in this article:
- Creating the Installer on page 67
- Deploying the Installer on page 68
- Managing Unattended Access in the Admin Center on page 69

Creating the Installer

Master Account Holders and Administrators can create MSI installers with the Access Wizard.

1. Log in to your LogMeIn Rescue account, and go to My Account.
2. Click Launch Access Wizard.
   The Access Wizard page is displayed.
   
   Note: At any time during the process, you can return to the My Account page by clicking Discard & close in the bottom right corner. This, however, will discard all the parameters you have configured.

3. Configure the parameters for the installer.
**Name**  
The name you provide here will identify the installer and the computers associated with it in the following places.

- In the Admin Center: On the **Computers** tab, under section **Unattended MSI-s** (for detailed information, see *Managing Unattended Access in the Admin Center* on page 69).
- In the Technician Console: In the **Description** field of the **Unattended Accessible** tab in the **Computers** window.

**Note:** To see the list of Unattended Accessible Computers, click the **Computers** icon on the Session Toolbar.

**Description**  
You must add a description. This will appear in the Admin Center as the description of the computers on which the installer has been deployed.

**Daily time range**  
Select a time range if you want the unattended machines to be available only during set hours (for example, business hours, or off hours only). If no range is defined, the default (12 AM - 12 AM) value means the unattended machines will be available 24 hours a day.

**Unattended access expires in**  
You can set an expiration date (defined in days or weeks) for Unattended Access, or check **Never expires** for permanent access.

4. Click **Next Step**.  
Step 2/3 of the Wizard is displayed.

5. Select the technician(s) and/or Technician Group(s) you want to enable to access any machine on which this particular installer is deployed.

- To select individual users, use the **Technicians** tab.
- To select one or more entire Technician Group, use the **Technician Group** tab.

**Note:** When you select a Technician Group, members of that group show as checked when reviewing the **Technicians** tab.

6. Click **Next step**.  
The final screen of the Wizard displays a summary of the package that is being created.

**Note:** If you need to make any changes, you can return to a previous step by clicking **Previous step**.

7. To generate and download the MSI installer, click **Download installer**.  
Once the installer is generated, you are prompted to save the file on your computer.

8. To exit the Wizard, click **Finish & close**.

**Deploying the Installer**

The MSI file can be shared and deployed in a number of ways thus offering Rescue users flexibility in how their Unattended Access devices are initially set up. Below you can find some examples for sharing and deploying the installer file:

- Sending the MSI via email to a vendor in a remote location
- A field service agent storing the MSI on a pendrive to install on machines in the field
- Placing a download link to the MSI on a portal page for self-service customer installs
• Deploying the MSI via group policy to machines on an internal network

**Note:** This option assumes you are familiar with and use built-in Windows software distribution methods such as Microsoft Group Policy Management.

**Managing Unattended Access in the Admin Center**

This section describes the management of the MSI installers created by the Access Wizard. For information about general management of unattended computers, see *How to Assign or Delete Unattended Computers* on page 69.

1. In the Administration Center, select the **Technicians** root or a **Technician Group** on the Organization Tree.
2. Select the **Computers** tab.
   Under section **Unattended MSI-s** the list of installers generated for the selected organizational entity is displayed.
3. You can manage the MSI installer in the following ways.
   - **Download the installer again**
     Under **Regenerate installer**, click **x86** or **x64** depending on your OS.
   - **Make the installer expire**
     Under **Regenerate installer**, click the **Make package expire** icon.

The installer cannot be downloaded anymore, and unattended access is revoked from computers on which the package was installed.

**How to Assign or Delete Unattended Computers**

Use the Computers tab to manage the unattended computers that are accessible to an organizational unit.

A computer is added to your Rescue organization each time a customer grants unattended access rights to a technician.

Each computer is named according to the value entered in the **Name** field for the session during which unattended access was enabled.

1. Select the **Technicians** root or a **Technician Group** on the Organization Tree.
2. Select the **Computers** tab.
   A list of all unattended access computers assigned to the selected unit is displayed.
3. Select computers and choose an action:
   - Use **Copy...** to assign the selected computers to an additional Technician Group or Computer Group while maintaining any current assignments.
   - Use **Move...** to assign the selected computers to a different Technician Group or Computer Group.
• Click **Delete** to remove the selected assignment(s). Any other assignments remain valid.
• To revoke unattended access for a given computer, select all assignments and click **Delete**.

4. Confirm your action.
The new assignment is reflected on the Organization Tree and Computers tab.

**Tip:** Right-click an item to delete an individual assignment.

To create a Computer Group, right-click on a **Technician Group** and select **Create Computer Group**.

Use drag-and-drop to assign individual computers to Technician Groups, Computer Groups, or technicians.

---

**How to Set the Authentication Method for Unattended Access**

You must decide how technicians will authenticate when they access an unattended computer.

1. On the Organization Tree, select the **Technician Group** you want to work with.
2. Select the **Settings** tab.
3. Under **Unattended Access**, set the **Technician enters administrator credentials at start of every session** option:
   • Clear this option to allow technicians to authenticate to an unattended computer using a customer's credentials. This is the default setting.
Important: The duration of unattended access is limited to two weeks when technicians authenticate using customer credentials.

- Select this option to force the technician to enter valid administrative credentials at the start of every unattended session.

4. Save your changes.
Controlling Technician Status

How to Set Technician Status Controls (Maximum sessions, Busy, Away, Auto-logout)

Rescue offers a group of settings that help you control technician status.

1. On the Organization Tree, select the Technician Group you want to work with.
2. Select the Settings tab.
3. Under Technician Console, select from the following options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technician can handle maximum X active sessions</td>
<td>Set the maximum number of simultaneous sessions that you want to allow technicians to handle. When the maximum number is reached, a technician will be unable to activate new sessions.</td>
</tr>
<tr>
<td><strong>Restriction:</strong> A technician can handle only one active Rescue Lens session at a time.</td>
<td></td>
</tr>
<tr>
<td>Technician automatically goes into Busy state when handling more than X active sessions</td>
<td>Sessions cannot be transferred to a Busy technician, but a Busy technician can see all sessions in his queue and pick up new sessions.</td>
</tr>
<tr>
<td>Technician automatically goes into Away state after X min(s) of inactivity</td>
<td>Sessions cannot be transferred to an Away technician, but an Away technician can see all sessions in his queue and pick up new sessions.</td>
</tr>
<tr>
<td>Technician automatically logs out after X min(s) of inactivity</td>
<td>Inactivity is measured as the time when no actions are taken in the Technician Console. Certain processes running in the Technician Console will prevent automatic log out, including the following: an open remote control, screen sharing, or file manager session; a pending file transfer; or an open save dialog.</td>
</tr>
</tbody>
</table>

4. Save your changes.
Customizing the Technician Console

See also:
- *Hiding Disabled Features* on page 20
- *How to Set Connection Methods Available to Technicians* on page 46
- *Setting up Custom Fields* on page 76

External Content Portal

Add a link to any source of information that may help technicians do their job, such as a Knowledge Base, documentation, or other valuable support material. Technicians will see a link added to the menu in the upper-left corner of the Technician Console interface.

![Sample Custom Informational Link](image)

**Figure 2: Sample Custom Informational Link**

1. On the Organization Tree, select the **Technician Group** you want to work with.
2. Select the **Settings** tab.
3. Under **Content Portals**, go to **External Content Portal**.
4. Select **Show link in Tech Console menu** to activate the feature.
5. Enter the **Link name** as you want it to be shown in the Technician Console.
6. In the **Link opens new window at** box, enter the URL of the site that will be opened when the link is clicked in the Technician Console.
7. Save your changes.

Integrated Content Portal

Administrators can set a URL that technicians can open within the Technician Console.

This feature integrates a modified Internet Explorer browser window into the Technician Console. The window can be set to display any URL.

**How to set the Integrated Content Portal URL**

The Integrated Content Portal URL is set per Technician Group in the Administration Center.

---

Fastpath:  Settings tab > Content Portals > Integrated Content Portal

Opens with session The given link opens when a session enters Active status.
Opens on launch

The given link opens when the Technician Console is launched, and stays open until there is a session.

Additionally, you can post session data to the URL by appending the following parameters:

- $cfield0$ Customer’s name
- $cfield1$ Custom Field 1
- $cfield2$ Custom Field 2
- $cfield3$ Custom Field 3
- $cfield4$ Custom Field 4
- $cfield5$ Custom Field 5
- $platform$ Platform
- $sessionid$ Session ID
- $techid$ Technician ID
- $techdescr$ Technician description
- $techemail$ Technician email
- $techname$ Technician name
- $techssoid$ Technician Single Sign-on ID
- Example: http://myurl.com/$techid$

How to Manage Predefined Replies and URLs

An Administrator with a technician license can create a set of standard replies and URLs and then export them to an XML file. Technicians in the Administrators’ organization will then be able to import the replies and URLs into their own Technician Console.

Create New Predefines Replies and URLs

1. Log in to the Rescue Technician Console.

   ![Restriction](image)
   
   **Restriction:** Only Administrators with a technician license can access the Technician Console.

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

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

4. Give the reply or URL a short **Name**.

5. Type the text of the reply or the URL in the **Content** box.
   All content is text only. Formatting is not available.

   ![Note](image)
   
   **Note:** You can also enter an FTP address.

6. Click **Save**.

Export a Set of Predefined Replies and URLs

1. Log in to the Rescue Technician Console.
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.

### Share a Set of Predefined Replies and URLs

Share the xml file with your technicians so they can start using your set of predefined replies and URLs by following the below procedure.

**Tip:** You can send the xml file attached to an email, or you can share the URL of the location where the xml file has been stored. Make sure the location is accessible to your technicians.

1. Log in to the Rescue Technician Console.
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 **Import**. The **Open** dialog box is displayed.
5. Locate the xml file and click **Open**. The replies are added to your list of predefined replies.
Setting up Custom Fields

How to Name Custom Fields

Custom Fields allow you to collect information about your customers or sessions. Set the name of fields as they will appear in reports and in the Technician Console.

1. Select the Global Settings tab.
2. Under Custom Fields, set the names of the various fields.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name for name field</td>
<td>This field is used as a primary session identifier. Some organizations may want to use an employee number or ID code instead of a given name.</td>
</tr>
<tr>
<td>Name for custom fields</td>
<td>These are further session identifiers. Technicians can add these fields as columns on their Session List. Technicians with permission to use Inline Editing of Queue will be able to edit the values entered in these fields during a session.</td>
</tr>
</tbody>
</table>

3. Click Save changes.

Field values are entered by the customer for Channel sessions; by the technician for Private.

Figure 3: Custom Fields as seen in the Technician Console

**Note:** To change the name of the custom fields used in a Channel Form, edit the code for Custom Live Support Forms when you integrate it into your website. See How to Make a Channel Available for Use on page 31.
Remember: The default language used by the Administration Center Organization Tree, channel names, and Custom Fields on the Global Settings tab is set according to the language used at the time when you register for a LogMeIn Rescue account. This feature protects your Custom Fields and Organization Tree entity names from unwanted changes.

How to Enable Custom Fields for Private Sessions

Custom Fields appear in the Technician Console on the Create New Session dialog box. They are seen by a technician while creating a new session.

1. On the Organization Tree, select the Technician Group you want to work with.
2. Select the Settings tab.
3. Under Custom Fields (Private Sessions), choose from the following options:
   - Select Enabled to activate a Custom Field. It will be displayed on the Create New Session dialog box
   - Select Mandatory for each field that must be completed by the technician before a new session can be generated
   - Select Open text if you want technicians to be able to enter any text in the field’s text box (up to 64 characters)
   - Select Drop-down to add a drop-down list and choices to a field
4. Save your changes.
Setting up Remote Control Defaults

How to Set up Screen Recording

Define how and when Remote Control and Desktop Viewing sessions are recorded.

1. On the Organization Tree, select the Technician Group you want to work with.
2. Select the Settings tab.
3. Under Screen Recording, select from the following options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Forced screen recording</td>
<td>Choose this option to record all Remote Control and Desktop Viewing sessions</td>
</tr>
<tr>
<td></td>
<td>conducted by members of the selected Technician Group.</td>
</tr>
<tr>
<td>Allow Remote Control when screen recording</td>
<td>Choose this option if you want technicians to be able to run Remote Control</td>
</tr>
<tr>
<td>cannot be saved</td>
<td>sessions even if a recording of the session cannot be saved. If you disable</td>
</tr>
<tr>
<td></td>
<td>this option, technicians can only launch remote control when a recording can</td>
</tr>
<tr>
<td></td>
<td>be saved on the technician's computer. Furthermore, remote control will end</td>
</tr>
<tr>
<td></td>
<td>if an error occurs during screen recording.</td>
</tr>
<tr>
<td>Screen recording location</td>
<td>Specify a central location to which recorded sessions will be saved. You can</td>
</tr>
<tr>
<td></td>
<td>save locally, to a network location, or to an FTP, HTTP, or HTTPS server.</td>
</tr>
<tr>
<td></td>
<td>Examples:</td>
</tr>
<tr>
<td></td>
<td>• Network: \computer\directorypath. For example, \support\recordings</td>
</tr>
<tr>
<td></td>
<td>• Local: C:\recordings</td>
</tr>
<tr>
<td></td>
<td>• External server:</td>
</tr>
<tr>
<td></td>
<td>&lt;scheme&gt;://&lt;user&gt;:&lt;pass&gt;@&lt;domain&gt;:</td>
</tr>
<tr>
<td></td>
<td>&lt;port&gt;&lt;path&gt;&lt;extra&gt;</td>
</tr>
<tr>
<td></td>
<td>where &lt;scheme&gt; is ftp, http, and https. For example,</td>
</tr>
<tr>
<td></td>
<td>ftp://user:<a href="mailto:password@company.org">password@company.org</a>:21/recordings</td>
</tr>
</tbody>
</table>

Restriction: For technicians working on Technician Console for Mac, uploading screen recordings to an HTTP or HTTPS server is not available.

Tip: User name and password in the URL are only required when the host or proxy requires authentication. When credentials are omitted from URL, the Technician Console will prompt for credentials. Credentials in the URL are allowed, but not recommended.

Deferred Upload of Screen Recordings

By default, screen recordings are uploaded to the screen recording location in real time, as the session occurs. This works well in a high bandwidth environment, but may cause performance issues if a technician is using a low bandwidth connection. Select Deferred Upload of Screen Recordings to
Description

Option | Description
---|---
temporarily save all screen recordings to the technician's local drive and then upload them to the screen recording location as bandwidth becomes available. If the Technician Console is closed while uploading a file, it starts the upload process upon restarting the Technician Console. If you select FTP, HTTP, or HTTPS as a Screen recording location, deferred upload is automatically enabled regardless of your settings.

**File Format**

Recorded sessions can be saved as AVI files or in RCREC format. RCREC is a LogMeIn proprietary format that must be converted to AVI using the Rescue AVI Converter on a Windows PC. Each AVI option offers similar file size, with some variations in color and smoothness. Experiment to find the best choice to meet your needs. The LogMeIn encoder (RASC) is designed to offer the highest overall quality, but requires the LogMeIn codec for playback (available for Windows only). Anyone viewing your recordings must have the appropriate codec for the chosen AVI type.

4. Save your changes.

How to Set Clipboard Synchronization Behavior

Define how you want clipboard synchronization to behave during Remote Control.

1. On the Organization Tree, select the **Technician Group** you want to work with.
2. Select the **Settings** tab.
3. Under **Technician Console**, go to **Clipboard Synchronization** and select from the following options:
   - Choose **Use universal clipboard across all sessions** to allow a technician's clipboard to store copied items from multiple sessions.
   - Choose **Use one unique clipboard for each session** to ensure that material copied during any given session can be pasted to the technician's computer, but never to another customer.

4. Save your changes.

How to Disable Wallpaper for all Remote Sessions

Force the customer's desktop wallpaper and all user interface effects to be disabled during remote control. User interface effects include transition effects (fade, scroll), shadows under menus, and trailing effects while dragging windows.

1. On the Organization Tree, select the **Technician Group** you want to work with.
2. Select the **Settings** tab.
3. Under **Technician Console**, select **Disable visual effects**.
4. Save your changes.

The **Disable wallpaper and visual effects** box in the Technician Console will be deactivated. Wallpaper and effects will be disabled for all remote control sessions.
Setting up Surveys

How to Set up the Technician Survey

Administrators can customize and activate a survey to be completed by technicians at the end of a session.

1. On the Organization Tree, select the Technician Group you want to work with.
2. Select the Settings tab.
3. Under Technician Survey, select the appropriate options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>No technician survey</strong></td>
<td>Choose No technician survey if you do not want your technicians to complete a survey at session end.</td>
</tr>
<tr>
<td><strong>Use Rescue technician survey</strong></td>
<td>Choose Use Rescue technician survey to collect responses using a standard Rescue survey interface. The form can contain up to ten questions, each with five possible predefined answers, or with free-form (open-ended) answers. Technicians will be shown the survey at session end. Survey results are reported in the Technician Survey report, generated on the Reports tab.</td>
</tr>
<tr>
<td><strong>Use self-hosted technician survey</strong></td>
<td>Choose Use self-hosted technician survey to redirect technicians to a self-hosted survey or third-party survey tool. Enter the URL of your survey in the URL field. Technicians will be taken to the specified site at session end. In this case, survey data is not reported in the Technician Survey report, but rather using the mechanism native to the self-hosted or third-party survey site.</td>
</tr>
<tr>
<td><strong>Add additional Rescue session details to this URL</strong></td>
<td>If you are using a self-hosted or third-party survey, select Add additional Rescue session details to this URL to send the value of the Session ID and Custom Fields to the survey. The survey URL will be appended with the following data: RescueSessionID=xxxxxxxxx&amp;CField0=xxxxx&amp;CField1=xxxxx&amp;CField2=xxxxx&amp;CField3=xxxxx&amp;CField4=xxxxx&amp;CField5=xxxxx These parameters can be used, for example, to map a Rescue report to an external report. Your survey should be coded to accept these parameters in a GET request.</td>
</tr>
</tbody>
</table>

4. Click the Edit button next to a question. The Type your question here box is activated.
5. Type your question.
6. Choose the question type:
   - open answer
   - drop-down
7. Select mandatory to force technicians to complete the question.
8. Select enable to activate the question.
   The question will be included in the survey.
9. Click Apply when you are satisfied with the question.
10. Add more questions as required.
11. Save your changes.

Tip: To view survey results, go to the Reports tab and generate a Technician Survey report.

How to Set Up the Customer Survey

Administrators can customize and activate a survey to be completed by the customer at the end of a session.

1. On the Organization Tree, select the channel or Technician Group you want to work with.
2. Select the Settings tab.
3. Under Customer Survey, select the appropriate options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>No customer survey</strong></td>
<td>Choose No customer survey if you do not want your customers to complete a survey at session end.</td>
</tr>
<tr>
<td><strong>Use Rescue customer survey</strong></td>
<td>Choose Use Rescue customer survey to collect responses using a standard Rescue survey interface. The form can contain up to ten questions, each with five possible predefined answers, or with free-form (open-ended) answers. Customers will be shown the survey at session end. Survey results are reported in the Customer Survey report, generated on the Reports tab.</td>
</tr>
<tr>
<td><strong>Use self-hosted customer survey</strong></td>
<td>Choose Use self-hosted customer survey to redirect customers to a self-hosted survey or third-party survey tool. Enter the URL of your survey in the URL field. Customers will be taken to the specified site at session end. In this case, survey data is not reported in the Customer Survey report, but rather using the mechanism native to the self-hosted or third-party survey site.</td>
</tr>
<tr>
<td><strong>Add additional Rescue session details to this URL</strong></td>
<td>If you are using a self-hosted or third-party survey, select Add additional Rescue session details to this URL to send the value of the Session ID and Custom Fields to the survey. The survey URL will be appended with the following data: RescueSessionID=xxxxxxxxx&amp;CField0=xxxxx&amp;CField1=xxxxx&amp;CField2=xxxxx&amp;CField3=xxxxx&amp;CField4=xxxxx&amp;CField5=xxxxx These parameters can be used, for example, to map a Rescue report to an external report. Your survey should be coded to accept these parameters in a GET request.</td>
</tr>
</tbody>
</table>
4. Click **enable** and then **edit** to activate and edit questions.
5. Save your changes.

**Tip:** To view survey results, go to the **Reports** tab and generate a **Customer Survey** report.
Setting up Instant Chat

You can set Instant Chat as the default running mode for all PC and Mac sessions. See *How to Set the Default Applet (Standard or Instant Chat)* on page 34.

Tip: Refer to the LogMeIn Rescue *Customization and Integration Guide* for detailed information about Instant Chat, including implementation tips and a “How to” guide to Instant Chat customization.
Setting up Calling Card

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

**Calling Card Setup, Task One: Generate a Calling Card**

The first task in the process of setting up a Calling Card is to generate a Calling Card installer for a channel.

1. On the Organization Tree, select the channel for which you want to generate a Calling Card.
2. Select the **Channels** tab and scroll to the **Generate Calling Card for this Channel** section.
3. Give the Calling Card a meaningful name in the **Installer Name** box.

**Tip:** In large organizations with many Calling Card installers, always use a meaningful installer name to help identify different installers.

4. Click **Generate**.
5. Run the .msi file to install it on the local machine or save the .msi file to a folder on the local machine or on a network for later manual distribution.

You will see the Calling Card details on the **Channels** tab in the **Generate Calling Card for this Channel** section.

Each Calling Card installer that you generate has a unique Referral ID. This Referral ID is tracked when a new Rescue session is started using the Calling Card application and it will appear in any session reports.

**Using Multiple Installers**

Every installer is linked to a particular channel; however, administrators can track sessions based on different installers by generating multiple installers for the same channel.

This may be useful, for example, if you have two Technician Groups and you want to measure how many sessions are launched from each group’s installer. The two Technician Groups will have two different Referral IDs for their Calling Card. Both of the groups then start to deploy Calling Cards and you are then able to see how many sessions originate from each deployment.

Similarly, you may want to use two website landing pages for your installers. By using separate Referral IDs, you can track which one is used more often, based on the number of sessions started.
Calling Card Setup, Task Two: Give a Technician Group Permission to Deploy the Calling Card

The second task in the process of activating a Calling Card is to give a Technician Group permission to be able to deploy the Calling Card.

1. On the Organization Tree, select the **Technician Group** you want to work with.
2. Select the **Organization** tab.
3. Under **Permissions**, select **Deploy Calling Card**.
4. Click **Save Changes**.

Calling Card Setup, Task Three: Apply a Calling Card Installer to a Technician Group

The third task in the process of activating a Calling Card is to apply a Calling Card to a Technician Group.

1. On the **Channels** tab in the **Generate Calling Card for this Channel** section, copy the **Referral ID** of the Calling Card you want to apply.
2. On the Organization Tree, select the **Technician Group** you want to work with.
3. Select the **Organization** tab.
4. Scroll to the **Apply Calling Card** section and enter the referral ID into the **Installer Referral ID** field.
5. Click **Save Changes**.

Any technician in the Technician Group will be able to deploy the Calling Card via the Technician Console.

Calling Card Setup, Task Four: Customize the Calling Card Applet

A Master Administrator can customize Calling Card appearance and content on the Calling Card tab.

1. Select the **Calling Card** tab.
2. Edit the following options, as required.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Application name</strong></td>
<td>How the Applet will be named on the user’s device. Choose a name that is easy for your customers to identify with your organization.</td>
</tr>
<tr>
<td><strong>Menu Bar color, text color</strong></td>
<td>These settings determine the color of the menu bar and the text that appears in the bar. It is important to ensure that these two colors contrast highly to ensure the text is clearly visible.</td>
</tr>
<tr>
<td><strong>Border</strong></td>
<td>Set the color of the border and its width in pixels.</td>
</tr>
<tr>
<td><strong>Footer</strong></td>
<td>Set the color and height of the footer in pixels.</td>
</tr>
<tr>
<td><strong>Icon file</strong></td>
<td>The icon that a customer will click to open the Calling Card. Maximum file size is 50 kilobytes. File format must be .ico.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Logo</td>
<td>The logo shown in the top-right corner of the Calling Card once the connection to the technician has been established. Download the template to see a sample that conforms to all format requirements.</td>
</tr>
<tr>
<td>Header image</td>
<td>The header image shown at the top of the Calling Card. Maximum file size is 100 kilobytes. File format must be .bmp, .png, or .jpg.</td>
</tr>
<tr>
<td>Background</td>
<td>The image shown in the background of the Calling Card. Maximum file size is 100 kilobytes. File format must be .bmp, .png, or .jpg.</td>
</tr>
<tr>
<td>Help URL</td>
<td>You may want to provide instructions to your customers regarding the Calling Card. The Help URL should point to these instructions.</td>
</tr>
<tr>
<td>Disable Help URL</td>
<td>Select this option if you do want to display the Help menu item on the Calling Card.</td>
</tr>
<tr>
<td>Footer text and links</td>
<td>There is space in the Calling Card footer to include up to five hyperlinks to other websites. You should keep the text as brief as possible since line space may become an issue if you use all five links or long link names.</td>
</tr>
<tr>
<td>Terms and Conditions</td>
<td>Use the Terms and Conditions fields to set up a custom link to your organization's Terms and Conditions or other legal text.</td>
</tr>
<tr>
<td>Text before form</td>
<td>Use these fields to specify up to three lines of text that will be seen at the top of the Calling Card. Example: “Please fill in all fields and click Connect to contact a technician”</td>
</tr>
<tr>
<td>Text after form</td>
<td>Use this field to specify one line of text that will be seen at the bottom of the Calling Card Connect to Remote Support dialog box. Example: “Thank You!”</td>
</tr>
<tr>
<td>Custom fields</td>
<td>Choose which input fields to include in the Calling Card interface. Custom Fields are named on the Global Settings tab.</td>
</tr>
<tr>
<td>Note: Select Retain text to preserve values entered by the customer. That is, the next time the customer starts the Calling Card, previously entered values will be retained.</td>
<td></td>
</tr>
<tr>
<td>Code lines</td>
<td>On the PIN code connection page, you can specify up to three lines of text to explain to the user what he must do to complete the form correctly. Example: “Please enter the 6-digit PIN code provided by your technician”</td>
</tr>
<tr>
<td>Supported connection methods</td>
<td>Calling Card can be used to initiate channel sessions, PIN code (Private) sessions, or both.</td>
</tr>
<tr>
<td>Default connection method</td>
<td>Set the connection method to be displayed by default when the Calling Card is opened. If both connection methods are active, the customer will be able to switch between methods using the Connect menu on the Calling Card.</td>
</tr>
<tr>
<td>Company ID validation</td>
<td>Select this option to ensure that the Calling Card only accepts PIN codes created by the same support organization that installed the Calling Card.</td>
</tr>
<tr>
<td>Note: The Company ID validation option is selected by default.</td>
<td></td>
</tr>
</tbody>
</table>

3. Click **Save Changes**.
**Note:** The name of your organization will appear on the Calling Card as entered in the Organization field of the My Account > Modify Contact Information page. The "Powered by LogMeIn Rescue" logo cannot be customized.

**Tip:** After making changes, use the Regenerate button on the Channel tab to regenerate the installer. The same referral ID is used. You will not need to inform your customers of the update, because the Calling Card application will automatically be updated when started. The exception to this is if you place the installer somewhere on your website for your customers to download. This installer will not be updated. However, once it is downloaded and run by your customers, it will then be automatically updated. If the original installer is deleted, use Regenerate to reinstall an identical copy of the installer onto your local hard drive.

**Calling Card Setup, Task Five: Deploy the Calling Card to a Customer's Computer**

Follow this procedure to install the Rescue Calling Card on a customer's computer during an active session. A technician installs the Calling Card to 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.

   **Remember:** This task is performed in the Technician Console.

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.
Setting Up External Technician Collaboration

Controlling How Your Technicians Collaborate With External Technicians

Define whether the members of a Technician Group will be able to invite external technicians, and more.

<table>
<thead>
<tr>
<th>Goal</th>
<th>Setting or Location in Administration Center</th>
</tr>
</thead>
<tbody>
<tr>
<td>Define whether the members of a Technician Group will be able to invite external technicians</td>
<td>Technician Group &gt; Organization tab &gt; Permissions &gt; Invite external technicians</td>
</tr>
<tr>
<td>Define whether members of a Technician Group can invite anyone or only approved external technicians</td>
<td>Technician Group &gt; Organization tab &gt; Permissions &gt; Invite external technicians &gt; anyone can be invited / only approved</td>
</tr>
<tr>
<td>Tip:</td>
<td>To make an external technician or group available to a specific technician or group, drag their name tag to the appropriate technician or group on the Organization Tree.</td>
</tr>
<tr>
<td>Note:</td>
<td>IP controls set in the Administration Center do not apply to external technicians.</td>
</tr>
<tr>
<td>Control how technicians are able to invite external technicians to a session</td>
<td>Technician Group &gt; Settings tab &gt; Connection method for external technician invitations.</td>
</tr>
<tr>
<td>Control how technicians are able to invite external technicians to a session</td>
<td>For maximum flexibility, select all options. For maximum control, only allow technicians to invite external technicians via email sent through Rescue servers.</td>
</tr>
<tr>
<td>Control how technicians are able to invite external technicians to a session</td>
<td>Invitation settings impact the tabs available on the Invitation to External Technician dialog box under Connection Method.</td>
</tr>
</tbody>
</table>

Note: You can also control how technicians are able to invite external technicians to a session by selecting the options under the Connection method for external technician invitations. For maximum flexibility, select all options. For maximum control, only allow technicians to invite external technicians via email sent through Rescue servers.

Setting Permissions for External Technicians

Define what approved external technicians can do during a session, and more.

What can approved external technicians do during a session?

For each group of approved external technicians, Administrators define the permissions that can be assigned by the lead technician to the approved external technician. The lead technician can toggle permissions on and off at the time of invite and during the session.
What can unapproved external technicians do during a session?
For each technician group with permission to invite any external technician, Administrators define the
permissions that can be assigned by the lead technician to the external technician. The lead technician
can toggle permissions on and off at the time of invite and during the session.

Can unique session permissions be set for a single external technician?
The lead technician can toggle permissions on and off at the time of invite and during the session. The
permissions that are available to lead technician are set in the Administration Center.

Security and Reporting for External Technician Collaboration
Follow these guidelines for maximum control and accountability when using external technician
collaboration.

<table>
<thead>
<tr>
<th>Goal</th>
<th>Setting or Location in Administration Center</th>
</tr>
</thead>
<tbody>
<tr>
<td>Only allow technicians to invite from an approved list</td>
<td>Select a Technician Group and go to Organization tab &gt; Permissions &gt; Invite external technicians &gt; only approved.</td>
</tr>
<tr>
<td>Prevent external technicians from using specific features</td>
<td>Select an External Technician Group and go to Organization tab &gt; Permissions &gt; clear permissions. Any permission that is cleared will not be available to the lead technician to grant to the external technician.</td>
</tr>
<tr>
<td>Only allow technicians to send invitations via email sent through Rescue servers</td>
<td>Select a Technician Group and go to Settings tab &gt; Connection method for external technician invitations &gt; Email &gt; Allow email via Rescue servers. Clear all other options.</td>
</tr>
<tr>
<td>Check reports for any External Technician Group or individual external technician</td>
<td>Select an External technician group or External technician and go to Reports &gt; Chatlog or Session.</td>
</tr>
<tr>
<td>Check reports for any Technician Group or individual technician</td>
<td>Select a Technician Group or technician and go to Reports &gt; External Technician Chatlog.</td>
</tr>
</tbody>
</table>
Setting up Scripting

Embedded Scripting for Applet and Calling Card

You can set up LogMeIn Rescue to run embedded scripts via the Customer Applet and Calling Card.

Fastpath: To configure embedded scripts, go to the Administration Center Resources tab.

Requirements

• The customer must be using a Windows-based computer
• The session must use the Customer Applet or Calling Card (not Mobile Applet or Instant Chat in chat-only mode)

How it works

• You can specify one script up to 64 KB, with an associated resource file up to 2 MB. A resource file is any file used by the script. For example, if the script sends a ZIP file to the customer, the ZIP file is the resource file.
• This is an organization-level setting. That is, the script will be transferred during each session that uses the Customer Applet or Calling Card, for every Technician Group and channel in your organization.
• The script is transferred when the Customer Applet is downloaded or Calling Card is started.
• The script is executed according to your preference:

  Remember: You can set your preference in the Configure Embedded Script section on the Resources tab.

  • Select Run after reboot to execute the script after restarting the customer’s computer.
  • Select Run after X minutes of disconnection to execute the script every X minutes for as long as the session remains disconnected (for example, due to a network connection problem).
  • Select Run event triggered script to execute the script after specified session events. To obtain a sample script with condition syntax for all valid parameters in its body, click Download an example script.
  • Additionally, technicians in a group with the Run embedded script permission set in the Administration Center can run an embedded script via the Technician Console Script tab. The Run embedded script permission is off by default.

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

How to Create a New Script Collection

Master Administrators can upload and organize scripts to a common repository and share them with technicians.

1. In the Administration Center, go to the Global Settings tab.
2. Under Centralized Scripts, click Manage Centralized Scripts. The Centralized Scripts window is displayed.
3. Click New collection.
4. Name the collection and click Create. The collection is created.
5. Add scripts. You have two options.
   - Option one: Add a new script by clicking Add script. Fill in the fields and select the necessary files. Fields with an asterisk are mandatory.
   - Option two: Import scripts from the Technician Console or from another collection by clicking Import XML.
6. Save your changes.

How to Share a Script Collection with a Technician Group

Master Administrators and Administrators can provide script collections to any Technician Group in their organization tree.

1. In the Administration Center on the Organization Tree, select the Technician Group to which you want to provide the script collection.
2. Select the Settings tab.
3. Under Centralized Scripts, select the desired script collection from the All collections box, and click << Add. The name of the script collection is listed in the Collections available to this group box.
   Tip: Want to add more script collections? Repeat this step for each collection that you want to provide to this Technician Group.
4. Click Save Changes.

The agent's Technician Group must have permission to deploy scripts. Make sure the Script deployment permission is enabled in the Administration Center at the group level on the Organization tab.

How to Modify a Script Collection

Master Administrators can modify their script collections.

1. In the Administration Center, go to the Global Settings tab.
2. Under Centralized Scripts, click Manage Centralized Scripts. The Centralized Scripts window is displayed.
3. Hover over the script collection you want to modify. You can perform the following modifications:
• To delete a collection, click the **Delete** button.

• To rename a collection, click the **Rename** button.

• To delete a script from the collection:
  1. In the Script Library, click the selected collection. The list of scripts belonging to the collection is displayed.
  2. Select the script you want to delete and click the **Delete** button.

**How to Modify a Script in the Collection**

Master Administrators can modify scripts in their script collections.

1. In the Administration Center, go to the **Global Settings** tab.
2. Under **Centralized Scripts**, click **Manage Centralized Scripts**. The **Centralized Scripts** window is displayed.
3. Select the script collection you want to modify. Scripts belonging to the selected script collection are listed.
4. Select the script you want to modify. You can perform the following modifications:
   • To modify data related to a script, select the script and click the **Edit** button.
   • To make a script run automatically upon session start, in the **Autostart** drop-down list select a numerical value. The actual value corresponds to the execution priority of the script upon session start relative to other autostart scripts in the collection. For example, when a support session is started, the script with value 1 will run first; the script with value 2 will run second, and so on.
Generating Reports

How to Generate a Report

Follow this procedure to generate a report in the LogMeIn Rescue Administration Center.

1. On the Organization Tree, select the organizational unit for which you want to generate a report.
2. Select the Reports tab.
3. Select the type of report you want to generate using the Report Area drop-down box.
4. For most report areas, you must select a List Type.
   - Choose List All to view information about specific sessions or logins
   - Choose Summary to view cumulative information
5. Specify the reporting period (Date Range) in one of two ways:
   - Choose a pre-defined report period (today, yesterday, etc.)
   - Choose a specific Start Date and End Date
6. Select the Time Zone to be applied:
   - Choose Local to report all times using your current time zone (where you are when you generate the report)
   - Choose UTC to report all times in Coordinated Universal Time, which is effectively the same as Greenwich Mean Time (GMT)
7. Choose a Daily Time Range. Generate reports covering any period of the day. This is useful for evaluating shift performance.
8. Select the type of file to generate from the drop-down list next to Get report.
   - Tip: To view the report on the Administration Center Reports tab without downloading a file, choose HTML.
9. Generate the report by clicking Get report.

Time Zone Example

Local time. Assume you are in New York and you generate a report for a Technician Group with technicians in San Francisco and Paris. Event times will be reported in local (New York) time. An event that occurred at 2:00:00 PM in San Francisco will be reported as 5:00:00 PM. An event that occurred at 2:00:00 PM in Paris will be reported as 8:00:00 AM.

UTC. Assume you generate a report for a Technician Group with technicians in San Francisco and Paris. Regardless of your location, event times will be reported in UTC. An event that occurred at 2:00:00 PM San Francisco time (UTC-8) will be reported as 10:00:00 PM. An event that occurred at 2:00:00 PM in Paris (UTC+1) will be reported as 1:00:00 PM.
## Customer Survey Report (List All)

This report returns the results of individual customer surveys submitted in response to sessions conducted by members of the selected unit during the selected period.

Each row represents one submitted survey.

| Source | The name of each channel or Technician Group for which a Customer Survey has been activated on the Settings tab > Customer Survey section. The value Technicians is returned when a global survey is assigned to all technicians in an organization. Data type: String. Data length: 128 characters. |
| Date | The date and time when the technician ended the session. Data type: DateTime. Data length: unspecified. |
| [Name] | The name of this column is derived from the following setting: Global Settings > Custom Fields > Name for name field. The actual reported value is entered by a customer or technician during session generation. By default this is the name of the customer. Data type: String. Data length: 128 characters. |
| [Survey Columns] | These variable columns will show responses to the survey questions defined on the Settings tab in the Customer Survey section. |
| **Open answers** | If open answers is selected under Settings > Customer Survey > Edit, the column displays the verbatim answer submitted by the customer. |
| **Drop-down** | If drop-down is selected under Settings > Customer Survey > Edit, the column displays the numeric value corresponding to the configured predefined reply. (For example, 1 corresponds to the first predefined answer from the drop-down list, while 2 corresponds to the second one, and so on.) Data type: String. Data length: 128 characters. |
| Technician Name | The technician's name as recorded in the Name field on the Organization tab. Data type: String. Data length: 128 characters. |
| Technician Email | The email address of the technician. For approved technicians, the email is recorded in the Email field on the Organization tab. For unlisted technicians, the email is recorded during the invitation process. Data type: String. Data length: 128 characters. |

## Customer Survey Report (Summary)

This report returns the cumulative results of customer surveys submitted in response to sessions conducted by members of the selected unit during the selected period.

Each row represents an organizational unit.
Source | The name of each channel or Technician Group for which a Customer Survey has been activated on the Settings tab > Customer Survey section. The value Technicians is returned when a global survey is assigned to all technicians in an organization. Data type: String. Data length: 128 characters.

Number of Surveys | The total number of surveys received. Data type: Integer. Data length: unspecified.

[Survey Columns] | These variable columns will show the total number of responses to the survey questions defined on the Settings tab in the Customer Survey section. Data type: String. Data length: 128 characters.

Customer Survey Issuance Report (List All)

This report returns the results of individual customer surveys submitted in response to sessions conducted by members of the selected unit during the selected period. It also displays whether the closing or the starting technician issued the customer survey.

Important: This report is only available if in the Administration Center you choose Global Settings > Customer Survey Issuance > Survey issued by > Closing technician.

Each row represents one submitted survey.

Source | The name of each channel or Technician Group for which a Customer Survey has been activated on the Settings tab > Customer Survey section. The value Technicians is returned when a global survey is assigned to all technicians in an organization. Data type: String. Data length: 128 characters.


Date | The date and time when the technician ended the session. Data type: DateTime. Data length: unspecified.

[Name] | The name of this column is derived from the following setting: Global Settings > Custom Fields > Name for name field. The actual reported value is entered by a customer or technician during session generation. By default this is the name of the customer. Data type: String. Data length: 128 characters.

Technician Name | The technician’s name as recorded in the Name field on the Organization tab. Data type: String. Data length: 128 characters.


Technician Email | The email address of the technician. For approved technicians, the email is recorded in the Email field on the Organization tab. For unlisted technicians, the email is recorded during the invitation process. Data type: String. Data length: 128 characters.

Survey issued by closing technician | Displays which technician issued the customer survey:
- Yes – the closing technician issued the survey
- No – the starting technician issued the survey
Customer Survey Issuance Report (Summary)

This report returns the cumulative results of customer surveys submitted in response to sessions conducted by members of the selected unit during the selected period. It also displays whether the closing or the starting technician issued the customer survey.

Important: This report is only available if in the Administration Center you choose Global Settings > Customer Survey Issuance > Survey issued by > Closing technician.

Each row represents an organizational unit.

**Source**
The name of each channel or Technician Group for which a Customer Survey has been activated on the Settings tab > Customer Survey section. The value Technicians is returned when a global survey is assigned to all technicians in an organization. Data type: String. Data length: 128 characters.

**Number of Surveys**
The total number of surveys received. Data type: Integer. Data length: unspecified.

**[Survey Columns]**
These variable columns will show the total number of responses to the survey questions defined on the Settings tab in the Customer Survey section. Data type: String. Data length: 128 characters.

**Survey issued by closing technician**
Displays which technician issued the customer survey:

- **Yes** – the closing technician issued the survey
- **No** – the starting technician issued the survey

Performance Report (List All)

This report returns individual performance data for each member of the selected unit for the selected period.

Each row represents a technician.

**Technician Name**
The technician’s name as recorded in the Name field on the Organization tab. Data type: String. Data length: 128 characters.

**Technician ID**

**Technician Email**
The technician’s email address as recorded in the Email field on the Organization tab. Data type: String. Data length: 128 characters.

**Total Login Time**
Per technician, the total time spent logged in to the Technician Console. Data type: DateTime. Data length: unspecified.

**Number of Sessions**
Per technician, the number of sessions handled. Data type: Integer. Data length: unspecified.

**Number of Sessions per Hour**
Per technician, the number of sessions divided by total login time. Use this value to assess how many sessions a technician can manage in an hour. Data type: String. Data length: 128 characters.
**Average Pick-up Speed**  
Per technician, the average elapsed time between the beginning of Waiting status and session start by the technician. From the customer's perspective, this is the amount of time the customer sees the message *Waiting for a technician*. Data type: DateTime. Data length: unspecified.

**Average Duration**  
Per technician, the average session duration. Data type: DateTime. Data length: unspecified.

**Average Work Time**  
Work Time is actual Technician Console utilization time during a session. It is the time spent actually using Technician Console functionality: (1) the session must be selected, (2) with an active connection to the Applet, (3) with the Technician Console in focus, and (4) the technician’s status must not be Away. Data type: DateTime. Data length: unspecified.

**Longest Session**  
Per technician, the length of the longest single session. Data type: DateTime. Data length: unspecified.

**Total Active Time**  
Per technician, the cumulative time spent in Active status for all sessions. Active time is measured from pickup (Active status) to close (Closed status), excluding Hold Time, Time in Transfer, Rebooting Time, and Reconnecting Time. Data type: DateTime. Data length: unspecified.

**Total Work Time**  
Work Time is actual Technician Console utilization time during a session. It is the time spent actually using Technician Console functionality: (1) the session must be selected, (2) with an active connection to the Applet, (3) with the Technician Console in focus, and (4) the technician’s status must not be Away. Data type: DateTime. Data length: unspecified.

---

**Performance Report (Summary)**

This report returns collective performance data for all members of the selected unit for the selected period.

**Number of Sessions**  
The total number of sessions handled. Data type: Integer. Data length: unspecified.

**Total Login Time**  
The total time spent logged in to the Technician Console. Data type: DateTime. Data length: unspecified.

**Average Number of Sessions per Hour**  
The average number of sessions handled per hour. Data type: String. Data length: 128 characters.

**Average Pick-up Speed**  
The average elapsed time between the beginning of Waiting status until entering Active status (when the session is picked up by the technician). From the customer's perspective, this is the amount of time the customer sees the message *Waiting for a technician*. Data type: DateTime. Data length: unspecified.

**Average Session Duration**  
The average length of sessions handled by technicians in the selected unit. Data type: DateTime. Data length: unspecified.

**Average Work Time**  
Work Time is actual Technician Console utilization time during a session. It is the time spent actually using Technician Console functionality: (1) the session must be selected, (2) with an active connection to the Applet, (3) with the Technician Console in focus, and (4) the technician's status must not be Away. Data type: DateTime. Data length: unspecified.
Total Session Time  The total length of sessions handled by technicians in the selected unit. Data type: DateTime. Data length: unspecified.

Longest Session  The length of the longest session conducted during the selected period by any member of the selected unit. Data type: DateTime. Data length: unspecified.

Total Active Time  The cumulative time spent in Active status for all sessions. Active time is measured from pickup (Active status) to close (Closed status), excluding Hold Time, Time in Transfer, Rebooting Time, and Reconnecting Time. Data type: DateTime. Data length: unspecified.

Total Work Time  Work Time is actual Technician Console utilization time during a session. It is the time spent actually using Technician Console functionality: (1) the session must be selected, (2) with an active connection to the Applet, (3) with the Technician Console in focus, and (4) the technician's status must not be Away. Data type: DateTime. Data length: unspecified.

**Login Report (List All)**

This report returns data for each **unique** login performed by a member of the selected unit during the selected period.

This report can be generated for any organizational unit.

Each row represents a unique login event.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login Date</td>
<td>The date when the login occurred, based on the selected time zone. Data type: DateTime. Data length: unspecified.</td>
</tr>
<tr>
<td>Name</td>
<td>The user's name as recorded in the Name field on the Organization tab. Data type: String. Data length: 128 characters.</td>
</tr>
<tr>
<td>Email</td>
<td>The Rescue user's email address as recorded in the Email field on the Organization tab. Data type: String. Data length: 128 characters.</td>
</tr>
<tr>
<td>Start Time</td>
<td>The exact login time. Data type: DateTime. Data length: unspecified.</td>
</tr>
<tr>
<td>End Time</td>
<td>The exact logout time. Data type: DateTime. Data length: unspecified.</td>
</tr>
<tr>
<td>Total Login Time</td>
<td>Length of time logged in to LogMeIn Rescue. Data type: DateTime. Data length: unspecified.</td>
</tr>
<tr>
<td>IP Address</td>
<td>The IP address from which login occurred. Data type: String. Data length: 15 characters.</td>
</tr>
<tr>
<td>Busy Time</td>
<td>Length of time in Busy status. Reported for technicians only. Data type: DateTime. Data length: unspecified.</td>
</tr>
<tr>
<td>Away Time</td>
<td>Length of time in Away status. Reported for technicians only. Data type: DateTime. Data length: unspecified.</td>
</tr>
<tr>
<td>Idle Time</td>
<td>Idle Time is when a technician is logged in to the Technician Console but has no sessions. Idle Time ends as soon as any session enters any status in the Technician Console. Data type: DateTime. Data length: unspecified.</td>
</tr>
</tbody>
</table>
Login Report (Summary)

This report returns cumulative login data for members of the selected unit for the selected period.

This report can be generated for any organizational unit.

Each row represents one member of the organization.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The Rescue user’s name as recorded in the Name field on the Organization tab. Data type: String. Data length: 128 characters.</td>
</tr>
<tr>
<td>Email</td>
<td>The Rescue user’s email address as recorded in the Email field on the Organization tab. Data type: String. Data length: 128 characters.</td>
</tr>
<tr>
<td>Nickname</td>
<td>The Rescue user’s nickname as recorded in the Nickname field on the Organization tab. Data type: String. Data length: 128 characters.</td>
</tr>
<tr>
<td>Group</td>
<td>The name of the Administrator Group or Technician Group to which the user belonged at the time of login. Data type: String. Data length: 128 characters.</td>
</tr>
<tr>
<td>User Created On</td>
<td>The date when the user was added to the organization with a valid name and email on the Organization tab. Data type: DateTime. Data length: unspecified.</td>
</tr>
<tr>
<td>Number of Logins</td>
<td>The number of unique login events recorded during the selected period. Data type: Integer. Data length: unspecified.</td>
</tr>
<tr>
<td>Average Login Time</td>
<td>The average length of time logged in to LogMeIn Rescue. Data type: DateTime. Data length: unspecified.</td>
</tr>
<tr>
<td>Total Login Time</td>
<td>The total time spent logged in to LogMeIn Rescue. Data type: DateTime. Data length: unspecified.</td>
</tr>
<tr>
<td>Total Busy Time</td>
<td>The total time in Busy status. Reported for technicians only. Data type: DateTime. Data length: unspecified.</td>
</tr>
<tr>
<td>Total Away Time</td>
<td>The total time in Away status. Reported for technicians only. Data type: DateTime. Data length: unspecified.</td>
</tr>
<tr>
<td>Total Idle Time</td>
<td>Idle Time is when a technician is logged in to the Technician Console but has no sessions. Idle Time ends as soon as any session enters any status in the Technician Console. Data type: DateTime. Data length: unspecified.</td>
</tr>
</tbody>
</table>

Session Report (List All)

This report returns data for each unique session conducted by members of the selected unit during the selected period.

Each row represents a unique session.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start Time</td>
<td>The exact time when the session entered Active status. Data type: DateTime. Data length: unspecified.</td>
</tr>
</tbody>
</table>
End Time  The exact time when the session entered Closed or Timed Out status. Data type: DateTime. Data length: unspecified.

Last Action Time  The exact time of the action that ended the technician's state of being "in action". A technician is in action if he is in a session, and for that session the Technician Console and the Applet have a working connection (that is, the sockets between the Technician Console and Applet are connected). Any of the following ends the technician's "in action" state:

• The technician's status Changes to "Away".
• The technician loses connection with customer.
• The session tab gets unselected, or the TC goes to background while there is no active tear-away window of the session.
• The tear-away window of the session gets inactive while either the session tab is unselected or the TC is in the background.
• The technician or Administrator ends, holds, or transfers the session.

Data type: DateTime. Data length: unspecified.

Technician Name  The technician's name as recorded in the Name field on the Organization tab. Data type: String. Data length: 128 characters.


Technician Email  The technician's email address as recorded in the Email field on the Organization tab. Data type: String. Data length: 128 characters.


Session Type  The customer-side technology applied. Data type: String. Data length: 100 characters. Possible values are as follows:

• Mobile Applet
• Calling Card
• Instant Chat
• Unattended
• Applet On LAN
• Applet

Status  The final status at the time of the last action performed by the given technician. Data type: String. Data length: 64 characters. Possible values are as follows:

• Connecting
• Waiting
• Active
• Closed by customer
• Closed by technician
• Transferring
• Transferred
• Closed by waiting customer
• Timed out
• Aborted: technician was deleted or disabled
• Rebooting
• Reconnecting
- On Hold
- Timed out: closed by technician
- Offline
- Disconnected
- Rebooted
- Declined by customer

**[Name]**
The name of this column is derived from the following setting: Global Settings > Custom Fields > Name for name field. The actual reported value is entered by a customer or technician during session generation. By default this is the name of the customer. Data type: String. Data length: 128 characters.

**[Custom Fields]**
The names of these columns are derived from the following settings: Global Settings > Custom Fields > Name for custom field. Data type: String. Data length: 64 characters.

**Tracking ID**
A custom field used for mapping Rescue sessions to a CRM system or for other custom administrative purposes. Data type: String. Data length: 256 characters.

**Customer IP**
The customer's IP address. If no value is reported, your organization probably chose not to store customer IP address information (Global Settings > Do not store customer IP address). Data type: String. Data length: 15 characters.

**Device ID**

**Incident Tool Used**
This column lists Technician Console tools used by the technician during the session. See the legend at the bottom of the report for a key to abbreviations. Data type: String. Data length: 128 characters.

**Resolved/Unresolved**
This column is no longer actively used though may show results when reporting on sessions held prior to May 2009 (Resolved/Unresolved, as submitted by the technician). Data type: String. Data length: 128 characters.

**Channel ID**
The Channel ID of the channel used during the session. Data type: Integer. Data length: unspecified.

**Channel Name**
The name of the channel used during the session. Data type: String. Data length: 64 characters.

**Calling Card**
The Installer Name of the Calling Card used during the session. Data type: String. Data length: 64 characters.

**Connecting Time**
From the beginning of Applet download until the session appears as Waiting in a queue. Data type: DateTime. Data length: unspecified.

**Waiting Time**
From the beginning of Waiting status until session start (Active status). Data type: DateTime. Data length: unspecified.

**Total Time**
The sum of Active Time, Hold Time, Time in Transfer, Rebooting Time, and Reconnecting Time; excluding Connecting and Waiting time. This is not the same as Total Time as shown in the Technician Console Session List. Data type: DateTime. Data length: unspecified.

**Active Time**
The total time the session was in Active status. Active time is measured from pickup (Active status) to close (Closed status), excluding Hold Time, Time in Transfer, Rebooting Time, and Reconnecting Time. Data type: DateTime. Data length: unspecified.
**Work Time**

Work Time is actual Technician Console utilization time during a session. It is the time spent actually using Technician Console functionality: (1) the session must be selected, (2) with an active connection to the Applet, (3) with the Technician Console in focus, and (4) the technician’s status must not be Away. Data type: DateTime. Data length: unspecified.

**Hold Time**

The length of time in Hold status. Data type: DateTime. Data length: unspecified.

**Time in Transfer**

The length of time in Transfer status. Data type: DateTime. Data length: unspecified.

**Rebooting Time**

The length of time in Rebooting status. Data type: DateTime. Data length: unspecified.

**Reconnecting Time**

The length of time in Reconnecting status due to a problem on the customer side. Data type: DateTime. Data length: unspecified.

**Platform**

The customer’s operating system. Data type: String. Data length: 20 characters.

**Browser Type**

The type of browser in which the customer started the Instant Chat session. Data type: String. Data length: unspecified.

---

### Session Report (Summary)

This report returns **cumulative** data for all sessions conducted by members of the selected unit during the selected period.

**Number of Sessions**

The total number of sessions handled. Data type: Integer. Data length: unspecified.

**Average Session Time**

The average length of sessions. Total Session Time divided by Number of Sessions. Data type: DateTime. Data length: unspecified.

**Total Session Time**

The cumulative length of all sessions. Data type: DateTime. Data length: unspecified.

**Average Pick-up Time**

The average elapsed time between the beginning of Waiting status and session start by the technician. From the customer’s perspective, this is the amount of time the customer sees the message *Waiting for a technician*. Data type: DateTime. Data length: unspecified.

**Total Pick-up Time**

For all sessions, the total elapsed time between the beginning of Waiting status and session start by the technician. Data type: DateTime. Data length: unspecified.

**Average Active Time**

The average time in Active status. Active time is measured from pickup (Active status) to close (Closed status), excluding Hold Time, Time in Transfer, Rebooting Time, and Reconnecting Time. Data type: DateTime. Data length: unspecified.

**Total Active Time**

For all sessions, the total time in Active status. Active time is measured from pickup (Active status) to close (Closed status), excluding Hold Time, Time in Transfer, Rebooting Time, and Reconnecting Time. Data type: DateTime. Data length: unspecified.

**Average Work Time**

Work Time is actual Technician Console utilization time during a session. It is the time spent actually using Technician Console functionality: (1)
the session must be selected, (2) with an active connection to the Applet, (3) with the Technician Console in focus, and (4) the technician's status must not be Away. Data type: DateTime. Data length: unspecified.

**Total Work Time**
Total Technician Console utilization time during all sessions. Data type: DateTime. Data length: unspecified.

**Average Hold Time**
The average time in Hold status. Data type: DateTime. Data length: unspecified.

**Total Hold Time**
The total time in Hold status. Data type: DateTime. Data length: unspecified.

**Average Transfer Time**
The average time in Transfer status. Data type: DateTime. Data length: unspecified.

**Total Transfer Time**
The total time in Transfer status. Data type: DateTime. Data length: unspecified.

**Average Rebooting Time**
The average time in Rebooting status. Data type: DateTime. Data length: unspecified.

**Total Rebooting Time**
The total time in Rebooting status. Data type: DateTime. Data length: unspecified.

**Average Reconnecting Time**
The average time in Reconnecting status. Data type: DateTime. Data length: unspecified.

**Total Reconnecting Time**
The total time in Reconnecting status. Data type: DateTime. Data length: unspecified.

**Longest Session Time**
The length of the longest single session. Data type: DateTime. Data length: unspecified.

**Number of Missed Sessions**
The number of sessions that were never picked up (that is, sessions that never entered Active status). Data type: Integer. Data length: unspecified.

---

**Chatlog Report**

This report retrieves the chatlog and session notes for each unique session conducted by a member of the selected unit during the selected period.

Each row represents a unique session.

**Start Time**
The exact time when the session entered Active status. Data type: DateTime. Data length: unspecified.

**End Time**
The exact time when the session entered Closed or Timed Out status. Data type: DateTime. Data length: unspecified.

**Total Time**
The sum of Active Time, Hold Time, Time in Transfer, Rebooting Time, and Reconnecting Time; excluding Connecting and Waiting time. This is not the same as Total Time as shown in the Technician Console Session List. Data type: DateTime. Data length: unspecified.

**Session ID**
The name of each channel or Technician Group for which a Customer Survey has been activated on the Settings tab > Customer Survey section. The value Technicians is returned when a global survey is assigned to all technicians in an organization. Data type: String. Data length: 128 characters.

Technician Name
The technician's name as recorded in the Name field on the Organization tab. Data type: String. Data length: 128 characters.

Technician ID

Technician Email
The email address of the technician. For approved technicians, the email is recorded in the Email field on the Organization tab. For unlisted technicians, the email is recorded during the invitation process. Data type: String. Data length: 128 characters.

Chat Log
An icon is displayed if a Chat Log is available. Click the icon to view the log. Data type: String. Data length: 2048 characters.

Notes
An icon is displayed if notes are available. Click the icon to view the notes. Data type: String. Data length: 1024 characters.

Note: For collaboration sessions, the log contains full details of the session, including system messages, chat between technicians, and chat between technicians and customer.

Sample Chat Log
This sample shows the Chat Log for the same session as shown in the sample for the Collaboration Chat Log report. Notice that the perspective is that of the Lead Technician.

9:19 AM Connecting to: [...]
9:19 AM Connected to Applet (RSA 2048 bits, AES256-SHA 256 bits)
9:19 AM Switched to P2P
9:19 AM Technician 2 invited to the session...
9:19 AM Technician 2 joined the session
9:19 AM «Technician 1»: This is between technicians
9:20 AM «Technician 2»: This is between technicians
9:20 AM «Technician 1»: This is between technician and customer
9:20 AM Technician 2: This is between technician and customer
9:20 AM Customer: This is from the customer to the technicians
9:20 AM The technician ended the session.

How to Delete Chatlogs
If sensitive information is communicated during a session, Master Administrators can choose to delete a session's chatlog, thereby excluding sensitive data from the Chatlog report.

1. When logged in as a Master Administrator, go to Organization Tree and select an organizational unit.
2. Select the Reports tab.
4. Find the sessions with chatlogs you want to delete:
   • Option 1. If you need to delete the chatlog for multiple sessions or do not know the exact Session ID, you should first generate the Chatlog report in HTML format. For step-by-step instructions, see How to Generate a Report on page 94.
• Option 2. If you already know the Session ID of a single session, enter it in the **Session ID** field and click **Find**.

5. In the **Delete** column, click the **trash can icon** for each appropriate session. The chatlog for each selected session is queued for deletion. Chatlogs are **not** deleted immediately.

   **Tip:** If you change your mind, you can revoke any deletion within 24 hours by clicking this icon 🔵 in the Delete column.

Chatlogs are deleted 24 hours from the moment they are queued for deletion. Pending deletions are reported in the Chatlog report; deleted chatlogs are not.

**Collaboration Chat Log Report**

This report returns the chat log from each unique session in which a member of the selected unit participated as a collaborating technician.

- **Start Time**
  For the collaborating technician. The exact time when the session entered Active status. Data type: DateTime. Data length: unspecified.

- **End Time**
  For the collaborating technician. The exact time when the session entered Active status. Data type: DateTime. Data length: unspecified.

- **Total Time**
  The amount of time that the collaborating technician spent in the session. Data type: DateTime. Data length: unspecified.

- **Session ID**

- **[Name]**
  The name of this column is derived from the following setting: **Global Settings > Custom Fields > Name for name field**. The actual reported value is entered by a customer or technician during session generation. By default this is the name of the customer. Data type: String. Data length: 128 characters.

- **Technician Name**
  The technician's name as recorded in the **Name** field on the Organization tab. Data type: String. Data length: 128 characters.

- **Technician ID**

- **Technician Email**
  The email address of the technician. For approved technicians, the email is recorded in the **Email** field on the **Organization** tab. For unlisted technicians, the email is recorded during the invitation process. Data type: String. Data length: 128 characters.

- **Chat Log**
  The Collaboration Chat Log contains full details of the collaboration session, including system messages, chat between technicians, and chat between technicians and customer. Click the icon to view the log. Data type: String. Data length: 2048 characters.

**Sample Collaboration Chat Log**

This sample shows the Collaboration Chat Log for the same session as shown in the sample for the **Chat Log** report. Notice that the perspective is that of the Collaborating Technician.
9:19 AM Incoming collaboration session from: Technician 1
9:19 AM Connecting to: [...] 
9:19 AM Connected to Applet (RSA 2048 bits, AES256-SHA 256 bits)
9:19 AM Switched to P2P 
9:19 AM «Technician 1»: This is between technicians
9:20 AM «Technician 2»: This is between technicians
9:20 AM Technician 1: This is between technician and customer
9:20 AM Technician 2: This is between technician and customer
9:20 AM Customer: This is from the customer to the technicians
9:20 AM The Lead Technician ended the session
9:20 AM Disconnected (Applet)
9:21 AM The technician ended the session.

---

Custom Fields Report

This report returns data entered into Custom Fields for individual sessions conducted by members of the selected unit during the selected period.

Each row represents a set of data submitted during a unique session.

- **Start Time**: The exact time when the session entered Active status. Data type: DateTime. Data length: unspecified.
- **End Time**: The exact time when the session entered Closed or Timed Out status. Data type: DateTime. Data length: unspecified.
- **Total Time**: The sum of Active Time, Hold Time, Time in Transfer, Rebooting Time, and Reconnecting Time; excluding Connecting and Waiting time. This is not the same as Total Time as shown in the Technician Console Session List. Data type: DateTime. Data length: unspecified.
- **Session ID**: An automatically generated, unique identification number. Data type: Integer. Data length: unspecified.
- **[Name]**: The name of this column is derived from the following setting: **Global Settings > Custom Fields > Name for name field**. The actual reported value is entered by a customer or technician during session generation. By default this is the name of the customer. Data type: String. Data length: 128 characters.
- **[Custom Fields]**: The names of these columns are derived from the following settings: **Global Settings > Custom Fields > Name for custom field**. Data type: String. Data length: 64 characters.
- **Tracking ID**: A custom field used for mapping Rescue sessions to a CRM system or for other custom administrative purposes. Data type: String. Data length: 256 characters.
- **Technician Name**: The technician’s name as recorded in the Name field on the Organization tab. Data type: String. Data length: 128 characters.
- **Technician Email**: The email address of the technician. For approved technicians, the email is recorded in the Email field on the Organization tab. For unlisted technicians, the email is recorded during the invitation process. Data type: String. Data length: 128 characters.

---

Copyright © 2020 LogMeIn, Inc.
Missed Sessions Report (List All)

This report returns data for each individual session missed by members of the selected unit during the selected period.

A missed session is any session that enters the queue and never enters Active status.

Each row represents a missed session.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start Time</td>
<td>The exact time when the session entered Waiting status. Data type: DateTime. Data length: unspecified.</td>
</tr>
<tr>
<td>End Time</td>
<td>The exact time when the customer ended the session (Closed status), or when the session timed out (Timed Out status). Data type: DateTime. Data length: unspecified.</td>
</tr>
<tr>
<td>Waiting Time</td>
<td>The length of time from Start Time to End Time. Data type: DateTime. Data length: unspecified.</td>
</tr>
<tr>
<td>Session Type</td>
<td>The customer-side technology applied. Data type: String. Data length: 100 characters. Possible values are as follows: Mobile Applet, Calling Card, Instant Chat, Unattended, Applet On LAN, Applet</td>
</tr>
<tr>
<td>Status</td>
<td>The final status at the time of session end. Data type: String. Data length: 64 characters.</td>
</tr>
<tr>
<td>[Name]</td>
<td>The name of this column is derived from the following setting: Global Settings &gt; Custom Fields &gt; Name for name field. The actual reported value is entered by a customer or technician during session generation. By default this is the name of the customer. Data type: String. Data length: 128 characters.</td>
</tr>
<tr>
<td>[Custom Fields]</td>
<td>The names of these columns are derived from the following settings: Global Settings &gt; Custom Fields &gt; Name for custom field. Data type: String. Data length: 64 characters.</td>
</tr>
<tr>
<td>Tracking ID</td>
<td>A custom field used for mapping Rescue sessions to a CRM system or for other custom administrative purposes. Data type: String. Data length: 256 characters.</td>
</tr>
<tr>
<td>Private Session</td>
<td>For Private Sessions, this column lists the name of the initiating technician. Data type: String. Data length: 128 characters.</td>
</tr>
<tr>
<td>Channel</td>
<td>For Channel Sessions, the name of the incoming channel. Data type: String. Data length: 64 characters.</td>
</tr>
<tr>
<td>Technician Group</td>
<td>The name of the Technician Group to which the technician belonged at the time of the missed session. Data type: String. Data length: 128 characters.</td>
</tr>
</tbody>
</table>
Missed Sessions Report (Summary)

This report returns **cumulative** data for all sessions missed by members of the selected unit during the selected period.

A missed session is any session that enters the queue and never enters Active status.

**Number of Missed Sessions**  
The total number of sessions that were never activated by a technician.  
Data type: Integer. Data length: unspecified.

**Average Waiting Time**  
Average time customers waited before abandoning the session or timing out. Data type: DateTime. Data length: unspecified.

**Total Waiting Time**  
Total time customers waited before abandoning the session or timing out. Data type: DateTime. Data length: unspecified.

**Longest Session**  
The longest time any one customer waited before abandoning the session or timing out. Data type: DateTime. Data length: unspecified.

Transferred Sessions Report

This report returns data for each transfer executed by a member of the selected unit during the selected period.

Each row represents one transfer event.

**Session ID**  

**Time of Transfer**  
The exact time of the transfer event. Data type: DateTime. Data length: unspecified.

**Waiting Time**  
The length of time before the customer either abandons the session or is transferred again. Data type: DateTime. Data length: unspecified.

**[Name]**  
The name of this column is derived from the following setting: Global Settings > Custom Fields > Name for name field. The actual reported value is entered by a customer or technician during session generation. By default this is the name of the customer. Data type: String. Data length: 128 characters.

**Transferred by**  
The entity that initiated the transfer. The value System is returned for channel sessions that are automatically transferred according to rules set at Settings > Session Management > Auto-transfer waiting sessions. Data type: String. Data length: 128 characters.

**Transferred from**  
The technician or channel from which the session was transferred. Data type: String. Data length: 128 characters.

**Transferred to**  
The technician or channel to which the session was transferred. Data type: String. Data length: 128 characters.

**Transfer Comment**  

**Time in Transfer**  
The length of time in Transfer. Data type: DateTime. Data length: unspecified.
Transferred Sessions - Extended Report

This report returns data for each transfer executed by a member of the selected unit during the selected period.

Each row represents one transfer event.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time of Transfer</td>
<td>The exact time of the transfer event. Data type: DateTime. Data length: unspecified.</td>
</tr>
<tr>
<td>Waiting Time</td>
<td>The length of time before the customer either abandons the session or is transferred again. Data type: DateTime. Data length: unspecified.</td>
</tr>
<tr>
<td>[Name]</td>
<td>The name of this column is derived from the following setting: Global Settings &gt; Custom Fields &gt; Name for name field. The actual reported value is entered by a customer or technician during session generation. By default this is the name of the customer. Data type: String. Data length: 128 characters.</td>
</tr>
<tr>
<td>Transferred by - Technician ID</td>
<td>An automatically generated, unique identification number of the technician that initiated the transfer. Data type: Integer. Data length: unspecified.</td>
</tr>
<tr>
<td>Transferred by</td>
<td>The entity that initiated the transfer. The value System is returned for channel sessions that are automatically transferred according to rules set at Settings &gt; Session Management &gt; Auto-transfer waiting sessions. Data type: String. Data length: 128 characters.</td>
</tr>
<tr>
<td>Transferred from - Technician/Channel ID</td>
<td>An automatically generated, unique identification number of the technician or channel from which the session was transferred. Data type: Integer. Data length: unspecified.</td>
</tr>
<tr>
<td>Transferred from</td>
<td>The technician or channel from which the session was transferred. Data type: String. Data length: 128 characters.</td>
</tr>
<tr>
<td>Transferred to - Technician/Channel ID</td>
<td>An automatically generated, unique identification number of the technician or channel to which the session was transferred. Data type: Integer. Data length: unspecified.</td>
</tr>
<tr>
<td>Transferred to</td>
<td>The technician or channel to which the session was transferred. Data type: String. Data length: 128 characters.</td>
</tr>
<tr>
<td>Time in Transfer</td>
<td>The length of time in Transfer. Data type: DateTime. Data length: unspecified.</td>
</tr>
<tr>
<td>Transferred from - Technician Group ID</td>
<td>An automatically generated, unique identification number of the technician group from which the session was transferred. Data type: Integer. Data length: unspecified.</td>
</tr>
<tr>
<td>Transferred from - Technician Group</td>
<td>The Technician Group from which the session was transferred. Data type: String. Data length: 128 characters.</td>
</tr>
</tbody>
</table>
### Technician Survey Report (List All)

This report returns the results of individual technician surveys (technician session evaluations) submitted by members of the selected unit during the selected period. Each row represents one submitted survey.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source</td>
<td>The name of the Technician Group the technician belonged to at the time of submitting the survey. Data type: String. Data length: 128 characters.</td>
</tr>
<tr>
<td>Note</td>
<td><strong>Note:</strong> For Technician Survey Reports concerning periods before 12 August 2014, the value <em>Technicians</em> is returned when a global survey is assigned to all technicians in an organization.</td>
</tr>
<tr>
<td>Date</td>
<td>The date and time when the technician submitted the survey. Data type: DateTime. Data length: unspecified.</td>
</tr>
<tr>
<td>[Name]</td>
<td>The name of this column is derived from the following setting: <strong>Global Settings &gt; Custom Fields &gt; Name for name field</strong>. The actual reported value is entered by a customer or technician during session generation. By default this is the name of the customer. Data type: String. Data length: 128 characters.</td>
</tr>
<tr>
<td>[Survey Columns]</td>
<td>These variable columns will show responses to the survey questions defined on the Settings tab under Session evaluation by technician. Data type: String. Data length: 128 characters.</td>
</tr>
<tr>
<td>Technician Name</td>
<td>The technician's name as recorded in the Name field on the Organization tab. Data type: String. Data length: 128 characters.</td>
</tr>
<tr>
<td>Technician Email</td>
<td>The technician's email address as recorded in the Email field on the Organization tab. Data type: String. Data length: 128 characters.</td>
</tr>
</tbody>
</table>

### Failed Sessions Report (List All)

This report returns data for each individual session that fails during Connecting status for members of the selected unit during the selected period.
A Failed session is any session successfully submitted by the customer, but which never proceeds from Connecting to Waiting status.

Note: A session enters Connecting status when the customer begins downloading the Applet.

**Start Time**
The exact time when the session entered Connecting status. Data type: DateTime. Data length: unspecified.

**Session ID**

**Session Type**
The customer-side technology applied. Data type: String. Data length: 100 characters.

**Status**
The final status at the time of session end. Data type: String. Data length: 64 characters.

[Name]
The name of this column is derived from the following setting: Global Settings > Custom Fields > Name for name field. The actual reported value is entered by a customer or technician during session generation. By default this is the name of the customer. Data type: String. Data length: 128 characters.

[Custom Fields]
The names of these columns are derived from the following settings: Global Settings > Custom Fields > Name for custom field. Data type: String. Data length: 64 characters.

**Customer IP**
The customer's IP address. Data type: String. Data length: 15 characters.

**Private Session**
For Private Sessions, the name of the technician who initiated the failed session. Data type: String. Data length: 128 characters.

**Channel**
For Channel Sessions, the name of the incoming channel. Data type: String. Data length: 64 characters.

---

**Failed Sessions Report (Summary)**

This report returns cumulative data for all sessions that fail during Connecting status for members of the selected unit during the selected period.

A Failed session is any session successfully submitted by the customer, but which never proceeds from Connecting to Waiting status.

Note: A session enters Connecting status when the customer begins downloading the Applet.

**Number of Failed Sessions**
The total number of failed sessions for members of the selected unit during the selected period. Data type: Integer. Data length: unspecified.

**Average Connecting Time**
The average time spent in Connecting status before failure. Data type: DateTime. Data length: unspecified.

**Total Connecting Time**
The total time spent in Connecting status before failure. Data type: DateTime. Data length: unspecified.
Failed Sessions - Extended

This report returns data for each individual session that fails during Connecting status for members of the selected unit during the selected period.

A Failed session is any session successfully submitted by the customer, but which never proceeds from Connecting to Waiting status.

**Note:** A session enters Connecting status when the customer begins downloading the Applet.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start Time</td>
<td>The exact time when the session entered Connecting status. Data type: DateTime. Data length: unspecified.</td>
</tr>
<tr>
<td>Session Type</td>
<td>The customer-side technology applied. Data type: String. Data length: 100 characters.</td>
</tr>
<tr>
<td>Status</td>
<td>The final status at the time of session end. Data type: String. Data length: 64 characters.</td>
</tr>
<tr>
<td>[Name]</td>
<td>The name of this column is derived from the following setting: Global Settings &gt; Custom Fields &gt; Name for name field. The actual reported value is entered by a customer or technician during session generation. By default this is the name of the customer. Data type: String. Data length: 128 characters.</td>
</tr>
<tr>
<td>[Custom Fields]</td>
<td>The names of these columns are derived from the following settings: Global Settings &gt; Custom Fields &gt; Name for custom field. Data type: String. Data length: 64 characters.</td>
</tr>
<tr>
<td>Private Session Technician Name</td>
<td>For Private Sessions, the name of the technician who initiated the failed session. Data type: String. Data length: 128 characters.</td>
</tr>
<tr>
<td>Channel</td>
<td>For Channel Sessions, the name of the incoming channel. Data type: String. Data length: 64 characters.</td>
</tr>
<tr>
<td>Technician Email</td>
<td>The technician's email address as recorded in the Email field on the Organization tab. Data type: String. Data length: 128 characters.</td>
</tr>
<tr>
<td>Technician Group ID</td>
<td>An automatically generated, unique identification number of the Technician Group to which the technician belonged at the time of generating the report. Data type: Integer. Data length: unspecified.</td>
</tr>
<tr>
<td>Technician Group</td>
<td>The name of the Technician Group to which the technician belonged at the time of generating the report. Data type: String. Data length: 128 characters.</td>
</tr>
</tbody>
</table>

External Technician Chatlog Report

This report retrieves the chat log and session notes for the selected period for each unique session conducted with an external technician.

You can run external technician chat log reports on your Rescue technicians and on invited external technicians. When you run a report on external technicians, only those sessions will be listed where
the invited technician was approved. When you run a report on your Rescue technicians, sessions with unlisted external technicians will also be listed.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Start Time</strong></td>
<td>The exact time when the session entered Collaborating status for the external technician. Data type: DateTime. Data length: unspecified.</td>
</tr>
<tr>
<td><strong>End Time</strong></td>
<td>The exact time when the session entered Closed or Timed Out status for the external technician. Data type: DateTime. Data length: unspecified.</td>
</tr>
<tr>
<td><strong>Total Time</strong></td>
<td>The sum of Active Time, Hold Time, Rebooting Time, and Reconnecting Time; excluding Waiting time. This is not the same as Total Time as shown in the Technician Console Session List. Data type: DateTime. Data length: unspecified.</td>
</tr>
<tr>
<td><strong>Session ID</strong></td>
<td>An automatically generated, unique identification number. Data type: Integer. Data length: unspecified.</td>
</tr>
<tr>
<td><strong>[Name]</strong></td>
<td>The name of this column is derived from the following setting: Global Settings &gt; Custom Fields &gt; Name for name field. The actual reported value is entered by a customer or technician during session generation. By default this is the name of the customer. Data type: String. Data length: 128 characters.</td>
</tr>
<tr>
<td><strong>External Technician Name</strong></td>
<td>The name of the external technician. For approved external technicians, the name is recorded in the Name field on the Organization tab. For unlisted technicians, the name is recorded during the invitation process. Data type: String. Data length: 128 characters.</td>
</tr>
<tr>
<td><strong>External Technician Email</strong></td>
<td>The email address of the external technician. For approved external technicians, the email is recorded in the Email field on the Organization tab. For unlisted technicians, the email is recorded during the invitation process. Data type: String. Data length: 128 characters.</td>
</tr>
<tr>
<td><strong>Inviter's Name</strong></td>
<td>The technician's name who invited the external technician. Data type: String. Data length: 128 characters.</td>
</tr>
<tr>
<td><strong>Inviter's Email</strong></td>
<td>The technician's email address who invited the external technician. Data type: String. Data length: 128 characters.</td>
</tr>
<tr>
<td><strong>Chat Log</strong></td>
<td>An icon is displayed if a Chat Log is available. Click the icon to view the log. Data type: String. Data length: 2048 characters.</td>
</tr>
</tbody>
</table>

**Audit Report (List All)**

This report returns data for each action taken by Administrators on the selected item of the Organization Tree during the selected period.

**Note:** Company-level actions only appear in the report when the report is generated either for the Administrator who performed the action, or for the root-level Master Administrators organizational unit.

**Requested by** The Administrator that performed the given action. The displayed value is the Administrator's name as recorded in the Name field on the Organization tab. Data type: String. Data length: 128 characters.
**Entity type**
The type of organizational entity affected by the action taken by an Administrator. Data type: String. Data length: 128 characters. Possible values are as follows:
- Channel
- Technician Group
- Technician
- Unattended Computer Group
- Unattended Computer
- Administrator Group
- Master Administrator
- Administrator
- Administrator Group link
- Administrator link
- External Technician Group
- External Technician
- External link

**Entity ID**
An automatically generated, unique ID of the organizational entity affected by the action taken by an Administrator. Data type: Integer. Data length: Unspecified.

**Entity name**
The name of the organizational entity affected by the action taken by an Administrator. The displayed value is the organizational entity's name as recorded in the **Name** field on the Organization tab. Data type: String. Data length: 256 characters.

**Change type**
The type of change action taken by the Administrator. Data type: String. Data length: 128 characters. Possible values are as follows:
- Add
- Delete
- Move
- Copy
- Assign
- Unassign
- Change
- View

**Last changed**
The exact time when the change action took place. Data type: DateTime. Data length: unspecified.

**Section**
The header in the Rescue Administration Center under which the change was made. Data type: String. Data Length: unspecified.

**Field**
The field under the **Section** header in the Rescue Administration Center that was affected by the change. Data type: String. Data Length: unspecified.

**Old Value**
The value of **Field** before the change action took place. Data type: String. Data Length: unspecified.

**Old Action**
The status of **Field** before the change action took place. Data type: String. Data Length: unspecified. Possible values are as follows:
- Enabled
- Disabled
- Selected
Rebooting/Reconnecting Report

This report returns data for each unique reconnecting or rebooting event that occurred during a session conducted by members of the selected unit during the selected period.

Each row represents a unique reconnecting/rebooting event.

**Session ID**

**[Custom Fields]**
The names of these columns are derived from the following settings: Global Settings > Custom Fields > Name for custom field. Data type: String. Data length: 64 characters.

**Technician Name**
The technician's name as recorded in the Name field on the Organization tab. Data type: String. Data length: 128 characters.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technician Email</td>
<td>The email address of the technician. For approved technicians, the email is recorded in the Email field on the Organization tab. For unlisted technicians, the email is recorded during the invitation process. Data type: String. Data length: 128 characters.</td>
</tr>
<tr>
<td>Channel ID</td>
<td>The Channel ID of the channel used during the session. Data type: Integer. Data length: unspecified.</td>
</tr>
<tr>
<td>Channel Name</td>
<td>The name of the channel used during the session. Data type: String. Data length: 64 characters.</td>
</tr>
<tr>
<td>Technician Group</td>
<td>The name of the Technician Group to which the technician belonged at the time of the session. Data type: String. Data length: 128 characters.</td>
</tr>
<tr>
<td>Start Time</td>
<td>The exact time when the session entered Active status. Data type: DateTime. Data length: unspecified.</td>
</tr>
<tr>
<td>End Time</td>
<td>The exact time when the session entered Closed or Timed Out status. Data type: DateTime. Data length: unspecified.</td>
</tr>
</tbody>
</table>
| Last Action Time     | The exact time of the action that ended the technician's state of being "in action". A technician is in action if he is in a session, and for that session the Technician Console and the Applet have a working connection (that is, the sockets between the Technician Console and Applet are connected). Any of the following ends the technician's "in action" state:  
  • The technician's status Changes to "Away".  
  • The technician loses connection with customer.  
  • The session tab gets unselected, or the TC goes to background while there is no active tear-away window of the session.  
  • The tear-away window of the session gets inactive while either the session tab is unselected or the TC is in the background.  
  • The technician or Administrator ends, holds, or transfers the session.  
  Data type: DateTime. Data length: unspecified.                          |
| Event type           | The type of event that triggered the report entry. Data type: String. Data length: unspecified. Possible values are as follows:    
  • Rebooting  
  • Reconnecting                                                        |
| Rebooting/Reconnecting Start Time | The exact time when the session entered Rebooting/Reconnecting status. Data type: DateTime. Data length: unspecified. |
| Rebooting/Reconnecting End Time | The exact time when the session moved to the next status from Rebooting/Reconnecting status. Data type: DateTime. Data length: unspecified. |

**Technician Status Report**

This report delivers cumulative status data for members of the selected unit for the selected period. Each row represents one technician.
### Technician ID

**Tip:** This node ID is displayed when you hover over the technician on the Organization Tree.

### Technician Name
The technician's name as recorded in the Name field on the Organization tab. Data type: String. Data length: 128 characters.

### Technician Email
The email address of the technician as recorded in the Email field on the Organization tab. Data type: String. Data length: 128 characters.

### Parent Group
The name of the Technician Group to which the technician belonged at the time of generating the report. Data type: String. Data length: 128 characters.

### Status
The status of the technician at the time of generating the report. Possible values are as follows:
- Active
- Inactive

Data type: String. Data length: 8 characters.

### Type
The type of user for whom data is retrieved. Possible values are as follows:
- Technician
- Administrator
- Master Administrator

Data type: String. Data length: 22 characters.

### Last Login Time
The time when the technician last logged in to the Rescue Technician Console. Data type: DateTime. Data length: unspecified.

### Last Used Technician Console Version
The version of the Technician Console to which the technician last logged in. Data type: String. Data length: 50 characters.

---

### Administrator Status Report
This report delivers cumulative status data for members of the selected unit for the selected period. Each row represents one Administrator.

### Administrator ID

**Tip:** This node ID is displayed when you hover over the Administrator on the Organization Tree.

### Administrator Name
The Administrator's name as recorded on the Name field of the Organization tab.

### Administrator Email
The email address of the Administrator as recorded in the Email field on the Organization tab. Data type: String. Data length: 128 characters.
<table>
<thead>
<tr>
<th><strong>Status</strong></th>
<th>The status of the Administrator at the time of generating the report. Possible values are as follows:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Active</td>
</tr>
<tr>
<td></td>
<td>• Inactive</td>
</tr>
<tr>
<td></td>
<td>Data type: String. Data length: 8 characters.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Type</strong></th>
<th>The type of user for whom data is retrieved. Possible values are as follows:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Technician</td>
</tr>
<tr>
<td></td>
<td>• Administrator</td>
</tr>
<tr>
<td></td>
<td>• Master Administrator</td>
</tr>
<tr>
<td></td>
<td>Data type: String. Data length: 22 characters.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Linked to</strong></th>
<th>The name of the Technician Group to which the Administrator is assigned.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Data type: String.</td>
</tr>
</tbody>
</table>

| **Last Login Time** | The exact time of the Administrator's last login to Rescue. Data type: DateTime. Data length: unspecified. |
Integration and API

See also the *Customization and Integration Guide*  (English and Japanese only).
For API documentation see the *LogMeIn Rescue API Guide*  (English only).

Setting up Single Sign-On Authentication

Using Single Sign-on, support technicians can securely log in to LogMeIn Rescue from other applications.
In the world of enterprise IT, many companies end up with multiple, disparate systems that all require
their own separate authentication. This proves to be a challenge for both administrators and end users.
LogMeIn Rescue’s Single Sign-on (SSO) capability helps you manage this issue.

Options

Setup takes place in the Administration Center on the Global Settings tab under Single Sign-On.
You have control over how technicians and administrators can log in to Rescue.
Here is a summary of options available under Global Settings > Single Sign-On > Allowed login method:

• Option One: **Standard or SSO**
  • Users will be able to login with either their standard Rescue email/password or their SSO ID. Both methods are valid.
  • Remember: When allowing SSO you must set a Master SSO password (on the Global Settings tab) and assign an SSO ID per user (on the Organization tab). Users without an SSO ID are unable to use SSO.

• Option Two: **SSO only**
  • Users will be able to login using their SSO ID only. With this option, users without an SSO ID will be unable to login.
  • Remember: When allowing SSO you must set a Master SSO password (on the Global Settings tab) and assign an SSO ID per user (on the Organization tab).

• Option Three: **SSO only** plus Allow users without an SSO ID to use standard login
  • Users with an SSO ID will be able to login using their SSO ID only.
  • Users without an SSO ID will be able to use standard login.

How it Works

SSO functionality makes use of API technology.

• The company-hosted script makes an HTTP request to the SSO login services
• SSO login service confirms the successful login and retrieves the login URL, or an error message upon failure
• The company-hosted script then evaluates the returned value
• If successful, the company-hosted script redirects the user to the URL provided, or if unsuccessful, error handling is triggered
The HTTP request is a simple formatted URL string, which contains the SSO URL, SSOID, CompanyID, and SSO Password.

**Single Sign-on URL (SSO URL)**

For logging in to the web-based Technician Console:
https://secure.logmeinrescue.com/SSO/GetLoginTicket.aspx

For logging in to the Desktop Technician Console:
https://secure.logmeinrescue.com/SSO/GetDTCLoginTicket.aspx

**Single Sign-on ID (SSOID)**

The ID you define in the **Single Sign-On ID** box on the **Organization** tab of the Administration Center when adding or editing organization members.

**CompanyID**

See the sample code on the **Global Settings** tab of the Administration Center.

**Master SSO Password**

The SSO password defined on the **Global Settings** tab.

An example of this formatted URL would be:

**In case of logging in to the web-based Technician Console:**

https://secure.logmeinrescue.com/SSO/GetLoginTicket.aspx?
ssoid=123456&Password=secretPassword&CompanyID=654321

**In case of logging in to the Desktop Technician Console:**

- **x86 DTC:**
  https://secure.logmeinrescue.com/SSO/GetDTCLoginTicket.aspx?
  ssoid=123456&Password=secretPassword&CompanyID=654321

- **x64 DTC:**
  https://secure.logmeinrescue.com/SSO/GetDTCLoginTicket.aspx?
  ssoid=123456&Password=secretPassword&CompanyID=654321&arch=64

When making this request, the **SSOID**, **Password**, and **CompanyID** are sent to the Rescue SSO service, which returns a string value. A successful authentication would return a string similar to:

**In case of the web-based Technician Console:**

OK: https://secure.logmeinrescue.com/SSO/Login.aspx?
Ticket=6ab9a0f6-d3ce-4f498-8ea7-b9a76a67a0c8

**In case of the Desktop Technician Console:**

- **x86 DTC:**
  https://secure.logmeinrescue.com/TechConsole/DesktopApp/DownloadSSO.aspx?
  companyid=654321&ticket=4c6f1815-1e0c-43ab-8117-d79b8f523824

- **x64 DTC:**
  https://secure.logmeinrescue.com/TechConsole/DesktopApp/DownloadSSO.aspx?
  companyid=654321&ticket=4c6f1815-1e0c-43ab-8117-d79b8f523824&arch=64

An unsuccessful authentication would return a string similar to:

ERROR: INVALIDPASSWORD

You can then process this string, process for errors, and handle them accordingly. In a typical scenario, you would use an IF condition to process the returned string, and check for the presence of OK: in the first three characters. If they are present, you would then take the URL (the last part of the string you processed) and either present it to the user or redirect them automatically.
Single Sign-On: Considerations

Since Single Sign-on requires a user ID to be authenticated, the logical step is to use Windows credentials. Most programming languages allow you to do this with server-side variables. The key driver is that the server connection needs to be an authenticated connection (not anonymous). This is an integration process through Internet Explorer, which would pass Domain credentials to the Intranet server automatically, provided you do not allow anonymous access. The best approach is to pass the authenticated user ID from your Intranet web server to the SSO service as the SSOID.

Single Sign-On and SAML 2.0

LogMeIn Rescue is compatible with Security Assertion Markup Language (SAML) 2.0. For detailed information about configuring LogMeIn Rescue to use SAML 2.0 with your Identity Provider, see the LogMeIn Rescue Web SSO via SAML 2.0 User Guide.

Note: The final step in the SSO configuration process needs to be performed by the LogMeIn Support team. Please contact your Customer Success Manager or LMI Support for assistance.

Generate API Token

Master Account Holders (MAH) and Master Administrators (MA) can generate a secret token that is used to authenticate the Rescue user and to prevent them from logging out if there is a timeout. This feature serves the same purpose as the requestAuthCode API call, but this code is shown to the MAH or MA only upon creation and will not be visible once they leave the page, thus increasing security.

1. To generate an API token, select the Global Settings tab in the Administration Center.
2. Under Generate API token, click Generate and Copy
   A new API token is generated, displayed, and automatically copied to your clipboard.
3. Optionally, select either or both from the following restrictions.
   - Select Deny access to the requestAuthcode endpoint to force your users to use the token obtained from Generate API token in API calls that require an AuthCode.
     
     Important: Users will not be able to use the requestAuthCode API endpoint.

   - Select Deny access to the login endpoint to stop users from being able to log in via the login API call.
     
     Remember: Users will still be able to use the Rescue website login.

For more information about the related API calls, see:

Sending Session Data to a URL (Post-to-URL)

About Post-to-URL
The Post to URL function is used in conjunction with CRM Integration APIs (particularly requestPINCode) to provide a complete set of integration tools for CRMs or other applications.

Post to URL allows you to host your own server script to handle the Rescue session data and to process them as you see fit. Some potential use examples include database importing and email notifications.

How it Works
• The Rescue technician starts a support session
• At the beginning and/or end of a session, the session data are transferred via HTTP Post or XML to the specified URL
• Your script processes the data as specified in your code

Post-to-URL Variables
These are the variables that are submitted via the Post to URL function.

[... ] is replaced with the actual data value. This method does an XML request to your URL. You would handle this via an XML parser.

<table>
<thead>
<tr>
<th>Rescue Session Data</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;sessionid&gt; [... ] &lt;/sessionid&gt;</td>
<td>Rescue Session ID</td>
</tr>
<tr>
<td>&lt;techid&gt; [... ] &lt;/techid&gt;</td>
<td>Technician ID</td>
</tr>
<tr>
<td>&lt;techssoid&gt; [... ] &lt;/techssoid&gt;</td>
<td>Technician Single Sign-on ID (as defined on the Organization tab in the Administration Center)</td>
</tr>
<tr>
<td>&lt;techname&gt; [... ] &lt;/techname&gt;</td>
<td>Technician name (as defined on the Organization tab)</td>
</tr>
<tr>
<td>&lt;techemail&gt; [... ] &lt;/techemail&gt;</td>
<td>Technician email (as defined on the Organization tab)</td>
</tr>
<tr>
<td>&lt;techdescr&gt; [... ] &lt;/techdescr&gt;</td>
<td>Technician description (as defined on the Organization tab)</td>
</tr>
<tr>
<td>&lt;cfield0&gt; [... ] &lt;/cfield0&gt;</td>
<td>Value returned for the Name field (as defined on the Global Settings tab in the Administration Center)</td>
</tr>
<tr>
<td>&lt;cfield1&gt; [... ] &lt;/cfield1&gt;</td>
<td>Value returned for Custom field 1 (as defined on the Global Settings tab)</td>
</tr>
<tr>
<td>&lt;cfield2&gt; [... ] &lt;/cfield2&gt;</td>
<td>Value returned for Custom field 2 (as defined on the Global Settings tab)</td>
</tr>
<tr>
<td>&lt;cfield3&gt; [... ] &lt;/cfield3&gt;</td>
<td>Value returned for Custom field 3 (as defined on the Global Settings tab)</td>
</tr>
<tr>
<td>&lt;cfield4&gt; [... ] &lt;/cfield4&gt;</td>
<td>Value returned for Custom field 4 (as defined on the Global Settings tab)</td>
</tr>
<tr>
<td>Description</td>
<td>Value</td>
</tr>
<tr>
<td>----------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>Value returned for Custom field 5 (as defined on the Global Settings tab)</td>
<td>&lt;cfield5&gt;...&lt;/cfield5&gt;</td>
</tr>
<tr>
<td>Value returned for the Tracking field; typically used for mapping Rescue</td>
<td>&lt;tracking0&gt;...&lt;/tracking0&gt;</td>
</tr>
<tr>
<td>sessions to a CRM</td>
<td></td>
</tr>
<tr>
<td>Transcript of all chat held since the previous post</td>
<td>&lt;chatlog&gt;...&lt;/chatlog&gt;</td>
</tr>
<tr>
<td>Notes saved by the technician</td>
<td>&lt;notes&gt;...&lt;/notes&gt;</td>
</tr>
<tr>
<td>From the beginning of Waiting status until session start (Active status)</td>
<td>&lt;waitingtime&gt;...&lt;/waitingtime&gt;</td>
</tr>
<tr>
<td>in seconds</td>
<td></td>
</tr>
<tr>
<td>The exact time when the session entered Active status (UTC)</td>
<td>&lt;pickuptime&gt;...&lt;/pickuptime&gt;</td>
</tr>
<tr>
<td>The exact time when the session entered Closed or Timed Out status (UTC)</td>
<td>&lt;closingtime&gt;...&lt;/closingtime&gt;</td>
</tr>
<tr>
<td>Actual Technician Console utilization time during the session (until the</td>
<td>&lt;worktime&gt;...&lt;/worktime&gt;</td>
</tr>
<tr>
<td>post) in seconds</td>
<td></td>
</tr>
<tr>
<td>The exact time of the last action taken by the technician in the Technician</td>
<td>&lt;lastactiontime&gt;...&lt;/lastactiontime&gt;</td>
</tr>
<tr>
<td>Console (UTC)</td>
<td></td>
</tr>
<tr>
<td>Amount of data transmitted during the session (until the post) in bytes</td>
<td>&lt;transmitted&gt;...&lt;/transmitted&gt;</td>
</tr>
<tr>
<td>The platform of the customer device</td>
<td>&lt;platform&gt;...&lt;/platform&gt;</td>
</tr>
<tr>
<td>Value returned for Technician Survey Question 1 (as defined on the Settings</td>
<td>&lt;tsurvey0&gt;...&lt;/tsurvey0&gt;</td>
</tr>
<tr>
<td>tab)</td>
<td></td>
</tr>
<tr>
<td>Value returned for Technician Survey Question 2</td>
<td>&lt;tsurvey1&gt;...&lt;/tsurvey1&gt;</td>
</tr>
<tr>
<td>Value returned for Technician Survey Question 3</td>
<td>&lt;tsurvey2&gt;...&lt;/tsurvey2&gt;</td>
</tr>
<tr>
<td>Value returned for Technician Survey Question 4</td>
<td>&lt;tsurvey3&gt;...&lt;/tsurvey3&gt;</td>
</tr>
<tr>
<td>Value returned for Technician Survey Question 5</td>
<td>&lt;tsurvey4&gt;...&lt;/tsurvey4&gt;</td>
</tr>
<tr>
<td>Value returned for Technician Survey Question 6</td>
<td>&lt;tsurvey5&gt;...&lt;/tsurvey5&gt;</td>
</tr>
<tr>
<td>Value returned for Technician Survey Question 7</td>
<td>&lt;tsurvey6&gt;...&lt;/tsurvey6&gt;</td>
</tr>
<tr>
<td>Value returned for Technician Survey Question 8</td>
<td>&lt;tsurvey7&gt;...&lt;/tsurvey7&gt;</td>
</tr>
<tr>
<td>Value returned for Technician Survey Question 9</td>
<td>&lt;tsurvey8&gt;...&lt;/tsurvey8&gt;</td>
</tr>
<tr>
<td>Value returned for Technician Survey Question 10</td>
<td>&lt;tsurvey9&gt;...&lt;/tsurvey9&gt;</td>
</tr>
</tbody>
</table>

**HTTP Post based**

This method submits the URL with the POST variables on the end. This is the same as submitting an HTML form. The variables use the same naming convention as the XML format.

```
&TechDescr=[...]&CField0=[...]&CField1=[...]&CField2=[...]&CField3=[...]&CField4=[...]
&CField5=[...]&Tracking0=[...]&ChatLog=[...]&Notes=[...]&WaitingTime=[...]
&PickupTime=[...]&ClosingTime=[...]&WorkTime=[...]&LastActionTime=[...]&Transmitted=[...]
&TSurvey0=[...]&TSurvey1=[...]&TSurvey2=[...]&TSurvey3=[...]&TSurvey4=[...]
&TSurvey5=[...]&TSurvey6=[...]&TSurvey7=[...]&TSurvey8=[...]&TSurvey9=[...]
```
How to Post Session Data to a URL

This feature allows you to take the Rescue session data from your technicians and have them posted to a script you create on your own server.

To implement this feature, knowledge of web forms or XML handling is recommended. This feature requires you to code and host the target page/URL to which Rescue is sending data.

Note: LogMeIn does not support code troubleshooting.

1. On the Organization Tree, select the Technician Group you want to work with.
2. Select the Settings tab.
3. Under Exporting session data, type the URL to which you want to post session details.

   Note: When the Hide post session URLs setting is enabled on the Global Settings tab, users are required to click Show URLs to see or modify the values set for the given Technician Group. Clicking this button is recorded in the Audit Report log. For more information, see How to Hide Post Session URLs on page 126.

You can post data in the following cases:

- Each time a session is started (each time it enters Active status)
- Only when a session is started for the first time (the first time it enters Active status)
- When a session is ended (enters Closed status)
- When a session is suspended by putting it on hold or transferring it to a technician
- When the Technician Console is refreshed or closed

   - Enter a URL your technicians can access. For example: http://webserver/path
   - For authentication, use this format: http://[username]:[password]@webserver/path

4. As appropriate, choose to post session details in one of the following formats:

   - HTML Form parameters
   - XML data
   - JSON

   Restriction: This format is only available with Technician Console version 7.12.3341 and above.

5. By default, the complete chat log is posted. To control how chat data is posted, select from the following options:

   - Select Omit chat text from post to URL to post only system messages. All chat between the technician and customer is excluded.
   - Select Omit chat from Rescue Data Center storage to ensure that only system messages are passed to the Rescue Data Center when a session is transferred or placed on hold, or when the browser that is running the Technician Console is refreshed or closed during a session. Only system messages will be posted at session end.

6. Save your changes.
How to Hide Post Session URLs

Master Administrators can force Administrators to click a dedicated button to see or modify session data URLs in the Exporting session data section of the Settings tab. Viewing or modifying the URLs will be recorded in the Audit Report log. This feature protects sensitive information (such as, username, password, API key) provided in the URLs, and allows companies to track which user viewed or modified these values.

1. Select the Global Settings tab.
2. Under Hide post session URLs, enable the Hide post session URLs setting.
3. Click Save.

Post session URLs are now hidden in the Exporting session data section of the Settings tab. Users need to click Show URLs to see or modify the values set for the given Technician Group.

Integrating Rescue with Other (CRM) Systems

LogMeIn Rescue Integration Services offer you the ability to access your remote support session data through a set of standard web services.

Service options can be called via SOAP and also both HTTP GET and POST methods, making it easy to integrate with your external applications and systems. Login authentication, remote session creation, and session data retrieval are just a few of the available API calls.

Support Statement

Integration with any platform via an API requires development. It is each customer’s responsibility to plan, resource, and develop its own integration effort.

The LogMeIn support team will help you with the following:

• Support can provide general assistance, overview, and documentation
• Support can provide best-effort troubleshooting upon implementation of an integration solution

The LogMeIn support team will not be able to provide detailed assistance, as follows:

• Support cannot provide detailed development support
• Support cannot write code for customers
• Support cannot debug customer code

Each customer remains responsible for building, verifying, and debugging its own custom code.

API Reference

For API documentation and other integration and customization information, see the LogMeIn Rescue API Guide (English only).
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
Administration Center 45
overview 6
administrator 16
administrator group 17
API reference 126
API token 122
APN 40
applet
applying a custom logo and icon 36
choosing the default applet 34
mobile 43
start as Windows System Service 34
audio 45
authcode 122
authentication
API Token 122
for technician monitoring 55
setting a global password policy 25
single-sign-on (SSO) 120
auto-start private sessions 47
auto-start waiting sessions 48
automatic logout 72
automatic transfer 48
away state 72

B
busy state 72

C
calling card
apply installer 86
generate 85
Calling Card 84
deploying to the customer 88
centralized script 93
channels
about 31, 92
activating 31
assigning to a group 31
denying access (individual technician) 32
editing custom fields 76
integrating 31
setting up auto-start logic 48
   Defer auto-start 48
setting up automatic transfer logic 48
setting working hours 49
testing 32
chat
permissions 21
clipboard synchronization behavior 79
Comman Center 56
compact view 27
connecting
   via Calling Card 84
connection methods 46
CRM integration 123, 126
custom fields 76, 77
customer data 13
customer survey 81
customize
applet appearance 36
Calling Card appearance 86
channel code 31
custom fields 76, 77
customer survey 81
informational link 73
Instant Chat 83
mobile applet appearance 43
technician survey 80

default
clipboard synchronization behavior 79
screen recording settings 78
Defer auto-start for Channel sessions 48
disable keys 37
disable wallpaper and visual effects 79
display custom terms of service 43

E
Email 46
enable technicians to use mobile add-on 39
Exempt from session auto-assignment 48
extended 110
extended view 27

F
firmware check 40

H
hierarchy visibility 27

I
Instant Chat
allowed URLs for Instant Chat customization 83
set as default 34
Instant Chat (continued)
  set up and customization 83
  integration 123, 126
  IP address retention 13

J
JSON 125

L
languages
  Administration Center 11
  customer-side settings 12
  set Technician Console language 12
  supported 10
lens 45
Lens 45
Link 46
LogMeIn123 84
logout
  technician 72

M
Mac daemon 34
managing unattended access computers 69
master administrator 15
maximum sessions 72
missing apps 40
mobile
  applet settings 43
mobile add-on
  activating 39
  overview 7
  purchase 39
modify script 93
monitor chat 62
monitoring 56
monitoring technicians
  step-by-step 54
mouse and keyboard priority during remote control 35

N
no technician available 49, 50
notification during desktop monitoring 55

O
organization tree 15

P
password
  setting a global policy 25
Permission 45
permissions
  prompt at start 38
  technician group 18
  Technician Group 86
personal data 13
PIN Code 46
predefined replies and URLs
  create 74
  export 74
  import 74
  manage 74
  share 74
prompt user with uninstall option 43
purchase subscriptions 6

R
report
  audit list all 114
  chatlog 104, 105
  collaboration chat log 106
  custom fields 107
  customer survey issuance list all 96
  customer survey issuance summary 97
  customer survey list all 95
  customer survey summary 95
  external technician chatlog 113
  failed sessions list all 111
  failed sessions summary 112
  generate 94
  login list all 99
  login summary 100
  missed sessions extended list all 113
  missed sessions list all 108, 113
  missed sessions summary 109
  performance list all 97
  performance summary 98
  rebooting 116
  reconnecting 116
  session list all 100
  session summary 103
status
  Administrator 118
  technician 117
report
  technician survey 111
  transferred sessions 109, 110
Rescue Applet
  supported languages 10

S
screen recording settings 78
script collection 92
security
  account 13
  overview 13
session data 13
session limits per technician 72
session management 48
session report 13
sessions
  close 52
  managing 46
  place on hold 52
  start 52
  start automatically 47, 48
    defer auto-start 48
  time-outs 51
  transfer 52
  transfer automatically 48
set authentication method 70
single sign-on (SSO) 120
SMS 46
subscription
  mobile add-on 39
system requirements 8

T

Technician Console
  overview 6
technicians
  adding 22
  editing 22
  import 22
  monitoring a technician's desktop 54
  setting permissions (technician group) 18
  survey completed by 80
terms and conditions 37
terms of service
  mobile 43
time-outs
  alarms 51
  connecting session 51
  idle session 51
  private code 51
  technician 72
  waiting session 51
transfer visibility 27
Two-factor authentication 25, 26
Two-step verification
  Administration Center 25
  Enforce 25
  Reset 26

U
unattended access 67, 69, 70
  about 67
unwanted apps 40

V
VoIP 45

W
wallpaper
  disable 79
Windows System Service 34
working hours 49