

Endpoint Privilege Management (EPM) | Linux

Product Version: 4.0

Linux Client: IT Admin Guide

Document Information

Code: PM-LC-ITAG

Version: 2.0

Date: 18 December 2025

Copyright © 2025 Admin By Request

All rights reserved.

Information in this document is subject to change without notice. The software described in this document is furnished under a license agreement or nondisclosure agreement (NDA). The software may be used or copied only in accordance with the terms of those agreements.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or any means electronic or mechanical, including photocopying and recording for any purpose other than the customer's stated use without the written permission of Admin By Request.

Contact Admin By Request



+64 21 023 57020



marketing@adminbyrequest.com



adminbyrequest.com



Unit C, 21-23 Elliot St, Papakura, NZ

Table of Contents

| | |
|--|-----------|
| Linux Client - Overview | 1 |
| Introduction | 1 |
| In this document | 1 |
| Audience | 1 |
| Product Release Notes | 1 |
| Linux Client - Install / Uninstall | 2 |
| Prerequisites | 2 |
| Your Tenant License | 2 |
| Installing Admin By Request | 2 |
| Upgrading Admin By Request | 4 |
| Deploying new releases | 5 |
| Uninstalling Admin By Request | 5 |
| User rights after installation | 6 |
| Tamper Prevention | 6 |
| Performance after Installation | 7 |
| File Locations | 7 |
| The Linux GUI Client User Interface | 8 |
| About Admin By Request | 8 |
| In this topic | 8 |
| About Admin By Request | 9 |
| Connecting via a Proxy Server | 14 |
| Ports and IP addresses | 15 |
| Using Run As Admin | 16 |
| MFA with Run As Admin | 17 |
| Requesting Administrator Access | 18 |
| MFA with Admin Sessions | 20 |
| Setting-up a Break Glass Account | 21 |
| About Break Glass | 21 |
| Security benefits | 21 |
| When would I use a Break Glass account? | 22 |
| Break Glass Prerequisites | 22 |
| Using the Break Glass feature | 22 |
| The Linux Command Line Interface | 26 |
| Introduction | 26 |
| Prerequisites | 26 |

| | |
|--|-----------|
| Commands | 27 |
| abr finish | 27 |
| abr settings | 28 |
| abr start | 29 |
| abr version | 29 |
| abr status | 30 |
| abr --help | 30 |
| abr --master-config-file | 31 |
| abr --system-config-file | 32 |
| abr --log-level | 32 |
| Auditlog | 33 |
| Portal Administration for Linux | 35 |
| Introduction | 35 |
| In this topic | 35 |
| Run As Admin Settings | 36 |
| Admin Session Settings | 37 |
| Changing Admin Session Duration | 38 |
| Endpoint Settings | 38 |
| Look & Feel tab | 38 |
| Instructions tab | 39 |
| Lockdown Settings | 40 |
| Admin Rights tab | 40 |
| Sudo tab | 41 |
| Root tab | 41 |
| App Control Settings | 42 |
| Pre-Approve tab | 42 |
| Block tab | 45 |
| Privacy Settings | 47 |
| Entra ID Support | 48 |
| Preventing Abuse | 50 |
| Policies for Linux | 51 |
| Overruling Portal Settings | 51 |
| Supplementary Technical Information | 53 |
| Local Administrator Accounts | 53 |
| Sub-Settings | 54 |
| Sudo | 54 |
| Tampering | 54 |
| Terms and Definitions | 55 |
| Privileged Access | 55 |

Glossary56

Document History58

Index60

Linux Client - Overview

Introduction

Admin By Request's Privileged Access Management (PAM) solution is designed to solve the security and productivity challenges relating to Local Administration rights usage within today's security conscious and highly distributed enterprises.

Employees achieve optimum productivity by using secure methods to safely elevate everyday trusted tasks. IT departments achieve significant time and resource savings as employee requests for elevation are offloaded and routed through streamlined, fully audited and automated workflows.

This guide describes key IT administrator concepts and tasks related to installing, configuring, deploying, and managing linux endpoints.

In this document

The content of this guide describes:

- How to install the Admin By Request client on endpoints running Linux.
- How to uninstall Admin By Request.
- The user interface, including screen panels associated with menu selections.
- Key portal administration tasks, specific to Linux.
- Selected Settings tables, describing how to use each setting.
- Terms and definitions.

Audience

The Linux Client: IT Admin Manual is intended for IT system administrators who install and manage user workstations running the Linux operating system and desktop software.

NOTE

Although the guide is written from the point of view of an IT Administrator, the procedure steps and screenshots are described from an end user's perspective. This has two benefits:

1. You can clearly see how something works from an end user's point of view.
2. If required, you can create your own customized end user documentation by simply copying and pasting the procedures with minimal rework.

Product Release Notes

Release notes for all product versions are available on the Admin By Request documentation website:

[Release Notes \(Linux\)](#)

Linux Client - Install / Uninstall

Prerequisites

1. An endpoint device running the Linux operating system. Admin By Request for **Linux 4.0** supports the following Linux distributions:
 - Ubuntu 20.04 LTS
 - Ubuntu 22.04 LTS
 - Ubuntu 24.04 LTS
 - Red Hat Enterprise Linux (RHEL9)
 - Rocky Linux 9.0These distributions that have been tested and approved for Admin By Request **Linux 4.0**.
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.
4. You will also need the following on every workstation that executes the installation client:
 - Administrator privileges (e.g., the ability to run sudo).
 - Python 3 installed - the installation client is a Python script. This is not required if Admin By Request is downloaded to the workstation as part of an image.

NOTE

The installation script uses standard package management features and may install or update some dependencies if necessary. Once installed, future updates to Admin By Request are handled completely by package management.

Your Tenant License

The installer file downloaded from the portal is **unique to your tenant**. Depending on the target operating system, it can be an executable file, a package or a script and it is signed with a license that applies *only* to installers downloaded from the tenant in which you are currently logged-in. The same license file is applied to each of the operating system client installers: Windows, macOS, Linux and Server.

This is true for free plans as well as paid plans.

When installed on an endpoint, once the endpoint connects successfully, you will see in real time the status of the endpoint in your Inventory, which is also unique to your tenant. You will not see any endpoints installed with files downloaded from other tenants - this is simply not possible.

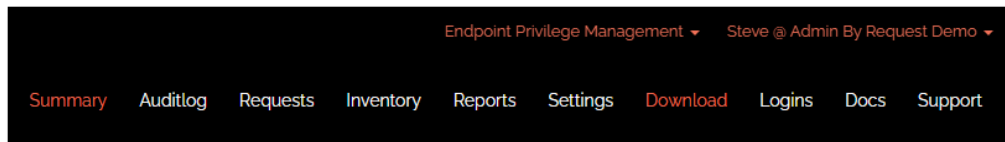
Installing Admin By Request

The following installation procedure is in two parts: the first outlines downloading and installing the Admin By Request package, and the second part describes how to test that installation was successful.

Installation steps are grouped into the following tasks:

A. Download and install the Admin By Request package.

1. If you haven't already, login to the Admin By Request [portal](#).
2. In the portal, click the [Download](#) menu link to download the Linux endpoint client and store the file in a suitable location:



3. Make a note of the installer file name - needed in the next steps.
4. If you haven't already, start a terminal session and make sure the file is executable:

```
chmod +x abr-installer*
```

5. Run the installation script:

```
sudo ./abr-installer\ 4.0.0
```

6. When the installation completes, the Admin By Request icon appears in the top right corner of the screen. Click the icon to show details about the client or start an Admin Session.

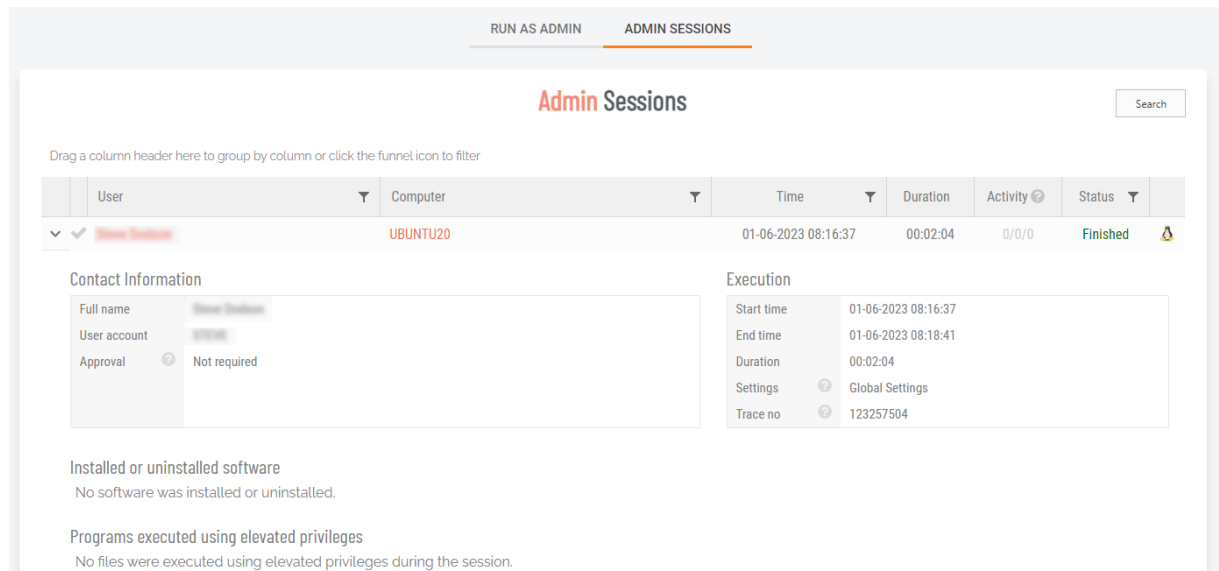
Installation is now complete.

B. Test the installation.

1. At the command line, enter a command that requires elevated privileges (e.g., **sudo apt update**).
The result should be a line explaining that sudo is not allowed by Admin By Request - an admin session is required.
2. Log in to the Admin By Request [portal](#).
3. From the portal menu at the top, select **Endpoint Privilege Management > Settings > Linux Settings**
4. Under **AUTHORIZATION**, check the current settings and change any that you wish to test. For example, you might set the *Access time (minutes)* to **5**.
5. Return to the Linux workstation and start an admin session:
 1. Click the Admin By Request icon in the top right corner of the screen and select **Request administrator access**.
 2. Confirm you want to start a session now (answering any questions that might pop up, such as **Reason**).
6. Run the sudo command above again and confirm that it works this time.
7. You can now finish the admin session or allow it to time out.

You might also want to check the audit log in the portal, to review the details that were logged as part of this admin session:

1. From the portal menu at the top, select **Auditlog**.
2. Under **ADMIN SESSIONS**, find the name of the logged-in user and expand the drop-down arrow:



The screenshot shows the 'Admin Sessions' interface. At the top, there are tabs for 'RUN AS ADMIN' and 'ADMIN SESSIONS'. Below the tabs, there's a search bar and a table of sessions. The table has columns for User, Computer, Time, Duration, Activity, and Status. A session for user 'Steve Baskin' on computer 'UBUNTU20' is highlighted. Below the table, there's a detailed view of the session, including 'Contact Information' (Full name, User account, Approval), 'Execution' (Start time, End time, Duration, Settings, Trace no), 'Installed or uninstalled software', and 'Programs executed using elevated privileges'.

3. Note the activity - in the example shown, no software was installed or uninstalled, and no files were executed using elevated privileges during the session.

Upgrading Admin By Request

To immediately upgrade Admin By Request on a Linux endpoint, simply run the standard `:system update / upgrade` commands at the command line:

You can either start an Admin Session or execute each `sudo` command via *Run As Admin*.

1. Start a terminal session.
2. If you're starting an Admin Session and need Admin By Request approval to run `sudo` commands, request it.
3. Once approved, execute the system update/upgrade commands:

Debian-based distributions

```
sudo apt update
sudo apt upgrade -y
```

Red Hat-based distributions

```
sudo dnf update --refresh
```

Upgrading Admin By Request typically changes one or more of the following packages:

- abr-gui
- abr-linux
- abr-pam-plugin
- abr-polkit-plugin
- abr-service
- abr-sudo-plugin
- abr-cli
- abr-nss

Deploying new releases

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.

Uninstalling Admin By Request

To uninstall Admin By Request:

1. Shutdown and reboot the computer.
2. Do one of the following:
 - If your computer boots using BIOS, *press and hold down* the **Shift** key while GRUB is loading.
 - If your computer boots using UEFI, press the Escape key (**Esc**) while GRUB is loading.
 - As you're booting the computer, wait for the manufacturer logo to flash from the BIOS. If your computer boots too quickly, you're going to need to do this immediately after powering it on. Quickly press the **Escape** key.

The timing has to be near perfect on some computers, so you may have to press the key repeatedly. If you miss the window, reboot and try again.

3. At the GRUB boot menu, you'll see an entry for "Advanced Options ...". Select it and press **Enter**.
4. Choose the most recent *recovery mode* option and press **Enter**.

5. If a menu similar to that shown below appears, choose the option that gets you to a shell prompt:

```
Recovery Menu (filesystem state: read-only)

resume          Resume normal boot
clean           Try to make free space
dpkg            Repair broken packages
fsck            Check all file systems
grub            Update grub bootloader
network         Enable networking
root            Drop to root shell prompt
system-summary  System summary

<Ok>
```

6. At the *Password:* prompt, enter the root password..
7. Now you can uninstall Admin By Request for Linux by executing the following command:

Debian-based distributions

```
apt -y purge abr-* && apt -y autoremove
```

Red Hat-based distributions

```
sudo dnf remove "abr-*"
```

User rights after installation

When a user logs on, the account is downgraded from Administrator to Standard User unless:

- You have turned off **Revoke Admins Rights** in the portal settings (**EPM > Settings > Linux Settings > Lockdown > ADMIN RIGHTS**).
- Also under **Revoke Admins Rights**, the user is in the list of *Excluded accounts*.
- The computer is domain-joined and the user is a domain administrator.

Please refer to ["Supplementary Technical Information" on page 53](#) for more information.

Tamper Prevention

When a user initiates an administrator session, the user's role is not actually changed from user to admin. The user is granted all administrator rights, *except* the right to add, modify or delete user accounts. Therefore, there is no case where the user can create a new account or change their own role and become a permanent administrator.

The user also cannot uninstall Admin By Request, as the only program, to keep the administrator session open forever. Furthermore, all settings, configuration and program files are monitored during administrator sessions. If the user tries to remove or change any of the Admin By Request files, these are restored straight away and the attempted activity is logged.

Performance after Installation

When users are not using Admin By Request, it does not consume resources, except for a brief daily inventory and settings check.

File Locations

Admin By Request maintains files and logs in the following locations:

- Executable Files: `/usr/bin`
- Configuration Files: `/etc/abr` and `/usr/share/abr/configuration`
- Log Files: `/var/log/abr`

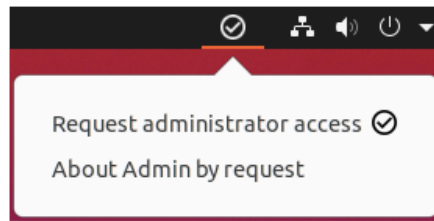
The Linux GUI Client User Interface

About Admin By Request

The user interface is graphical and is accessed via the icon menu in the menu bar (top right) of the screen:



Click the icon to display the menu and select *About Admin By Request* for further information:



In this topic

"About Admin By Request" on the next page

"Connecting via a Proxy Server" on page 14

"Using Run As Admin" on page 16

"Requesting Administrator Access" on page 18

"Setting-up a Break Glass Account" on page 21

About Admin By Request

Once installed, Admin By Request is running in the background for as long as the endpoint is powered-on. Selecting the app from the menu bar launches the *user interface*, which comprises a simple window with two buttons down the left-hand side:



The default panel is *About Admin By Request*, which is accessed via the top button. It shows the current workstation edition, license details, website link, and copyright information.

Click the **About** button to get back to this panel if viewing one of the other panels.

There are two buttons in the Linux client: *About* and *Connectivity*, each displaying a panel. The About panel includes a link that opens further panels for each of the Linux client *Components*.

Other Panels (accessed via their respective buttons/links).

- **About** – the default panel (see description above).

Components

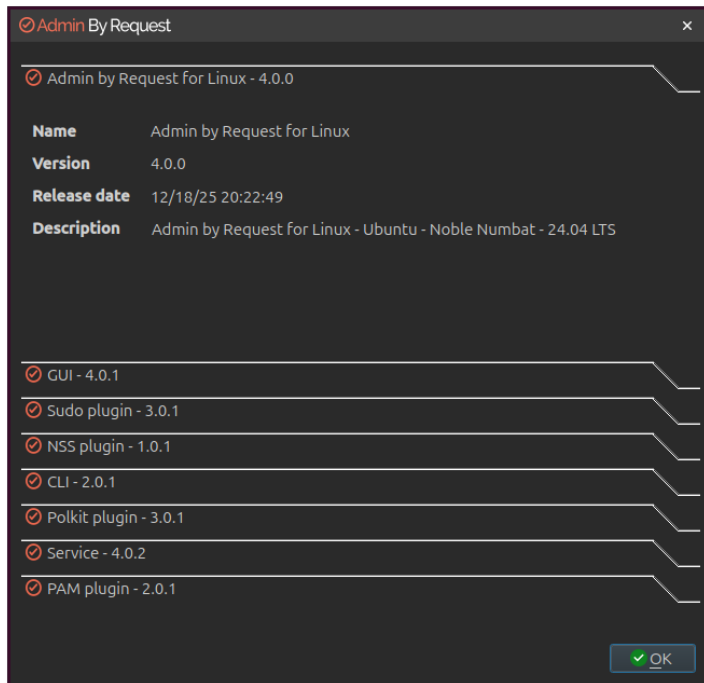
Clicking link *Components* on the About panel displays information about the individual modules that make up Admin By Request.

The modularized architecture means components can be updated as required via Linux distribution package management with minimal impact on other parts of the system.

The following screens show current component versions. Refer to these should the need arise during troubleshooting.

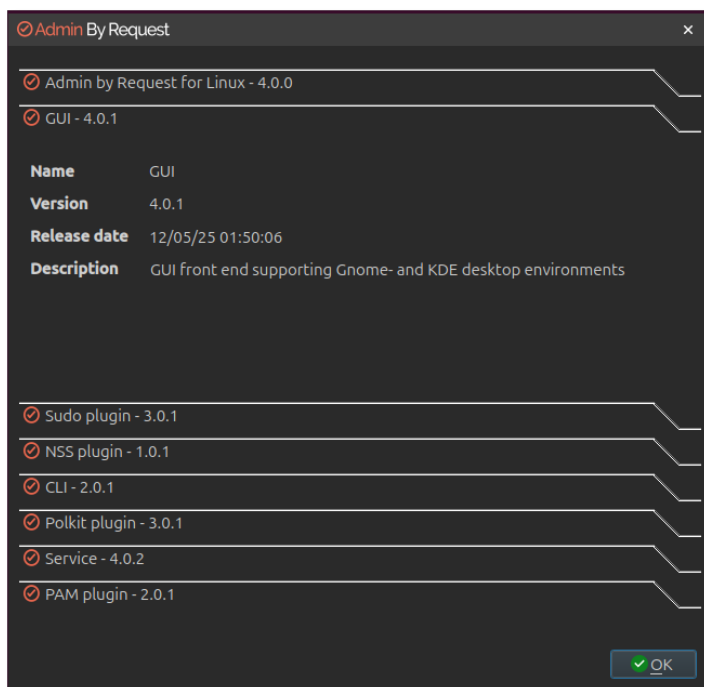
1. Admin By Request for Linux:

The main module for logic and functionality carried out by the application. This module also supplies the version number of the Linux client that is installed.



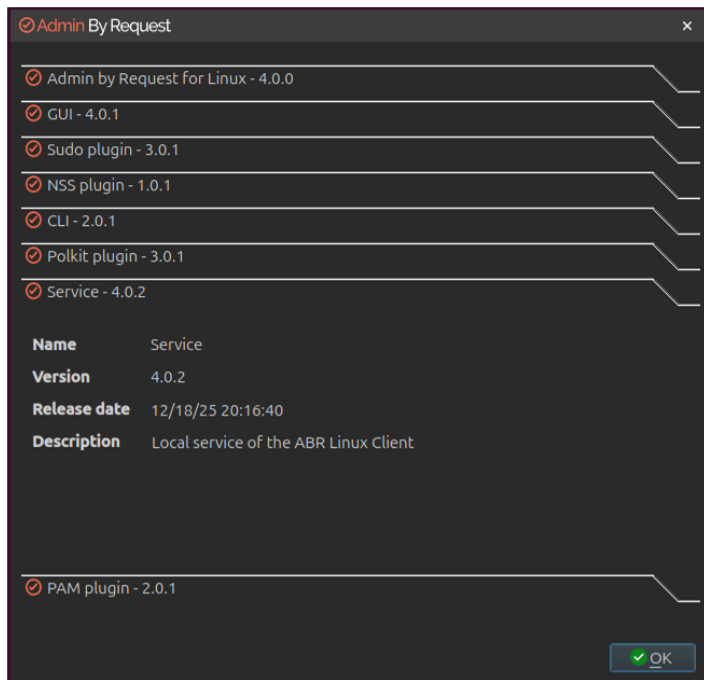
2. GUI:

User interface front-end, supporting both Gnome and KDE desktop environments.



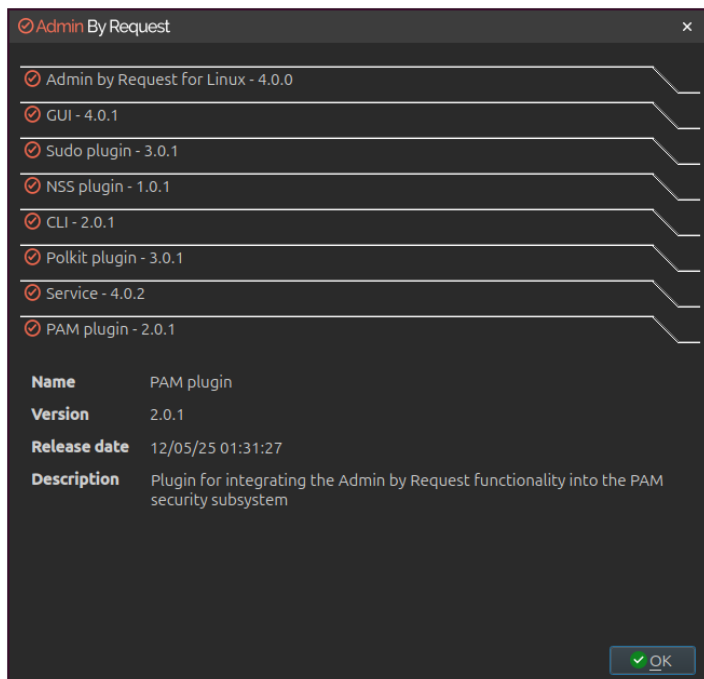
3. Service:

The local service for the Admin By Request Linux client.



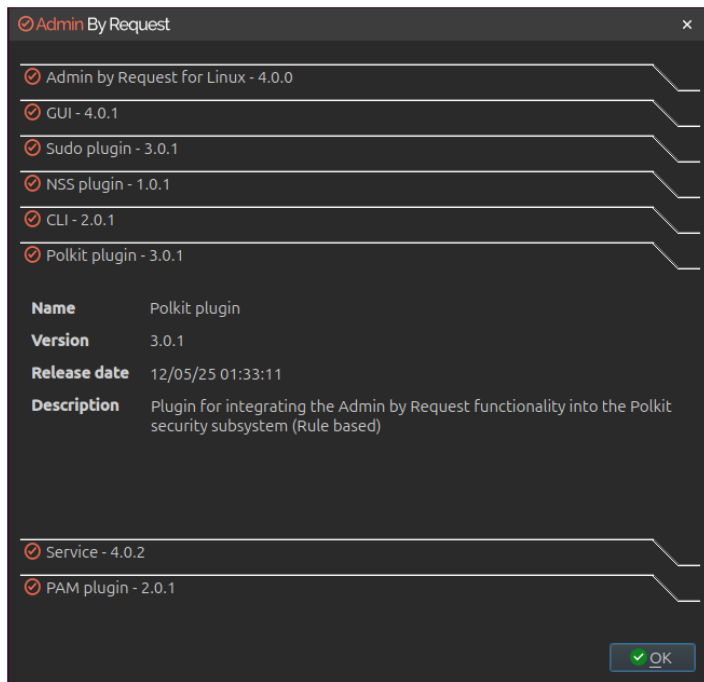
4. PAM plugin:

Privileged Access Management plugin, supporting the main module.



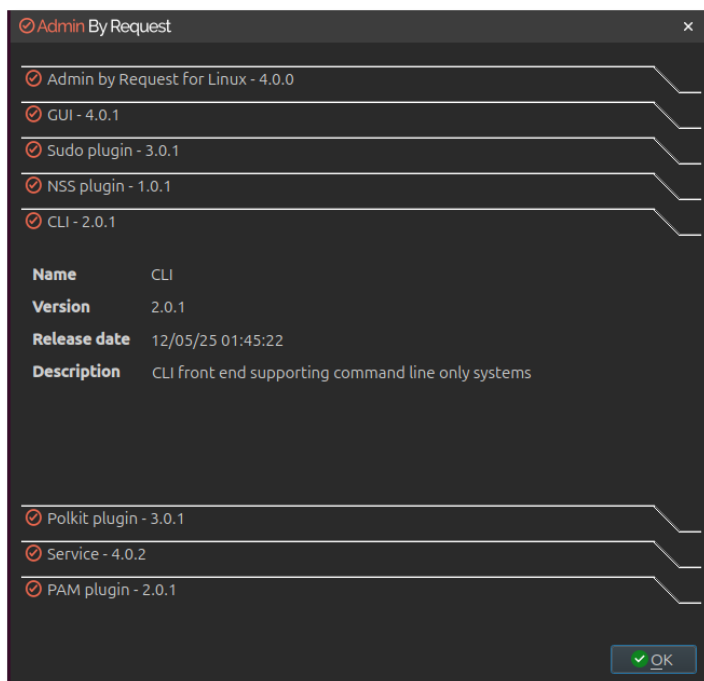
5. Polkit plugin:

A plugin for integrating application functionality into the Polkit security subsystem.



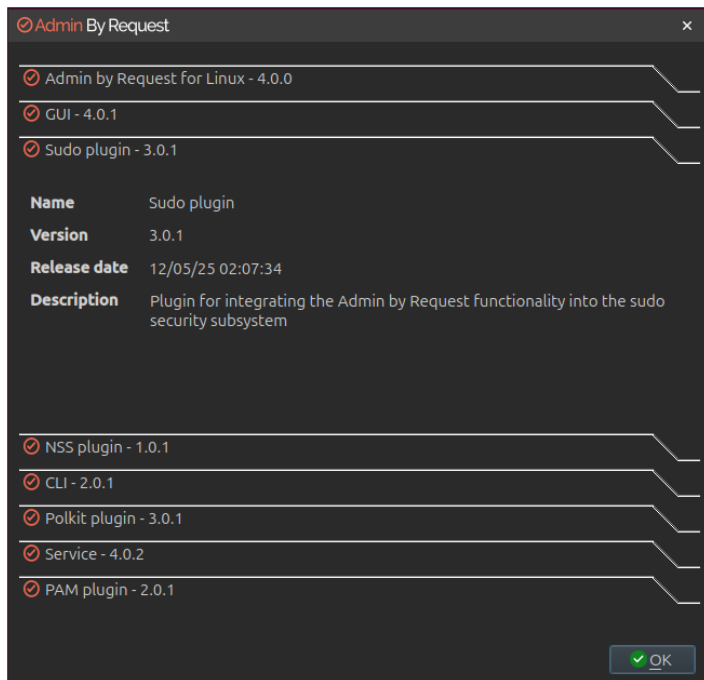
6. CLI plugin:

The Command Line Interface plugin for enabling user input and app responses via the command line.



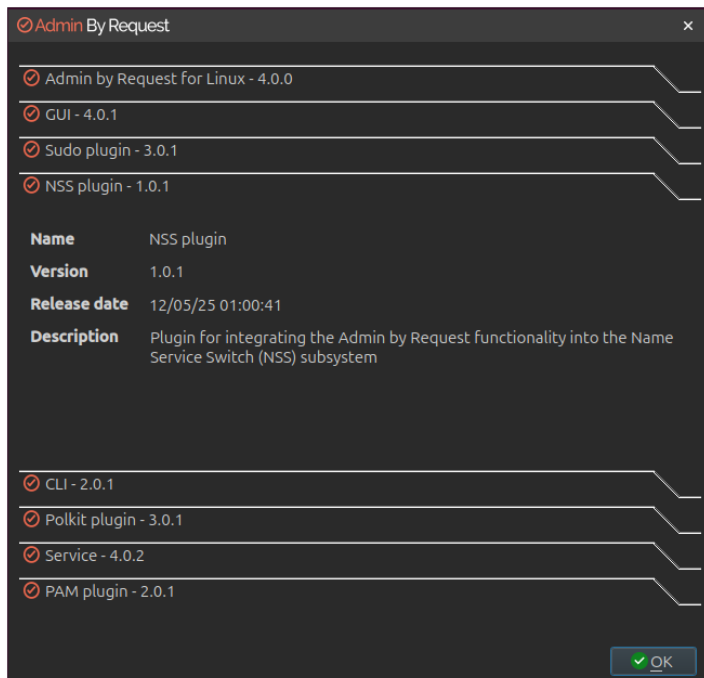
7. Sudo plugin:

A plugin for integrating application functionality into the sudo security subsystem.



8. NSS plugin:

A plugin for integrating application functionality into the Name Service Switch subsystem.



- **Connectivity** – displays the current operational status of the Admin By Request system, including Internet and Cloud connectivity, and details about the current workstation and user (see ["Connecting via a Proxy Server" on the next page](#) for panel).

- **Components - CLI**

To view components from the command line, use command:

```
abr version --components
```

```
erich@Linux-VM2:~$ abr version --components
```

| Name | Version |
|----------------------------|---------|
| GUI | 4.0.1 |
| Sudo plugin | 3.0.1 |
| Admin by Request for Linux | 4.0.0 |
| NSS plugin | 1.0.1 |
| CLI | 2.0.1 |
| Polkit plugin | 3.0.1 |
| Service | 4.0.2 |
| PAM plugin | 2.0.1 |

```
erich@Linux-VM2:~$
```

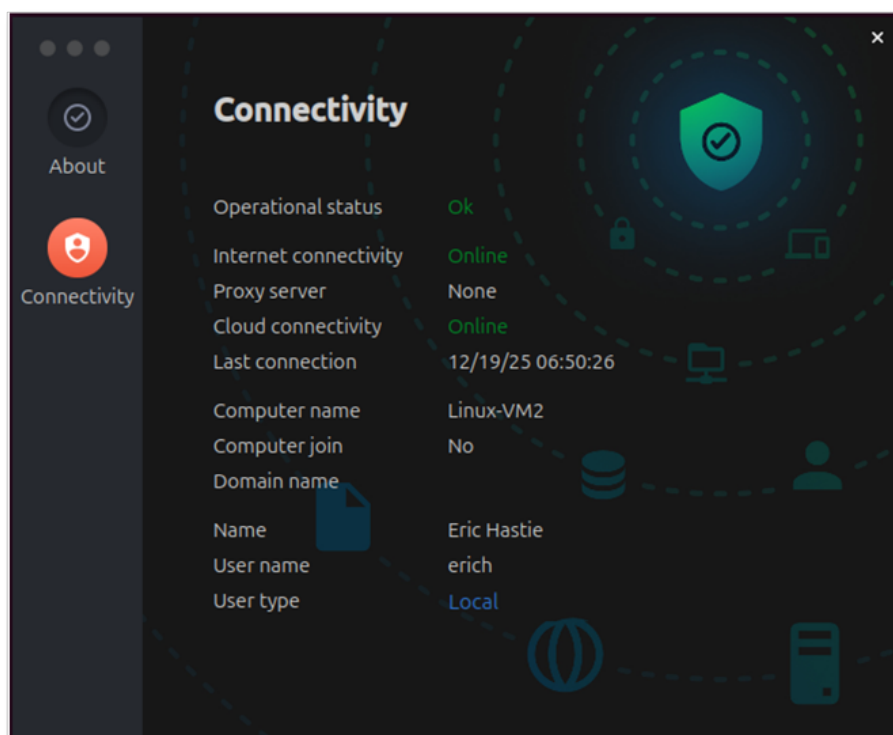
Connecting via a Proxy Server

Endpoints can be configured to route privilege requests through a proxy server, which works transparently with Admin By Request.

If the user does have a proxy server enabled, its configuration is passed to the underlying service that will in turn use this proxy for cloud service communications. The proxy traffic uses NO-AUTH (no credentials) and will be seen as the computer account generating the traffic.

NOTE

The **Connectivity** panel shows a proxy server and AD information *only* if they are used for the connection. This is different from previous versions of the client, where, if none were found, proxy server and AD connector were indicated with "None" and "Not applicable" respectively.



Ports and IP addresses

Admin By Request uses port **443** and the IP addresses and API URLs that need access through firewalls are as follows.

If your data is located in Europe (Netherlands):

- IP: **104.45.17.196**
- DNS: **linuxapi1.adminbyrequest.com**

If your data is located in the USA:

- IP: **137.117.73.20**
- DNS: **linuxapi2.adminbyrequest.com**

If your data is located in the UK:

- IP: **85.210.211.164**
- DNS: **linuxapi3.adminbyrequest.com**

If your data is located in Europe (Germany):

- IP: **9.141.94.162**
- DNS: **linuxapi4.adminbyrequest.com**

If your data is located in Asia (Singapore):

- IP: **52.230.54.129**
- DNS: **linuxapi6.adminbyrequest.com**

Wherever you are, you can also use **api.adminbyrequest.com**, but the regional URLs will likely be more responsive.

When the endpoint starts up, Admin By Request checks to see if it can connect directly to its host cloud server. If it can, then no proxy server is required and no proxy server details are shown in the **Connectivity** panel.

If it cannot connect directly, it checks the following configuration file and works through the listed servers one by one until a connection is possible:

```
/etc/abr/configurations.d/proxy.conf.template
```

The default entries in this file are listed below. If you need to configure a proxy server, replace the information in this file with your proxy server information.

```
{
  "proxy":
  [
    {
      "type": "HTTPS",
      "hostname": "my-proxy-01.anyone.com",
      "port": 8080
    },
    {
      "type": "HTTPS",
      "hostname": "my-proxy-02.anyone.com",
      "port": 8080
    }
  ],
}
```

If the endpoint connects via a server configured in this file, **None** is replaced by the *hostname* of the proxy server and all privilege requests are routed through it.

Refer to [How We Handle Your Data](#) for more information.

Using Run As Admin

In Linux, a single line `sudo` command implements *Run As Admin*, where elevated privileges are required.

The following steps illustrate how to download and install Foxit PDF Reader (64-bit) on Ubuntu 22.04 using a terminal session:

1. Download the installation tar file and change to the Downloads directory:

```
wget -P ~/Downloads
http://cdn01.foxitsoftware.com/pub/foxit/reader/desktop/linux/2.x/2.4/en_
us/FoxitReader.enu.setup.2.4.4.0911.x64.run.tar.gz

cd ~/Downloads
```

2. Unpack the tar file to create a `.run` file:

```
tar xzvf FoxitReader*.tar.gz
```

3. Check that the `.run` file is executable. If not, make it so:

```
chmod a+x FoxitReader*.run
```

4. Use `sudo` to install Foxit PDF Reader system-wide (installs in `/opt` rather than `/home`):

```
sudo ./FoxitReader*.run
```

If approval is required, a pop-up will appear asking for information, including reason. If approval is not required, a reason might still be needed for logging purposes.

5. Continue with the installation. When the `sudo` command is complete, check details logged for the install in the portal under **Auditlog > RUN AS ADMIN** rather than **Auditlog > ADMIN SESSIONS**. The `sudo` command is logged under RUN AS ADMIN.

Pre-approved applications run without prompting for a reason and the activity is logged under RUN AS ADMIN. (e.g. the `sleep` command).

Check the audit log in the portal for details on the user, the endpoint, the application run and execution history.

NOTE

Elevated privileges last only for the duration of the install and apply only to the particular application or package authorized.

MFA with Run As Admin

Prerequisites

Using MFA with Linux endpoints requires a hybrid Active Directory setup, including a local Active Directory domain controller which is synced to a cloud identity provider, such as Microsoft Entra ID, Okta or Google Cloud.

At the time of writing, a local domain controller is essential if authenticating to **any** cloud identity provider.

Usage

MFA is available as an option for authenticating users prior to granting *Run As Admin* privileges. The options in the portal for authenticating users are:

1. **Confirm** - User must confirm with **Yes** or **No** to elevate via *Run As Admin*.
2. **Multi-factor Authentication** - User must validate identity using MFA through SSO.

The MFA options are:

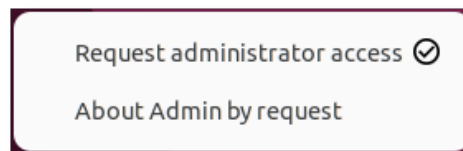
- **No matching** - This option is not available for Linux endpoints, (which is why a hybrid setup is required).
- **Email match** - The logged-in user must authenticate using the email associated with the login credentials.
- **Account separation** - The logged-in user must authenticate using a secondary account. Required for **Cyber Essentials Plus** compliance.

Refer also to [Linux Settings \(Authentication tab\)](#).

Requesting Administrator Access

Requesting administrator access is also known as requesting an *Admin Session*, which is a time-bound period during which a standard user has elevated privileges and can carry out administrator-level tasks..

As with *About Admin By Request*, click the menu bar icon to display the menu and select **Request administrator access**:



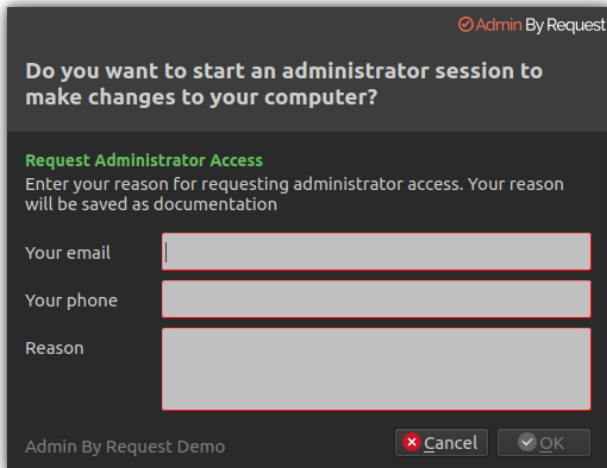
NOTE

Timing can be important when an admin session is started for some GUI operations:

- If you start an admin session *after* you have started the GUI interface (for example, add a new user account in Settings), you might need to refresh the current GUI screen by selecting another option in Settings, then going back to User Accounts.
- If you start the admin session *before* opening Settings, there is no need to refresh the user interface.

A standard user making this selection *where approval is required* initiates the following sequence of events.

1. An empty *Request Administrator Access* form appears:



2. The user enters *email*, *phone* and *reason* information into the form and clicks **OK**.

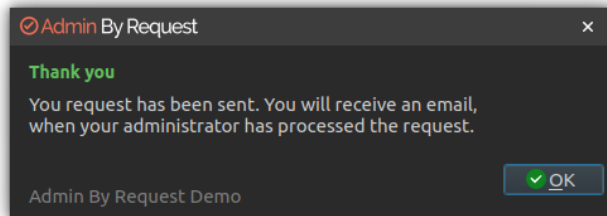
NOTE

Settings in the portal control the full extent of what is displayed to the user:

- If *Code of Conduct* is enabled, the user must acknowledge a Code of Conduct pop-up to continue (**EPM > Settings > Linux Settings > Endpoint > INSTRUCTIONS**).

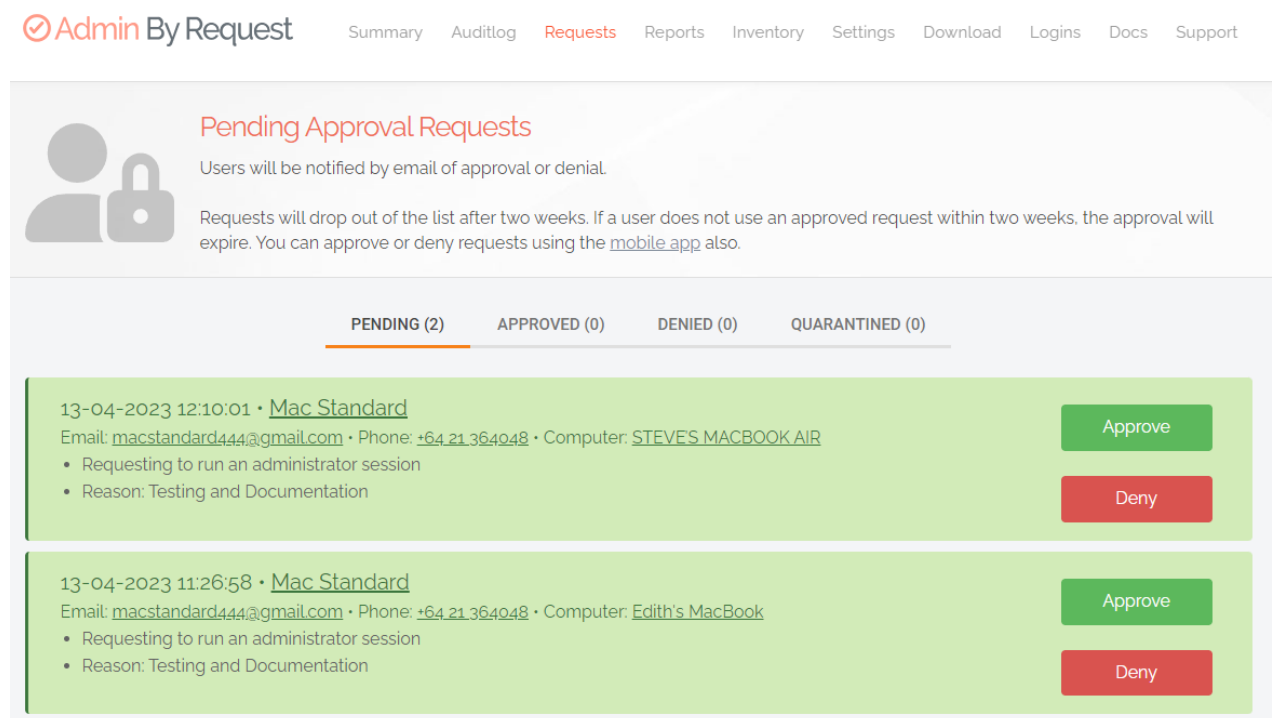
- If *Require approval* is OFF, the approval steps are skipped (**EPM > Settings > Linux Settings > Authorization > AUTHORIZATION > Admin Session**).

3. The request is submitted to the IT administration team and the user is advised accordingly:

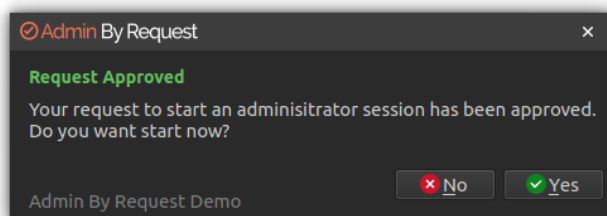


4. The IT administration team is notified via the Admin By Request portal that a new request for administrator access has arrived.

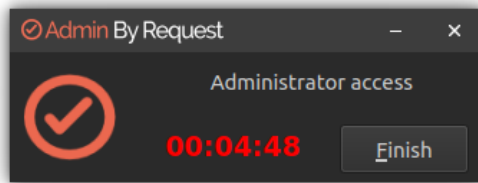
The following example shows how two new requests might appear in the portal:



5. One of the team either approves or denies the request. If approved, the user is advised accordingly:

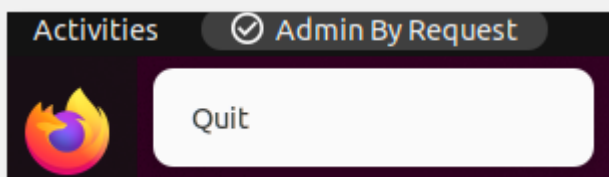


6. The user clicks **Yes**, which starts the session and displays a countdown timer:



7. The duration of an admin session is set via the portal (5 minutes in this example) and the countdown timer ticks down to zero, at which time the session ends. The user can optionally end the session at any time once it has started by clicking **Finish**.

On Linux endpoints, clicking the countdown timer window enables an app menu with a single item:



Selecting **Quit** does not end the admin session - it simply closes the countdown timer window. The admin session continues running (and counting down) in the background. If you click the ABR menu bar icon and select **Request administrator access** again, the countdown timer will reappear (unless it has expired, in which case you'll be prompted to start a new session).

See ["Changing Admin Session Duration" on page 38](#) for more information on changing the duration of the countdown timer.

During an *Admin Session*, users can install programs requiring admin rights, install drivers and change system settings other than user administration. All activity during the elevated session is audited, so you can see in the audit log the reason why the person needs the elevation; anything installed, uninstalled, or executed.

IMPORTANT

During an *Admin Session*, users **cannot** uninstall Admin By Request, or add, remove or modify user accounts.

MFA with Admin Sessions

Prerequisites

Using MFA with Linux endpoints requires a hybrid Active Directory setup, including a local Active Directory domain controller which is synced to a cloud identity provider, such as Microsoft Entra ID, Okta or Google Cloud.

At the time of writing, a local domain controller is essential if authenticating to **any** cloud identity provider.

Usage

MFA is available as an option for authenticating users prior to granting *Admin Session* privileges. The options in the portal for authenticating users are:

1. **Confirm** - User must confirm with **Yes** or **No** to elevate via *Admin Session*.
2. **Multi-factor Authentication** - User must validate identity using MFA through SSO.

The MFA options are:

- **No matching** - This option is not available for Linux endpoints, (which is why a hybrid setup is required).
- **Email match** - The logged-in user must authenticate using the email associated with the login credentials.
- **Account separation** - The logged-in user must authenticate using a secondary account. Required for **Cyber Essentials Plus** compliance.

Refer also to [Linux Settings \(Authentication tab\)](#).

Setting-up a Break Glass Account

About Break Glass

The *Break Glass* feature provides additional security for Linux endpoints. It creates a new, temporary, one-time-use administrator account on an endpoint that works on domains, Entra ID, and stand-alone, which audits all elevated activity, and terminates within a pre-defined amount of time or on log out.

Specifically, a *Break Glass* account is for situations such as when the domain trust relationship is broken or someone without logon credentials needs to service the endpoint. The provisioned account is a **temporary local user** in the local administrators group that must be used **within one hour** of creation, so do not create a Break Glass account until you are ready to use it.

Once logged-in via the Break Glass account, you have a limited time (typically **2 hours**) to get the work done before *Expiry*. At expiry time, the temporary local user is forcibly logged off (if still logged-in), the session terminated and the temporary account removed.

For Linux endpoints:

- Unused Break Glass accounts are automatically removed on reboot.
- In the portal, access Break Glass settings via menu : **Inventory > [Computer] > Break Glass**

Security benefits

The *Break Glass* feature includes the following security benefits:

- Break Glass **circumvents the need to use the built-in local Administrator account** – you can disable it completely to add an extra layer of security to your endpoints.
- The account **must be used within an hour of being generated**, minimizing the potential attack window and risk of account compromise.
- Risk is further minimized by a **one-time-only log in functionality**: the user can log in once, and after log out, the account is terminated.
- The user has **only the time specified under Expiry** when the Break Glass account was generated to use the administrator account; this duration (2 hours by default) is indicated on the built-in desktop background of each account. When the time-period is up, the session is terminated.

- Measures are in place to ensure **the Expiry time cannot be tampered with**: if the Account user attempts to extend their time limit by adjusting the clock, the Account automatically logs out / terminates.
- All **Usernames and Passwords are automatically generated**, random, and complex, minimizing the possibility for a successful brute force attack.
- Passwords are **stored within the web application**, only accessible by Portal users / IT Admins via credentials – a safer option compared to MS LAPS' storage of admin account passwords in plain text along with the AD computer record.

When would I use a Break Glass account?

A Break Glass account is useful in the following scenarios:

1. **Regaining Domain-Trust Relationship**
As the name suggests, the Break Glass feature is ideal for "last resort" situations, such as when the domain-trust relationship is broken and needs to be reconnected using an Administrator account.
2. **Provisioning a Just-In-Time Administrator Account**
The Break Glass Account doubles up as a *Just-In-Time* account that can be used for specific purposes / situations when necessary; e.g., provisioning an account for someone who doesn't have credentials, but requires access to service an endpoint.

Break Glass Prerequisites

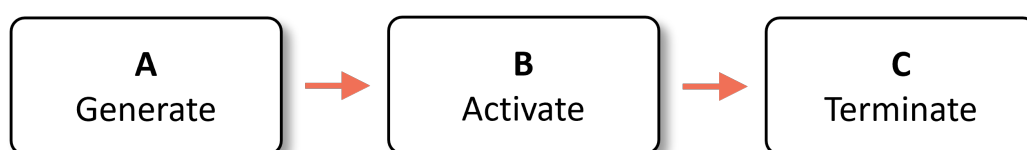
Endpoints making use of this feature must be able to contact the MQTT broker:

Outbound MQTT broker connectivity via Websockets - port **443** - for the following:

- If your data is located in Europe (Netherlands):
Ten nodes (**FastTrackHubEU1.azure-devices.net** to **FastTrackHubEU10.azure-devices.net**)
- If your data is located in the USA:
Ten nodes (**FastTrackHubUS1.azure-devices.net** to **FastTrackHubUS10.azure-devices.net**)
- If your data is located in the UK:
Ten nodes (**FastTrackHubUK1.azure-devices.net** to **FastTrackHubUK10.azure-devices.net**)
- If your data is located in Europe (Germany):
Ten nodes (**FastTrackHubGermany1.azure-devices.net** to **FastTrackHubGermany10.azure-devices.net**)
- If your data is located in Asia:
Ten nodes (**FastTrackHubSingapore1.azure-devices.net** to **FastTrackHubSingapore10.azure-devices.net**)

Using the Break Glass feature

Setting-up and using a Break Glass account comprises three tasks:



A. Generate

Create a Break Glass account:

1. Log in to the Portal and navigate to the **Inventory** page. Select an endpoint on which you want to enable the Break Glass account and select **Break Glass** from the left-hand menu.
2. From the **Expiry** drop-down menu, select an amount of time for which you want the account to be active once logged-in. The default is **2 hours**, but the period can range from a minimum of 15 minutes, to an unlimited amount of time.
3. Click the **Generate Account** button, which issues a Break Glass account and displays its *User* and *Password* in the read-only text boxes:

The screenshot shows the 'BREAK GLASS ACCOUNT' page. On the left is a sidebar with a 'Close' button and a menu containing 'Inventory', 'PIN Code', 'Break Glass' (highlighted), 'Events', and 'Auditlog'. The main content area is titled 'Break Glass Account' and features a 'Credentials' section with read-only fields for 'User' (ABR979482) and 'Password' (Came191Police26), and a dropdown for 'Expiry' set to '2 hours'. Below these is a 'Clear Account' button. A section titled 'Want to send credentials to someone?' includes a 'Phone No' input field and a 'Send SMS' button. On the right, an 'Instructions' panel shows the status 'WAITING FOR ENDPOINT' and provides detailed instructions for activating the account, including a QR code at the top right of the page.

IMPORTANT

If the account is not used within *one hour of generation*, it is automatically removed and you will need to create another. All creation activity is logged.

4. Once generated, the status of the Break Glass account is updated in real-time in the Portal. The four possible states are:
 - **Waiting for Endpoint** – The account is generated in the User Portal but not yet created on the endpoint (to create the account on the endpoint, see the next section "**Activate**" on the next page).
 - **Ready to Log On** – The account is created but has not yet been activated / used (i.e., logged-in to).
 - **Session in Progress** – The account is currently in use.
 - **Account Removed** – The account has been terminated either due to the user logging out, or the pre-defined *Expiry* time being reached.

The following screenshots illustrate a Windows endpoint example - Mac and Linux endpoints display similar status messages and events:

The first three screenshots show the 'Instructions' section of the endpoint status page. The first screenshot shows 'STATUS: WAITING FOR ENDPOINT'. The second screenshot shows 'STATUS: READY TO LOG ON'. The third screenshot shows 'STATUS: SESSION IN PROGRESS'. All three screenshots include instructions on how to activate the account and how to log in.

The fourth screenshot shows a table titled 'Break Glass Account Events on DESKTOP-LMSEFL8'. The table has columns for 'Your Time', 'Event', 'Account', 'Name', and 'Endpoint Time'. The table contains four rows of events:

| Your Time | Event | Account | Name | Endpoint Time |
|---------------------|-------------------------------|-----------|-------|---------------------|
| 20-12-2023 11:24:11 | Break Glass Account removed | ABR855696 | | 20-12-2023 11:24:11 |
| 20-12-2023 09:28:25 | Break Glass Account logged on | ABR855696 | | 20-12-2023 09:28:25 |
| 20-12-2023 09:21:48 | Break Glass Account created | ABR855696 | | 20-12-2023 09:21:48 |
| 20-12-2023 09:11:59 | Break Glass Account issued | ABR855696 | Steve | 20-12-2023 09:11:59 |

Below the table, there are buttons for 'Export to PDF', 'Export to XLSX', 'Export to CSV (J)', and 'Export to CSV (J)'. A 'Reload' button is also present.

5. Optionally, you can send the new Break Glass account credentials via SMS (i.e., text message) by entering the intended recipient's mobile number into the text box and clicking **Send SMS**.

B. Activate

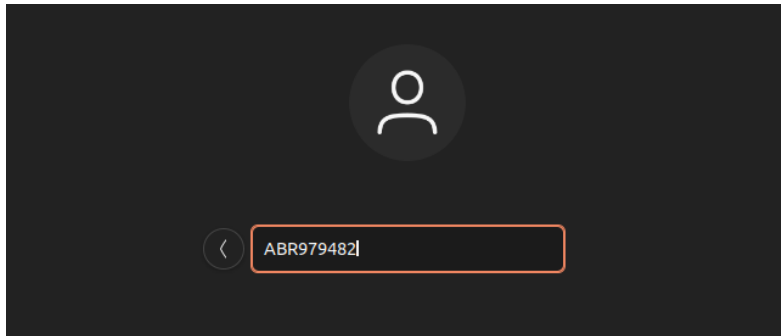
Activate the Break Glass account using one of the following methods:

- a. Restart the device, then wait approximately **30 seconds** for the account to be created. The portal will update the STATUS message when the account is ready:

The screenshot shows the 'Instructions' section of the endpoint status page. The status is 'READY TO LOG ON'. The instructions state: 'The user name must be entered as LINUX-VM1\ABR979482 on the login screen. Click here for LAN Remote Desktop Connect.'

- b. If enabled, you can select **Not listed?** on the login screen and enter the generated Break Glass account at the credential prompt.

On Linux endpoints, simply select the account from the list or type it directly into the user account field (e.g. **ABR979482**):



NOTE

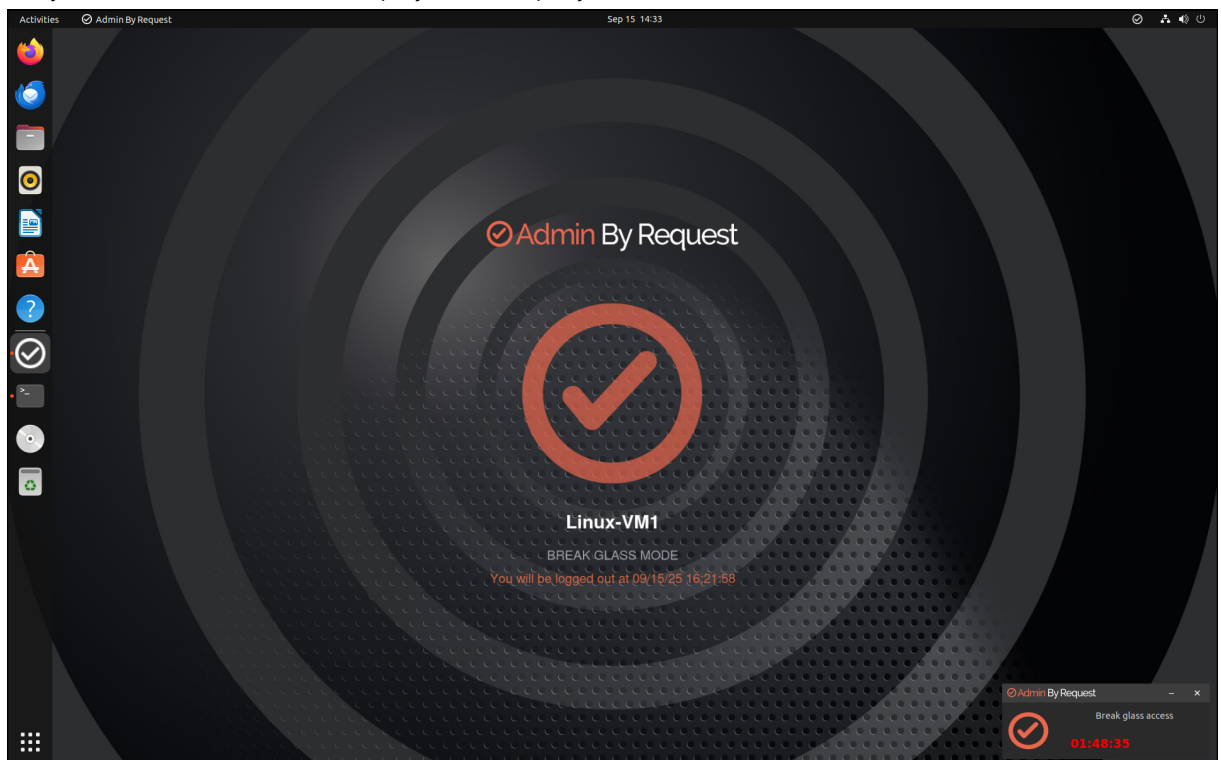
Remember, this may fail on the first attempt; if so, wait **10 seconds** and then try again.

- C. A third method to activate the account is by logging in to another account on the endpoint (if possible), selecting the Admin By Request icon from the toolbar, and clicking the **About** item from the menu.

C. Terminate

Use the account and log out:

1. Once logged in to the Break Glass account, the user has administrator privileges to do what they need to do, within the *Expiry* time displayed:



2. Terminate the account by either logging-out, or allowing the account to log out automatically when the *Expiry* time is reached – whichever comes sooner.

The Linux Command Line Interface

Introduction

This topic describes the Linux command line interface (CLI).

Prerequisites

1. The CLI commands are designed for the command line. If run inside a graphical interface's terminal window, certain commands will defer to the GUI version.

Example - abr start

Running **abr start** in a GUI terminal window shows the following message:

```
steve@Linux-VM1:~$
steve@Linux-VM1:~$
steve@Linux-VM1:~$ abr start
Please use the ABR for Linux GUI instead to start an administration session.
steve@Linux-VM1:~$
```

NOTE

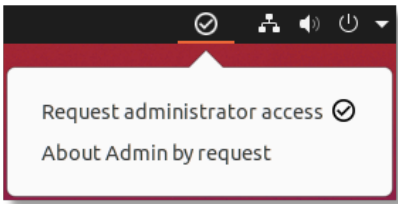
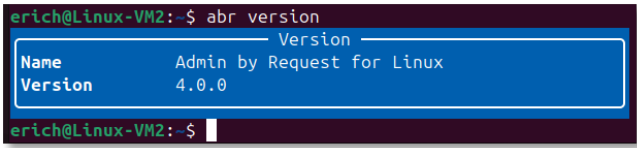
The screenshots in this section were taken on a Linux Ubuntu 22.04 desktop, switching between GUI and command line interfaces:

- From GUI to command line:
systemctl set-default multi-user.target
reboot
- From command line to GUI:
systemctl set-default graphical.target
reboot

2. Using the CLI requires Admin By Request for Linux **version 3.1.9** or greater.

Check version at endpoint

You can check which version of Admin By Request you have installed on a Linux endpoint as follows:

| GUI | Command line |
|---|--|
| <p>From the icon in the menu bar, select About Admin By Request:</p>  | <p>At the command prompt, enter abr version:</p>  |

Check version in portal

You can also check the version using the Admin Portal. Log in to the portal and click **Inventory**. Find the device concerned and note the version listed in column **SW**:

| Computer | User | Operating system | Model | SW | PIN | Details |
|--------------------|---------------|--------------------------------|-------------------------|-------|-----|---------|
| DC0 | Administrator | Windows Server 2022 Datacenter | VMware20,1 | 8.6.2 | PIN | Details |
| LINUX-VM1 | Eric Hastie | Ubuntu 22.04.5 LTS | VMware Virtual Platform | 4.0.0 | PIN | Details |
| LINUX-VM2 | Eric Hastie | Ubuntu 24.04.3 LTS | VMware Virtual Platform | 4.0.0 | PIN | Details |
| OLIVIA'S MAC | Olivia Lim | macOS 12 Monterey | | 5.1.1 | PIN | Details |
| Steves-Macbook-Air | Steve Dodson | macOS 15.7 | MacBookAir 10.1 | 5.2.0 | PIN | Details |
| SUES-MAC | Sue Jones | macOS 13 Ventura | VMware 20.1 | 5.2.0 | PIN | Details |
| WIN11-VM1 | Steve Dodson | Windows 11 Pro | VMware20,1 | 8.6.2 | PIN | Details |

Commands

From version 3.1.9, the following commands are supported:

- `abr finish`
- `abr settings`
- `abr start`
- `abr status`
- `abr version`

There are also four global options:

- `abr --help`
- `abr --master-config-file <arg>`
- `abr --system-config-file <arg>`
- `abr --log-level <arg>`

Run **abr --help** to see a full list of commands and options.



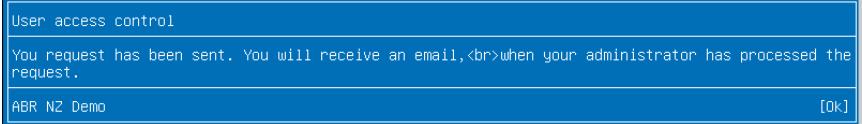
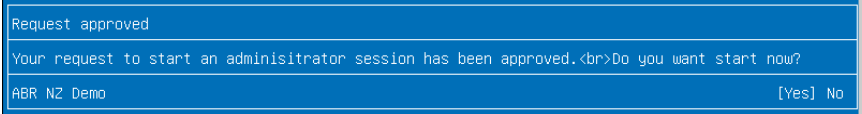

abr finish

| Command | Output |
|---|---|
| abr finish Ends an admin session. | <pre>Status Finished admin session Connecting ...</pre> <p>When the pop-up message above disappears, the countdown timer in the bottom right of the status bar also disappears.</p> |

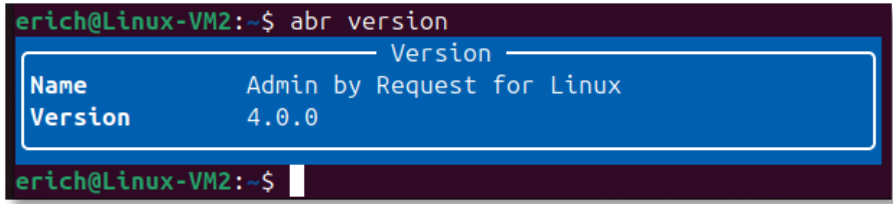
h2>abr settings

| Command | Output |
|---|--|
| abr settings Lists the settings from the portal that currently apply to this endpoint. To output settings to a text file: abr settings > settings.txt | <pre> steve@Linux-VM1:~\$ abr settings ===== Settings ===== UpdateTime = "2024-05-23T11:53:55.906" ComputerDistinguishedName = "" ComputerGroups = [] ComputerOrganizationalUnit = [] SIDC = "8fb8c607-5263-41ba-a35c-7f37ac5fdfb8" SID = "9697897e-ba55-4bb8-9819-2f43d764af78" UploadInventory = "true" DebugMode = "true" SupportAssistEnabled = "false" EnableAppElevations = "true" BlockAppElevations = "false" RequireAppApproval = "false" RequireAppReason = "false" EnableSessions = "true" RequireApproval = "false" RequireReason = "false" AdminMinutes = "180" AuthenticateMode = "Authenticate" SSOEmailMatch = "true" SSORestrictiveSessions = "false" SSORestrictivePreApprovals = "false" AllowAppStore = "true" AllowSudo = "true" AllowSudoForEveryone = "true" AllowSudoInteractive = "true" AllowRootLogin = "false" AllowChangeRootPassword = "false" ShowInstructions = "false" ShowAppInstructions = "false" InternetUpdate = "false" AzureADConnector = "false" PreferAzureAD = "true" UseLogo = "false" DockIcon = "true" OwnerLock = "false" IntuneComplianceLock = "false" RemoveRights = "false" LastAdminCheck = "false" EnableBlockedApps = "false" LockedPreferences = ["com.apple.LoginItems-Settings.extension", "com.apple.Users-Groups-Settings.extension"] EmailFieldBehavior = "Mandatory" PhoneNoFieldBehavior = "Mandatory" ComputerName = "Linux-VM1" ConnectionStatus = "true" ===== Policies ===== SessionEndRemindTime = "30" RemoveGroups = ["root","adm","sudo"] AddGroups = [] steve@Linux-VM1:~\$ </pre> |

abr start

| Command | Output |
|---|---|
| abr start Starts an admin session. The sequence of messages that follow depends on settings in the portal; i.e. whether or not the user must have requests approved before running elevated tasks. | <div> <div>1. </div> <div>2. </div> <div>3. </div> <div> <p>IMPORTANT</p> <p>Check email for approval.</p> <p>Once approval is granted, start the admin session <i>before</i> entering any commands that require elevation, including sudo. If an admin session is not running, sudo is treated as "Run As Admin" and will prompt again for a reason even if approval has already been given for the admin session.</p> <p>To start the session, enter abr start a second time.</p> </div> <div>4. </div> <div>5. </div> </div> <p>The final screenshot shows a countdown timer in the status bar. When the timer reaches zero, the session will terminate.</p> |

abr version

| Command | Output |
|--------------------|--|
| abr version |  <pre> erich@Linux-VM2:~\$ abr version Name Admin by Request for Linux Version 4.0.0 erich@Linux-VM2:~\$ </pre> |

abr status

| Command | Output |
|--|---|
| <p>abr status</p> <p>Equivalent to selecting About Admin By Request > Connectivity in the GUI app (see "Connecting via a Proxy Server" on page 14).</p> | <pre> steve@Linux-VM1:~\$ abr status Operational status Ok Internet connectivity Online Proxy server None Cloud connectivity Online Last connection 05/23/24 10:19:55 Computer name Linux-VM1 Computer join No Domain name Name Steve Dodson User name steve User join No </pre> <p>In this example, both <i>Internet</i> and <i>Cloud</i> connectivity are Online, and neither the computer nor the user is joined to a domain.</p> |

abr --help

Entering **abr --help** shows all available commands and options:

```

steve@Linux-VM1:~$ abr --help
Description:
  Command line client for ABR for Linux

  It is possible to start and stop Admin sessions through the various commands below.
  For help with any of those, simply call them with --help.

Usage:
  abr [command]

Available commands:
  finish
  settings
  start
  status
  version

Global options:
  --help                produce help message
  --master-config-file arg (=usr/share/abr/configuration/cli.conf)
                        File path to the master configuration
                        file, which will be loaded first.
  --system-config-file arg (=etc/abr/cli.conf)
                        File path to the system configuration
                        file
  --log-level arg       log level for the application

```

abr --master-config-file

Shows the master configuration file.

NOTE

This is for the use of Admin By Request and not something customers should be changing. It is provided here for information only and may be hidden in future releases.

```
steve@Linux-VM1:~$ cat /usr/share/abr/configuration/cli.conf
{
  "log_level": "INFO",
  "terminal_raw_input": "/var/log/abr/${username}/raw-input.txt",
  "terminal_unhandled_input": "/var/log/abr/${username}/unhandled-input.txt",
  "terminal_raw_output": "/var/log/abr/${username}/raw-output.txt",
  "terminal_unhandled_output": "/var/log/abr/${username}/unhandled-output.txt",
  "log_destinations":
  [
    {
      "type": "journal",
      "enable": false
    },
    {
      "type": "console",
      "enable": false
    },
    {
      "type": "file",
      "enable": true,
      "file_path": "/var/log/abr/${username}/cli.log",
      "rotation_size": 10485760
    }
  ]
}
steve@Linux-VM1:~$
```

abr --system-config-file

Shows the system configuration file.

NOTE

This is for the use of Admin By Request and not something customers should be changing. It is provided here for information only and may be hidden in future releases.

```
steve@Linux-VM1:~$ cat /etc/abr/cli.conf
{
  "log_level": "INFO",
  "terminal_raw_input": "/var/log/abr/${username}/raw-input.txt",
  "terminal_unhandled_input": "/var/log/abr/${username}/unhandled-input.txt",
  "terminal_raw_output": "/var/log/abr/${username}/raw-output.txt",
  "terminal_unhandled_output": "/var/log/abr/${username}/unhandled-output.txt",
  "log_destinations":
  [
    {
      "type": "journal",
      "enable": false
    },
    {
      "type": "console",
      "enable": false
    },
    {
      "type": "file",
      "enable": true,
      "file_path": "/var/log/abr/${username}/cli.log",
      "rotation_size": 10485760
    }
  ]
}
```

abr --log-level

Sets the level for logging (e.g. info, debug etc.). Use this option together with a command as indicated in the following examples:

```
abr -log-level info start
```

```
abr -log-level info status
```

```
abr -log-level debug start
```

```
abr -log-level debug status
```

The default level is **info** and the current level can be seen in either the master config file or the system config file.

Auditlog

In the same way as the graphical interface, all activity is logged, both for *Run As Admin* and *Admin Sessions*.

The following examples show typical activity recorded in the auditlog.

RUN AS ADMIN


ADMIN SESSIONS

SERVERS

Run As Admin

Search

Drag a column header here to group by column or click the funnel icon to filter

| | Application | User | Computer | Time | Duration | Activity | Status | |
|---|-------------|--------------|-----------|---------------------|----------|----------|----------|---|
| ▼ | apt | Steve Dodson | LINUX-VM1 | 24-05-2024 13:50:58 | 00:00:16 | 1/1/1 | Finished |  |

Contact Information

| | |
|--------------|-------------------------|
| Full name | Steve Dodson |
| User account | STEVE |
| Email | stevehd@slingshot.co.nz |
| Phone | 555 123456 |
| Approved by | Steve Dodson |
| Response In | 00:00:20 |
| Reason | Need to run as root |

Execution

| | |
|------------|---------------------|
| Start time | 24-05-2024 13:50:58 |
| End time | 24-05-2024 13:51:14 |
| Duration | 00:00:16 |
| Settings | Global Settings |
| Trace no | 71504904 |

Application

| | |
|-----------|----------|
| Name | apt |
| File name | apt |
| Path | /usr/bin |

Actions

| | |
|--------------|------------------------------|
| Malware scan | Not available |
| Virustotal | Check status |

Installed or uninstalled software

| Action | Application | Version | Publisher |
|-----------|-------------|------------------|-----------|
| Install | rr | 5.5.0-1ubuntu0.1 | Ubuntu |
| Uninstall | rr | 5.5.0-1build1 | Ubuntu |

Programs executed using elevated privileges

| Program | File | Parameters | | |
|---------|--------------|------------|-----------------------|----------------------|
| apt | /usr/bin/apt | update | Check | Path |

RUN AS ADMINADMIN SESSIONSSERVERS

Admin Sessions

Search

Drag a column header here to group by column or click the funnel icon to filter

| | User | Computer | Time | Duration | Activity | Status | |
|---|----------------|-----------|---------------------|----------|----------|----------|--|
| ▼ | ✓ Steve Dodson | LINUX-VM1 | 24-05-2024 21:04:52 | 00:01:56 | 0/0/2 | Finished | |

Contact Information

| | |
|--------------|--------------------------|
| Full name | Steve Dodson |
| User account | STEVE |
| Email | stevehd@slingshot.co.nz |
| Phone | 555 123456 |
| Approved by | Steve Dodson |
| Response In | 00:00:40 |
| Reason | Operating system updates |

Execution

| | |
|------------|---------------------|
| Start time | 24-05-2024 21:04:52 |
| End time | 24-05-2024 21:06:48 |
| Duration | 00:01:56 |
| Settings | Global Settings |
| Trace no | 61513892 |

Installed or uninstalled software

No software was installed or uninstalled.

Programs executed using elevated privileges

| Program | File | Parameters | | |
|---------|--------------|------------|-----------------------|----------------------|
| apt | /usr/bin/apt | upgrade | Check | Path |
| apt | /usr/bin/apt | update | Check | Path |

Portal Administration for Linux

Introduction

This topic documents configuration parameters in the Admin Portal that can be used to manage *Linux Settings* and *Sub Settings*.

Fields that can be set/configured in the portal are presented in tables, with each table showing:

- **Setting** - the name of the field that controls the setting
- **Type** - the type of value that can be entered or selected and its default value
- **Description** - how the setting is used and notes about any implications it may have on other settings

To change any of the settings in the portal, log in to the [portal](#) and select the setting from the menu.

In this topic

["Run As Admin Settings" on the next page](#)

["Admin Session Settings" on page 37](#)

["Endpoint Settings" on page 38](#)

["Lockdown Settings" on page 40](#)

["App Control Settings" on page 42](#)

["Block tab" on page 45](#)

["Privacy Settings" on page 47](#)

["Entra ID Support" on page 48](#)

["Preventing Abuse" on page 50](#)

["Policies for Linux" on page 51](#)

["Supplementary Technical Information" on page 53](#)

Run As Admin Settings

Portal menu: **Endpoint Privilege Management > Settings > Linux Settings > Authorization > AUTHORIZATION**

Settings Table - Run As Admin

Run As Admin (also known as Application Elevation) elevates privileges for only the file or application selected.

It is invoked when a user runs a sudo command.

On Linux endpoints, *Run As Admin* can **only** be performed using the sudo command.

| Setting | Type | Description |
|--|---|--|
| Allow Run As Admin | Toggle On Off Default: On | <p>On - Allows users to elevate privileges for a selected file. Enables <i>Require approval</i> and <i>Require reason</i>. Disables <i>Block Run As Admin</i>.</p> <p>Off - Denies users the ability to elevate privileges for a selected file. Enables <i>Block Run As Admin</i>, which is how users with admin credentials can still elevate privileges.</p> |
| Block Run As Admin (enabled only if <i>Allow Run As Admin</i> is OFF) | Toggle On Off Default: Off | <p>On - Denies users the ability to execute <i>Run As Admin</i> even if administrator credentials are available (i.e. no authentication window is presented).</p> <p>Off - Allows users with administrator credentials to execute <i>Run As Admin</i> (i.e. authentication window pops-up asking for admin credentials).</p> |
| Require approval (hidden if <i>Allow Run As Admin</i> is OFF) | Toggle On Off Default: Off | <p>On - Sends a request to the IT team, which must be approved before elevation is granted. Makes <i>Require reason</i> mandatory (i.e. must be On).</p> <p>Off - Allows the user to elevate file privileges (and thus perform the action) as soon as the action is selected. For example, selecting "Run as administrator" to execute a program occurs immediately, without requiring approval. Makes <i>Require reason</i> optional (i.e. can be either On or Off).</p> <div> <p>IMPORTANT</p> <p>The Free Plan default for this setting is Off, which means that users simply have to request elevated access and it will be <i>automatically granted</i>.</p> <p>We recommend changing this setting to On. Note that the default setting may be changed in a future release.</p> </div> |
| Require reason (hidden if <i>Allow Run As Admin</i> is OFF) | Toggle On Off Default: On | <p>On - Extends the authentication window and asks the user to enter email address, phone number and reason. Reason must comprise at least <i>two words</i>. This information is stored in the Auditlog.</p> <p>Off - No reason is required by the user, but details of the actions performed are stored in the Auditlog.</p> |
| Save | Button | <p>Saves customization and changes to any fields.</p> <p>Note that reloading any defaults does not take effect until Save is clicked.</p> |

Admin Session Settings

Portal menu: **Endpoint Privilege Management > Settings > Linux Settings > Authorization > AUTHORIZATION**

Settings Table - Admin Session

Admin Session (also known as User Elevation) elevates the current user's privileges across the endpoint for the duration of the session.

Invoked when the user clicks the menu bar icon to request a protected administrator session.

On Linux endpoints, when a user requests administrative rights, these are granted via a number of plugins that interact with both the ABR service and the Linux security system. Refer to "[Other Panels \(accessed via their respective buttons/links\).](#)" [on page 9](#) for more information.

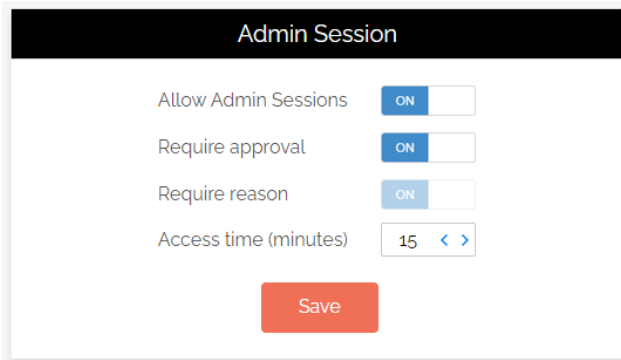
| Setting | Type | Description |
|-----------------------|--|---|
| Allow Admin Sessions | Toggle On Off Default: On | <p>On - Allows users to effectively become a local administrator for the number of minutes specified in <i>Access time (minutes)</i>. Enables <i>Require approval</i>, <i>Require reason</i> and <i>Access time (minutes)</i>.</p> <p>Off - Denies users the ability to become a local administrator. Hides all other options under Admin Session.</p> |
| Require approval | Toggle On Off Default: Off | <p>On - Sends a request to the IT team, which must be approved before the request is granted. Makes <i>Require reason</i> mandatory (i.e. must be On).</p> <p>Off - Allows the user to become a local administrator as soon as the request is made. Makes <i>Require reason</i> optional (i.e. can be either On or Off).</p> <div> <p>IMPORTANT</p> <p>The Free Plan default for this setting is Off, which means that users simply have to request elevated access and it will be <i>automatically granted</i>.</p> <p>We recommend changing this setting to On. Note that the default setting may be changed in a future release.</p> </div> |
| Require reason | Toggle On Off Default: Off | <p>On - Extends the authentication window and asks the user to enter email address, phone number and reason. This information is stored in the Auditlog.</p> <p>Off - No further information is required by the user, but user and computer details are stored in the Auditlog.</p> |
| Access time (minutes) | Integer Default: 15 (minutes) | The maximum duration in minutes an Admin Session may last. This time must be sufficient for the user to install software or perform any other tasks that require elevation. |
| Save | Button | Saves customization and changes to any fields. Note that reloading any defaults does not take effect until Save is clicked. |

Changing Admin Session Duration

Admin session duration (access time) is the maximum amount of time in minutes an Admin Session may last. This time must be sufficient for the user to install software or perform any other necessary tasks.

To change the time allocated for an administrator session:

1. Log in to the Portal and select menu **Settings > Linux Settings**.
2. From the *Authorization* left menu, make sure the **AUTHORIZATION** tab is displayed (it is the default) and update the **Access time (minutes)** field in the Admin Session panel:



3. Click **Save** when done.

Endpoint Settings

The Endpoint menu allows control over the following settings:

- Look & Feel
- Instructions

Look & Feel tab

Portal menu: **Endpoint Privilege Management > Settings > Linux Settings > Endpoint > LOOK & FEEL**

Settings Table - Look & Feel

Email and phone settings control the behavior of the fields in the request form.

Skin determines if user interfaces are light or dark. Active skin choice can be used as an easy way to determine if sub-settings are in effect.

| Setting | Type | Description |
|-------------|--|---|
| Skin | Selection Default: Auto-detect | <p>Auto-detect - The skin (light or dark) depends on what is currently being used by the operating system.</p> <p>Light - Uses a light skin for Admin By Request dialog boxes.</p> <p>Dark - Uses a dark skin for Admin By Request dialog boxes.</p> <p>Follow Operating System - The skin (light or dark) depends on what is currently being used by the operating system.</p> |
| Email field | Selection Default: Mandatory | Mandatory - Field appears in dialog boxes and must be filled-in. |

| Setting | Type | Description |
|----------------|---|--|
| | | Optional - Field appears in dialog boxes, but does not have to be filled-in. Hide - Field does not appear in dialog boxes. |
| Phone no field | Selection Default: Mandatory | Mandatory - Field appears in dialog boxes and must be filled-in. Optional - Field appears in dialog boxes, but does not have to be filled-in. Hide - Field does not appear in dialog boxes. |
| Save | Button | Saves customization and changes to any fields. Note that reloading any defaults does not take effect until Save is clicked. |

Instructions tab

Portal menu: **Endpoint Privilege Management > Settings > Linux Settings > Endpoint > INSTRUCTIONS**

Settings Table - Instructions

Run As Admin instructions

Instructions for *Run As Admin* are shown after the user invokes "Run As Administrator" and after the optional reason screen.

Instructions can be used as a Code of Conduct to inform the user of the consequences of abuse, what is logged or it could be used to show contact information for your help desk in case of problems. URLs are automatically detected and will appear as clickable links.

| Setting | Type | Description |
|--|---|--|
| Show instructions before start | Toggle On Off Default: Off | On - Instructions are shown to the user per the period selected below via the drop-down. User clicks OK to close the instructions window. Off - Instructions are not shown. |
| <Code of Conduct> <Instructions> <Display Frequency> | Text Text (multiline) Selection | A title for the instructions window. The instructions displayed to the user. A frequency indicating when instructions are to be displayed: <ul style="list-style-type: none"> • Show every time • Show once a day • Show once a week • Show once a month |
| Save | Button | Saves customization and changes to any fields. Note that reloading any defaults does not take effect until Save is clicked. |

Admin Session instructions

Instructions for *Admin Session* are shown after the user invokes "Request Administrator Access" and after the optional reason screen.

Instructions can be used as a Code of Conduct to inform the user of the consequences of abuse, what is logged or could be used to show contact information for your help desk in case of problems. URLs are automatically detected and will appear as clickable links.

| Setting | Type | Description |
|--|---|--|
| Show instructions before start | Toggle On Off Default: Off | On - Instructions are shown to the user per the period selected below via the drop-down selection field. User clicks OK to close the instructions window. Off - Instructions are not shown. |
| <Code of Conduct> <Instructions> <Display Frequency> | Text Text (multiline) Selection | A title for the instructions window. The instructions displayed to the user. A frequency indicating when instructions are to be displayed: <ul style="list-style-type: none"> • Show every time • Show once a day • Show once a week • Show once a month |
| Save | Button | Saves customization and changes to any fields. Note that reloading any defaults does not take effect until Save is clicked. |

Lockdown Settings

The Lockdown menu allows control over the following settings:

- Admin Rights
- Sudo
- Root

Admin Rights tab

Portal menu: **Endpoint Privilege Management > Settings > Linux Settings > Lockdown > ADMIN RIGHTS**

Settings Table - Admin Rights

Revoke admin rights at logon means that all user accounts will be downgraded from an Admin role to a User role, unless the account appears in the *Excluded accounts* list.

Excluded accounts are not removed at logon.

| Setting | Type | Description |
|---------------------|--|--|
| Revoke admin rights | Toggle On Off Default: On | On - Admin privileges are removed for all users except those appearing in the <i>Excluded accounts</i> list.. |

| Setting | Type | Description |
|-------------------|--------|--|
| | | Off - Admin privileges are not removed for users configured locally as administrators. |
| Excluded accounts | Text | The account name(s) to retain local admin privileges. Multiple accounts must be specified on separate lines. Domain accounts must be prefixed with domain and backslash. |
| Save | Button | Saves customization and changes to any fields. Note that reloading any defaults does not take effect until Save is clicked. |

Sudo tab

Portal menu: **Endpoint Privilege Management > Settings > Linux Settings > Lockdown > SUDO**

Settings Table - Sudo

Allowing sudo is strongly discouraged, because it gives the user full control over the endpoint and therefore allows the user to tamper with or completely remove any endpoint software.

The safest course is to leave this setting **Off**, which completely disables *Run As Admin* file elevation attempts.

Excluded accounts are not removed at login.

| Setting | Type | Description |
|---------------------------------|---|---|
| Allow sudo terminal commands | Toggle On Off Default: Off | On - The logged-in user is in the sudoers file and can run sudo commands. Off - The user cannot run sudo commands, even though they are in the sudoers file. |
| Allow sudo for non-sudoers | Toggle On Off Default: Off | On - The logged-in user is not in the sudoers file, but can run sudo commands. Off - The user cannot run sudo commands. |
| Allow sudo interactive sessions | Toggle On Off Default: Off | On - The logged-in user can start a sudo interactive session. Off - The user cannot start a sudo interactive session. |
| Save | Button | Saves customization and changes to any fields. Note that reloading any defaults does not take effect until Save is clicked. |

Root tab

Portal menu: **Endpoint Privilege Management > Settings > Linux Settings > Lockdown > ROOT**

Settings Table - Root

Allow root login controls whether or not it is possible to log in as root on Linux devices.

Logging-in as root can circumvent the ABR client entirely. The safest course is to leave this setting **Off**, which completely disables the ability to login as root, regardless of whether or not the root password is known.

Allow root password change controls whether or not it is possible to change the password of the root account.

| Setting | Type | Description |
|----------------------------|---|--|
| Allow root login | Toggle On Off Default: Off | On - This endpoint allows users to login as root, or the logged-in user can su (switch user) to root. Off - The endpoint does not allow root logins. |
| Allow root password change | Toggle On Off Default: Off | On - This endpoint allows users to login as root, and also allows the logged-in user to change the root password. Off - The endpoint allows root logins, but the root password cannot be changed. |
| Save | Button | Saves customization and changes to any fields. Note that reloading any defaults does not take effect until Save is clicked. |

App Control Settings

Pre-Approve tab

Portal menu: **Endpoint Privilege Management > Settings > Linux Settings > App Control > PRE-APPROVE**

Pre-Approval (known sometimes as Whitelisting) refers to the method of working out which applications are trusted and frequently used, and adding them to a list that automatically allows users to elevate those applications when they need to. This is essentially the opposite of Blocklisting/Blacklisting – creating a list of applications that cannot be elevated.

This method of “allow most, deny some” has proven to be extremely resource-efficient for large enterprises compared to the method of denying all applications and only allowing elevations on a case-by-case basis.

Admin By Request allows for quick pre-approval of trusted applications from the Auditlog. Pre-Approval is based on the application vendor or checksum, visible when the *Application Control* screen is displayed (step 3 below).

NOTE

At the time of writing, pre-approval from the Auditlog is not available for Linux clients.

Once an application has been installed on an endpoint with Admin By Request:

1. Log in to the portal and navigate to the application's corresponding entry in the portal **Auditlog**.
2. Expand on the application entry, and select **Pre-approve this file** under Actions:
3. On the *Application Control* screen, modify any settings as required. For more information on pre-approval settings, refer to the Settings Table below.
4. Click **Save** verify that the app has been added to the list of pre-approved applications.

For example, the following applications are pre-approved:

The screenshot displays the 'Linux Application Control' interface. On the left is a sidebar with navigation options: Authorization, Endpoint, Lockdown, App Control (selected), and Emails. The main content area has tabs for 'PRE-APPROVE' (active) and 'BLOCK'. Below the tabs, there's a 'New entry' button and an 'Enabled' toggle set to 'ON'. A table lists pre-approved applications with columns for Application, File, Protection, Location, Type, Log, UAC, and actions (Edit, Delete). Two entries are shown: 'apt' and 'docker', both with 'Read-only location' protection and 'Any location' type. The interface also includes pagination (Page 1 of 1 (2 items)), a page size dropdown (25), and export buttons for PDF, XLSX, and CSV.

| | Application | File | Protection | Location | Type | Log | UAC | |
|------|-------------|--------|--------------------|--------------|--------------|-------------------------------------|-------------------------------------|--------|
| Edit | apt | apt | Read-only location | Any location | Pre-approval | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Delete |
| Edit | docker | docker | Read-only location | Any location | Pre-approval | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Delete |

Settings Table - Pre-Approve

Pre-approved applications are SUDO commands that are pre-approved to run *Run As Admin*, when approval would normally be required. The intention is to remove trivial approval flows and avoid flooding the audit log with trivial data for applications known to be good, such as Visual Studio or Adobe Reader installs.

When an application is on the pre-approval list, the difference is:

- The application is auto-approved, so the approval flow is bypassed
- A reason is not required
- You have the option to not log to the Auditlog (e.g. for trivial data)
- If *Run As Admin* is disabled, a pre-approved application will still run

Enabled toggle

A global setting that indicates whether pre-approved applications are allowed at all (**On**) or not at all (**Off**).

New entry (APPLICATION tab)

Click button **New entry** to create a new pre-approved application.

| Setting | Type | Description |
|---|--|---|
| Type | Selection Default: Run As Admin application pre-approval | <p>Run As Admin application pre-approval - Pre-approve this application for Run As Admin.</p> <p>Run As Admin location pre-approval (all files in folder tree) - Pre-approve all applications in the specified folder, including any sub-folders.</p> <p>Selecting this option enables the <i>Directory</i> field and hides all other fields.</p> |
| Protection | Selection Default: File must be located in read-only directory | <p>Prevent users from bypassing pre-approval by file renaming.</p> <p>File must be located in read-only directory - The recommended method. File must be in a read-only location. You only need to know the name and location and you are not bound to a specific file version.</p> <p>File must match checksum - A checksum of a specific file version. If the file is updated, the checksum no longer matches and a new one must be collected.</p> <p>No protection (not recommended) - Not recommended for anything except testing. The file can be located anywhere and is a file renaming vulnerability, in case a user is aware of (or can guess) the file name.</p> |
| Directory (enabled when other selections are in effect): | Text | A read-only location where the application to be added is stored. |
| Application name | Text | The name of the application. Mandatory, although used for convenience only to help identify applications in the list. |
| File name | Text | Enter file name. Note that adding the app via the Auditlog will auto-populate this field. |
| Save | Button | Saves customization and changes to any fields. Note that reloading any defaults does not take effect until Save is clicked. |
| Cancel | Button | Cancels all work done in this setting and returns to the Linux Workstation Global Settings page. |

New entry (ADVANCED tab)

Additional toggle settings that apply to the pre-approval entry being created.

| Setting | Type | Description |
|-------------------|--|---|
| User confirmation | Toggle On Off Default: On | On - The user must confirm elevation on the endpoint before the application can be run. This is the typical authentication window. |

| Setting | Type | Description |
|--|--|---|
| | | Off - The user does not need to confirm elevation on the endpoint before execution. Hides the <i>Log to auditlog</i> field. |
| Log to auditlog (hidden if <i>User confirmation</i> is Off) | Toggle On Off Default: On | On - Relevant details about the application are logged. Off - No logging is performed for this application. |
| Save | Button | Saves customization and changes to any fields. Note that reloading any defaults does not take effect until Save is clicked. |
| Cancel | Button | Cancels all work done in this setting and returns to the Linux Workstation Global Settings page. |

Block tab

You can specify programs and applications that you wish to prevent users from executing with administrator privileges. You can block applications based on one or more of the conditions: file name, checksum, vendor or file location.


NOTE

You should never block solely based on the file name, as this will open up the endpoint to simple file renaming to bypass the blocking.

PIN code exceptions: The option is available to use a PIN code in case you allow the execution as an exception - simply retrieve the PIN code from the computer's inventory. If you do not wish to offer a PIN option, you can disable this under the Run As Admin tab.

Defining a blocked application:

Application Control



Blocked Application

Type

Block file from running as administrator

Condition


No condition (block always)

Application name

File name

Blocking message (optional)

Internal comments (optional)



About Blocked Application

Block Application allows you to point to a file name that will be blocked from executing.

Application name is only used for convenience in the list.

Condition is when a file is only blocked, if the condition is met:

Directory File must be located in this directory or a sub-folder.

Checksum A checksum of a specific file version. If the file is updated, the checksum no longer matches and a new must be collected.

Blocking Message will appear as a rejection to the user, when the application is attempted to be executed.

Please contact us using the "Contact" menu, if you have questions about blocking.

Type:

- Block file from running as administrator
- Block vendor files from running as admin (digital certificate)
- Block location from running as admin (all files in folder tree)
- Block always

Condition:

- No condition (block always)
- Block if located in directory
- Block if matching digital certificate
- Block if matching checksum

Application name is a label only - used for convenience in the overview list.

File name allows you to point to a file name that will be blocked from executing. You can specify wildcards in the file name, such as *.sh.

Blocking message will appear as a denial message to the user when execution of the application is attempted.

Settings Table - Block

Blocked applications are effectively the opposite of pre-approved applications - the feature allows you to point to a file name that will be *blocked* from executing rather than pre-approved for execution. Wildcards can be specified in the file name.

As with other activity, attempts to run blocked applications are recorded in the auditlog.

NOTE

Please contact us using the [Contact menu](#), if you have questions about blocking.

Enabled toggle

A global setting that indicates whether blocked applications are allowed at all (**On**) or not (**Off**).

New entry

Click button **New entry** to add a blocked application.

| Setting | Type | Description |
|-----------|---|--|
| Type | Selection Default: Block file from running as administrator | Block file from running as administrator - Block this application for Run As Admin. Block location from running as admin (all files in folder tree) - Block all applications in the specified folder, including any sub-folders. Selecting this option enables the <i>Directory</i> field and hides all fields except the optional fields. |
| Condition | Selection Default: No condition (block always) | Condition applies only when a file is blocked. No condition (block always) - The default (and recommended) method. Block if located in directory - File must be located in this folder or directory to be blocked. |

| Setting | Type | Description |
|------------------------------|------------------|--|
| | | Block if matching checksum - A checksum of a specific file version. If the file is updated, the checksum no longer matches and a new one must be collected. |
| Application name | Text | The name of the application. Mandatory, although used for convenience only to help identify applications in the list. |
| File name | Text | The file name of the app to be blocked. Note that blocking the app via the Auditlog will auto-populate this field. |
| Blocking message (optional) | Text (multiline) | A message that appears as a rejection to the user, when the application is attempted to be executed. |
| Internal comments (optional) | Text (multiline) | Optional comments that IT admins might wish to add about the blocked application. |
| Save | Button | Saves customization and changes to any fields. Note that reloading any defaults does not take effect until Save is clicked. |
| Cancel | Button | Cancels all work done in this setting and returns to the Linux Workstation Global Settings page. |

Privacy Settings

Portal menu: **Settings > Tenant Settings > Data > PRIVACY**

Settings Table - Privacy

The PRIVACY tab provides a way to anonymize data collection, so that data is still logged and available for analysis, but identification of individual users is not possible.

Key points:

- Obfuscation creates an alias for each user. You can track activity, but you cannot decode the true identity of any user.
- Collection of data should be left on unless you have a reason not to do this. If disabled, you will have to find contact information elsewhere.
- Inventory collects both hardware and software inventory. If disabled, only the computer name is collected and shown in the "Inventory" menu.
- Geo-tracking maps the endpoint IP address to location using a public IP-to-location database to show in inventory and reports.

NOTE

Changes apply *only to new data*. This is by design to avoid accidentally deleting existing data.

| Setting | Type | Description |
|-------------------------|---|---|
| Obfuscate user accounts | Toggle On Off Default: Off | On - Create an alias for each user. Off - Do not create aliases for users. |

| Setting | Type | Description |
|------------------------------|--|---|
| Collect user names | Toggle On Off Default: On | On - Record the name of each user associated with an ABR event. Off - Do not record user names. |
| Collect user email addresses | Toggle On Off Default: On | On - Record email addresses associated with a user. Off - Do not record email addresses. |
| Collect user phone numbers | Toggle On Off Default: On | On - Record phone numbers associated with a user. Off - Do not record phone numbers. |
| Collect inventory | Toggle On Off Default: On | On - Record hardware and software inventory data. Off - Do not record inventory data. |
| Allow geo-tracking | Toggle On Off Default: On | On - Record the location of the public IP address associated with the user's endpoint. Off - Do not record IP addresses. |
| Save | Button | Saves customization and changes to any fields. Note that reloading any defaults does not take effect until Save is clicked. |

Entra ID Support

NOTE

Azure AD has been renamed by Microsoft to Entra ID. This version of the document uses both terms interchangeably, but future versions will refer to Entra ID only.

A selling point for the Admin By Request PAM solution is its flexibility and tools for granular access control; organizations can configure every setting to their specific needs and the needs of all, some, or even individual users.

Settings act as rules, such as whether the *Run as Admin* or *Admin Session* features are enabled, and whether or not users need approval to use them. You likely wouldn't want the rules applied for an IT Administrator to be the same as those applied for a Customer Relations employee, so settings can be differentiated based on Sub-Settings, which allow different rules to be applied to different users and/or groups.

For all endpoint clients, we've built in support for Entra ID groups, meaning you can now apply Sub-Settings to existing Entra ID / Azure AD user and device groups.

Tenant Settings

Settings here are global tenant settings on top of all other settings. If you have any questions, feel free to contact us [here](#).

Groups

Retention

API Keys

Webhooks

Email Domain

Policies

ENTRA ID / AZURE AD

Identity Groups

Entrada ID Connector

Enable Connector ☐ OFF

Tenant

Application ID

Secret Key

Hybrid Preference

National Cloud ☐ OFF

Save

About Entra ID Connector

Entra ID Connector allows endpoints to retrieve Entra ID (previously Azure Active Directory) groups for subsettings.

If you are using **on-premises Active Directory**, you do not need to configure anything. Collection of groups for Active Directory is configuration-less.

The Entra ID Connector is **NOT** used for single sign-on to the portal; it is solely used for subsetting groups. Example values:

Tenant **acme.onmicrosoft.com**

Application ID **xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx**

Secret Key **azVqedkQlVX9bHLBZjGCQZ6+iZl4goI7u53i9WlZN8-**

Hybrid Preference is when a computer is AD joined and the user made an Azure Workjoin.

[Please refer to this page for Entra ID Connector documentation](#)

For more information, refer to the [Entra ID Connector](#).

Settings Table - Entra ID

The *Entra ID Connector* allows endpoints to retrieve Entra ID (previously Azure AD) groups for sub-settings. The Entra ID Connector is NOT used for single sign-on to the portal; it is used solely for sub-setting groups.

If you are using on-premise Active Directory, you do not need to configure anything - collection of groups for Active Directory is "configuration-less".

Example values:

- Tenant **acme.onmicrosoft.com**
- Application ID **xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx**
- Secret Key **azVqedkQlVX9bHLBZjGCQZ6+iZl4goI7u53i9WlZN8-**

Refer to <https://learn.microsoft.com/en-us/entra/identity-platform/quickstart-register-app> for more information on registering apps with the Microsoft identity platform.

NOTE

The *National Cloud* regions of Azure are designed to make sure that data residency, sovereignty, and compliance requirements are honored within geographical boundaries.

| Setting | Type | Description |
|------------------|---|--|
| Enable Connector | Toggle On Off Default: Off | On - Turns on the Entra ID Connector and allows endpoints to retrieve Entra ID groups for sub-settings. |

| Setting | Type | Description |
|--|--|--|
| | | Off - The Entra ID Connector is disabled and endpoints will use sub-settings as described under "Sub-Settings", rather than using Entra ID rules. |
| Tenant | Text | Standard email address format. Use a new line for each address. |
| Application ID | Text | The value assigned to an application when it is registered with the Microsoft identity platform. |
| Secret Key | Text | The application certificate or client secret generated when the app is registered. |
| Hybrid Preference | Selection Default: Prefer Active Directory | An option available for selection when a computer is both AD-joined and the user makes an Entra ID Workjoin: <ul style="list-style-type: none"> Prefer Active Directory - User is AD-joined only. Prefer Entra ID / Azure AD - User is AD-joined and makes an Entra ID Workjoin. |
| National Cloud | Toggle On Off Default: Off | On - Enables selection of a physically isolated instance of Azure. Reveals <i>National Service</i> , which is where the actual geographic instance is selected. Off - Disables selection of a physically isolated instance of Azure. Hides <i>National Service</i> . |
| National Service (hidden if <i>National Cloud</i> is Off) | Selection Default: US Government L4 / GCC High | The geographic instance selected: <ul style="list-style-type: none"> US Government L4 / GCC High - Azure portal (global service) US Government L5 / DoD - Azure portal for US Government China (21Vianet) - Azure portal China operated by 21Vianet |
| Save | Button | Saves customization and changes to any fields. Note that reloading any defaults does not take effect until Save is clicked. |

Preventing Abuse

So what prevents the user from abusing an Admin Session? The fact that the user has to ask IT for access will in itself prevent the most obvious abuse. But as part of your settings, you can also configure a *Code of Conduct* page. Here you customize wording that suits your company policy. For example, what the penalty is for using the administrator session for personal objectives. You can also choose to explain the things you can monitor from the portal.

When you enable the *Code of Conduct* ("instructions") screen in the settings, this screen appears right before the administrative session starts. You can also customize company name and logo for all screens, so there is no doubt this message is authentic and indeed from the user's own company. This is the configuration part of the portal, where you set authorization, company logo, policies, email communications, etc.

For example:

Policies for Linux

Settings in the Admin By Request client application are controlled under "Linux Settings" in the *Settings* menu (**Portal > Settings > Linux Settings**), when logged-in to the portal. If, for whatever reason, you want to overrule these settings on specific clients, you can set overruling policies in a policy file.

IMPORTANT

Please note we do not recommend that you use a policy file to control client behavior. Instead, we recommend that you use portal settings and sub settings for better transparency and for real-time control of computers not connected to your LAN.

If you have any questions about portal settings or would like a demo of these, please feel free to [contact us](#).

Overruling Portal Settings

To overrule portal settings with a policy file, edit this file:

```
/etc/abr/policies.d/adminbyrequest.policy.template
```

Note that this file is protected during administrator sessions and therefore cannot be hacked by end-users. The file is in json format and has an example non-used setting by default, as shown below. Simply add more settings from the following table to overrule web settings.


```
{
  "ExampleSetting": "ExampleValue"
}
```

Also note that any change to the policy file will take effect after the next reboot. Alternatively, if a policy change must take effect immediately without a reboot, an admin user or MDM can refresh the service using:

```
abr settings --reload
```

| Key | Type | Default | Description |
|---------------------|------------------|---------|---|
| AdminMinutes | Integer | 15 | Number of minutes the user is administrator. This can also be set in your portal settings. |
| AllowSudo | Boolean | 0 | Allow users to run sudo commands. Should not be enabled unless there is a good reason to, because it allows the user to tamper the endpoint software. |
| CompanyName | String | | Overrules the company name that appears on user interfaces, which is by default the licensed company name. |
| ComputerGroups | Array of Strings | | Computer groups to match machine to sub settings when not using Active Directory. |
| ExcludedAccounts | Array of Strings | | List of accounts that will not be downgraded to user role, such as service accounts. |
| EnableSessions | Boolean | 1 | User can request an admin session. |
| EnableAppElevations | Boolean | 1 | User can authenticate apps without session. |
| Instructions | String | | Body text on Code of Conduct ("Instructions") screen. |
| InstructionsHeader | String | | Header text on Code of Conduct ("Instructions") screen. |
| LogoUrl | String | | URL from which to download logo. If not specified, default icons will be used. |
| RemoveRights | Boolean | 1 | Downgrade users from Admin to User, unless the account is in excluded accounts or is a domain administrator in on a domain-joined device. |
| RequireApproval | Boolean | 0 | Elevate without requiring someone to approve requests. |
| RequireReason | Boolean | 1 | Require reason to elevate. |
| RequireAppApproval | Boolean | 0 | Elevate Run As Admin without requiring someone to approve requests. |
| RequireAppReason | Boolean | 1 | Require reason to Run As Admin. |

| Key | Type | Default | Description |
|------------------|----------------------------------|---------|---|
| ShowInstructions | Boolean | 0 | Show Code of Conduct screen. |
| UploadInventory | Boolean | 1 | Upload inventory data to the portal. |
| UserGroups | Dictionary with Array of Strings | | User groups to match machine to sub settings when not using Active Directory. |

Supplementary Technical Information

This section provides more information on the following:

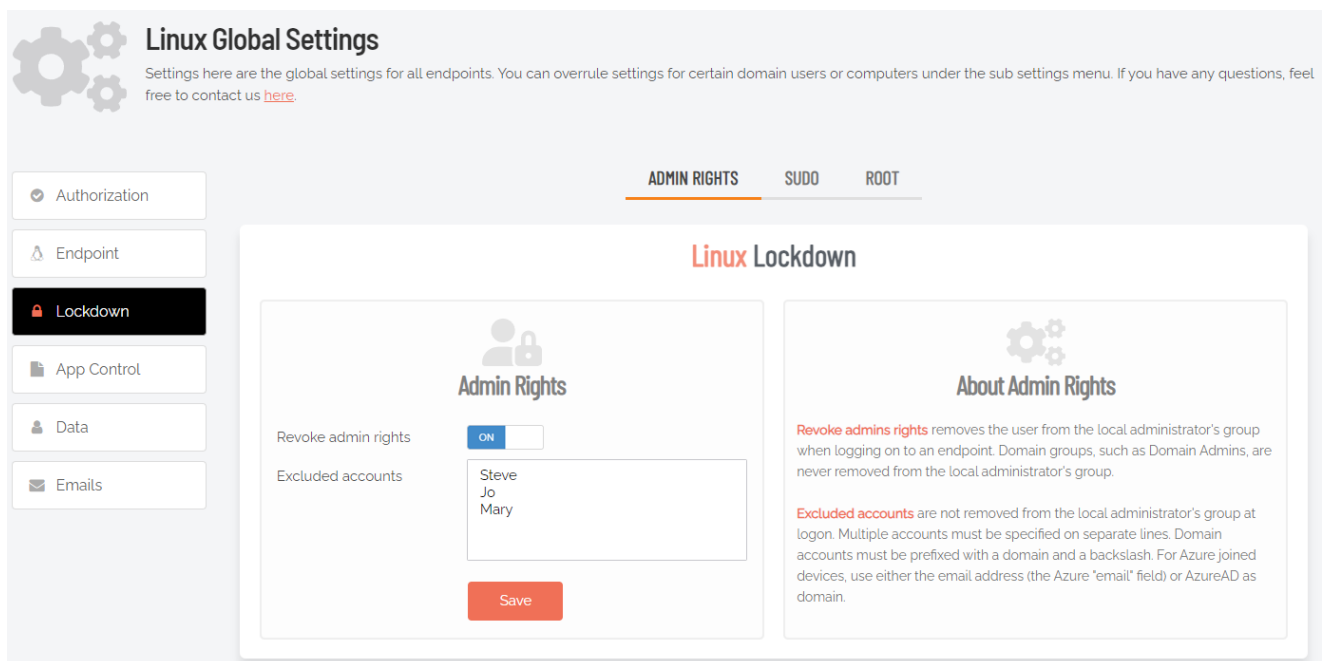
- Local Administrator Accounts
- Sub-Settings
- Sudo
- Tampering

Local Administrator Accounts

By default, users logging on to a Linux workstation are not downgraded from administrator to user unless the setting 'Revoke admin rights' is enabled in the portal and the user is *not* in the excluded accounts list. The reason all users are not downgraded immediately is because you may have service accounts that you have forgotten to list in the excluded accounts list.

Also, if someone cleared the excluded accounts list and clicked **Save** by mistake, the result would be unusable endpoints; no users would be able to gain elevated privileges and would instead have very limited ability on their devices.

The following graphic shows *Revoke Admin Rights* **ON**, *except* for user accounts Steve, Jo and Mary:



Linux Global Settings

Settings here are the global settings for all endpoints. You can overrule settings for certain domain users or computers under the sub settings menu. If you have any questions, feel free to contact us [here](#).

ADMIN RIGHTS | SUDO | ROOT

Linux Lockdown

Admin Rights

Revoke admin rights: ☒ ON

Excluded accounts: Steve, Jo, Mary

Save

About Admin Rights

Revoke admins rights removes the user from the local administrator's group when logging on to an endpoint. Domain groups, such as Domain Admins, are never removed from the local administrator's group.

Excluded accounts are not removed from the local administrator's group at logon. Multiple accounts must be specified on separate lines. Domain accounts must be prefixed with a domain and a backslash. For Azure joined devices, use either the email address (the Azure "email" field) or AzureAD as domain.

Sub-Settings

The portal has two levels of settings:

1. *Linux Settings* (also known as Global Settings) apply to all users by default, **except** those settings overridden under Sub Settings.
2. *Linux Sub Settings*, where you can define special settings based on Active Directory computer or user groups and/or Organizational Unit(s).

Settings here are the global settings for all endpoints participating in the feature. You can overrule settings for listed domain users or computers under the sub-settings menu.

Sub settings will *override* the global settings for the users or computers to which they apply. Both users and computers can be in Active Directory groups or organizational units.

If a user or computer hits multiple sub settings, the first in listed order *that includes the setting concerned* wins.

Example sub-settings

This can be used, for example, to allow sudo access for *developers* or automatically approve requests from *users in the IT department*.

Sudo

For security reasons, sudo access is disabled during administrator sessions by default. This can be enabled in the settings. We do not recommend enabling sudo access unless absolutely necessary.

Admin By Request has checks in place to prevent system tampering using sudo, but due to the root-level access, it is impossible to fully protect against tampering using sudo.

If only certain commands need to be run with sudo, consider using the built-in `/etc/sudoers` file. The Admin By Request sudo settings will not override normal `/etc/sudoers` settings.

Tampering

To prevent tampering with Admin By Request, the software monitors all important files during an administrator session. During a session, access to the Users & Groups preference panel is disabled to prevent users from adding new administrators. Further, by default, sudo access is disabled to prevent calling system-critical tools and user management from the terminal.

The service also monitors users and groups during the session to prevent tampering if sudo access is enabled. If Admin By Request detects that the clock has been changed, the administrator session will end instantly to prevent users from extending their session.

Terms and Definitions

Privileged Access

Privileged access refers to abilities and permissions that go above and beyond what is considered "standard", allowing users (with privileged access) more control and reach in the system and network.

The following table describes several common privileged access terms.

| Term | Definition |
|--|--|
| Blocklist | The opposite of a pre-approved list. A list of blocked programs or applications that are denied access in an IT environment (i.e., they are denied the ability to run) when everything is allowed by default. All items are checked against the list and granted access unless they appear on the list. Might also be known as a "blacklist" – a term no longer used. See also "Pre-Approved List" on the next page . |
| Elevated Application | An application that has been given greater privileges than what is considered standard, which enables the application user to have more control over its operation, and the app itself to have more abilities and access within the computer. |
| Elevated Privileges | Also known as "privileged access". Elevated privileges provide the ability to do more than what is considered standard; for example, install and uninstall software, add and edit users, manage Group Policy, and modify permissions. Elevated privileges are sought after by attackers, who can use them to propagate through a network, remain undetected, and gain a strong foothold from which to launch further attacks. |
| Endpoint | A physical device that is capable of connecting to and exchanging information with a computer network. Endpoints include mobile devices, desktop computers, virtual machines, embedded devices, servers, and Internet-of-Things (IoT) devices. |
| Endpoint Security | An holistic approach to securing a network that goes beyond traditional anti-malware and aims to protect every endpoint from potential threats. See also "EDR" on the next page in the glossary. |
| Horizontal Privilege Escalation | Also known as "account takeover". Occurs when access to an account of a certain level (e.g., Standard User) is obtained from an account at that same level. Usually occurs when a malicious actor compromises a lower-level account and propagates through the network by compromising other lower-level accounts. See also "Vertical Privilege Escalation" on the next page . |
| Just-In-Time Access (JIT) | A way of enforcing the Principle of Least Privilege (POLP) by allowing access to privileged accounts and resources only when it is needed, rather than allowing "always on" access (also known as "standing access"). This reduces an organization's attack surface by minimizing the amount of time an internal or external threat has access to privileged data and capability. |
| Lateral Movement | A common technique used by malicious actors, in which they spread from the initial entry point further into the network, while evading detection, retaining access, and gaining elevated privileges using a combination of tactics. The purpose is generally to compromise as many accounts as possible, access high-value assets, and/or locate a specific target or payload. |

| Term | Definition |
|--------------------------------------|--|
| Phishing | A type of social engineering attack in which the victim is tricked into clicking a malicious link that can lead to malware installation or further duping of the victim into providing sensitive information such as credentials or credit card details. |
| Pre-Approved List | The opposite of a blocklist. A list of approved programs or applications that are trusted (considered safe) when everything is denied by default. Items are checked against the already approved list and are only able to run if they are included in that list. Might also be known as a "whitelist" – a term no longer used. See also "Blocklist " on the previous page. |
| Privileged Account | An account that has been granted access and privileges beyond those granted to non-privileged accounts. More sought after by attackers because, if compromised, they provide a better vantage point from which to launch an attack. |
| Privileged User | A trusted user who is authorized to leverage privileged access, such as through a privileged account, to perform high-value functions for which standard users are not authorized. |
| Standard User Account | A basic account for undertaking day-to-day tasks, for users who is not authorized or required to perform activities that require elevated privileges. These accounts are typically safer than those with higher access and permissions, as they do not provide the capability to perform administrative tasks, such as change system settings, install new software, manage the domain, and change local user credentials. |
| Vertical Privilege Escalation | Occurs when a lower-privileged account gains privileged access beyond what it is intended to have. Usually occurs when a malicious actor compromises an account (e.g., a "Standard User" account) and then exploits system flaws or overrides privilege controls to escalate that account to one with higher privileges (e.g., a "Local Administrator" account). See also "Horizontal Privilege Escalation" on the previous page. |

Glossary

The following table lists the meanings of many acronyms used when discussing privileged access management and endpoint protection.

| Term | Short for | Definition |
|-----------------|---------------------------------|---|
| Azure AD | Azure Active Directory | Azure Active Directory is part of Microsoft Entra, which is an enterprise identity service that provides single sign on, multi-factor authentication, and conditional access to guard against security threats. |
| Entra ID | Microsoft Entra | Microsoft Entra is a family of multi-cloud identity and access solutions that includes Azure AD. The term "Entra ID" replaces the term "Azure AD". |
| EDR | Endpoint Detection and Response | A method of securing endpoints that focuses on detecting and responding to threats that are present. Works in conjunction with EPP. |

| Term | Short for | Definition |
|----------------|-------------------------------|---|
| EPP | Endpoint Protection Platform | A method of securing endpoints that focuses on preventing threats from arriving. Combines analysis, monitoring & management, anti-malware software, EDR capabilities and other security features into a comprehensive endpoint security platform. |
| FIDO | Fast Identity Online | <p>With FIDO Authentication, users sign in with phishing-resistant credentials, called "Passkey" below. Passkeys can be synced across devices or bound to a platform or security key and enable password-only logins to be replaced with secure and fast login experiences across websites and apps.</p> <p>Passkeys are more secure than passwords and SMS OTPs, simpler for consumers to use, and easier for service providers to deploy and manage.</p> |
| Intune | Microsoft Intune | Microsoft Intune is a cloud-based UEM solution. It manages user access and simplifies device and application management for multiple platforms, including mobile devices, desktop computers, and virtual endpoints. |
| MAM | Mobile Application Management | Software and processes that secure and enable IT control over enterprise applications on end users' corporate and personal devices. |
| MDM | Mobile Device Management | A methodology and toolset used to provide a workforce with mobile productivity tools and applications, while keeping corporate data secure. |
| PAM | Privileged Access Management | A set of cybersecurity technologies and strategies that allow organizations to secure their infrastructure and applications by managing privileged access and permissions for all users across the IT environment. |
| Passkey | Passkey | Passkeys are a replacement for passwords that provide faster, easier, and more secure sign-ins to websites and apps across a user's devices. Unlike passwords, passkeys are always strong and phishing-resistant. |
| POLP | Principle of Least Privilege | The idea that users, applications, programs, and processes should be allowed only the bare minimum privileges necessary to perform their respective functions. |
| UEM | Unified Endpoint Management | A way to securely manage all the endpoints in an enterprise or an organization from a central location. |

Document History

| Document | Product | Changes |
|-------------------------|--------------------------|--|
| 1.0 31 May 2023 | 2.2 19 September 2022 | Initial document release |
| 1.1 7 August 2023 | 3.0 7 August 2023 | <p>Included 3.0 features</p> <ul style="list-style-type: none"> Improved Run As Admin sudo sessions Support for pre-approved and blocked applications in sudo sessions Revoke admin rights now automatically removes local admin groups from user accounts Audit logging on programs executed in sudo sessions Option for disabling interactive sudo sessions Option for disabling the root account Option for allowing or disallowing changing of the root password Integration of identity management such as Active Directory, FreeIPA and LDAP domain using SSSD client software <p>Applied new document template and formatting</p> |
| 1.2 16 February 2024 | 3.0 7 August 2023 | <p>Added proxy server configuration section.</p> <p>Added multiple Settings Tables to chapter Portal Administration.</p> <p>Restructured User Interface chapter.</p> <p>Fixed pagination.</p> |
| 1.3 28 March 2024 | 3.0 7 August 2023 | <p>Added Settings Table for Linux Settings > Data > PRIVACY.</p> <p>Added Settings Tables for tabs under Linux Settings > Lockdown.</p> <p>[Online only] Added FAQ explaining distorted fonts under UI scaling.</p> <p>Updated portal menu selection paths.</p> |
| 1.4 24 May 2024 | 3.1 22 May 2024 | <p>Added Command Line Interface chapter.</p> <p>Updated screenshots for v3.1.9</p> <p>Added remaining settings tables for <i>Endpoint</i> and <i>App Control</i> menus.</p> |

Document

2.0
18 December 2025

Product

4.0
18 December 2025

Changes

Included 4.0 features:

- Support for Break Glass one-time-use admin accounts.
- Support for Multi-Factor Authentication (MFA).
- MFA on both graphics and command line interfaces
- Separate account for privilege elevation, to comply with Cyber Essentials Plus
- A significant number of performance & stability improvements and bug fixes

Updated manual structure and layout.

Added section *Your Tenant License* in chapter "Linux Client - Install / Uninstall".

Added commands for Red Hat-based as well as Debian-based distributions.

Index

A

| | |
|------------------------------|----|
| About ABR | |
| About | 9 |
| Connectivity | 13 |
| About Admin By Request | 9 |
| Admin Rights | |
| Tab | 40 |
| Admin Session | |
| Settings | 37 |
| Administrator Access | |
| User Interface | 18 |
| Audience | 1 |
| Auditlog | 33 |
| Azure AD | 48 |

B

| | |
|----------------------|----|
| BIOS | 5 |
| Break Glass Account | |
| User Interface | 21 |

C

| | |
|--------------------------------|----|
| Check version | 26 |
| chmod | 3 |
| Command | |
| abr finish | 27 |
| abr settings | 28 |
| abr start | 29 |
| abr status | 30 |
| abr version | 29 |
| Command Line Interface | 26 |
| Command option | |
| abr --help | 30 |
| abr --log-level | 32 |
| abr --master-config-file | 31 |
| abr --system-config-file | 32 |

| | |
|----------------------------|----|
| Component | |
| CLI plugin | 12 |
| GUI | 10 |
| Main module | 10 |
| PAM plugin | 11 |
| Polkit plugin | 12 |
| Service | 11 |
| sudo plugin | 13 |
| Condition (blocking) | 46 |

D

| | |
|----------------|---|
| Download | 3 |
|----------------|---|

E

| | |
|-------------------------|----|
| Endpoint | |
| Setting | 38 |
| Entra ID | 48 |
| Execution history | 17 |

F

| | |
|----------------------|----|
| File Blocking | |
| Settings | 45 |
| File Locations | 7 |

G

| | |
|--------------------------|---|
| GUI User Interface | 8 |
|--------------------------|---|

I

| | |
|--------------------|----|
| Install | 2 |
| Instructions | |
| Tab | 39 |
| IP addresses | 15 |

L

| | |
|------------------------------------|----|
| Local Administrator Accounts | 53 |
| Lockdown | |
| Setting | 40 |
| Look & Feel | |
| Tab | 38 |

M

| | |
|-----------------------------------|--------|
| Multi-Factor Authentication | 17, 20 |
|-----------------------------------|--------|

O

| | |
|----------------------------------|----|
| Overruling Portal Settings | 51 |
| Overview | 1 |

P

| | |
|------------------------|----|
| Packages | 5 |
| Performance | 7 |
| Policies | |
| Linux | 51 |
| Policy file | 51 |
| Portal Administration | |
| Linux | 35 |
| Ports | 15 |
| Pre-Approval | |
| Settings | 42 |
| Pre-Approve | |
| Tab | 42 |
| Prerequisites | 2 |
| Preventing Abuse | 50 |
| Privacy | |
| Settings | 47 |
| Proxy Server | 14 |

R

| | |
|----------------------|----|
| Release Notes | 1 |
| Root | |
| Tab | 41 |
| Run As Admin | |
| Settings | 36 |
| User Interface | 16 |

S

| | |
|---|---------|
| Sub-Settings | 54 |
| sudo | 3-4, 16 |
| Sudo | 54 |
| Tab | 41 |
| Supplementary Technical Information | 53 |

T

| | |
|-------------------------|----|
| Tamper prevention | 6 |
| Tampering | 54 |
| Tenant License | 2 |
| Test | 3 |
| Type (blocking) | 46 |

U

| | |
|---------------------|----|
| UEFI | 5 |
| Uninstall | 2 |
| Upgrade | |
| Debian-based | 4 |
| Red Hat-based | 4 |
| Upgrading | 4 |
| User accounts | 20 |
| User rights | 6 |