# LogMeIn Rescue Getting Started with Two-Step Verification

User Guide

LogMeIn®

# Contents

# 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:

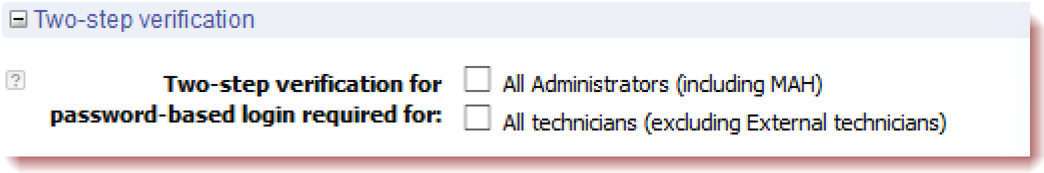
1. Master Administrators force members of their organization to use two-step verification for logging in to Rescue. This is set up in the Rescue Administration Center.
2. Members of the Rescue organization required to use two-step verification set up the LastPass authenticator app to verify their identity. 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.



⊟ Two-step verification

**Two-step verification for password-based login required for:** □ All Administrators (including MAH) □ All technicians (excluding External technicians)

**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

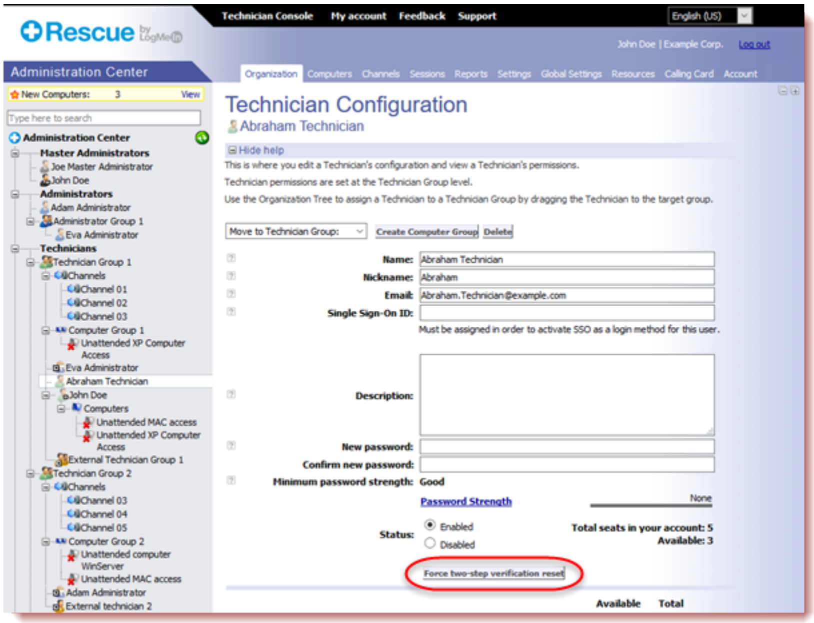
Resetting two-step verification is necessary when a member of the Rescue organization required to use two-step verification needs to reinstall the LastPass Authenticator app.

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.



Technician Configuration

Abraham Technician

⊟ Hide help

This is where you edit a Technician's configuration and view a Technician's permissions.

Technician permissions are set at the Technician Group level.

Use the Organization Tree to assign a Technician to a Technician Group by dragging the Technician to the target group.

Name: Abraham Technician

Nickname: Abraham

Email: Abraham.Technician@example.com

Single Sign-On ID:

Must be assigned in order to activate SSO as a login method for this user.

Description:

New password:

Confirm new password:

Minimum password strength: Good

Password Strength None

Status: ● Enabled ○ Disabled

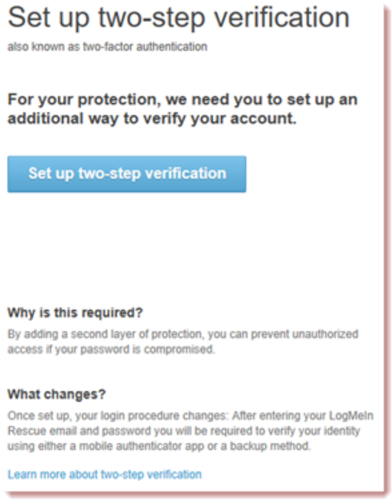
Total seats in your account: 5
Available: 3

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.



Set up two-step verification

also known as two-factor authentication

**For your protection, we need you to set up an additional way to verify your account.**

**Why is this required?**

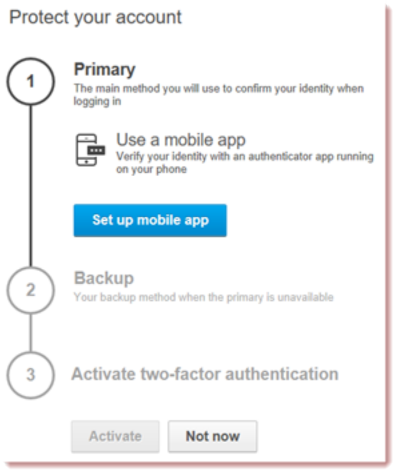
By adding a second layer of protection, you can prevent unauthorized access if your password is compromised.

**What changes?**

Once set up, your login procedure changes: After entering your LogMeIn Rescue email and password you will be required to verify your identity using either a mobile authenticator app or a backup method.

Learn more about two-step verification

2. On the **Set up two-step verification** page, click **Set up two-step verification**.
   The **Protect your account** page is displayed.



Protect your account

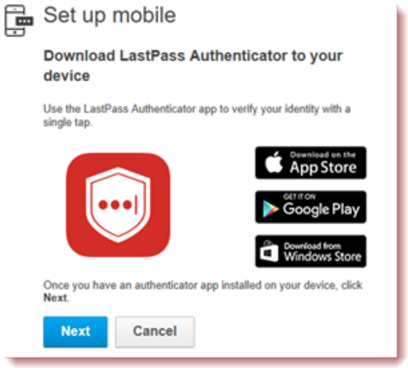
1 **Primary**
The main method you will use to confirm your identity when logging in

Use a mobile app
Verify your identity with an authenticator app running on your phone

2 Backup
Your backup method when the primary is unavailable

3 Activate two-factor authentication

3. On the **Protect your account** page, click **Set up mobile app**.
   The **Set up mobile app** page is displayed.



Set up mobile

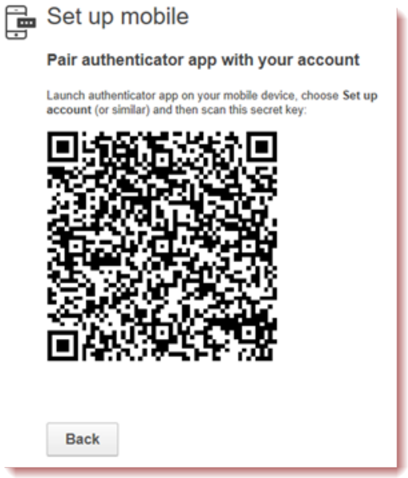
**Download LastPass Authenticator to your device**

Use the LastPass Authenticator app to verify your identity with a single tap.

Once you have an authenticator app installed on your device, click **Next**.

**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:



Set up mobile

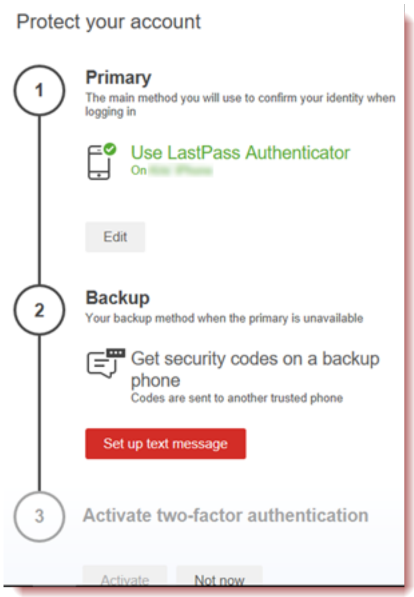
**Pair authenticator app with your account**

Launch authenticator app on your mobile device, choose **Set up account** (or similar) and then scan this secret key:

   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.



Protect your account

1 **Primary**
The main method you will use to confirm your identity when logging in

Use LastPass Authenticator
On [redacted]

Edit

2 **Backup**
Your backup method when the primary is unavailable

Get security codes on a backup phone
Codes are sent to another trusted phone

Set up text message

3 Activate two-factor authentication

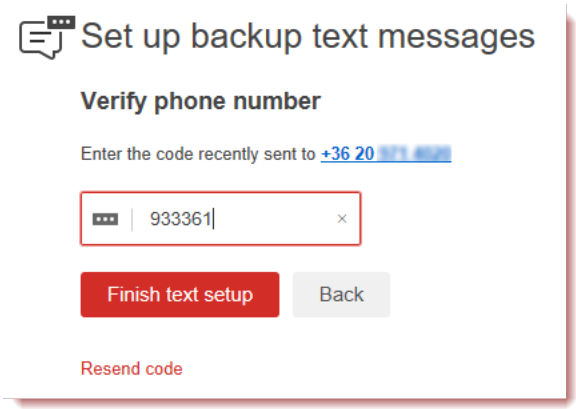
Activate Not now

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.



Set up backup text messages

**Verify phone number**

Enter the code recently sent to +36 20 [redacted]

933361 ×

Finish text setup Back

Resend code

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