Red Hat Customer Portal 1

使用双因素身份验证

使用双因素身份验证访问您的红帽用户帐户

Last Updated: 2024-06-22

Red Hat Customer Portal 1 使用双因素身份验证

使用双因素身份验证访问您的红帽用户帐户

法律通告

摘要

本指南介绍了如何使用身份验证器应用程序或恢复代码设置和删除双因素身份验证来访问红帽用户帐户。 有关 Red Hat SSO (RH-SSO)产品的详情，请参考 Red Hat Single Sign-On 产品文档。

目录

前言

双因素身份验证为登录过程添加额外的安全层。除了红帽登录和强大的密码外，还需要一次性代码来完成登录操作。在智能手机上由身份验证应用程序生成的一次性代码。如果身份验证应用程序不可用，恢复代码身份验证会生成一次性代码列表，它可以用作备份。

使开源包含更多

红帽承诺替换我们的代码、文档和网页属性中存在问题的语言。我们从这四个术语开始：master、slave、黑名单和白名单。由于此项工作十分艰巨，这些更改将在即将推出的几个发行版本中逐步实施。详情请查看 CTO Chris Wright 的信息。

第 1 章 关于红帽用户帐户的双因素身份验证(2FA)

红帽允许用户启用双因素身份验证作为额外的安全层，以登录到其红帽用户帐户。启用双因素身份验证后，您可以使用您的密码加一个一次性代码来登录到您的帐户。一次性代码是第二个身份验证因子。

客户可以通过两种方式使用双因素身份验证功能：

- **组织双因素身份验证。**当您的组织启用双因素身份验证时，每次进行身份验证时，所有属于特定机构帐户的用户都需要使用第二个因素。系统会在组织帐户注册后在第一次登录时提示用户启用双因素身份验证。
- **个人选择的双因素身份验证。**个人用户可以为其红帽帐户启用或禁用双因素身份验证。当组织启用双因素身份验证时，单个用户无法禁用它。

注意

双因素身份验证的当前实现只适用于使用基于浏览器的身份验证流程的应用程序。它不适用于通过命令行进行身份验证的验证流程。

1.1. 机构双因素身份验证

帐户的机构管理员可以启用机构范围内的双因素身份验证。启用后，该帐户上的所有用户必须在登录时使用双因素身份验证进行身份验证。请参阅 第 2.1 节 “配置机构范围内的身份验证因素”。

1.2. 双因素身份验证和令牌支持

对双因素身份验证的令牌支持仅限于智能手机或其他设备，这些设备可以从 Apple App Store 或 Google Play 中安装以下应用程序。

- Google Authenticator
- FreeOTP Authenticator

Google Authenticator 和 FreeOTP Authenticator 是唯一支持的令牌生成器。不支持硬件令牌、SMS（文本消息）令牌和其他应用程序。

第 2 章 使用双因素身份验证

使用双因素身份验证由以下活动组成：

- 机构管理员配置机构范围内的双因素身份验证。
  第 2.1 节 “配置机构范围内的身份验证因素”
- 验证您的帐户信息（根据需要）
  第 2.2 节 “验证您的帐户信息”
- 为您的红帽用户登录启用 2FA。
  第 2.3 节 “为红帽用户帐户启用双因素身份验证”
- 使用您的 2FA 身份验证代码登录。
  第 2.4 节 “使用双因素身份验证登录”
- 为您的用户登录禁用 2FA。
  第 2.5 节 “为红帽用户帐户移除双因素身份验证(2FA)”

注意

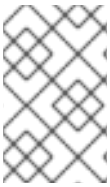
Google Authenticator 和 FreeOTP Authenticator 是唯一支持的令牌生成器，用于提供双因素身份验证一次性代码。不支持硬件令牌、SMS （文本消息）令牌和其他应用程序。您可以在智能手机或其他兼容 Android 或 iOS 设备上安装这些应用程序。

当您更新选项中的签名时，可能会要求您再次登录。这是正常操作，为提高帐户安全性而提供。

2.1. 配置机构范围内的身份验证因素

机构管理员可以为其机构中所有用户启用双因素身份验证。启用后，除了启用双因素身份验证外，还需要使用双因素身份验证来登录其红帽用户帐户。

为所有用户启用双因素身份验证后，系统会提示用户设置其身份验证应用程序，然后才能继续。当他们完成双因素身份验证集后，每次登录时，都必须使用来自其验证器应用程序的一次性代码。



注意

当用户选择通过 **Signing in** 设置来为用户帐户启用双因素身份验证时，无论组织双因素身份验证设置如何，无论组织双因素身份验证设置如何，都会为其帐户启用双因素身份验证。

前提条件

- 只有具有机构管理员权限的用户才能启用机构范围内的双因素身份验证。

流程

1. 以具有机构管理员权限的用户身份登录 Red Hat Hybrid Cloud Console 。
2. 登录后，从主页中，单击 iwl (**Settings**)。
3. 单击 **Authentication Policy**。
4. 出现 **Authentication Policy** 窗口时，单击 **Authentication Factors**。

5. 在 **Authentication factors** 页面中，检查 为**您的组织启用双因素身份**验证。
6. 点击 **Save**。

现在，您的机构中的所有用户都需要双因素身份验证。

2.2. 验证您的帐户信息

在继续启用双因素身份验证前，您可能需要验证您的帐户信息。在启用双因素身份验证前，红帽会验证您的账户是否有已确认的电子邮件地址及其关联的电话号码。电话号码是必需的，如果您需要恢复您的帐户，则必须直接向您接收电话通话。

2.2.1. 确认您的电子邮件信息

当您收到确认请求时，请确认您的当前电子邮件地址。如果您的电子邮件尚未确认，则会出现警告信息："Your email address has been confirmed"。

前提条件

- 注册的 Red Hat 用户帐户。
- 您可以收到确认通知的电子邮件地址。

流程

如果您在登录到红帽门户时收到一封电子邮件确认请求，请按照以下步骤操作。

1. 登录到您的红帽用户帐户。
2. 出现确认警报消息时，如果您尚未收到 **确认电子邮件，请单击 Resend** 确认电子邮件。
3. 查看您的电子邮件以获取来自 **no-reply@redhat.com** 的电子邮件确认消息。
4. 按照电子邮件中的说明确认您的电子邮件地址。
5. 完成说明后，会出现一个确认窗口。

2.2.2. 验证您的电话信息

如果您的帐户没有电话号码，您可能会看到验证通知，要求您提供电话号码。

注意

电话号码是必需的，如果您需要恢复您的帐户，则必须直接向您接收电话通话。

前提条件

- 注册的 Red Hat 用户帐户。
- 您可以接收直接语音调用的电话号码。

流程

如果您在登录到红帽门户时收到电话号码验证通知，请按照以下步骤操作。

1. 登录到您的红帽用户帐户。

2. 在验证窗口中输入您的联系电话号码，包括任何国家代码。

3. 点 **Submit**。

2.3. 为红帽用户帐户启用双因素身份验证

您的帐户的机构管理员可以启用机构范围内的双因素身份验证，这需要机构中的每个人在登录时使用双因素身份验证。

注意

如果您的公司策略需要双因素身份验证才能访问您的红帽帐户，并且您尚未启用双因素身份验证，那么您会在登录后马上启用双因素身份验证。

如果不需要机构范围内的双因素身份验证，您可以为您的红帽用户帐户启用或启用双因素身份验证。启用双因素身份验证后，除了红帽登录和密码外，您还可以使用一次性代码来登录到您的红帽帐户。一次性代码由您在智能手机或其他支持的设备上安装的验证器应用程序生成。

前提条件

- 注册的 Red Hat 用户帐户。
- 安装了 Google Authenticator 应用程序或 FreeOTP 应用程序的智能手机或其他设备。

流程

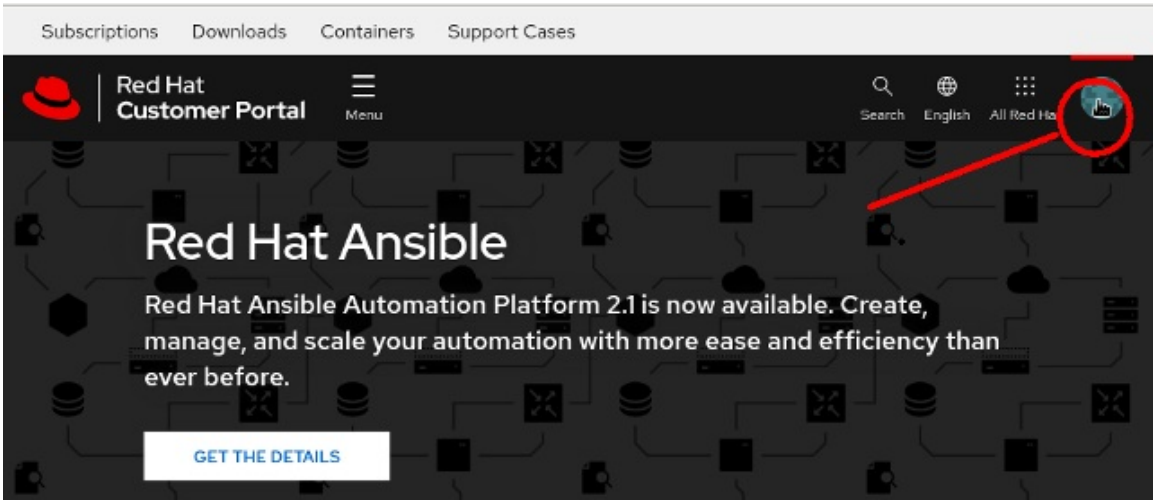
以下步骤假定您已安装了受支持的验证器应用程序。

1. 在任何红帽站点（如 红帽客户门户网站 ）上登录到您的红帽用户帐户。

2. 点面板右上角的用户 avatar。

   a. 点 **帐户 详情**。此时将打开一个页面，您可以在其中编辑帐户信息。

   b. 如果您通过 Red Hat Hybrid Cloud Console 登录，点用户 avatar 下的 **My profile** 来编辑您的帐户信息。



   此时将打开一个页面，您可以在其中查看您的帐户信息。

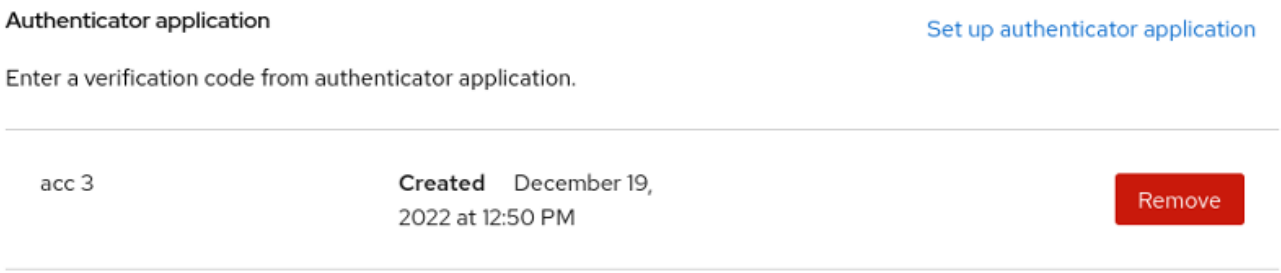
注意

根据您使用的登录门户，可能会出现不同的图标。

3. 点 **Login and password**。
4. 在 **登录和密码页面中**，点 **Manage two-factor authentication**。此时会打开 **Signing in** 页面。
5. 在 **Signing in** 页面中，单击 **Set up authenticator application**。您必须先登录才能验证您的帐户，然后才能显示 **Enable two-factor authentication** 页面。
6. 在您的智能电话中打开验证器应用程序，并选择添加令牌的选项。您可以使用这些方法之一为红帽双因素身份验证添加令牌。
   a. 使用 authenticator 应用程序扫描在 **双因素** 验证页面上打开的 QR 代码。
   b. 或者，您可以点 **Unable to scan?输入密钥**，它显示一个 32 个字符的键字符串，您必须输入您的验证器应用程序。
7. 扫描 QR 代码（或输入密钥字符串）后，验证器应用程序会创建一个初始一次性 6 位代码。在 **一次性代码字段中输入此代码**。
8. 您可以在 **Device name** 字段中输入可选名称。此名称可以提醒您哪个移动设备具有用于此登录的验证器应用程序。
   - 点 **Enable** 完成设置双因素身份验证。

验证

页面中的签名会显示何时设置 authenticator 应用程序以及您提供给应用程序的任何可选名称。



2.4. 使用双因素身份验证登录

使用您的验证器应用程序提供的一次性代码，登录到任何红帽站点（如 红帽客户门户网站 ）上的红帽用户帐户。验证器应用程序每 30 秒刷新一次性代码。由于时间，如果初始代码无法正常工作，您可能需要输入刷新的代码。

前提条件

- 注册的红帽用户帐户启用了双因素身份验证。
  第 2.3 节 “为红帽用户帐户启用双因素身份验证”
- 安装了 Google Authenticator 应用程序或 FreeOTP 应用程序的智能手机或其他设备。

流程

1. 打开验证器应用程序。

2. 使用您的浏览器导航到 Red Hat 站点，如 红帽客户门户网站。
3. 输入您的电子邮件或您的红帽账户。
4. 输入您的红帽密码。此时将打开一个页面来验证双因素身份验证。
5. 在一次性代码框中输入 6 位 **的一次性代码**，然后单击 **中的 Log**。
   您的 Red Hat 账户问候页面将打开。

验证

如果不接受 6 位的一次性代码，您将保留在验证页面中。您可以尝试以下操作。

1. 等待几秒钟，然后从您的验证器应用程序输入新代码。
2. 如果您在 authenticator 应用中启用了多个令牌，请确保将令牌用于红帽帐户。例如，对于 Google 帐户、银行帐户和红帽帐户，可能具有双因素身份验证令牌。
3. 如果您无法在启用了双因素身份验证的情况下成功登录到红帽，请联系红帽客户服务以协助 重置您的帐户。

2.5. 为红帽用户帐户移除双因素身份验证(2FA)

您可以删除红帽用户帐户的双因素身份验证。如果机构管理员设置了需要用户帐户启用双因素身份验证的策略，在下次在删除双因素身份验证后登录时，您必须为用户登录重新启用双因素身份验证。

每次重新启用用户登录的双因素身份验证时，您都会向 authenticator 应用添加新令牌。您最多可在智能手机上管理禁用的令牌。

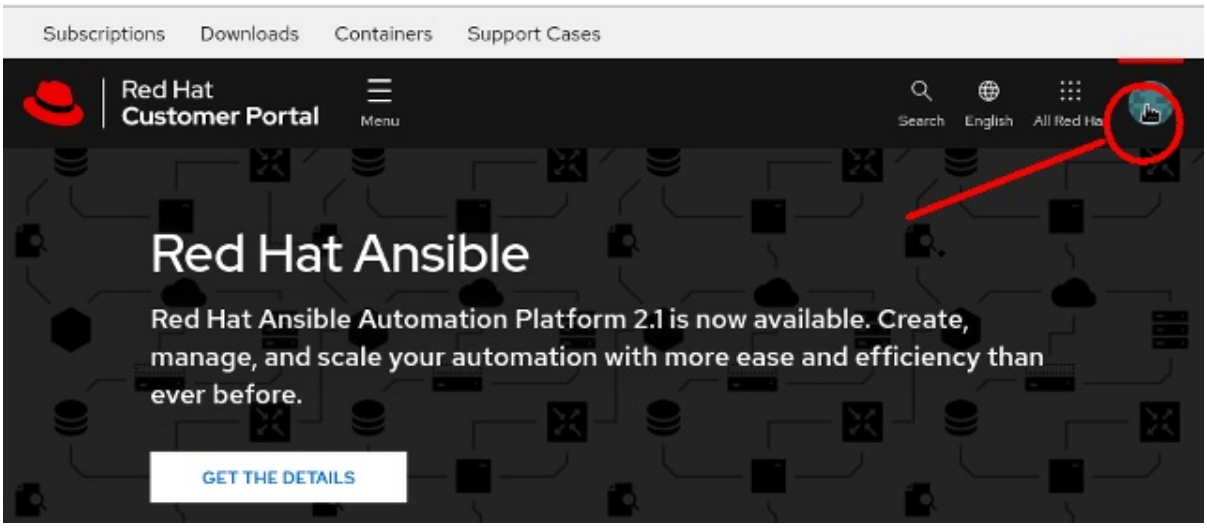
如果您丢失了验证器设备并需要 Red Hat Customer Service 来撤销双因素身份验证，请参阅 第 4 章 *当您的验证器设备丢失时，撤销双因素身份验证*。

前提条件

- 注册的 Red Hat 用户帐户。
- 安装了 Google Authenticator 应用程序或 FreeOTP 应用程序的智能手机或其他设备。
- 启用双因素身份验证的红帽用户帐户。

流程

1. 使用双因素身份验证登录到您的红帽用户帐户。
   第 2.4 节 “使用双因素身份验证登录”
2. 点页面右上角的用户 avatar。
   a. 点 **帐户 详情**。此时将打开一个页面，您可以在其中编辑帐户信息。
   b. 如果您通过 Red Hat Hybrid Cloud Console 登录，点用户 avatar 下的 **My profile** 来编辑您的帐户信息。



+ 页面将打开，您可以在其中查看您的帐户信息。

注意

根据您使用的登录门户，可能会出现不同的图标。

3. 点 **Login and password**。
4. 在 **登录和密码页面中**，点 **Manage 2factor authentication**。此时会打开 **Signing in** 页面。
5. 点 **Delete** 以删除您的用户登录的双因素身份验证。

注意

Delete 按钮会禁用，或者为您的用户登录关闭双因素身份验证。如果您重新启用双因素身份验证，您将重复启用身份验证步骤，这会向 authenticator 应用添加新令牌。与禁用验证器关联的令牌将不再工作。

6. 若要进行验证，您必须使用双因素身份验证再次登录。此时会出现一个页面，**您可以在其中单击确认**，以从您的用户帐户中删除双因素身份验证。确认删除后，您返回到 **Signing in** 页面。

第 3 章 将恢复代码用于双因素身份验证

如果身份验证器应用程序不可用，则恢复代码提供了一种替代的方法来验证您的双因素身份验证。当您设置恢复代码时，您将获得一个与您的登录的唯一代码列表。每个代码都可使用一次，系统会像使用时跟踪每个代码。您还可以删除用户帐户的恢复代码。

您可以使用恢复代码作为辅助双因素身份验证，或者您可以在智能电话中设置身份验证的情况下将其用作主要双因素身份验证。但是，首选的操作是使用恢复代码作为您的验证器应用程序的备份。

当您更新选项中的签名时，可能会要求您再次登录。这是正常操作，为提高帐户安全性而提供。

如果您无法成功登录到启用了恢复代码的红帽，请联系红帽客户服务以协助 重置您的帐户。

3.1. 为双因素身份验证创建恢复代码

为帐户启用双因素身份验证后创建恢复代码。如果丢失了验证器设备，您可以使用恢复代码来验证并登录到您的帐户。

重要

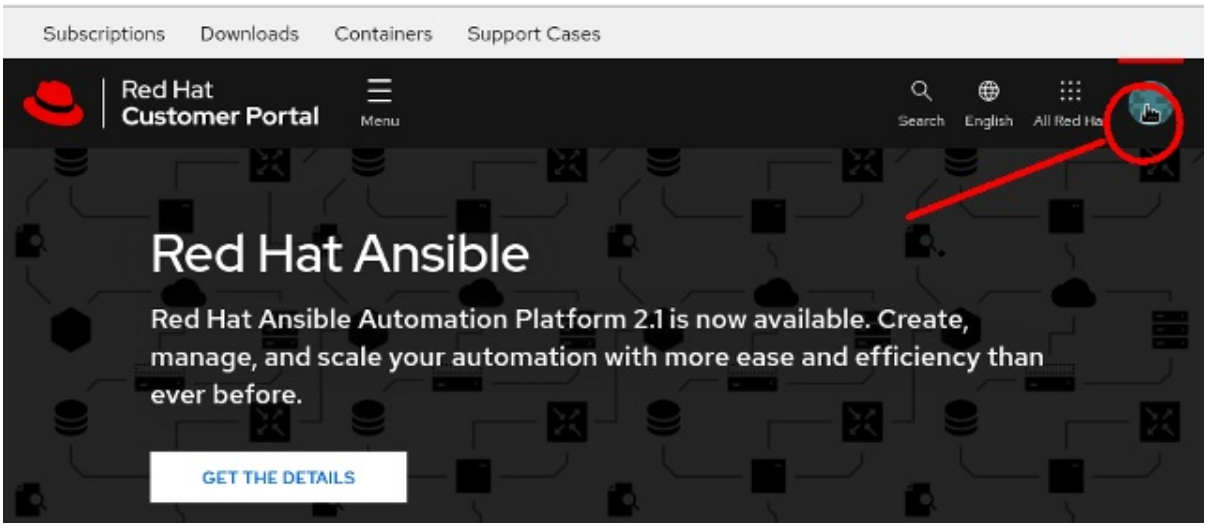
如果您选择设置恢复代码，则可能会丢失对帐户的访问。

前提条件

- 为您的帐户启用双因素身份验证。
  第 2.3 节 “为红帽用户帐户启用双因素身份验证”

流程

1. 在任何红帽站点（如 红帽客户门户网站 ）上登录到您的红帽用户帐户。
2. 点页面右上角的用户 avatar。
   a. 点 **帐户 详情**。此时将打开一个页面，您可以在其中编辑帐户信息。
   b. 如果您通过 Red Hat Hybrid Cloud Console 登录，点用户 avatar 下的 **My profile** 来编辑您的帐户信息。



+ 页面将打开，您可以在其中查看您的帐户信息。

注意

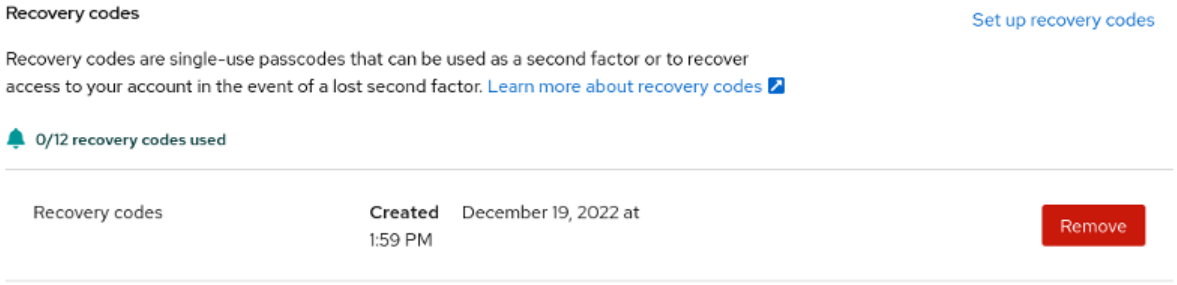
根据您使用的登录门户，可能会出现不同的图标。

3. 点 **帐户 详情**。此时将打开一个页面，您可以在其中编辑帐户信息。
4. 点 **Login and password**。
5. 在 **Login & password** 页面中，向下滚动到双因素身份验证，然后点 **Manage 2-factor authentication**。此时会打开 **Signing in** 页面。
6. 点 **Set up recovery code**。
7. 此时会打开 **Recovery** code 页面，并显示唯一的代码列表。
8. 请仔细按照此页面中的说明进行打印、下载或复制代码列表。

重要

将恢复代码保存在安全的地方。当您启用恢复代码时，您下次登录时将要求您进行恢复代码。

9. 单击 **Complete setup**，以返回到 **页面中的 Signing**。
10. **在页面中，Signing 会** 确认您创建恢复码以及已使用多少。



3.2. 使用双因素身份验证的恢复代码登录

使用恢复代码登录到您的红帽帐户。

前提条件

- 注册的红帽用户帐户启用了双因素身份验证。
  第 2.3 节 “为红帽用户帐户启用双因素身份验证”
- 您必须有权访问您的恢复代码。
  第 3.1 节 “为双因素身份验证创建恢复代码”

流程

1. 使用您的浏览器导航到 Red Hat 站点，如 红帽客户门户网站。
2. 使用您的电子邮件或您的红帽登录名登录。
3. 输入您的红帽密码。此时将打开一个页面来验证双因素身份验证，并要求进行一次性代码。
4. 点 **Try other way**。
   系统将提示您选择恢复代码。
5. 输入您列表中的恢复代码并点 **Log in**。
   您的 Red Hat 账户问候页面将打开。

3.3. 为双因素身份验证删除恢复代码

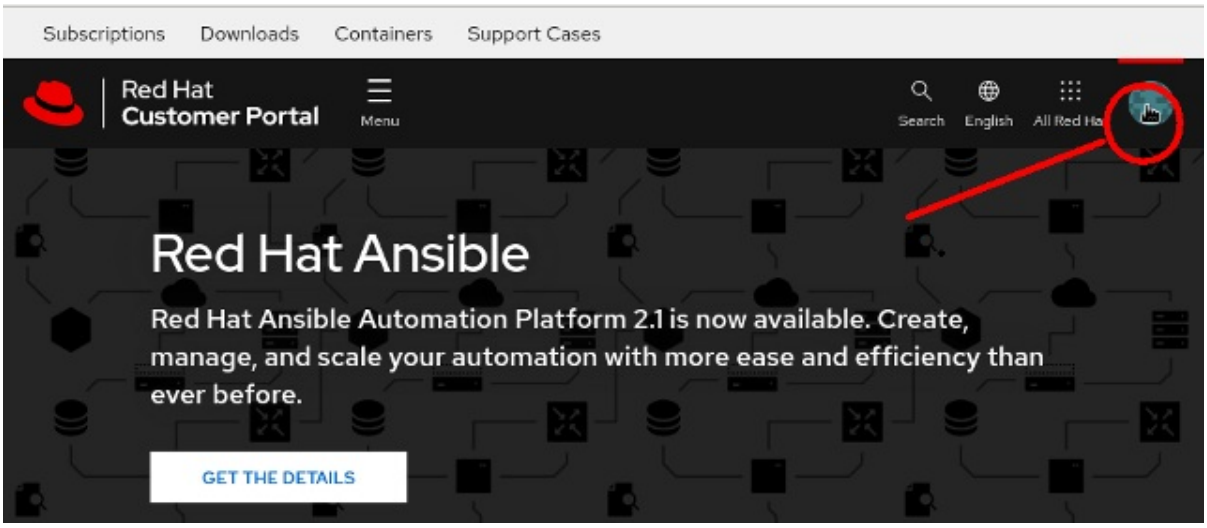
您可以删除现有的恢复代码。如果您删除帐户的恢复代码，则在登录到您的红帽帐户时，不会提示您使用**恢复代码**。

前提条件

- 您为您的红帽帐户创建了恢复代码。
  第 3.1 节 “为双因素身份验证创建恢复代码”
- 您可以登录到您的用户帐户。

流程

1. 在任何红帽站点（如 红帽客户门户网站 ）上登录到您的红帽用户帐户。
2. 点面板右上角的用户 avatar。
   a. 点 **帐户 详情**。此时将打开一个页面，您可以在其中编辑帐户信息。
   b. 如果您通过 Red Hat Hybrid Cloud Console 登录，点用户 avatar 下的 **My profile** 来编辑您的帐户信息。

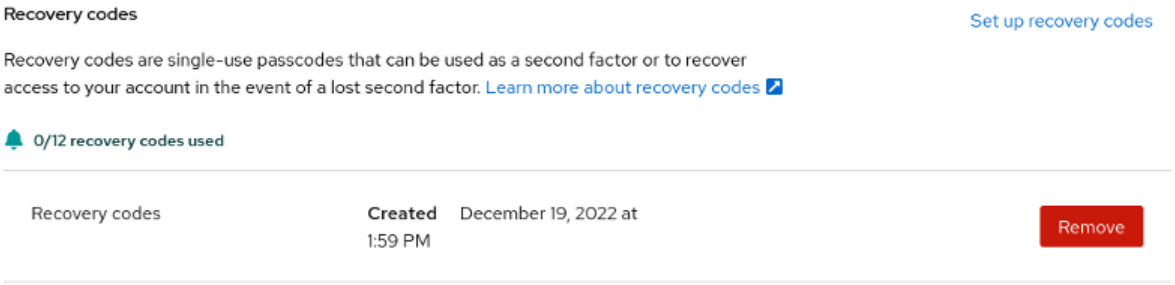


+ 页面将打开，您可以在其中查看您的帐户信息。

注意

根据您使用的登录门户，可能会出现不同的图标。

3. 点 **帐户 详情**。此时将打开一个页面，您可以在其中编辑帐户信息。
4. 点 **Login and password**。
5. 在 **Login & password** 页面中，向下滚动到双因素身份验证，然后点 **Manage 2-factor authentication**。此时会打开 **Signing in** 页面。
6. 向下滚动到 **恢复代码**。
7. 单击 **Remove**。



删除恢复代码后，您可以创建新集合。

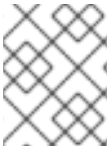
第 4 章 当您的验证器设备丢失时，撤销双因素身份验证

当您的验证器设备丢失并且没有可用的恢复代码时，您可以撤销对红帽帐户的双因素验证保护，或者您没有其他方法登录到启用了双因素身份验证的帐户。红帽客户服务 可以通过电话电话或 7 天电子邮件回复立即执行此操作。所有用于撤销双因素身份验证的请求都必须通过电话进行。您不能使用电子邮件请求或其他在线请求撤销双因素身份验证。

有关设置联系电话号码的详情，请参考 第 2.2 节 “验证您的帐户信息”。

重要

从 红帽客户服务 到您的帐户电话号码的电话验证帐户验证是红帽安全团队批准的唯一方法，以便快速撤销双因素身份验证设置。这个过程没有例外。



注意

密码重置通过电子邮件使用您帐户的电子邮件地址来完成。您不能通过电子邮件撤销双因素身份验证，您无法通过电话调用重置密码。

4.1. 立即撤销双因素身份验证

要立即撤销帐户上的双因素身份验证，您必须可以通过电话访问。红帽客户服务会 给您账户的电话号码打电话。这两步过程带有传出调用确认，可保护您的帐户的安全性。它是红帽安全团队批准的唯一方法，它允许通过电话撤销双因素身份验证设置。

如果您无法接受来自 红帽客户服务 的返回通话，则您的帐户上的双因素身份验证无法快速撤销。

撤销双因素身份验证后，您可以使用有效的密码登录。根据您的机构策略，您可能需要在登录后立即启用双因素身份验证。

4.2. 使用 7 天的等待期限撤销双因素身份验证

当您无法接受到您帐户的电话号码的电话时，红帽客户服务团队 会向与您的帐户关联的电子邮件地址发送电子邮件通知。此电子邮件通知帐户持有者将在 7 天后撤销双因素身份验证。如果您决定不希望撤销双因素身份验证，您可以回复通知电子邮件。