Access & Security

To keep your data safe and gain access to Red Hat's network and internal systems, you will need to use multiple passwords. This page defines the purpose of each password and links to steps for changing your passwords.

Table of Contents

What passwords are used at Red Hat?

Reference the table below to learn about the most commonly-used passwords at Red Hat, including IPA/Kerberos , PIN+Token, LUKS, Active Directory, and more.

Below, you can find a more detailed description of these passwords as well as information on how to set or reset them as needed.

Platform	Password Name	What do I use it for?
All Platforms	IPA/Kerberos (IPA) Password	Logging in to a RHEL CSB laptop and managing tokens at token.redhat.com
	PIN+Token Code	Accessing the Red Hat Virtual Private Network (VPN), accessing Gmail and Google Apps, logging in to Workday, logging in to Rover | Apps, and connecting to the "Red Hat" wireless network. In some places, you will see your PIN+Token referred to as your "SAML" login.
	Temporary Token Code	A temporary substitute for your PIN+Token, as a new hire it was

		sent to you to your **personal email address**, which you provided during your pre-hire onboarding, it **expires in two days**. Before it expires, you will need to use this temporary token to set your IPA/ Kerberos Password, which will then enable you to set up your permanent PIN + Token.
	Red Hat Guest Wireless Password	Connecting to the "Red Hat Guest" wireless network (this password changes annually)
RHEL/FEDORA CSB	LUKS Password	Encrypting and decrypting the data on a RHEL CSB laptop
Windows CSB	Active Directory Password	Logging in to a Windows CSB laptop
	BitLocker Password	Encrypting and decrypting the data on a Windows CSB laptop
macOS	Login Password	Logging in to a macOS laptop
	FileVault Recovery Key	Accessing a macOS laptop if you forget the User Account password

NOTE: This page describes the passwords most commonly used at Red Hat. For other passwords not mentioned here, try searching help.redhat.com to find more information.

What is PIN+Token (Two-Factor Authentication)

The tutorial video clip of what is PIN+Token

At Red Hat, we use a PIN and Token code (two-factor authentication) to keep our internal resources secure. A PIN+Token code is more secure than a password alone because it requires two parts: a PIN (permanent password) that only you know, and an associated Token code (one-time use password) generated by a device that only you have. Even if someone finds out your password or gets your token device, one cannot be used without the other.

You can use a smartphone application as a soft token or a Gemalto hard token, or both for two-factor authentication.

The screenshot of the soft token and hard token

Soft Token

Hard Token

How do I set up my PIN+Token?

The tutorial video clip of how to set-up PIN+Token

Visit the PIN+Token (PrivacyIDEA) Self-Service Guide for step by step instruction on how to set up PIN+Token

How do I request a new temporary token code for a new hire?

If your manager did not receive or provide you with a temporary token code on day one or your temporary token code has expired before you set up your permanent passwords, please open a ticket with IT or call the IT Emergency Voicemail number for your country to request a new temporary token code.

What are LDAP groups and how do I get added to one?

Some applications and environments require you to be a member of a group in our LDAP directory to get access. Your manager or team should be able to tell you which LDAP groups you need to get access to, if any.

To request access, fill out the Add User to POSIX LDAP Group. Using the form, you can search for an associate who has the groups you need to make finding them easier.

How can I change my passwords?

IPA/Kerberos Password

If you would like to set a new IPA/Kerberos password, follow Change Your Kerberos Password.

PIN+Token

To change your PIN for two-factor authentication, follow Set a New PIN for a Hard or Soft Token at token.redhat.com.

Windows Active Directory Password

If you are using Windows CSB, you can change your login password by following Change Active Directory Password.

Mac Login Password

If you want to change your Login password, visit Apple's Change or reset the password of a macOS user account article.

Encryption Password

Red Hat requires all associates to encrypt their laptops to protect their data in the event their laptop is lost or stolen. To change the password used to encrypt the data on your laptop's har drive, click the link beside your operating system.

Platform	Instructions
RHEL/FEDORA CSB	Change Your LUKS Encryption Password
Windows CSB	Change Your BitLocker Encryption Password
macOS	FileVault uses a recovery key that you will not need unless you forget your Mac login password.

	While completing the laptop setup guide, you were asked to encrypt your hard drive, and should have received a prompt to copy the key and save it in a safe place. During this process, the key is also sent to IT for emergency use via the escrow tool in the Mac Managed Software Center.

What about Customer Portal access / External SSO?

If your role involves accessing the Red Hat Customer Portal (https://access.redhat.com), you will log in via Red Hat's external single sign-on (SSO) system (which is separate from internal SSO used to log in to applications listed in Rover | Apps). External SSO also allows you to log in to redhat.com and other sites.

All Red Hat employees receive a Customer Portal account automatically, so you should not need to request a new account. However, associates who are part of certain organizations, like Customer Experience & Engagement (CEE), automatically receive additional access and entitlements.

What should I do if I forget one of my passwords?

PIN+Token

You can set a new PIN without knowing your previous PIN by following the steps in Set a New PIN for a Hard or Soft Token at token.redhat.com.

Other Passwords

If you cannot remember your IPA/Kerberos, LUKS, Active Directory, Bitlocker, or Mac Login password, use IT's Report an Issue webform to request help. When submitting the webform, specify the password that you cannot remember and IT will help you reset your password.

How can I set up an SSH Key?

Some Red Hatters may need to set up an SSH key for secure access to remote systems. For instructions, see SSH - Help in Gitlab.

Additional Resources

The Information Security Operating Guidelines outline Red Hat's policies for the use of email, personal devices, and more.

If you need information on access permissions within The Source, Red Hat's intranet, review KB0012581: What are the access and permissions rules for content in The Source?