Configuring Two Factor Authentication

August 18, 2026

Checking Your Current 2-Factor Authentication Status

Open the **Security** screen in Pams before you change any sign-in protection settings. This screen contains the **2-factor Authentication** control and the **Trusted Login Devices** area for the administrator account.

1. Open **Security** and locate **2-factor Authentication**.
2. Check the status shown for the setting. Pams identifies whether 2-Factor Authentication is currently enabled or disabled.
3. If the setting is enabled, review the **Trusted Login Devices** area beneath or alongside the 2-Factor Authentication controls.
4. Compare the listed devices or browser sessions with the computers and browsers you currently use for Pams.
5. Before making any change, confirm that you can still complete the verification challenge shown by Pams when you sign in.

When 2-Factor Authentication is enabled, Pams can request an additional verification step after you sign in. A device listed under **Trusted Login Devices** has already completed that verification and may not be asked for it again during later sign-ins from that same browser or device.

[Screenshot: The Security screen showing the 2-factor Authentication status and the Trusted Login Devices area.]

Pay particular attention to device entries you do not recognize, old browser sessions, or devices you no longer control. A trusted device can bypass the additional verification prompt, so the list should reflect only devices that are appropriate for administrator access.

If you are reviewing access for other users, manage their access separately through **Users**, **Principal Users**, and the assigned **Roles** and **Teams**. For guidance on those areas, see Managing Pams Users, Managing Principal Users, and Managing Roles and Teams. The **Security** screen is specifically where you review the 2-Factor Authentication setting and trusted-device access.

Enabling 2-Factor Authentication

Enable 2-Factor Authentication from the **Security** screen when the administrator account should require an additional verification step during sign-in. Keep the Security screen open until Pams confirms that the setting is active.

1. Open **Security** and find the **2-factor Authentication** control.
2. Select the option to enable 2-Factor Authentication.
3. Read the verification or enrollment prompt displayed by Pams.
4. Complete the requested second-factor confirmation using the method available to the administrator account.
5. Wait for Pams to confirm that verification was accepted.
6. Return to the **2-factor Authentication** control and confirm that its status shows as enabled.

[Screenshot: The 2-factor Authentication control with the enabled status displayed after successful verification.]

The verification prompt is part of the activation process. Do not close the page or assume the change is complete until Pams displays the enabled status. If the confirmation does not succeed, leave the setting unchanged and repeat the verification prompt from the Security screen when you have access to the required verification method.

After activation, Pams may request the additional verification step when the administrator signs in from a browser or device that is not trusted. This allows you to keep normal access from approved work devices while ensuring that unfamiliar devices must be verified before use.

Enabling 2-Factor Authentication does not replace your existing user setup. User access remains controlled through the **Users**, **Principal Users**, **Roles**, and **Teams** areas. Use 2-Factor Authentication alongside those access assignments, rather than using it as a substitute for removing access that a former user or external party should no longer have.

Trusting a Device After Verification

Pams can offer a trusted-device choice after you successfully complete a 2-Factor Authentication challenge. Use this option only for a browser or device that is under administrator control and regularly used to access Pams.

1. Sign in to Pams from a device or browser that is not currently trusted.

2. Complete the 2-Factor Authentication verification prompt shown during sign-in.
3. If Pams presents a trusted-device option after verification, review the device you are using.
4. Select the trusted-device option only when the device and browser are appropriate for continued administrator access.
5. Finish signing in, then open **Security** and review **Trusted Login Devices** to confirm that the device appears in the list.

[Screenshot: A successful verification prompt offering the option to trust the current device.]

Trusting a device changes the sign-in experience for that specific browser or device. On later sign-ins from the trusted browser or device, Pams may not request the additional verification challenge. This helps reduce repeated prompts on an approved work computer without removing 2-Factor Authentication from the administrator account.

A trusted-device choice does not automatically apply to every device you use. For example, verifying Pams in one browser does not mean another browser on the same computer is automatically trusted. Each listed entry represents a browser or device that Pams recognizes as previously verified.

Do not select the trusted-device option on:

- Shared office computers
- Public or temporary devices
- A browser used by more than one person
- A device that you do not control
- A device you plan to replace or hand over to another user

If you accidentally trust an unsuitable device, remove it promptly from **Trusted Login Devices** on the **Security** screen.

Reviewing and Removing Trusted Devices

Use the **Trusted Login Devices** list on the **Security** screen to keep control over browsers and devices that can sign in without repeating the 2-Factor Authentication challenge. Review this list whenever an administrator changes computers, stops using a browser, or has any concern about a previously trusted session.

1. Open **Security** in Pams.

2. Locate **Trusted Login Devices**.
3. Review each device or browser entry in the list.
4. Compare each entry with the administrator-controlled devices and browsers currently approved for Pams access.
5. Select the remove option for any entry that is no longer appropriate.
6. Confirm the removal if Pams asks you to do so.
7. Refresh or revisit the **Trusted Login Devices** list to make sure the entry no longer appears.

[Screenshot: The Trusted Login Devices list with a device entry selected for removal.]

Remove a trusted entry when it relates to a device that is no longer used, an older browser session, a replaced computer, or a device that may no longer be secure. You should also remove an entry if you cannot clearly identify it as an approved administrator browser or device.

Removing a device does not prevent the administrator from using Pams on that device in the future. Instead, Pams will require 2-Factor Authentication again when that browser or device next signs in. After the verification challenge is completed, Pams may present the trusted-device option again.

Keep the list limited to active, known devices. A shorter list makes it easier to identify unexpected entries and keeps the trusted-device setting aligned with the computers and browsers that are actually used for Pams administration.

Disabling 2-Factor Authentication

Disable 2-Factor Authentication only when the administrator account no longer needs the additional verification step. Because this changes the account’s sign-in protection, review the status and trusted devices carefully before confirming the change.

1. Open the **Security** screen in Pams.
2. Locate the **2-factor Authentication** control.
3. Select the option to disable 2-Factor Authentication.
4. Review the confirmation prompt displayed by Pams.
5. Confirm the change when you are certain that 2-Factor Authentication should be disabled.
6. Return to the 2-Factor Authentication control and verify that the status now shows as disabled.
7. Open **Trusted Login Devices** and review any entries that remain listed.

[Screenshot: The Security screen showing the disabled 2-factor Authentication status and the Trusted Login Devices list.]

When 2-Factor Authentication is disabled, Pams no longer uses the additional verification challenge associated with this setting for the administrator account. Therefore, do not rely on the trusted-device list as an extra sign-in checkpoint while the setting is disabled.

After disabling the setting, remove trusted-device entries that should no longer remain recorded. This is especially important when you are changing administrator access arrangements, replacing devices, or reviewing older browser sessions. Removing unneeded entries keeps the **Trusted Login Devices** area current if 2-Factor Authentication is enabled again later.

If you only need to stop a particular browser or device from bypassing verification, do not disable 2-Factor Authentication for the entire administrator account. Instead, keep the setting enabled and remove that browser or device from **Trusted Login Devices**. The next sign-in from the removed device will require verification again.

Verifying the Security Configuration

After enabling, disabling, or changing trusted-device entries, confirm that Pams behaves as expected during an actual sign-in. Testing the result immediately helps you identify whether the current browser is still trusted or whether a change was not completed.

1. Check the status displayed beside **2-factor Authentication** on the **Security** screen.
2. If the setting is enabled, sign out of Pams and sign in again from a browser or device that is not listed under **Trusted Login Devices**.
3. Confirm that Pams displays the additional verification challenge.
4. Complete the verification prompt and confirm that you can sign in successfully.
5. Remove a test device from **Trusted Login Devices** if appropriate.
6. Sign out and sign in again from that removed browser or device.
7. Confirm that Pams asks for 2-Factor Authentication again before allowing access.
8. If 2-Factor Authentication is disabled, confirm that the Security screen shows the disabled status after you sign in again.

[Screenshot: A sign-in verification prompt shown after a device has been removed from Trusted Login Devices.]

If Pams does not display the expected verification prompt, first return to **Security** and confirm that **2-factor Authentication** is enabled. Then check whether the current browser or device still appears under **Trusted Login Devices**. A trusted entry can explain why a second-factor prompt is not shown on that device.

Before changing the setting again, make sure you can complete the verification method available to the administrator account. If that method is unavailable, do not make further changes until you can use Pams' supported access process to restore administrator access. This avoids leaving the account unable to complete the sign-in process.

Overview

2-Factor Authentication adds a second verification step to administrator sign-in in Pams. The setting is managed from the **Security** screen, where you can see whether **2-factor Authentication** is enabled or disabled and where you can review **Trusted Login Devices**.

The main controls work together as follows:

Pams area or control	What you use it for	Result
2-factor Authentication	Enable or disable the extra sign-in verification step	Pams either requires or does not require additional verification during sign-in
Trusted Login Devices	Review browsers and devices that have already been verified	Approved devices may bypass repeated verification prompts
Remove trusted device	Withdraw trusted status from a browser or device	The removed device must verify again at its next sign-in

Use 2-Factor Authentication to protect the administrator account while allowing practical day-to-day access from approved work devices. A trusted device is not a general permission for every browser, computer, or person. It applies only to the specific device or browser session that was verified and appears in **Trusted Login Devices**.

The **Security** screen does not replace the user-access controls in Pams. Continue to manage who can enter Pams through **Users** and **Principal Users**, and control what each person can access through **Roles** and **Teams**. Those tasks are covered in Managing Pams Users, Managing Principal Users, and Managing Roles and Teams.

When reviewing account protection, use the Security screen to answer three practical questions:

- Is **2-factor Authentication** enabled for the administrator account?
- Does **Trusted Login Devices** contain only recognized, approved browsers and devices?
- Can the administrator complete the verification prompt if Pams requests it during sign-in?

Prerequisites

Before you change 2-Factor Authentication in Pams, make sure you can access the **Security** screen as an administrator and can complete any verification prompt that Pams displays. The change is not complete until Pams accepts the required confirmation and updates the status shown for **2-factor Authentication**.

Prepare the following before enabling, disabling, or testing the setting:

- Access to the administrator account that manages the **Security** screen
- Access to the browser or device you are currently using to sign in to Pams
- Access to the second-factor verification method used by the administrator account
- Time to sign out and sign back in when you need to test the result
- A clear list of the administrator-controlled devices and browsers that should remain under **Trusted Login Devices**

If you are enabling 2-Factor Authentication, complete the change from a device you can continue to use while Pams displays the enrollment or verification prompt. Do not begin the process if you cannot access the available verification method, because you need to complete the prompt before Pams can show the enabled status.

If you are reviewing trusted devices, identify devices that should be removed before opening the list. Typical examples include a replaced computer, an old browser session, or a device that is no longer used for administrator work. Removing those entries means Pams will request verification again if that browser or device tries to sign in later.

For access-assignment changes rather than sign-in protection changes, use the relevant Pams screens described in Managing Pams Users, Managing Principal Users, and Managing Roles and Teams.