Red Hat Customer Portal 1

Using Two-Factor Authentication

Using two-factor authentication to access your Red Hat user account

Red Hat Customer Portal 1 Using Two-Factor Authentication

Using two-factor authentication to access your Red Hat user account

Legal Notice

Abstract

This guide explains how to set up and remove two-factor authentication to access a Red Hat user account by using an authenticator application or recovery codes. For information about the Red Hat SSO (RH-SSO) product, see Product Documentation for Red Hat Single Sign-On.

Table of Contents

PREFACE

Two-factor authentication adds an additional layer of security to the login process. In addition to a Red Hat login and a strong password, a one-time code is required to complete the login action. One-time codes generated by an authentication application on a smart phone. Recovery code authentication generates a list of one-time codes that you can use as a backup if your authentication application is not available.

Making open source more inclusive

Red Hat is committed to replacing problematic language in our code, documentation, and web properties. We are beginning with these four terms: master, slave, blacklist, and whitelist. Because of the enormity of this endeavor, these changes will be implemented gradually over several upcoming releases. For more details, see our CTO Chris Wright's message .

CHAPTER 1. ABOUT TWO-FACTOR AUTHENTICATION (2FA) FOR RED HAT USER ACCOUNTS

Red Hat allows users to enable two-factor authentication as an additional layer of security for logging in to their Red Hat user accounts. When two-factor authentication is enabled, you use your password plus a one-time code to log in to your account. The one-time code is the second authentication factor.

The two-factor authentication feature is available to customers in one of two ways:

- **Organizational two-factor authentication.** When your organization enables two-factor authentication, all users who belong to a specific organization account will be required to use a second factor each time they authenticate. Users will be prompted to enable two-factor authentication upon the first log in attempt after the organization account is enrolled.

- **Individual opt-in two-factor authentication.** Individual users can enable or disable two-factor authentication for their Red Hat account. When organizational two-factor authentication is turned on, individual users cannot disable it.

> **NOTE**
>
> The current implementation of two-factor authentication only applies to applications using a browser-based authentication flow. It does not apply to command line authentication flows.

1.1. ORGANIZATIONAL TWO-FACTOR AUTHENTICATION

The Organization Administrator for an account can enable organization-wide two-factor authentication. When enabled, all users on that account must use two-factor authentication for authentication when they log in. See Section 2.1, "Configuring organization-wide authentication factors".

1.2. TWO-FACTOR AUTHENTICATION AND TOKEN SUPPORT

Token support for two-factor authentication is limited to smartphones or other devices that can install either of the following applications from Apple App Store or Google Play.

- Google Authenticator

- FreeOTP Authenticator

Google Authenticator and FreeOTP Authenticator are the only supported token generators. Hardware tokens, SMS (text-message) tokens, and other apps are not supported.

CHAPTER 2. USING TWO-FACTOR AUTHENTICATION

Using two-factor authentication consists of the following activities.

- Organization Administrator configuring organization-wide two-factor authentication.
  Section 2.1, "Configuring organization-wide authentication factors"

- Verifying your account information (as required)
  Section 2.2, "Verifying your account information"

- Enabling 2FA for your Red Hat user login.
  Section 2.3, "Enabling two-factor authentication for a Red Hat user account"

- Logging in with your 2FA authentication code.
  Section 2.4, "Logging in with two-factor authentication"

- Disabling 2FA for your user login.
  Section 2.5, "Removing two-factor authentication (2FA) for a Red Hat user account"

> **NOTE**
>
> Google Authenticator and FreeOTP Authenticator are the only supported token generators for providing two-factor authentication one-time codes. Hardware tokens, SMS (text-message) tokens, and other apps are not supported. You can install these apps on your smartphone or other compatible Android or iOS device.

While you update your signing in options, you might be asked to log in again. This is a normal action and is provided to increase account security.

2.1. CONFIGURING ORGANIZATION-WIDE AUTHENTICATION FACTORS

The Organization Administrator can enable two-factor authentication for all users in their organization. When enabled, two-factor authentication must be used in addition to a password for a user to log in to their Red Hat user account.

After two-factor authentication is enabled for all users, users are prompted to set up their authentication app before they can proceed. When they complete the two-factor authentication set up, they must use the one-time code from their authenticator app each time they log in.

> **NOTE**
>
> When a user optionally chooses to enable two-factor authentication for their user account through their **Signing in** settings, the two-factor authentication remains enabled for their account regardless of the organizational two-factor authentication settings.

Prerequisites

- Only a user with Organization Administrator permissions can enable organization-wide two-factor authentication.

Procedure

1. Log in to [Red Hat Hybrid Cloud Console](#) as a user who has Organization Administrator permission.

2. From the home page after you log in, click ⚙ (**Settings**).

3. Click **Authentication Policy**.

4. When the **Authentication Policy** window appears,click **Authentication Factors**.

5. On the **Authentication factors** page, check **Enable two-factor authentication for your organization**.

6. Click **Save**.

Two-factor authentication is now required for all users in your organization.

2.2. VERIFYING YOUR ACCOUNT INFORMATION

You might be asked to verify your account information before you can continue to enable two-factor authentication. Red Hat verifies that your account has a confirmed email address and a phone number associated with it before you can enable two-factor authentication. The phone number is required and must be able to receive phone calls directly to you if you need to recover your account.

2.2.1. Confirming your email information

Confirm your current email address when you receive a confirmation request while logging in to a Red Hat portal. If your email is not yet confirmed, an alert message appears: "Your email address has not been confirmed."

Prerequisites

- A registered Red Hat user account.

- An email address where you can receive a confirmation notice.

Procedure

Follow these steps if you receive an email confirmation request notice when you log in to a Red Hat portal.

1. Log in to your Red Hat user account.

2. When a confirmation alert message appears, click **Resend confirmation email** if you have not yet received a confirmation email.

3. Check your email for an email confirmation message from **no-reply@redhat.com**.

4. Follow the instructions in the email for confirming your email address.

5. When you complete the instructions, a confirmation window appears.

2.2.2. Verifying your phone information

If your account does not have a phone number, you might see a verification notice that asks you to provide a phone number.

> **NOTE**
>
> The phone number is required and must be able to receive phone calls directly to you if you need to recover your account.

Prerequisites

- A registered Red Hat user account.

- A telephone number where you can receive direct voice calls.

Procedure

Follow these steps if you receive a phone number verification notice when you log in to a Red Hat portal.

1. Log in to your Red Hat user account.

2. Enter your contact phone number, including any country code, in the verification window.

3. Click **Submit**.

2.3. ENABLING TWO-FACTOR AUTHENTICATION FOR A RED HAT USER ACCOUNT

The Organization Administrator for your account can enable organization-wide two-factor authentication, which requires everyone in the organization to use two-factor authentication when they sign in.

> **NOTE**
>
> If your company policy requires two-factor authentication to access your Red Hat account and you have not yet enabled two-factor authentication, you will see the instructions to enable two-factor authentication immediately after you log in.

If organization-wide two-factor authentication is not required, you can enable, or turn on, two-factor authentication for your Red Hat user account. After you enable two-factor authentication you will use a one-time code in addition to your Red Hat login and password to log in to your Red Hat account. The one-time code is generated by an authenticator app that you install on your smartphone or other supported device.

Prerequisites

- A registered Red Hat user account.

- A smartphone or other device with the Google Authenticator app or the FreeOTP app installed.

Procedure

The following steps assume that you have installed a supported authenticator app.

1. Log in to your Red Hat user account on any Red Hat site, such as Red Hat Customer Portal.

2. Click your user avatar in the upper right corner of the panel.

    a. Click **Account details**. A page opens where you can edit your account information.

b. If you log in through Red Hat Hybrid Cloud Console, click **My profile** under your user avatar to edit your account information.
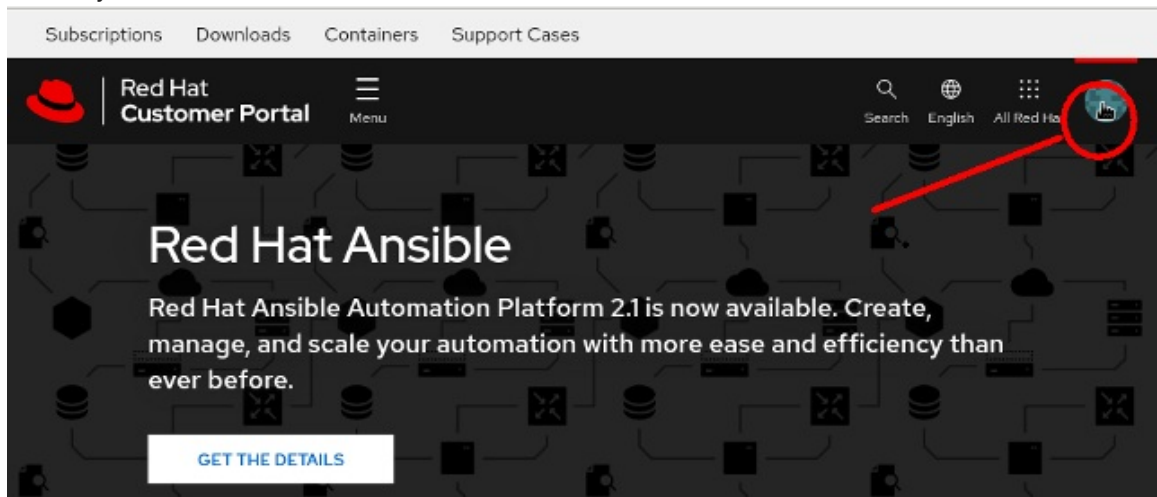
A page opens where you can review your account information.

NOTE

Depending on which login portal you use, a different icon may appear.

3. Click **Login & password**.

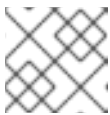4. On the **Login & password** page click **Manage two-factor authentication**. The **Signing in** page opens.

5. On the **Signing in** page, click **Set up authenticator application**. You must log in again to verify your account before the **Enable two-factor authentication** page appears.

6. Open the authenticator app on your smart phone and select the option to add a token. You can use one of these methods to add a token for the Red Hat two-factor authentication.

   a. Use the authenticator app to scan the QR code that opens on the **two-factor authentication** page.

   b. Alternatively, you can click **Unable to scan? Enter the key instead** which displays a 32-character key string that you must enter into your authenticator app.

7. After you scan the QR code (or enter the key string), the authenticator app creates an initial one-time 6-digit code. Enter this code into the **One-time code** field.

8. You can enter an optional name in the **Device name** field. This name can remind you which of your mobile devices has the authenticator app for this login.

   - Click **Enable** to complete setting up two-factor authentication.

Verification

The signing in page shows when the authenticator app was set up and any optional name you gave to the app.

Authenticator application   Set up authenticator application

Enter a verification code from authenticator application.

acc 3   **Created**   December 19,   Remove
                                                           2022 at 12:50 PM

2.4. LOGGING IN WITH TWO-FACTOR AUTHENTICATION

Use a one-time code provided by your authenticator app to log in to your Red Hat user account on any Red Hat site, such as Red Hat Customer Portal. The authenticator app refreshes the one-time code every 30 seconds. Because of the timing, you might need to enter a refreshed code if the initial code does not work.

Prerequisites

- A registered Red Hat user account with two-factor authentication enabled.
  Section 2.3, "Enabling two-factor authentication for a Red Hat user account"

- A smartphone or other device with the Google Authenticator app or the FreeOTP app installed.

Procedure

1. Open the authenticator app.

2. Use your browser to navigate to a Red Hat site, such as Red Hat Customer Portal.

3. Enter your email or your Red Hat login.

4. Enter your Red Hat password. A page opens to verify two-factor authentication.

5. Enter the 6-digit one-time code from your authenticator app into the **One-time code** box and click **Log in**.
   Your Red Hat account greeting page opens.

Verification

If the 6-digit one-time code is not accepted, you will remain on the verification page. You can try the following actions.

1. Wait a few seconds and enter a new code from your authenticator app.

2. If you have more than one token enabled in your authenticator app, make sure you are using the token for your Red Hat account. For example, you might have two-factor authentication tokens for a Google account, a banking account, and a Red Hat account.

3. If you cannot successfully log in to your Red Hat with two-factor authentication enabled, contact Red Hat Customer Service for assistance in resetting your account.

2.5. REMOVING TWO-FACTOR AUTHENTICATION (2FA) FOR A RED HAT USER ACCOUNT

You can remove the two-factor authentication for your Red Hat user account. If the Organization

Administrator has set a policy that requires user accounts to enable two-factor authentication, the next time you log in after removing two-factor authentication you must reenable two-factor authentication for your user login.

Each time you reenable two-factor authentication for your user login, you add a new token to your authenticator app. It is up to you to manage the disabled tokens on your smartphone.

See Chapter 4, *Revoking two-factor authentication when your authenticator device is lost* if you have lost your authenticator device and need Red Hat Customer Service to revoke your two-factor authentication.

Prerequisites

- A registered Red Hat user account.

- A smartphone or other device with the Google Authenticator app or the FreeOTP app installed.

- A Red Hat user account with two-factor authentication enabled.

Procedure

1. Log in to your Red Hat user account using two-factor authentication.
   Section 2.4, "Logging in with two-factor authentication"

2. Click your user avatar in the upper right corner of the page.

   a. Click **Account details**. A page opens where you can edit your account information.

   b. If you log in through Red Hat Hybrid Cloud Console, click **My profile** under your user avatar to edit your account information.
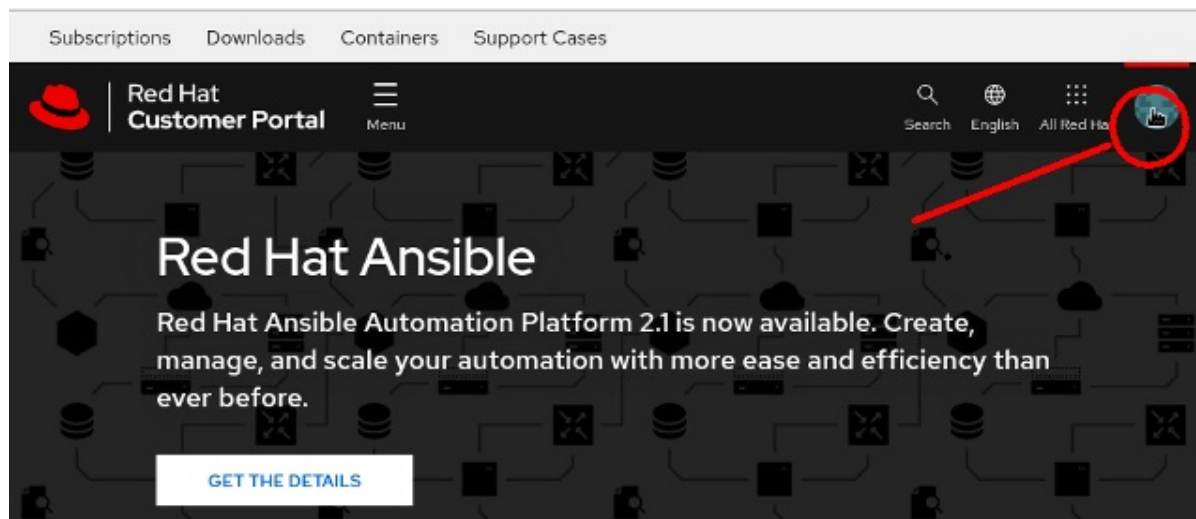
+ A page opens where you can review your account information.

> **NOTE**
>
> Depending on which login portal you use, a different icon may appear.

3. Click **Login & password**

4. On the **Login & password** page click **Manage 2-factor authentication** The **Signing in** page opens.

5. Click **Delete** to remove two-factor authentication for your user login.

> **NOTE**
>
> The **Delete** button disables, or turns off two-factor authentication for your user login. If you reenable two-factor authentication, you will repeat the enable authentication steps, which adds a new token to your authenticator app. The token associated with the disabled authenticator will no longer work.

6. For verification you must log in again with two-factor authentication. A page appears where you click **CONFIRM DELETION** to remove two-factor authentication from your user account. After you confirm deletion, you return to the **Signing in** page.

CHAPTER 3. USING RECOVERY CODES FOR TWO-FACTOR AUTHENTICATION

A recovery code provides an alternative method to verify your two-factor authentication if your authenticator app is not available. When you set up recovery codes, you get a list of codes that are unique to your login. Each code can be used once, and the system tracks each code as it is used. You can also remove the recovery codes for your user account.

You can use recovery codes as a secondary two-factor authentication or you can use them as your primary two-factor authentication without setting up an authenticator app on your smart phone. However, the preferred action is to use recovery codes as a backup to your authenticator app.

While you update your signing in options, you might be asked to log in again. This is a normal action and is provided to increase account security.

If you cannot successfully log in to your Red Hat with recovery codes enabled, contact Red Hat Customer Service for assistance in resetting your account.

- Section 3.1, "Creating recovery codes for two-factor authentication"

- Section 3.2, "Logging in with recovery codes for two-factor authentication"

- Section 3.3, "Removing recovery codes for two-factor authentication"

3.1. CREATING RECOVERY CODES FOR TWO-FACTOR AUTHENTICATION

Create recovery codes after you enable two-factor authentication for your account. You can use a recovery code to authenticate and log in to your account if you lose your authenticator device.
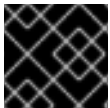

IMPORTANT

If you choose not to set up recovery codes, you might lose access to your account.

Prerequisites

- Enable two-factor authentication for your account.
  Section 2.3, "Enabling two-factor authentication for a Red Hat user account"

Procedure

1. Log in to your Red Hat user account on any Red Hat site, such as Red Hat Customer Portal.

2. Click your user avatar in the upper right corner of the page.

   a. Click **Account details**. A page opens where you can edit your account information.

   b. If you log in through Red Hat Hybrid Cloud Console, click **My profile** under your user avatar to edit your account information.
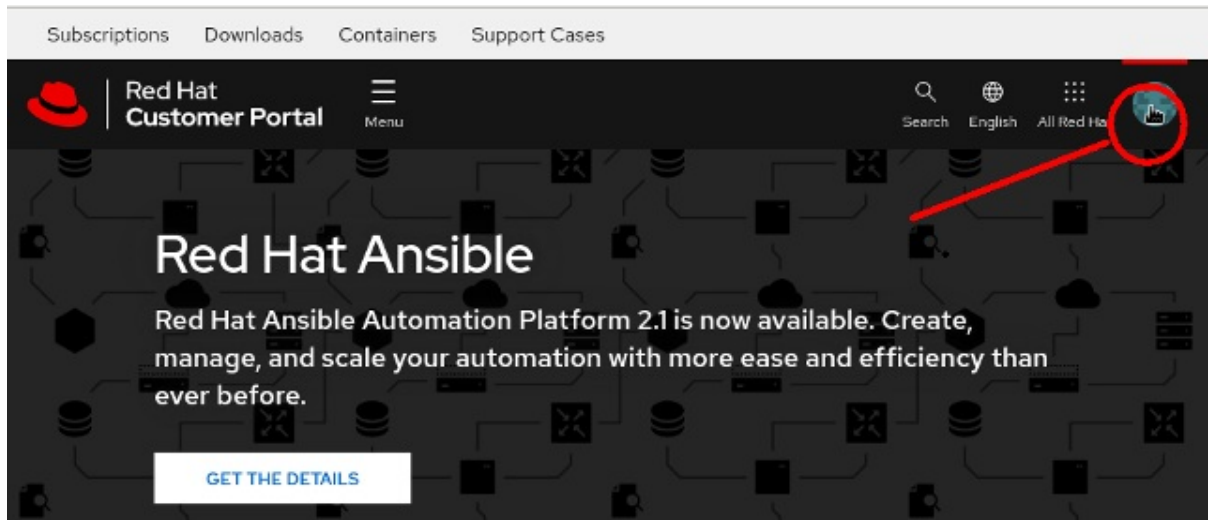
+ A page opens where you can review your account information.

> **NOTE**
>
> Depending on which login portal you use, a different icon may appear.

3. Click **Account details**. A page opens where you can edit your account information.

4. Click **Login & password**.

5. On the **Login & password** page scroll down to **2-factor authentication** and click **Manage 2-factor authentication**. The **Signing in** page opens.

6. Click **Set up recovery codes**.

7. The **Recovery codes** page opens and shows a list of unique codes.

8. Carefully follow the instructions on this page to print, download, or copy the list of codes.
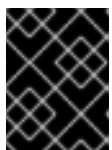
> **IMPORTANT**
>
> Keep the recovery codes in a safe place. When you enable recovery codes, the next time you log in you will be asked for a recovery code.

9. Click **Complete setup** to return to the **Signing in** page.

10. The **Signing in** page confirms when you created the recovery codes and how many have been used.

3.2. LOGGING IN WITH RECOVERY CODES FOR TWO-FACTOR AUTHENTICATION

Use a recovery code to log in to your Red Hat account.

Prerequisites

- A registered Red Hat user account with two-factor authentication enabled.
  Section 2.3, "Enabling two-factor authentication for a Red Hat user account"

- You must have access to your recovery codes.
  Section 3.1, "Creating recovery codes for two-factor authentication"

Procedure

1. Use your browser to navigate to a Red Hat site, such as Red Hat Customer Portal.

2. Log in using your email or your Red Hat login.

3. Enter your Red Hat password. A page opens to verify two-factor authentication and asks for a one-time code.

4. Click **Try another way**.
   You are prompted to choose recovery codes.

5. Enter the recovery code from your list and click **Log in**.
   Your Red Hat account greeting page opens.

## 3.3. REMOVING RECOVERY CODES FOR TWO-FACTOR AUTHENTICATION

You can remove your existing recovery codes. If you remove recovery codes for your account, you are not prompted to **Use a recovery code instead**when you log in to your Red Hat account.

Prerequisites

- You created recovery codes for your Red Hat account.
  Section 3.1, "Creating recovery codes for two-factor authentication"

- You can log in to your user account.

Procedure

1. Log in to your Red Hat user account on any Red Hat site, such as Red Hat Customer Portal.

2. Click your user avatar in the upper right corner of the panel.

   a. Click **Account details**. A page opens where you can edit your account information.

   b. If you log in through Red Hat Hybrid Cloud Console, click **My profile** under your user avatar to edit your account information.
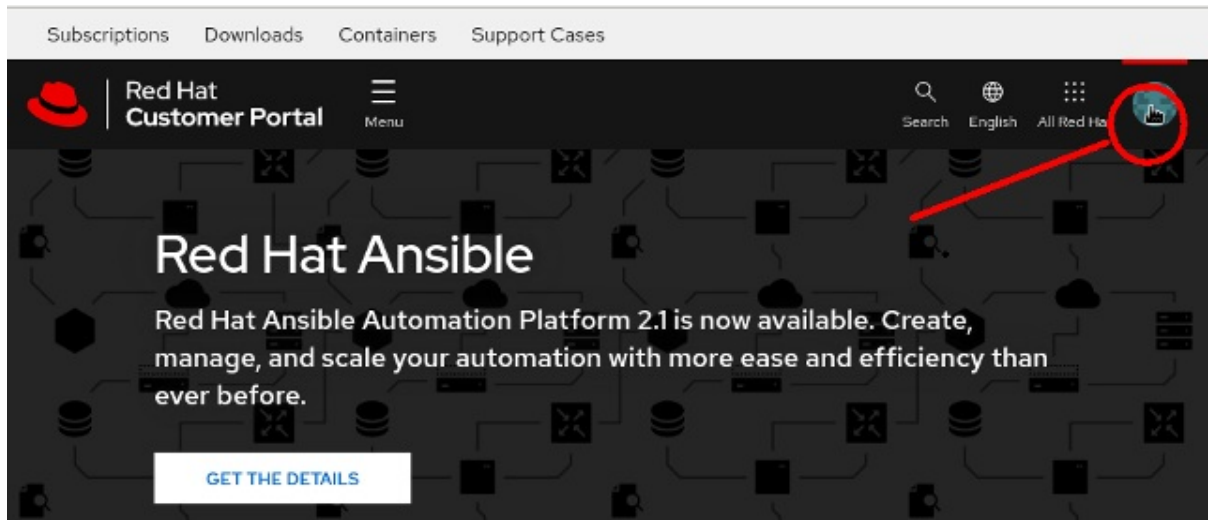
+ A page opens where you can review your account information.

> **NOTE**
>
> Depending on which login portal you use, a different icon may appear.

3. Click **Account details**. A page opens where you can edit your account information.

4. Click **Login & password**

5. On the **Login & password** page scroll down to **2-factor authentication** and click **Manage 2-factor authentication**. The **Signing in** page opens.

6. Scroll down to **Recovery codes**.

7. Click **Remove**.

After you remove recovery codes, you can create a new set.

CHAPTER 4. REVOKING TWO-FACTOR AUTHENTICATION WHEN YOUR AUTHENTICATOR DEVICE IS LOST

You can revoke the two-factor authentication protection on your Red Hat account when your authenticator device is lost and you have no recovery codes available, or when you have no other way to log in to your account with two-factor authentication enabled. Red Hat Customer Service can do this immediately with a phone call or with a seven-day email response. All requests to revoke two-factor authentication must be made by phone. You cannot revoke two-factor authentication with an email request or other online request.

See Section 2.2, "Verifying your account information" for information about setting up your contact phone number.

> **IMPORTANT**
>
> Account verification through a phone call from Red Hat Customer Service to your account phone number is the only method approved by the Red Hat security teams for quickly allowing two-factor authentication settings to be revoked. There are no exceptions to this process.

> **NOTE**
>
> Password resets are done through email, using the email address for your account. You cannot revoke two-factor authentication through email, and you cannot reset your password through a phone call.

4.1. REVOKING TWO-FACTOR AUTHENTICATION IMMEDIATELY

To immediately revoke two-factor authentication on your account, you must be reachable by phone. Red Hat Customer Service places a call to the phone number of record for your account. This two-step process with outgoing call confirmation protects the security of your account. It is the only method approved by the Red Hat security team that allows two-factor authentication settings to be revoked by phone.

If you can't accept a return call from Red Hat Customer Service, the two-factor authentication on your account can't be quickly revoked.

After two-factor authentication is revoked, you can log in using your valid password. Depending on your organization policy, you might be required to immediately enable two-factor authentication after you log in.

4.2. REVOKING TWO-FACTOR AUTHENTICATION WITH A 7-DAY WAITING PERIOD

When you cannot accept a call to the phone number of record for your account, the Red Hat Customer Service team sends an email notification to the email address associated with your account. The email notifies the account holder that two-factor authentication will be revoked in 7 days. You can reply to the notification email if you decide you do not want two-factor authentication revoked.