

# LogMeIn Rescue Getting Started with Two-Step Verification

User Guide



---

# Contents

<b>Two-Step Verification at a Glance.....</b>	<b>3</b>
<b>How to Enforce Two-Step Verification.....</b>	<b>4</b>
How to Reset Two-Step Verification.....	4
<b>How to Set Up LastPass Authenticator for Rescue Two-Step Verification.....</b>	<b>6</b>

---

## Two-Step Verification at a Glance

Two-step verification is an optional feature that adds a second layer of protection to your Rescue account by requiring members of your organization to set up an additional way of verifying their identity.

This document gives an overview of how to start using Rescue two-step verification. The main steps explained in detail below are:

1. Master Administrators force members of their organization to use two-step verification for logging in to Rescue. This is set up in the Rescue Administration Center.
2. Members of the Rescue organization required to use two-step verification set up the LastPass authenticator app to verify their identity. Setting up the authenticator app is triggered in any of the following cases:
  - The selected member tries to log in to their Rescue account.
  - The selected member tries to log in to the Desktop Technician Console (in case of technicians and Administrators with a technician license).
  - The selected member tries to change their Rescue password.

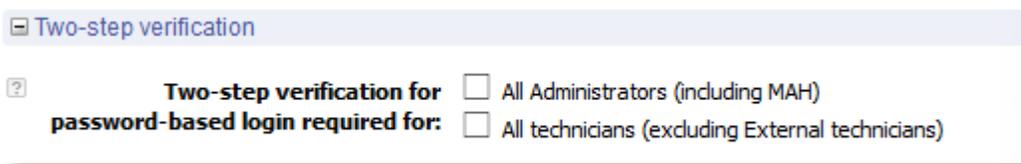
This document focuses on the steps Rescue users (Administrators and technicians) need to take to start using two-step verification. For detailed information on LastPass, visit the [LastPass Support Center](#).

---

## 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.



**Important:** Administrators with both an administrator and a technician license will be required to use two-step verification if either group is selected.

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.

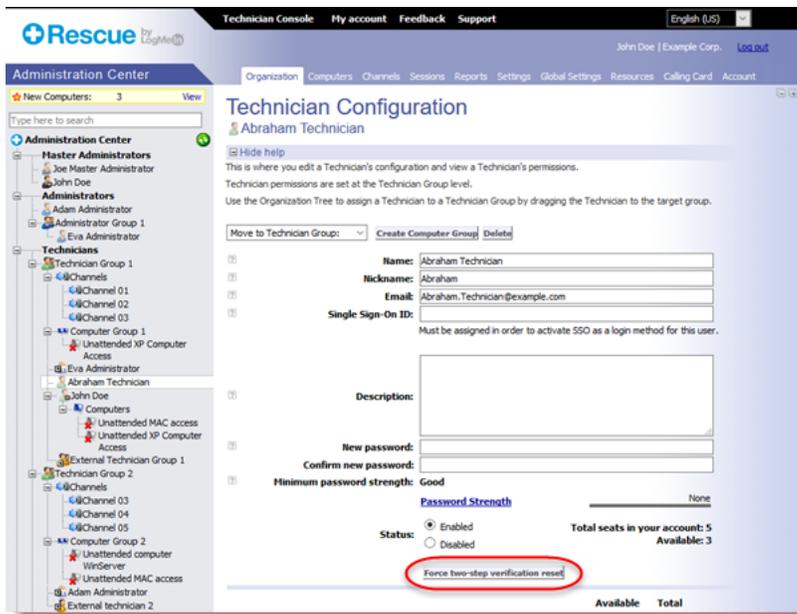
Examples when reinstalling the Authenticator app is necessary:

- 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 Up LastPass Authenticator for Rescue Two-Step Verification

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

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



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

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

---

# Index

## A

Authenticator app 6

## L

LastPass 6

## Q

QR code 6

## S

Security 6

## T

Two-factor authentication 3, 4, 6

Two-step verification 6

Administration Center 4

Enforce 4

overview 3

Reset 4