

Release Note

Release Information

Product Platform: **Linux**

Product Version: **4.0**

Date: **18 December 2025**

Linux 4.0

Introduction

Admin By Request for Linux 4.0 contains significant stability and performance improvements, a number of bug fixes and two new features. The new features are *Break Glass* and *Multi-Factor Authentication (MFA)*, for both graphical user and command line interfaces.

In addition, the Linux client now supports *Account Separation*, whereby a secondary account can be used for tasks requiring elevated privileges.

In this document

"Prerequisites" on page 2

"Support for Break Glass" on page 2

"Multi-Factor Authentication (MFA)" on page 2

"Account Separation" on page 3

"How does the Update Process work?" on page 3

Refer to the [Admin By Request Documentation Center](#) for full details on these new features or any other aspect of Admin By Request.

Prerequisites

Organizations wishing to evaluate endpoints running Linux 4.0 need the following:

1. One or more devices running one of the following operating systems:
 - Ubuntu 20.04 LTS
 - Ubuntu 22.04 LTS
 - Ubuntu 24.04 LTS
 - Red Hat Enterprise Linux (RHEL9)
 - Rocky Linux 9.0
2. Credentials to access the Admin By Request portal at **<https://adminbyrequest.com/login>**
3. Admin By Request for **Linux 4.0** client software, downloaded from the portal and available to each endpoint

Support for Break Glass

The *Break Glass* feature is now available on Linux endpoints. A Break Glass Account is for situations such as when the domain trust relationship is broken or an administrator without credentials needs to service the endpoint. The provisioned account is a temporary local user created in the local administrators group. Once logged-in, the account must be used within a pre-configured time (typically **2 hours**) and the account is removed after a single use.

Conceptually, this works in the same way as for the Windows and Mac clients:

- In the portal inventory, you issue a new, temporary, one-time-use administrator account for a specific endpoint.
- Behind-the-scenes, we instruct the endpoint that these credentials are now available.
- At the endpoint, the user (e.g. IT Admin) logs in using this account and receives full administrative permissions.
- When the user logs out, or the pre-configured time expires, the session is terminated and the account is removed.

Refer to [Setting-up a Break Glass Account](#) for more information.

Multi-Factor Authentication (MFA)

Portal administrators can now use *Multi-Factor Authentication (MFA)* to authenticate users logging-in on Linux endpoints. As with the *Break Glass* feature, the concept is the same as on Windows and Mac endpoints; portal admins can direct that elevation requests should be authenticated with MFA using a portal setting. This means that when Linux users attempt to elevate, or optionally run a pre-approved app, they need to authenticate via a single sign-on (SSO) email match against Entra ID or Active Directory.

This works on both graphical systems and in the command-line interface. On GUI systems a browser appears that allows users to authenticate – much like Windows and Mac clients. In the command-line console, users are instead presented with a URL and an ASCII-rendered QR-code that can be scanned on their phones to get the authentication window to pop up.

Refer to [Using MFA with Run As Admin](#) or [Using MFA with Admin Sessions](#) for more information.

Account Separation

Account Separation for Cyber Essentials Plus compliance is now available on Linux endpoints, allowing administrators to enforce that privilege elevation requires an account that is different from the day-to-day account used on the endpoint.

Refer to [Cyber Essentials Plus](#) for more information.

Bug fixes

Several minor bugs have been fixed in Admin By Request for Linux 4.0. Inaccurate text and screenshots have also been updated in the portal.

How does the Update Process work?

Admin By Request software updates to Linux endpoints are delivered via the distribution package update process. Please note that, when we release a new version, we do not make it immediately available to the update process. This is simply to mitigate any unforeseen issues.

Our rule-of-thumb for a new release is to make it available within **4 - 8 weeks** of release, but this is subject to change, depending on feedback and any potential issues that might arise.

[Contact us](#) if you wish to receive the latest version right now. You can also raise a support ticket requesting the latest update.