Document Code: **PM-WC-ITAG**

Document Version: **1.5**

Document Date: **11 March 2024**

Windows Client: IT Admin Guide

Configure, deploy and manage your Windows workstations

Admin By Request

Windows Product Version: **8.2**

Admin By Request

Contact Admin By Request

1390 Market Street, Suite 200
San Francisco, CA 94102

Phone and Email:
adminbyrequest.com/contact

www.adminbyrequest.com
linktr.ee/adminbyrequest

Table of Contents

Windows 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 windows endpoints.

In This Document

The content of this guide describes:

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

Audience

The Windows Client: IT Admin Manual is intended for IT system administrators who install and manage user workstations running the Windows 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 website:

Resources > Documentation > Release Notes (Windows)

Windows Client - Install / Uninstall

Prerequisites

Admin By Request, version 8.2 supports all current Windows versions, including:

- Windows 11
- Windows 10
- Windows 7 and 8 (Pro and Enterprise only)
- Windows Server (with Desktop Experience only)

If installing individually on client endpoints, you will need administrator privileges. on every workstation that executes the installation client.

If installing via Intune, you need to be able to create Intune packages.

You'll also need valid credentials to access your Admin By Request online portal at Admin By Request Portal.

Installing Admin By Request

There are three installation scenarios covered here:

I Single Workstation	II Unattended	III Using Intune

> **NOTE:**
> These scenarios are not sequential - pick one or a combination of all three, depending on your requirements.

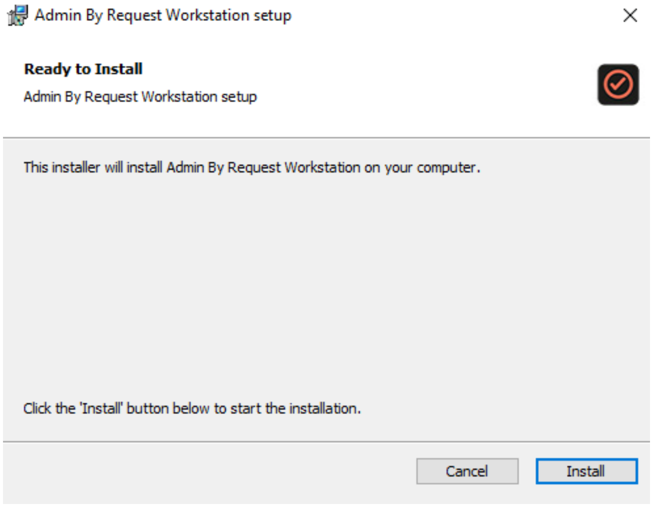
I. Installing a single workstation

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

A. Download and install the Admin By Request Windows client.

1. Download the Windows client from https://account.adminbyrequest.com/ABRDownload and store the msi file in a suitable location.

2. Double-click the msi file to start the installation and click **Install** when prompted:



Admin By Request Workstation setup

Ready to Install

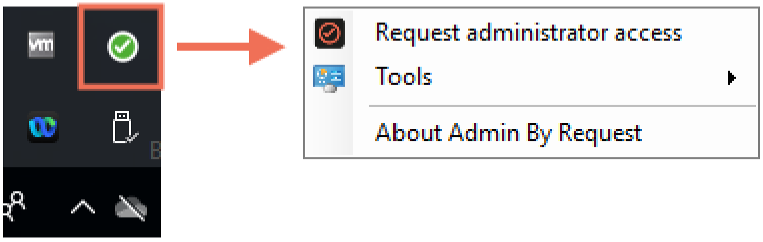
Admin By Request Workstation setup

This installer will install Admin By Request Workstation on your computer.

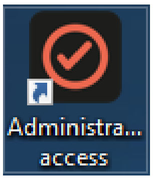
Click the 'Install' button below to start the installation.

> **NOTE:**
> You might be prompted for administrator credentials depending on the endpoint's UAC configuration.

3. When the installation completes, the Admin By Request icon appears in the system tray in the bottom right corner of the screen. Click the icon to show details about the client or to start an Admin Session:



Depending on installation preferences, an Admin By Request shortcut icon may also be placed on the desktop:

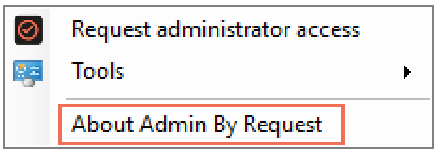


Installation is now complete.

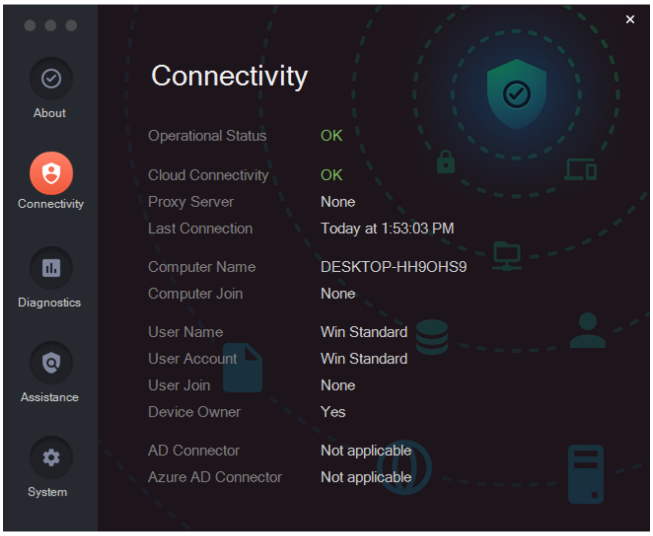
B. Test the installation

Testing the installation involves a quick connection check:

1. On an endpoint with Admin By Request installed, launch the application by selecting it from the system tray and clicking **About Admin By Request**:



2. Select **Connectivity** and check that *Operational Status* and *Cloud Connectivity* are **OK**:

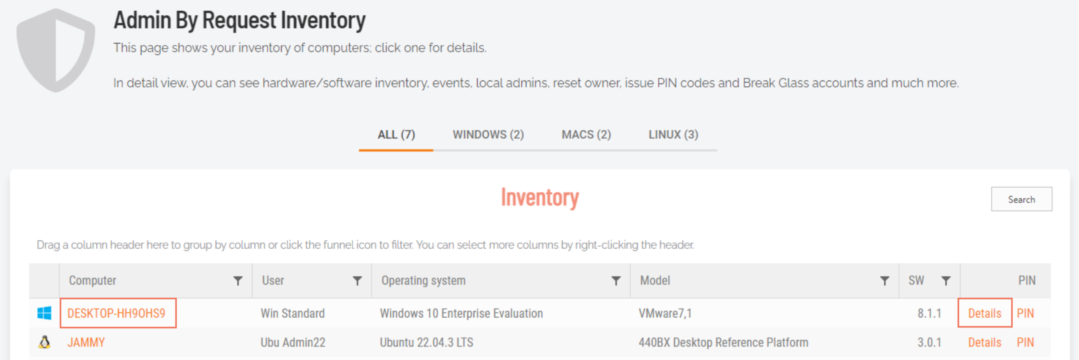


Connectivity

Operational Status	OK
Cloud Connectivity	OK
Proxy Server	None
Last Connection	Today at 1:53:03 PM
Computer Name	DESKTOP-HH9OHS9
Computer Join	None
User Name	Win Standard
User Account	Win Standard
User Join	None
Device Owner	Yes
AD Connector	Not applicable
Azure AD Connector	Not applicable

You might also want to check the inventory in the portal, to review the details that are now being logged for this endpoint:

1. From the portal top menu, select **Inventory**.
2. Locate the endpoint and click either the computer name link or the **Details** link:



Admin By Request Inventory

This page shows your inventory of computers; click one for details.

In detail view, you can see hardware/software inventory, events, local admins, reset owner, issue PIN codes and Break Glass accounts and much more.

Inventory

Drag a column header here to group by column or click the funnel icon to filter. You can select more columns by right-clicking the header.

Computer	User	Operating system	Model	SW		PIN
DESKTOP-HH9OHS9	Win Standard	Windows 10 Enterprise Evaluation	VMware7,1	8.1.1	Details	PIN
JAMMY	Ubu Admin22	Ubuntu 22.04.3 LTS	440BX Desktop Reference Platform	3.0.1	Details	PIN

II. Unattended installation

To install unattended, use standard msiexec.exe switches (/I and /QN):

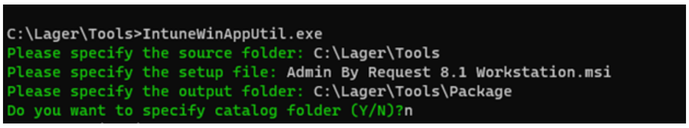
```
msiexec.exe /I AdminByRequest.msi /QN
```

> **NOTE:**
> As part of the overall installation process, pick several endpoints at random and test that installation was successful (see "Test the installation" on the previous page).

III. Creating an Intune package

1. Before adding the application to Intune, create a package in the **.intunewin** format using the Microsoft Win32 Content Prep Tool.

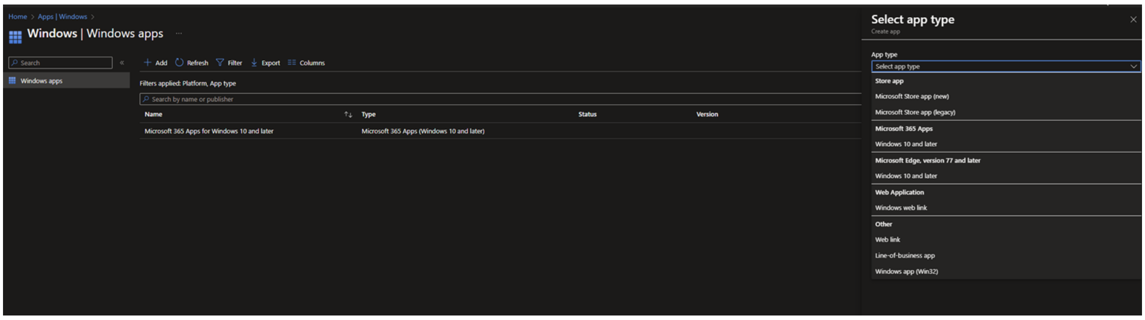
2. Run the tool (**IntuneWinAppUtil.exe**) at a Windows command line, entering data as shown:



```
C:\Lager\Tools>IntuneWinAppUtil.exe
Please specify the source folder: C:\Lager\Tools
Please specify the setup file: Admin By Request 8.1 Workstation.msi
Please specify the output folder: C:\Lager\Tools\Package
Do you want to specify catalog folder (Y/N)?n
```

   This creates an Admin By Request package file that can be used by Intune.

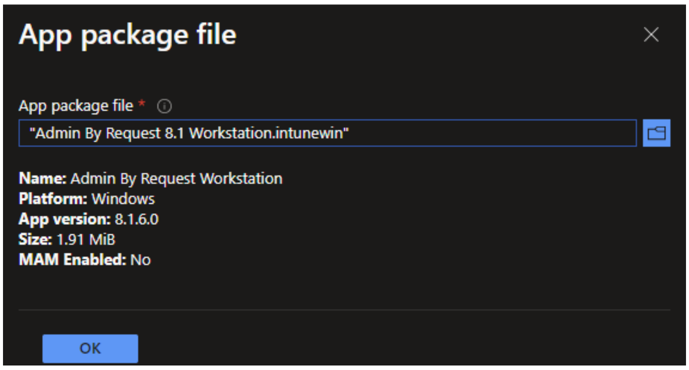
3. Go to Intune and open **Apps > Windows** and click **Add**:



Filters applied: Platform, App type

Name	Type	Status	Version
Microsoft 365 Apps for Windows 10 and later	Microsoft 365 Apps (Windows 10 and later)		

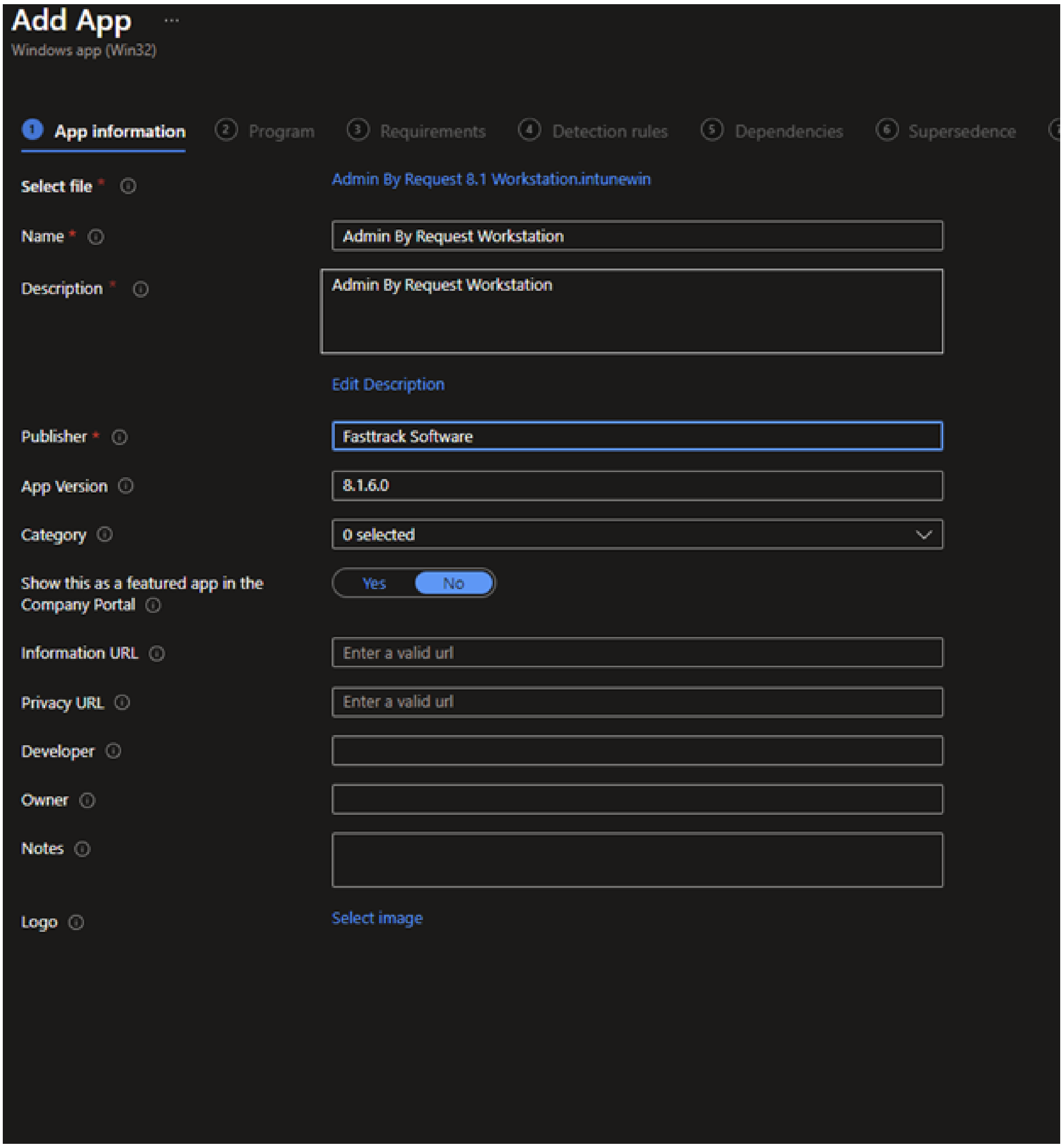
4. Select **Windows app (Win32)** and click **Select**.
5. Choose the Admin By Request package file created in step 2 and click **OK**:



App package file * "Admin By Request 8.1 Workstation.intunewin"

Name: Admin By Request Workstation
Platform: Windows
App version: 8.1.6.0
Size: 1.91 MiB
MAM Enabled: No

6. In the *(1) App information* window, enter **Publisher** and **App Version** if not already given:



Add App ...

Windows app (Win32)

Select file * : Admin By Request 8.1 Workstation.intunewin

Name * : Admin By Request Workstation

Description * : Admin By Request Workstation

Edit Description

Publisher * : Fasttrack Software

App Version : 8.1.6.0

Category : 0 selected

Show this as a featured app in the Company Portal : Yes [✓ No]

Information URL : Enter a valid url

Privacy URL : Enter a valid url

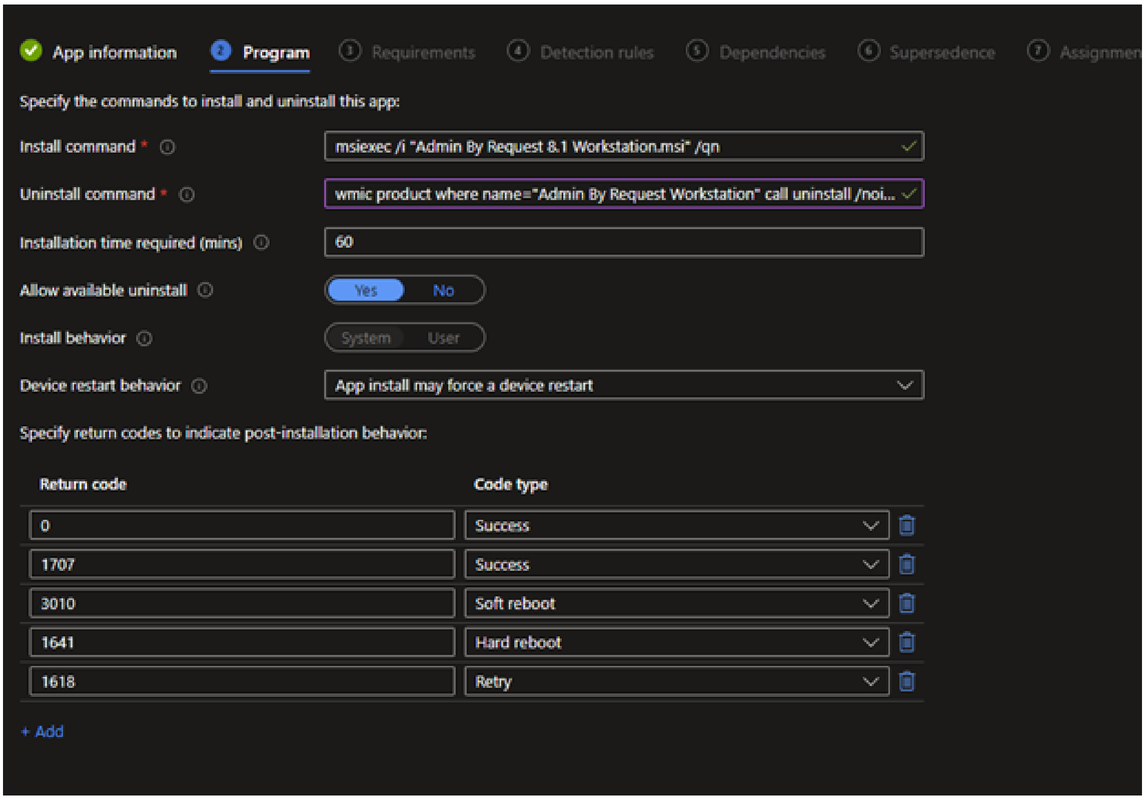
Developer :

Owner :

Notes :

Logo : Select image

7. In the *(2) Program* window, enter change the **Uninstall command** to: **wmic product where name="Admin By Request Workstation" call uninstall /nointeractive**



Specify the commands to install and uninstall this app:

Install command *: msiexec /i "Admin By Request 8.1 Workstation.msi" /qn

Uninstall command *: wmic product where name="Admin By Request Workstation" call uninstall /noi...

Installation time required (mins): 60

Allow available uninstall: [✓ Yes] No

Install behavior: System User

Device restart behavior: App install may force a device restart

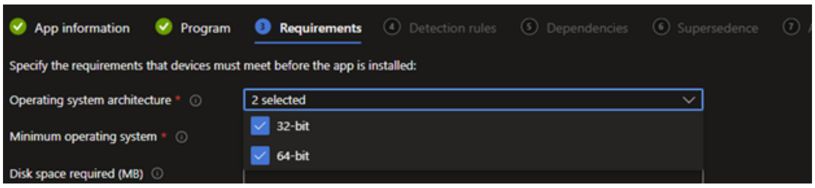
Specify return codes to indicate post-installation behavior:

Return code	Code type
0	Success
1707	Success
3010	Soft reboot
1641	Hard reboot
1618	Retry

+ Add

8. In the *(3) Requirements* window:

   a. For **Operating system architecture**, select both **32-bit** and **64-bit**:



Specify the requirements that devices must meet before the app is installed:

Operating system architecture *: 2 selected

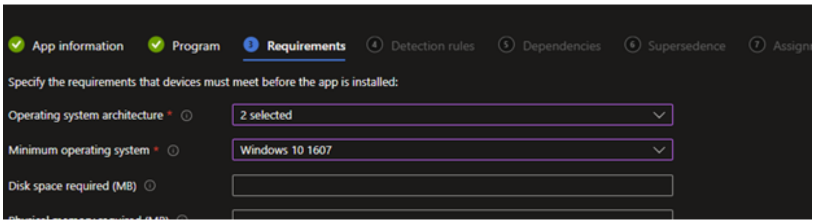
☑ 32-bit

☑ 64-bit

Minimum operating system *

Disk space required (MB)

   b. For **Minimum operating system**, select **Windows 10 1607**:



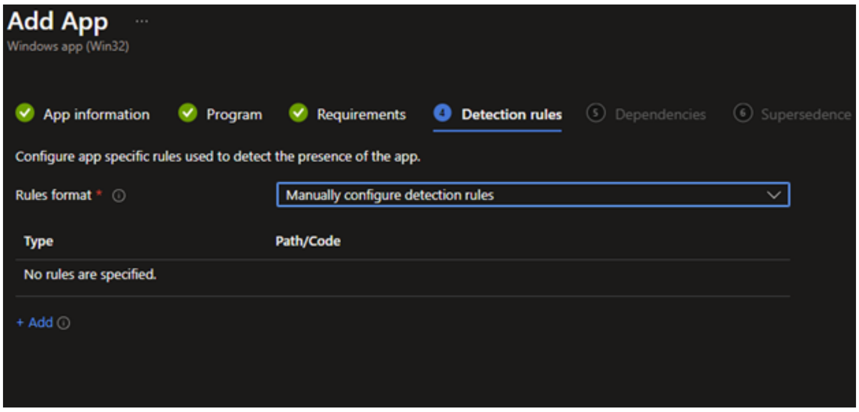
Specify the requirements that devices must meet before the app is installed:

Operating system architecture *: 2 selected

Minimum operating system *: Windows 10 1607

Disk space required (MB):

9. In the *(4) Detection rules* window, for **Rules format**, select **Manually configure detection rules** and click **+ Add**::



Add App ...

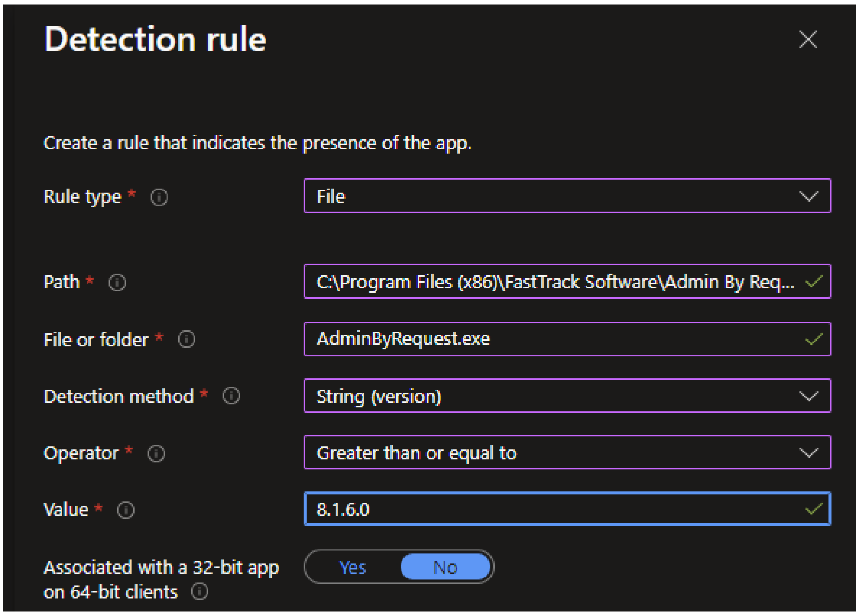
Windows app (Win32)

Configure app specific rules used to detect the presence of the app.

Rules format * ⓘ Manually configure detection rules

Type	Path/Code
No rules are specified.	

10. In the *Detection rule* window, change the **Path** to **C:\Program Files (x86)\FastTrack Software\Admin By Request**:



Detection rule

Create a rule that indicates the presence of the app.

Rule type * ⓘ File

Path * ⓘ C:\Program Files (x86)\FastTrack Software\Admin By Req... ✓

File or folder * ⓘ AdminByRequest.exe ✓

Detection method * ⓘ String (version)

Operator * ⓘ Greater than or equal to

Value * ⓘ 8.1.6.0 ✓

Associated with a 32-bit app on 64-bit clients ⓘ Yes [✓ No]

11. Continue with the Intune package process, accepting the defaults for all remaining prompts/questions.

> **NOTE:**
> As part of the overall installation process, pick several endpoints at random and test that installation was successful (see "Test the installation" on page 3).

Upgrading Admin By Request

As the installer is a standard MSI file, upgrading is automatically detected.

If you deploy a newer version of the Admin By Request Windows client, **msiexec.exe** will automatically perform an uninstall of the old version and an install of the new version.

Deploying new releases

Admin By Request software updates are deployed by our Auto-Update process. However, when we release a new version we do not deploy it right away to all customers via auto-update. This is simply to mitigate any issues that arise after beta testing.

Our rule-of-thumb is to activate auto-update of new releases within 4 - 8 weeks of release, but this is subject to change, depending on feedback and any potential issues that might arise.

Uninstalling Admin By Request

There are four uninstallation scenarios covered here, one that can be initiated by a Standard User and three that require Administrator capability throughout:

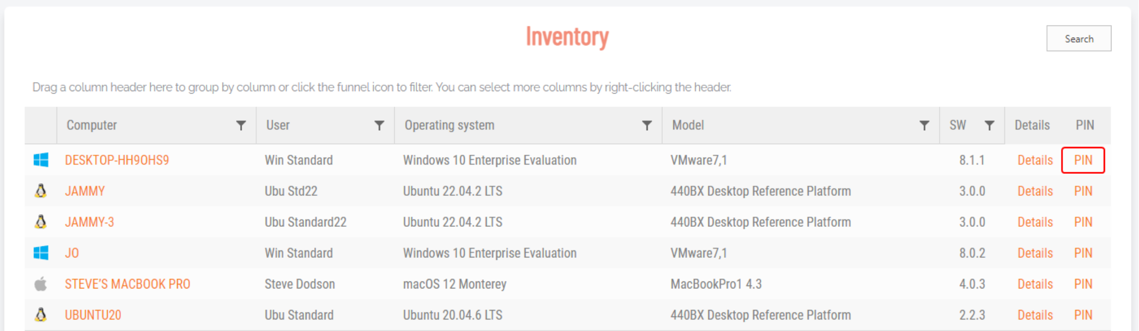
I	II	III	IV
PIN Code (Standard User)	Unattended (Administrator)	Via msi file (Administrator)	Using PsExec (Administrator)

> **NOTE:**
> These scenarios are not sequential - pick one or more, depending on requirements.

I. **PIN Code (Standard User)**

The first few steps in this procedure require access to the portal.

1. In the Admin By Request portal, navigate to the *Inventory* page and identify the device on which to perform the uninstall.
2. Locate the device in the inventory list - in the PIN column, click **PIN** for that device (columns can be switched around - the PIN column in your portal might not be the right-most column):

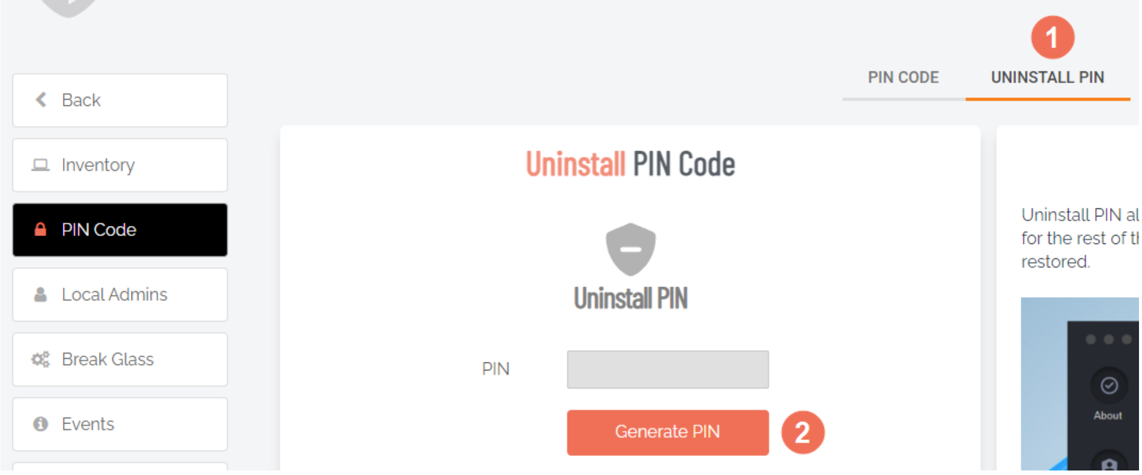


Inventory

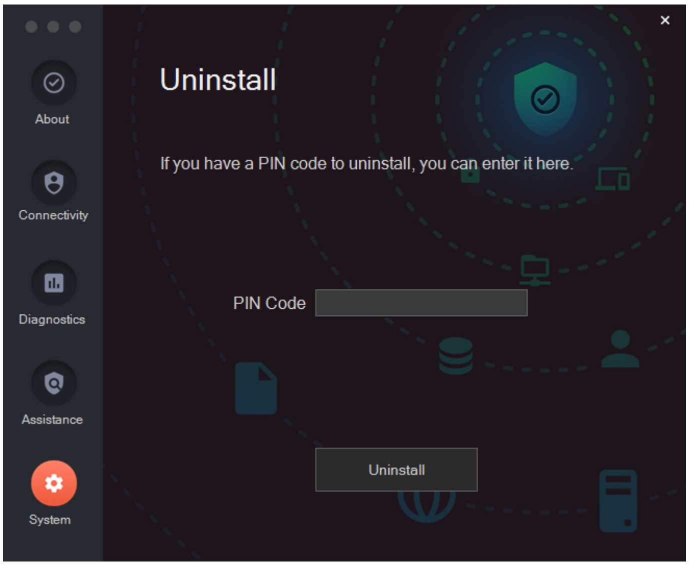
Drag a column header here to group by column or click the funnel icon to filter. You can select more columns by right-clicking the header.

	Computer	User	Operating system	Model	SW	Details	PIN
	DESKTOP-HH9OHS9	Win Standard	Windows 10 Enterprise Evaluation	VMware7,1	8.1.1	Details	PIN
	JAMMY	Ubu Std22	Ubuntu 22.04.2 LTS	440BX Desktop Reference Platform	3.0.0	Details	PIN
	JAMMY-3	Ubu Standard22	Ubuntu 22.04.2 LTS	440BX Desktop Reference Platform	3.0.0	Details	PIN
	JO	Win Standard	Windows 10 Enterprise Evaluation	VMware7,1	8.0.2	Details	PIN
	STEVE'S MACBOOK PRO	Steve Dodson	macOS 12 Monterey	MacBookPro1 4.3	4.0.3	Details	PIN
	UBUNTU20	Ubu Standard	Ubuntu 20.04.6 LTS	440BX Desktop Reference Platform	2.2.3	Details	PIN

3. Click tab **UNINSTALL PIN** and then click button **Generate PIN**:



4. Back on the device on which you want to uninstall Admin By Request, select the *Admin By Request* icon from the system tray and click **About Admin By Request**.
5. Select **System**, enter the Uninstall PIN generated above into the *PIN Code* field and click **Uninstall**:



II. Unattended uninstallation (Administrator)

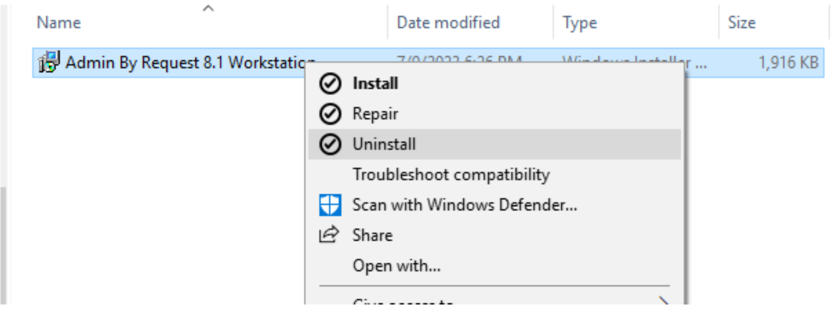
To remove unattended, use standard msiexec.exe switches (/X and /QN):

```
msiexec.exe /X AdminByRequest.msi /QN
```

III. Via the msi installation file (Administrator)

The client installer is a standard msi file. Simply right-click the msi file, select **Uninstall** and all components will be removed:

1. Log in as an Administrator.
2. Right-click the msi installation file and select **Uninstall**:


Name
Date modified
Type
Size
Admin By Request 8.1 Workstatio
1,916 KB
Install
Repair
Uninstall
Troubleshoot compatibility
Scan with Windows Defender...
Share
Open with...

> **NOTE:**
> At the time of writing, the confirmation windows that pop-up refer to *installing* Admin By Request rather than *uninstalling* it. Provided **Uninstall** was selected at step 2, the program will indeed be uninstalled.

IV. Using PsExec (Administrator)

> **NOTE:**
> The following code lines might wrap, especially if viewing in PDF format.. When copying, make sure there are **no line breaks** and replace place holders such as \\REMOTECOMPUTERNAME and \\path\to\ABR\MSI with the correct information for your environment.

- Uninstall via **Path**:

```
psexec -s -e -h -u DOMAIN\user -p password \\REMOTECOMPUTERNAME msiexec
/x "\\path\to\ABR\MSI\Admin By Request x.x.x (xxxxx) Workstation.msi
(file://path/to/ABR/MSI/Admin%20By%20Request%20x.x.x%20
(xxxxx)%20Workstation.msi)" /qn
```

- Uninstall via **MSI-code**:

```
psexec -s -e -h -u DOMAIN\user -p password \\REMOTECOMPUTERNAME msiexec
/x {MSI-PRODUCT-CODE} /passive
```

- Uninstall via **Endpoint Name**:

```
psexec -s -e -h -u DOMAIN\user -p password \\REMOTECOMPUTERNAME wmic
product where "name like 'admin by request%%'" call uninstall
```

User rights after installation

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

- You have turned off **Revoke Admins Rights** in the portal settings (**Settings Workstation Settings > Windows 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.

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

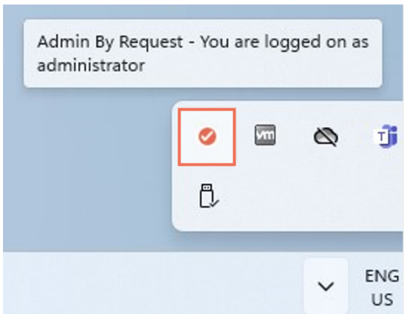
When users are not using Admin By Request, it does not consume resources, except for a brief daily inventory and settings check.

The Windows Client User Interface

Introduction

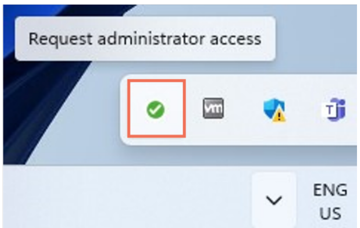
The user interface is graphical and is accessed via the tray icon on the task bar.

The color of the tray icon depends on the currently logged-in user: if the user is an administrator, the icon is red, whereas if the user is a standard user, the tray icon is green. The difference is illustrated below, when the logged-in user *mouses-over* the tray icon:



Admin By Request - You are logged on as administrator

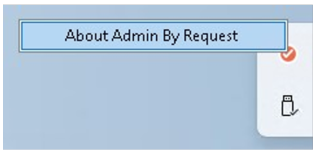
Administrator



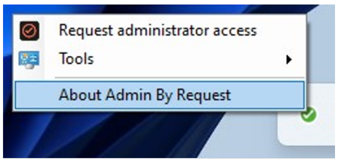
Request administrator access

Standard User

Clicking (rather than mousing-over) the icon displays a menu, which again depends on the currently logged-in user:



Administrator

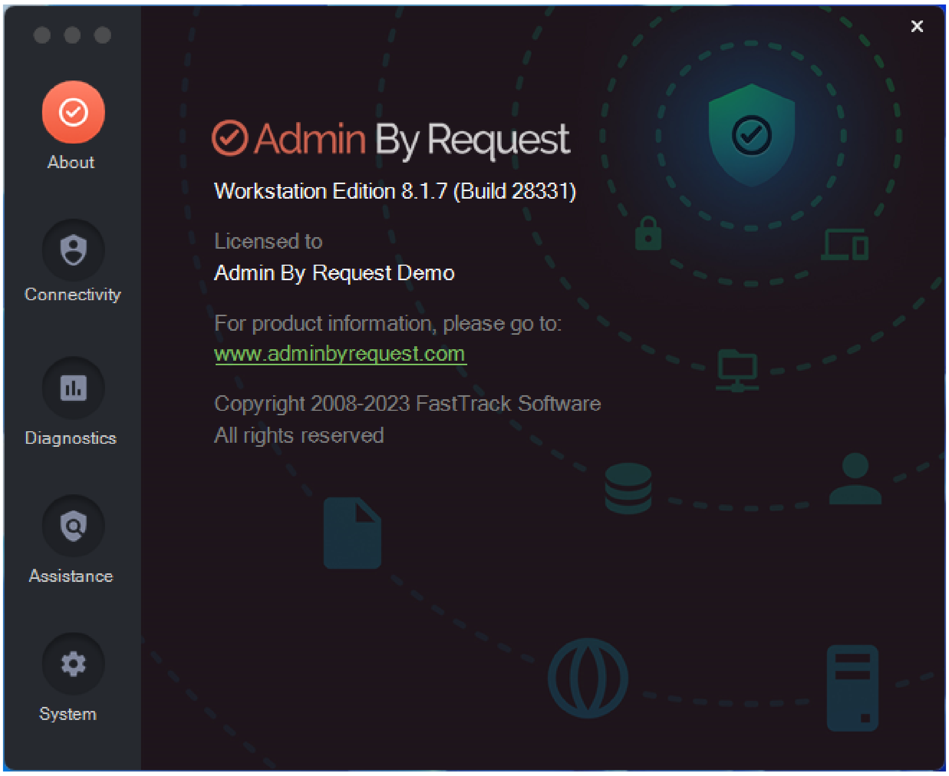


Standard User

In this topic

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 tool tray (or launching from the desktop if the shortcut is installed) launches the *user interface*, which comprises a simple window with five buttons down the left-hand side:



Workstation Edition 8.1.7 (Build 28331)

Licensed to
Admin By Request Demo

For product information, please go to:
www.adminbyrequest.com

Copyright 2008-2023 FastTrack Software
All rights reserved

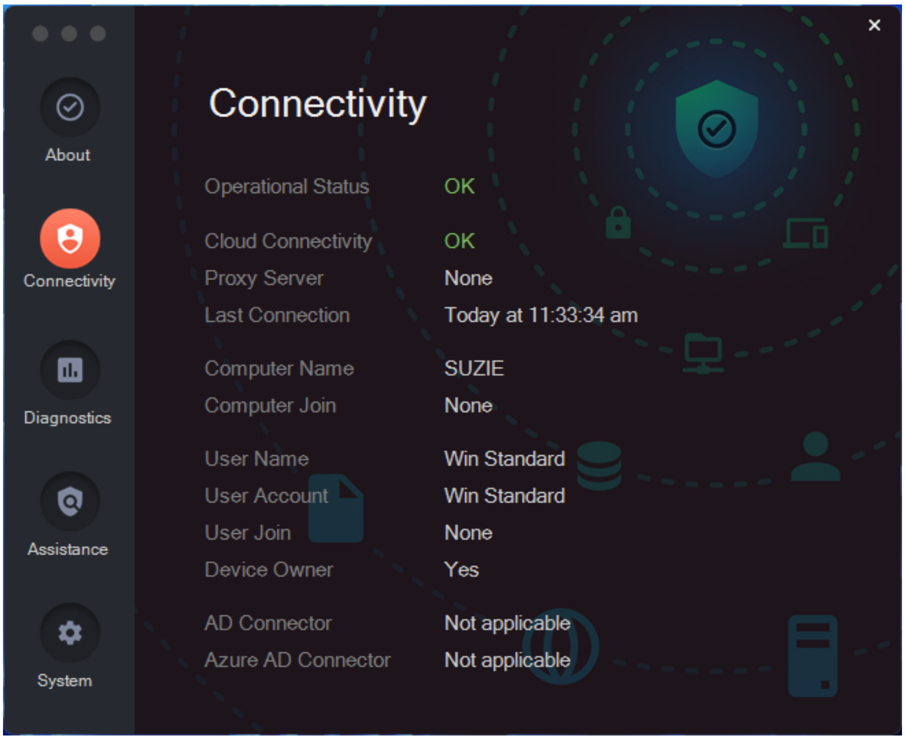
The default panel is *About Admin By Request*, which is accessed via the top button. It shows the current workstation edition, license details, website link, and copyright information.

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

Other Panels (accessed via their respective buttons).

> **NOTE:**
> In the *About Admin By Request* screens, all buttons are visible if the currently logged-in user is a Standard User, whereas only **About**, **Connectivity** and **Diagnostics** are visible for an Administrator.

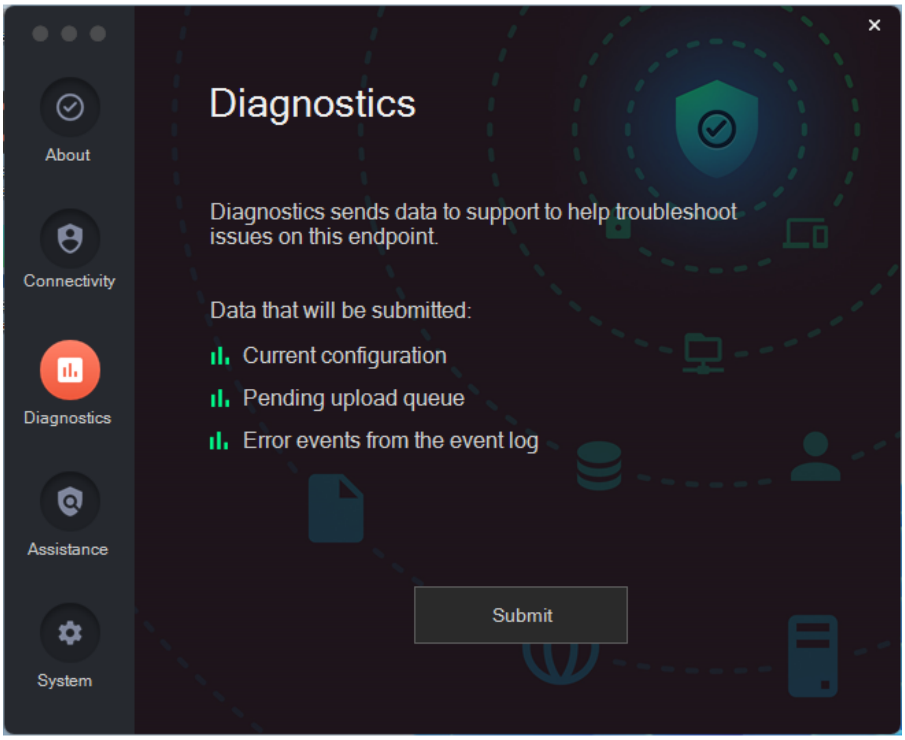
- **Connectivity** – displays the current operational status of the Admin By Request system, including Internet and Cloud connectivity, and details about the current workstation and user (see "Connecting via a Proxy Server" on page 17 for more information):



Connectivity

Operational Status	OK
Cloud Connectivity	OK
Proxy Server	None
Last Connection	Today at 11:33:34 am
Computer Name	SUZIE
Computer Join	None
User Name	Win Standard
User Account	Win Standard
User Join	None
Device Owner	Yes
AD Connector	Not applicable
Azure AD Connector	Not applicable

- **Diagnostics** – provides a way to send useful diagnostic data on this workstation to the ABR support team (see "Submitting Diagnostics" on page 18 for more information):



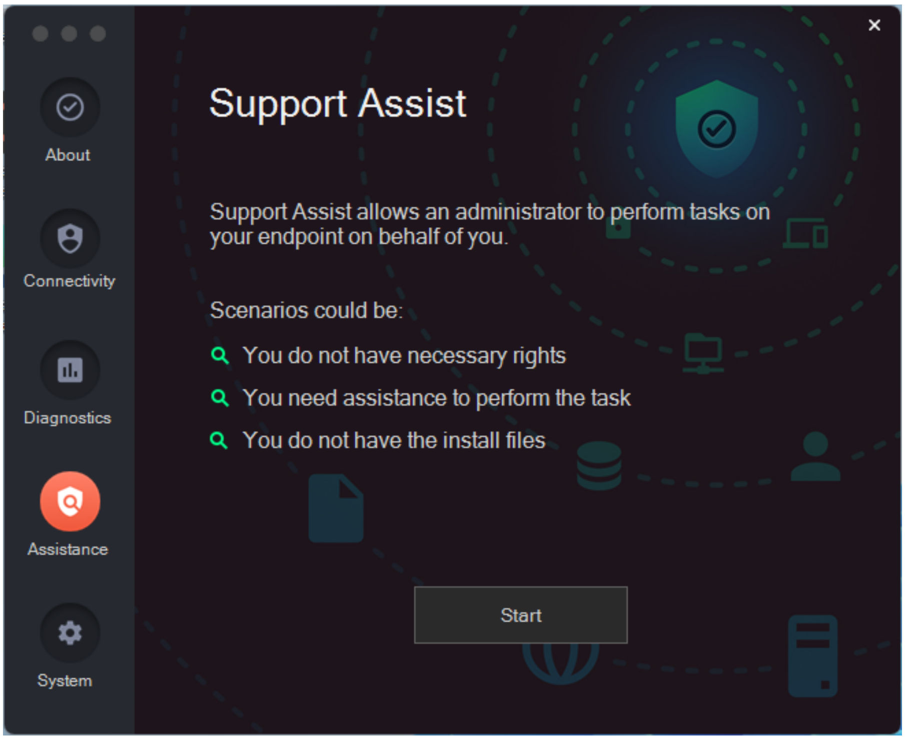
Diagnostics

Diagnostics sends data to support to help troubleshoot issues on this endpoint.

Data that will be submitted:

- Current configuration
- Pending upload queue
- Error events from the event log

- **Assistance** - (Standard User only) allows users to ask an IT administrator to access the endpoint remotely and carry out tasks on the user's behalf (see "Requesting Assistance" on page 18 for more information):



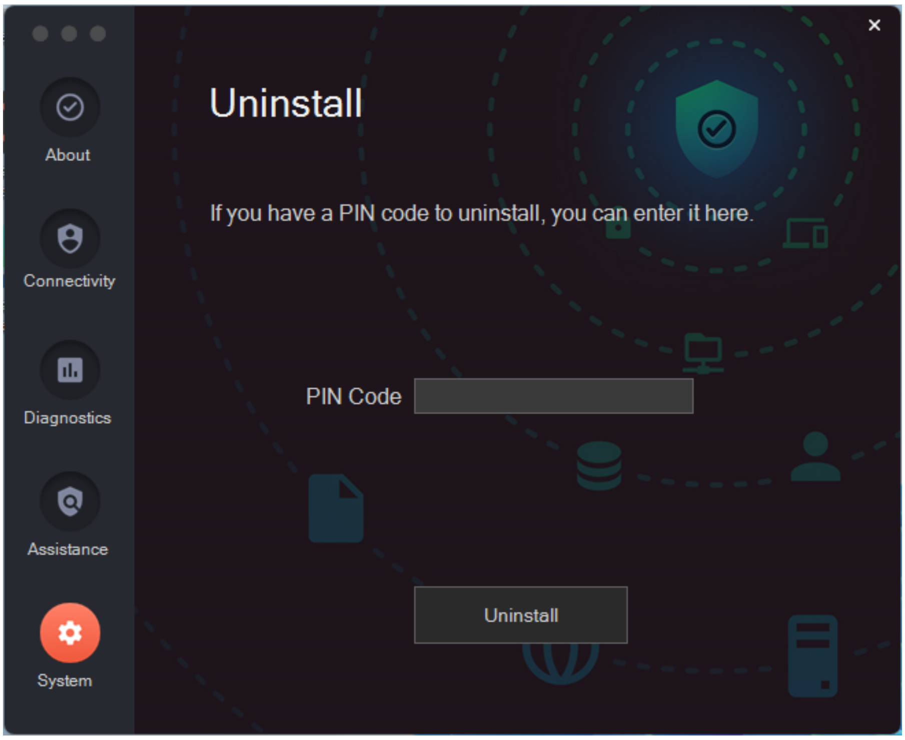
Support Assist

Support Assist allows an administrator to perform tasks on your endpoint on behalf of you.

Scenarios could be:

- You do not have necessary rights
- You need assistance to perform the task
- You do not have the install files

- **System** – (Standard User only) allows users to request a *PIN Code* that can be used to uninstall Admin By Request from this workstation. See "Uninstalling via PIN Code" on page 21 for more information:



Uninstall

If you have a PIN code to uninstall, you can enter it here.

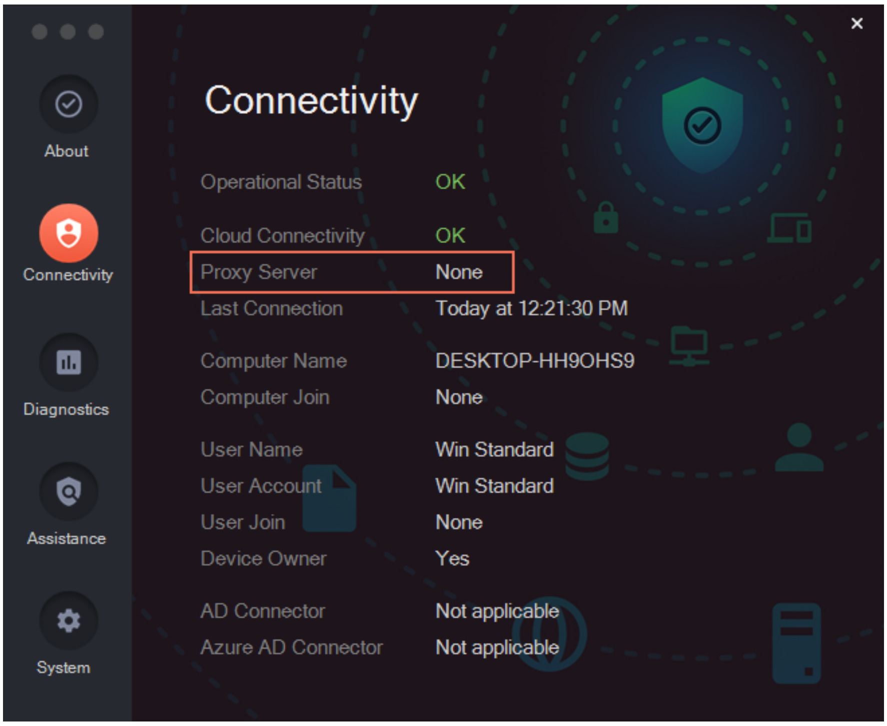
PIN Code

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.

The *Connectivity* panel indicates whether or not a proxy server is used for an endpoint:



Connectivity

Operational Status OK

Cloud Connectivity OK

Proxy Server None

Last Connection Today at 12:21:30 PM

Computer Name DESKTOP-HH9OHS9

Computer Join None

User Name Win Standard

User Account Win Standard

User Join None

Device Owner Yes

AD Connector Not applicable

Azure AD Connector Not applicable

Ports and IP addresses

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

If your data is located in Europe:

- IP: **104.45.17.196**
- DNS: **api1.adminbyrequest.com**

If your data is located in the USA:

- IP: **137.117.73.20**
- DNS: **api2.adminbyrequest.com**

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 the value of *Proxy server* will be **None**.

The application that you see in the system tray (AdminByRequest.exe, which is running in the user space), detects whether or not the current user has a proxy server enabled for the IP addresses that are used for the cloud service.

Refer to How We Handle Your Data for more information.

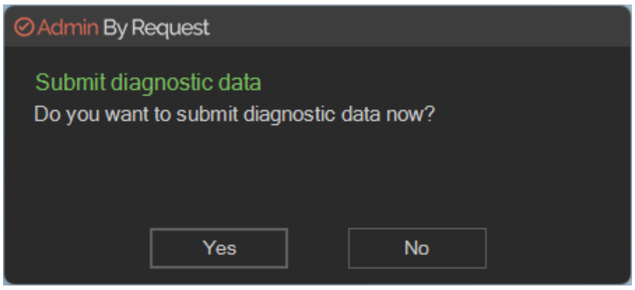
Submitting Diagnostics

Diagnostic information is available on each endpoint that has Admin By Request installed. The details recorded help IT administrators and the Admin By Request support team to troubleshoot issues that might be occurring.

The following data is recorded and submitted:

- Current configuration
- Pending upload queue
- Error events from the event log

To send diagnostic information about how Admin By Request is running on this workstation, select the **Diagnostics** button on the *About Admin By Request* panel and click **Submit**:



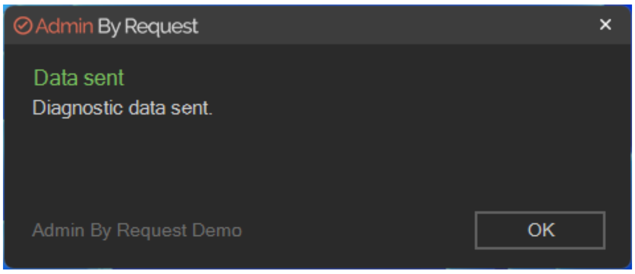
Admin By Request

Submit diagnostic data

Do you want to submit diagnostic data now?

Click **Yes** to confirm. An "in progress" message at the bottom right corner of the screen appears during diagnostics collection

When done, the following message confirms that collection is complete and diagnostics have been submitted:



Admin By Request

Data sent

Diagnostic data sent.

Admin By Request Demo

> **NOTE:**
> It's a good idea to submit diagnostics when raising a support ticket for a new issue. The Admin By Request support team will frequently ask for diagnostics when responding to tickets if the information is not already available.

Requesting Assistance

Assistance (also known as *Support Assist* or *Remote Assist*) is a feature that allows users to ask for help from someone who can connect remotely to the user's computer and provide technical assistance with tasks that the logged-on user would not normally be able to complete.

Support Assist has been designed to be used with a **non-admin user**, so that customers can apply the best practice principle of least privilege also to help desk staff, not just end users.

IMPORTANT:
The feature is not designed to be used with full admin credentials. Rather, it is designed for a **non-admin user**, who is helping the logged-on user and can carry out a task with less restrictive settings than the logged-on user during a remote control session.

Support Assist does not establish a remote control session - a third-party tool must be used for that.

The following scenarios are examples of when this might be useful:

- End users who are not allowed to install software at all (i.e. both *Run As Admin* and *Admin Sessions* are disabled).
- End users who don't know where to get the software they need to use.
- End users who are not IT savvy enough to self-service.
- End users who refuse to take on the responsibility of installing software on their work computer, knowing they will be audited.

Assistance example scenario

An example of the first scenario could be in Customer Relations, where users do not need to install software by default. When the time inevitably arrives that new or upgraded software is required, they have to call your help desk. If the request is accepted, a help desk staff member can assist by connecting remotely and using screen sharing with the end user.

Let's take this scenario and say Customer Relations employee, Peter Bloggs, calls Steve at the help desk to assist with a task for which Peter does not have privileges, but Steve does.

There are several (problematic) ways this could be solved *without* the Support Assist feature, with or without Admin By Request:

1. Steve could have a local administrator account to all computers. However, this is an absolute security no-no and there is no auditing.
2. You could have Microsoft's Local Administrator Password System (LAPS) in place, but this also lacks proper auditing and doesn't work without a LAN or VPN connection.
3. Peter and Steve could agree to use the Admin By Request feature *Run As Admin* and use Peter's credentials, but then Peter gets audited for Steve's changes.
4. Steve could log on and use *Run As Admin*, but then Steve gets audited for Peter's request and furthermore, Peter cannot see Steve executing the request.

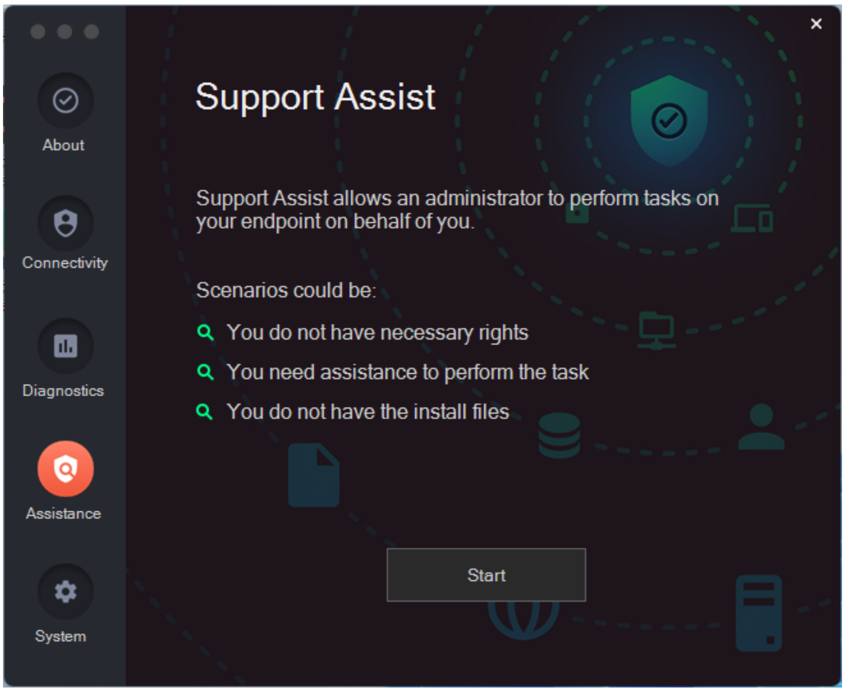
Ideally, Steve should execute the request with Peter watching and auditing should clearly show that Peter requested the change and Steve executed it.

If you have a change management or ticketing system, you would also want a reference to document this change. This is exactly what the Support Assist feature does.

Assistance sequence

1. Peter submits a request for help to the Help Desk.
2. Steve is assigned the task and connects remotely to Peter's computer using a third-party application.

3. Steve starts Admin By Request, selects **Assistance** from the About panel and clicks **Start**:



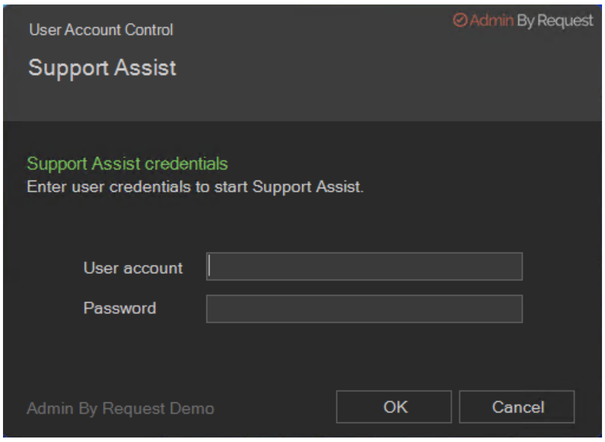
Support Assist

Support Assist allows an administrator to perform tasks on your endpoint on behalf of you.

Scenarios could be:

- You do not have necessary rights
- You need assistance to perform the task
- You do not have the install files

4. At the *UAC Support Assist* window, Steve enters his own **User account** and **Password** credentials:



User Account Control

Support Assist

Support Assist credentials

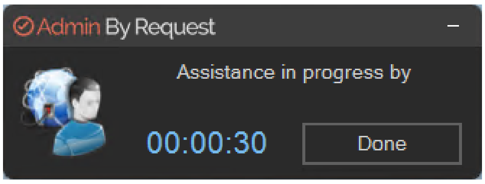
Enter user credentials to start Support Assist.

User account

Password

Admin By Request Demo

5. The session starts, indicated by a progress timer, which displays for the duration of the session:

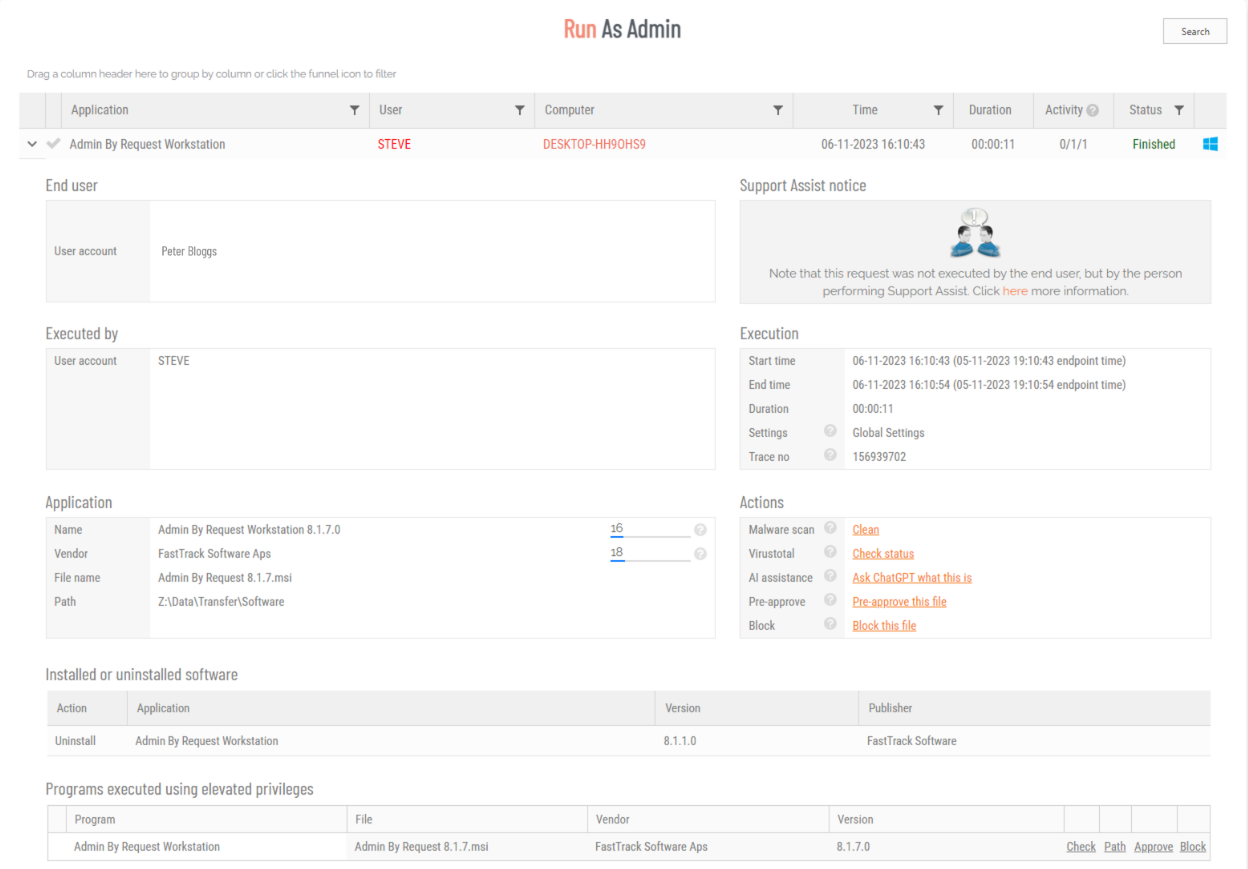


Assistance in progress by

00:00:30

6. When the assist task is complete, Steve clicks **Done**. If he forgets, Peter can click done before the timer counts down, or it will simply expire. Note that Peter cannot use his credentials while Steve is signed-in to Admin By Request.

You can see clearly in the Auditlog that Steve executed Win's change request with the reference **156939702** (field *Trace no* under Execution in the *Run As Admin* screenshot below):



Run As Admin

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

Application	User	Computer	Time	Duration	Activity	Status
Admin By Request Workstation	STEVE	DESKTOP-HH9OHS9	06-11-2023 16:10:43	00:00:11	0/1/1	Finished

End user

User account	Peter Bloggs

Support Assist notice

Note that this request was not executed by the end user, but by the person performing Support Assist. Click here more information.

Executed by

User account	STEVE

Execution

Start time	06-11-2023 16:10:43 (05-11-2023 19:10:43 endpoint time)
End time	06-11-2023 16:10:54 (05-11-2023 19:10:54 endpoint time)
Duration	00:00:11
Settings	Global Settings
Trace no	156939702

Application

Name	Admin By Request Workstation 8.1.7.0	16
Vendor	FastTrack Software Aps	18
File name	Admin By Request 8.1.7.msi	
Path	Z:\Data\Transfer\Software	

Actions

Malware scan	Clean
Virustotal	Check status
AI assistance	Ask ChatGPT what this is
Pre-approve	Pre-approve this file
Block	Block this file

Installed or uninstalled software

Action	Application	Version	Publisher
Uninstall	Admin By Request Workstation	8.1.1.0	FastTrack Software

Programs executed using elevated privileges

Program	File	Vendor	Version				
Admin By Request Workstation	Admin By Request 8.1.7.msi	FastTrack Software Aps	8.1.7.0	Check	Path	Approve	Block

Security checks

Is it risky if a user finds and clicks the *Start* button from the Assistance panel? No - the UAC window at step 4 checks the credentials supplied to see if the person logging-on has the necessary privileges to carry out the task. If they don't, the task is denied and this is logged.

For Help Desk employee Steve, it is essentially the same as logging in to Windows: whatever Admin By Request settings are in effect for Steve are also in effect when he uses Support Assist. For example, if Steve is not allowed to start an Admin Session, he is also not allowed to while using Support Assist.

Think of Support Assist as a shortcut to logging in to Windows and starting Admin By Request. If someone who is not from the Help Desk uses this feature, nothing is achieved as this would be the same as if this user was simply logging in to Windows.

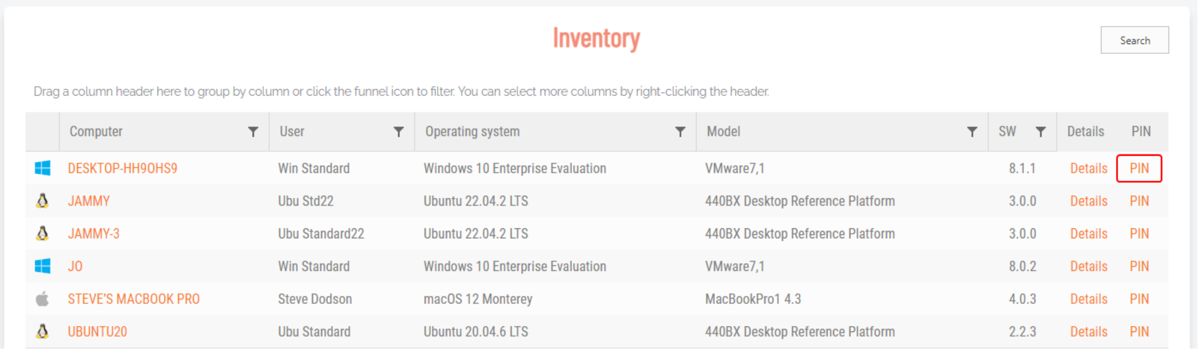
Uninstalling via PIN Code

Offline users can obtain a challenge/response PIN, which allows the user to perform tasks requiring elevated privileges. A PIN Code can also be used to uninstall Admin By Request when online and this is the purpose of the Uninstall panel in the *About Admin By Request* window.

The first few steps in this procedure require access to the portal.

1. In the Admin By Request portal, navigate to the *Inventory* page and identify the device on which to perform the uninstall.

2. Locate the device in the inventory list - in the PIN column, click **PIN** for that device (columns can be switched around - the PIN column in your portal might not be the right-most column):

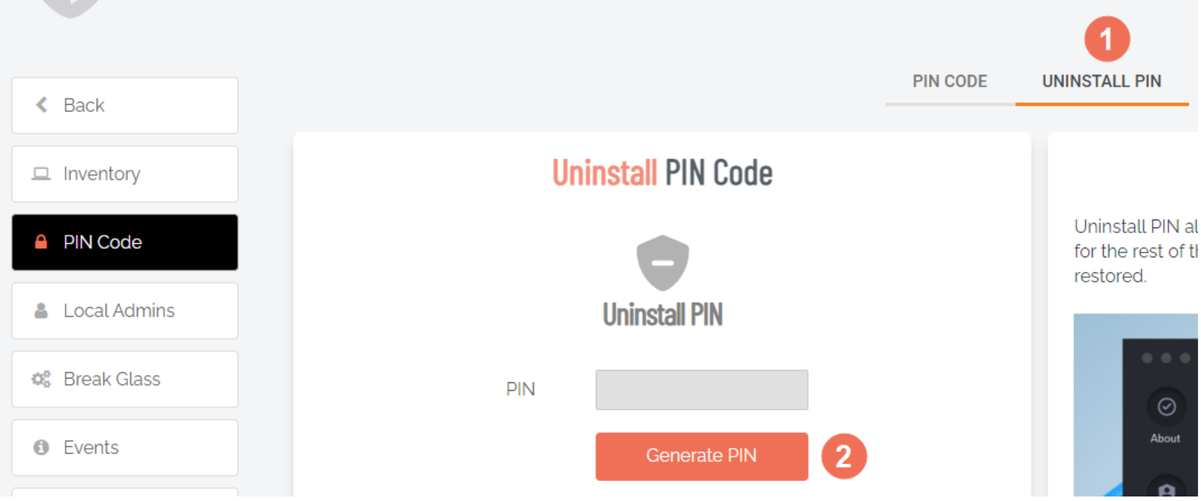


Inventory

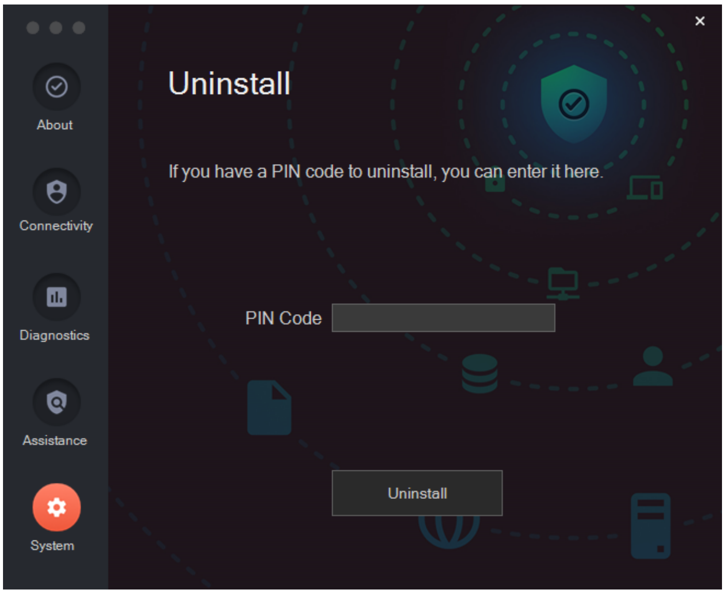
Drag a column header here to group by column or click the funnel icon to filter. You can select more columns by right-clicking the header.

	Computer	User	Operating system	Model	SW	Details	PIN
	DESKTOP-HH9OHS9	Win Standard	Windows 10 Enterprise Evaluation	VMware7,1	8.1.1	Details	PIN
	JAMMY	Ubu Std22	Ubuntu 22.04.2 LTS	440BX Desktop Reference Platform	3.0.0	Details	PIN
	JAMMY-3	Ubu Standard22	Ubuntu 22.04.2 LTS	440BX Desktop Reference Platform	3.0.0	Details	PIN
	JO	Win Standard	Windows 10 Enterprise Evaluation	VMware7,1	8.0.2	Details	PIN
	STEVE'S MACBOOK PRO	Steve Dodson	macOS 12 Monterey	MacBookPro1 4.3	4.0.3	Details	PIN
	UBUNTU20	Ubu Standard	Ubuntu 20.04.6 LTS	440BX Desktop Reference Platform	2.2.3	Details	PIN

3. Click tab **UNINSTALL PIN** and then click button **Generate PIN**:



4. Back on the device on which you want to uninstall Admin By Request, select the *Admin By Request* icon from the system tray and click **About Admin By Request**.
5. Select **System**, enter the Uninstall PIN generated above into the *PIN Code* field and click **Uninstall**:

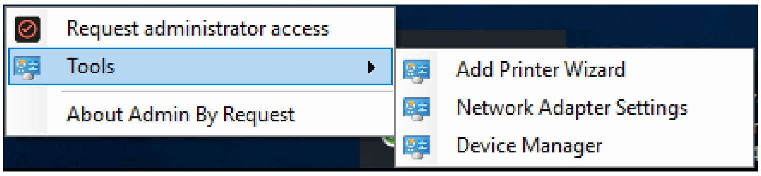


Uninstall

If you have a PIN code to uninstall, you can enter it here.

Using Tray Tools

Tray Tools are items that appear when you click the Admin By Request system tray icon:



The items in the list of tools can be executable programs (or apps), web links with instructions, Control Panel applets or program shortcuts. They are generally tools that perform useful, routine tasks that have been pre-approved and thus do not require requests for administrator access.

> **NOTE:**
>
> - The Tools menu shown in the image is what a Standard User sees - an Administrator has no need of pre-approved access to tools and so the menu is not shown to users logged in as administrators.
> - The IT administration team uses the portal to add or remove items from the Tools list.

Refer to "Tray Tools Settings" on page 35 for information on configuring Tray Tools.

Using Run As Admin

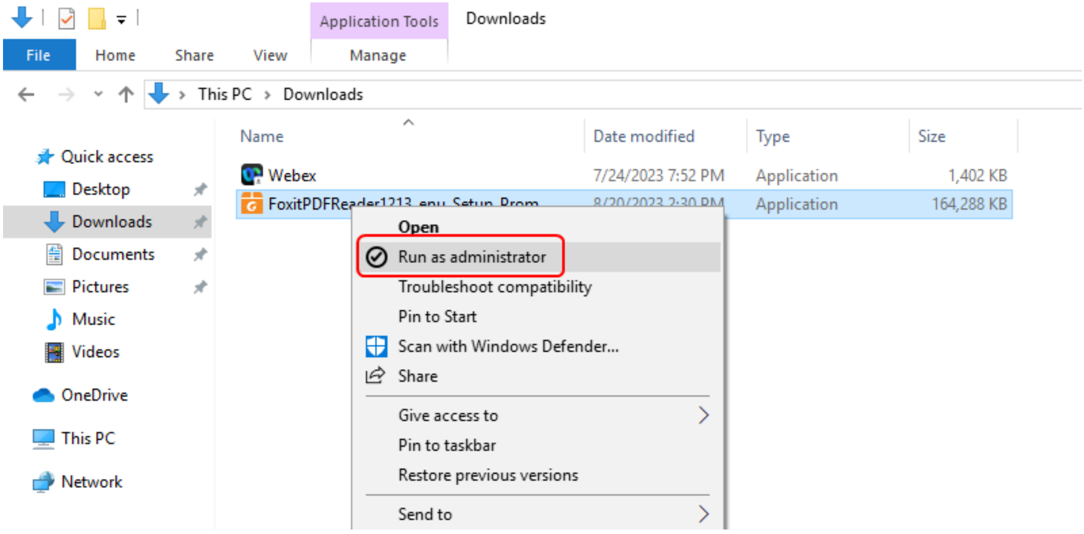
Run As Administrator (also known as *App Elevation)* allows for the elevation of a single application.

This capability negates the need for users to initiate an Administrator Access session (i.e., an extended period of time during which the user has elevated privileges on the device) to simply install one program.

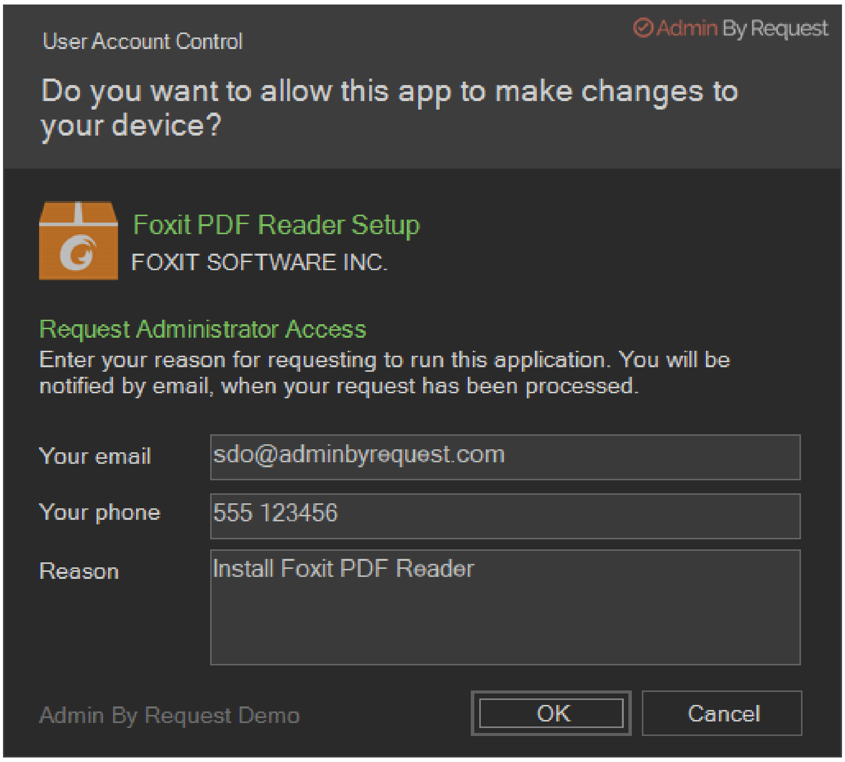
Elevating privileges for execution of a single file is the much safer option compared to elevating the user's privileges across the endpoint.

A standard user executing a program that requires elevated privileges to install initiates the following sequence of events::

1. Download the file for installation.
2. Start the installation by right-clicking and selecting Run as Administrator:



3. Admin By Request suspends installation and asks for phone, email, and reason. Enter these details and click **OK** to continue:



User Account Control

Admin By Request

Do you want to allow this app to make changes to your device?

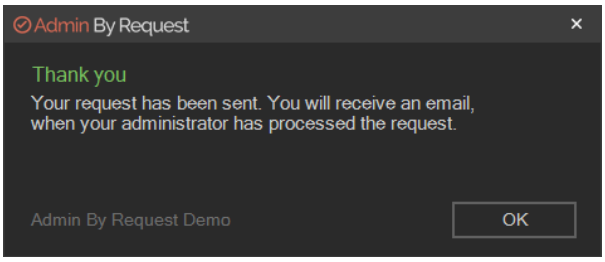
Foxit PDF Reader Setup
FOXIT SOFTWARE INC.

Request Administrator Access

Enter your reason for requesting to run this application. You will be notified by email, when your request has been processed.

Your email	sdo@adminbyrequest.com
Your phone	555 123456
Reason	Install Foxit PDF Reader

4. A notification now advises that the request for approval has been sent:

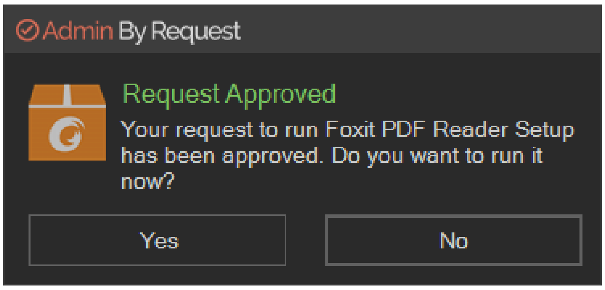


Admin By Request

Thank you

Your request has been sent. You will receive an email, when your administrator has processed the request.

5. When the request is approved, a further notification advises the request has been approved:



Admin By Request

Request Approved

Your request to run Foxit PDF Reader Setup has been approved. Do you want to run it now?

6. Now the installer has the elevated privileges required to run - click **Yes** to start authorized installation with elevated privileges.

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

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

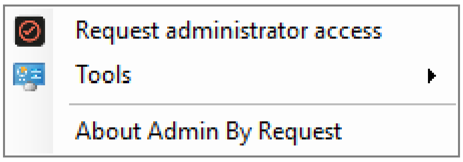
Refer to "Run As Admin Settings" on page 33 for information on configuring Run As Admin.

Requesting Administrator Access

Administrator Access (also known as *Session Elevation)* allows for elevated privileges system-wide for a predefined amount of time (session duration).

Any user given full session elevation gets full local admin rights on their system. Full session elevation mode is ideal for situations such as when elevated access to 'system' resources such as drivers or printers etc. is required, when a user needs elevation only for a specific amount of time, or when a Developer requires the use of multiple elevated applications.

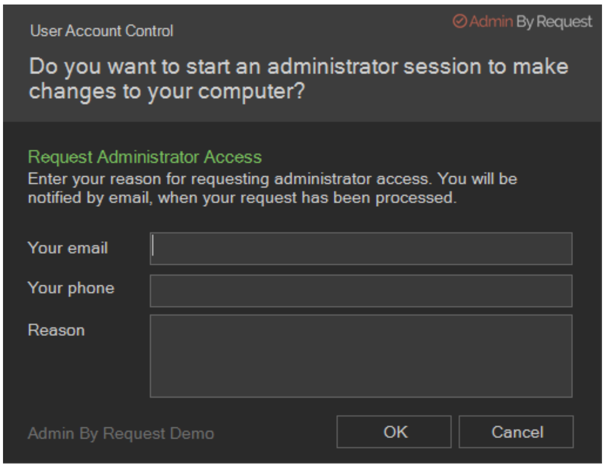
As with *About Admin By Request*, users can double-click the Admin By Request desktop icon, or select the icon from tray tools to display the menu and select **Request administrator access**:



Submitting a request for Administrator access is the primary mechanism for gaining elevated privileges.

A standard user making this selection initiates the following sequence of events.

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



User Account Control

Admin By Request

Do you want to start an administrator session to make changes to your computer?

Request Administrator Access

Enter your reason for requesting administrator access. You will be notified by email, when your request has been processed.

Your email

Your phone

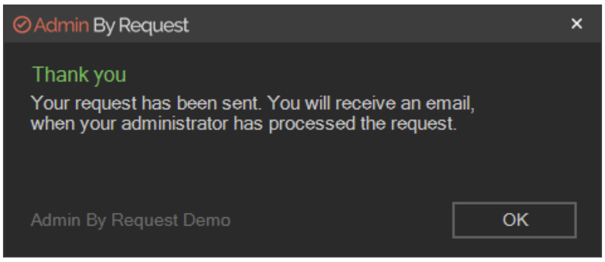
Reason

Admin By Request Demo

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 (**Portal > Settings > Workstation Settings > Windows Settings > Endpoint > INSTRUCTIONS**).
> - If *Require approval* is OFF, the approval steps are skipped (**Portal > Settings > Workstation Settings > Windows Settings > Authorization > AUTHORIZATION > Admin Session**).

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

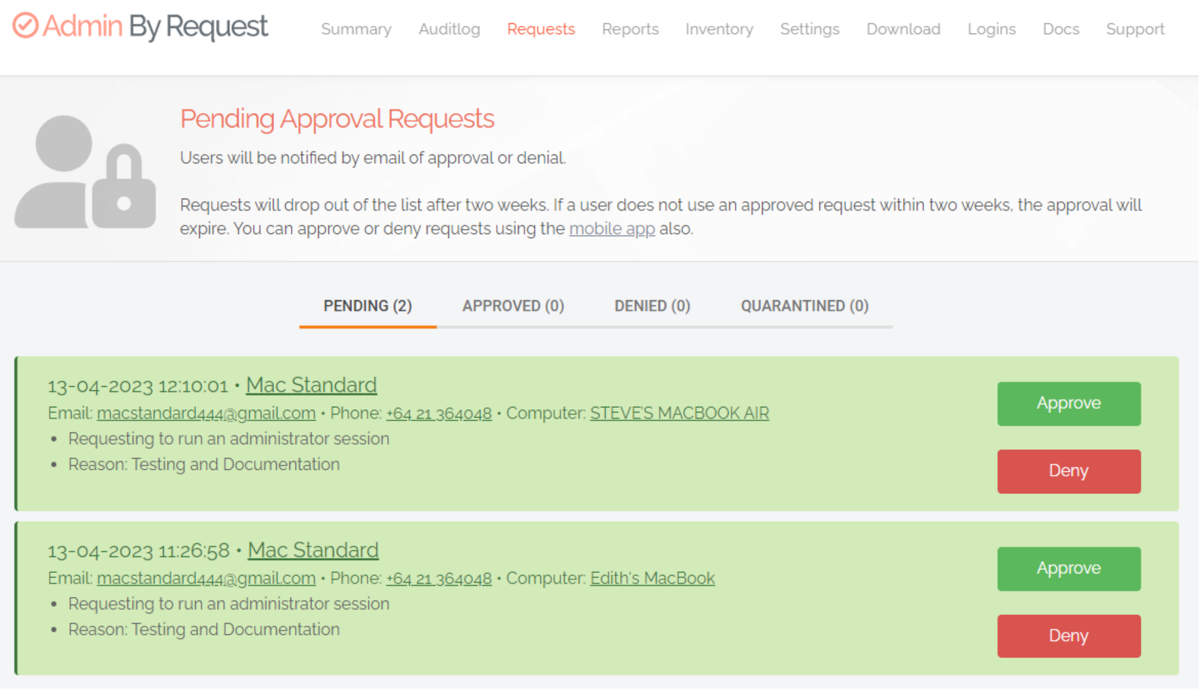


Thank you

Your request has been sent. You will receive an email, when your administrator has processed the request.

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:



Pending Approval Requests

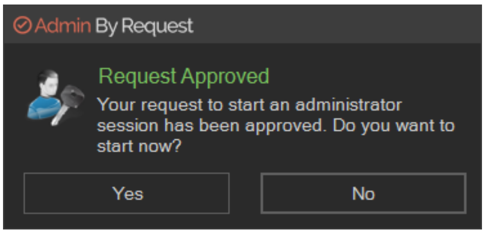
Users will be notified by email of approval or denial.

Requests will drop out of the list after two weeks. If a user does not use an approved request within two weeks, the approval will expire. You can approve or deny requests using the mobile app also.

13-04-2023 12:10:01 • Mac Standard
Email: macstandard444@gmail.com • Phone: +64 21 364048 • Computer: STEVE'S MACBOOK AIR
- Requesting to run an administrator session
- Reason: Testing and Documentation

13-04-2023 11:26:58 • Mac Standard
Email: macstandard444@gmail.com • Phone: +64 21 364048 • Computer: Edith's MacBook
- Requesting to run an administrator session
- Reason: Testing and Documentation

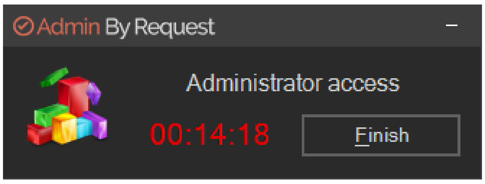
5. One of the team either approves or denies the request. If approved, the user is advised accordingly:



Request Approved

Your request to start an administrator session has been approved. Do you want to start now?

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 (15 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**.

See "Changing Admin Session Duration" on page 34 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.

Refer to "Admin Session Settings" on page 34 for information on configuring Admin Sessions.

Setting-up a Break Glass Account

The Break Glass feature extends the functionality of MS LAPS. It creates a new, temporary, one-time-use Administrator account on an endpoint, that works on domains, Azure AD, and stand-alone, which audits all elevated activity, and terminates within a pre-defined amount of time or on log out.

Security benefits

The Break Glass feature includes the following security benefits:

- Break Glass **circumvents the need to use the built-in Windows local Administrator account** – you can disable it completely to add an extra later 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 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?

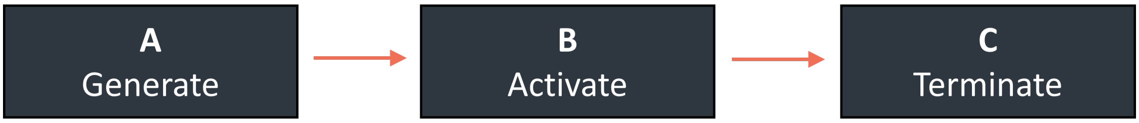
A Break Glass account is useful in the following scenarios:

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.
3. **Extra Possibilities with Server Edition**
   Further to point 2, with Admin By Request Windows Server Edition you can provision an admin account to a consultant without giving them domain-wide permissions at any point in time.

Using the Break Glass feature

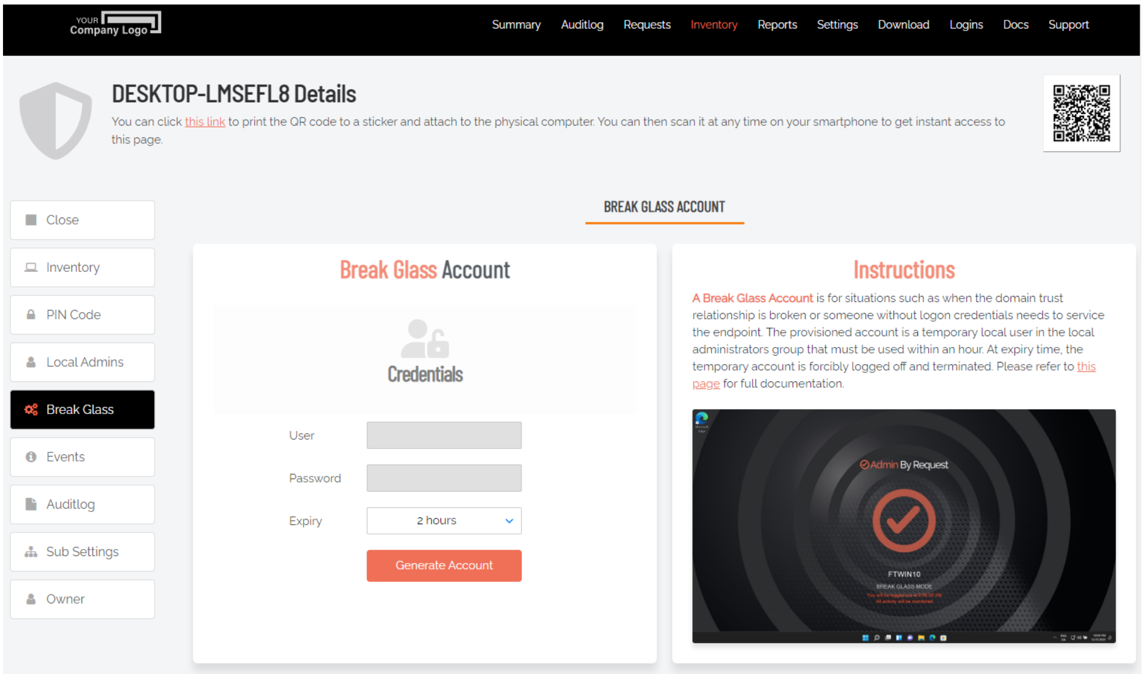
Setting-up and using a Break Glass account comprises three tasks:



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:



DESKTOP-LMSEFL8 Details

You can click this link to print the QR code to a sticker and attach to the physical computer. You can then scan it at any time on your smartphone to get instant access to this page.

Break Glass Account

User

Password

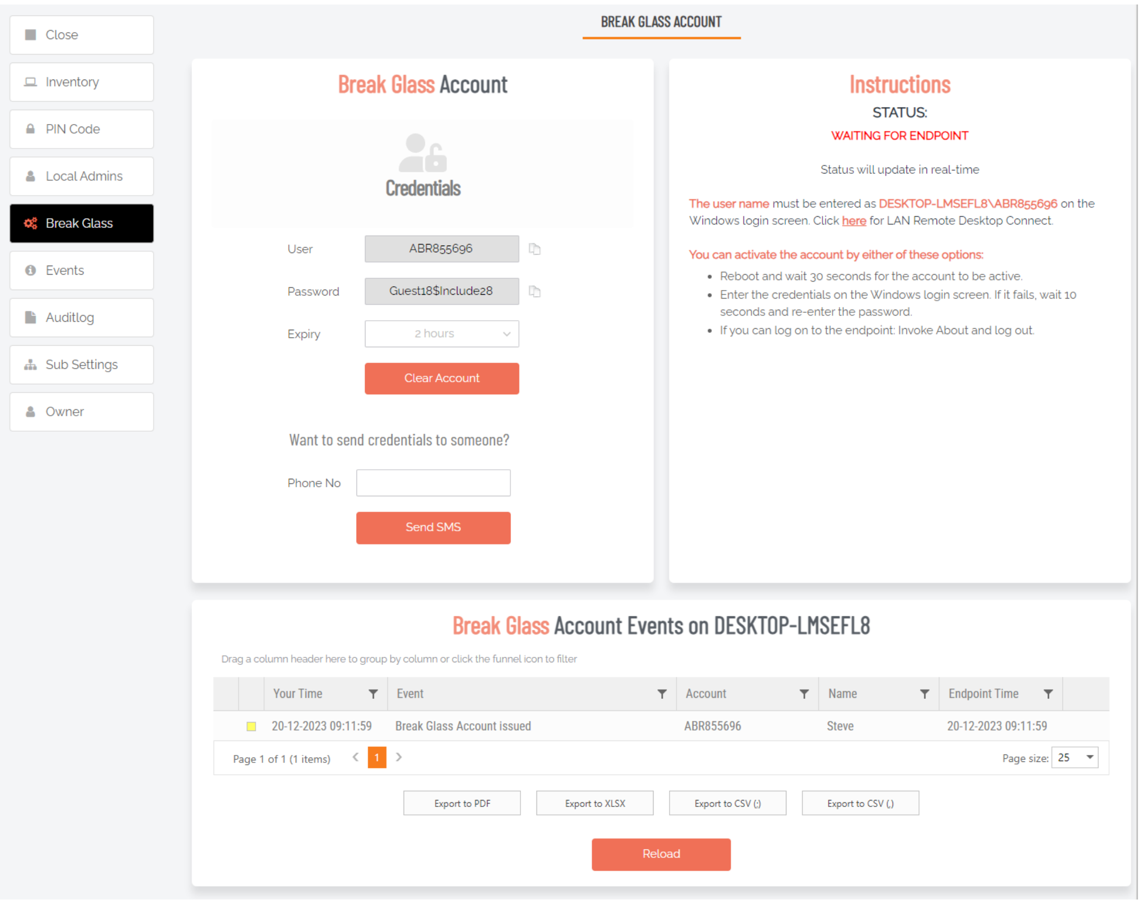
Expiry: 2 hours

Instructions

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 an hour. At expiry time, the temporary account is forcibly logged off and terminated. Please refer to this page for full documentation.

2. From the **Expiry** drop-down menu, select an amount of time for which you want the Account to be available. 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:



Break Glass Account

User ABR855696

Password Guest18$Include28

Expiry 2 hours

Want to send credentials to someone?

Phone No

Instructions

STATUS:

WAITING FOR ENDPOINT

Status will update in real-time

The user name must be entered as DESKTOP-LMSEFL8\ABR855696 on the Windows login screen. Click here for LAN Remote Desktop Connect.

You can activate the account by either of these options:

- Reboot and wait 30 seconds for the account to be active.
- Enter the credentials on the Windows login screen. If it fails, wait 10 seconds and re-enter the password.
- If you can log on to the endpoint: Invoke About and log out.

Break Glass Account Events on DESKTOP-LMSEFL8

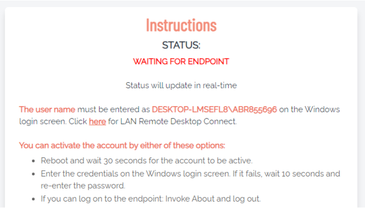
Drag a column header here to group by column or click the funnel icon to filter

	Your Time	Event	Account	Name	Endpoint Time
🟨	20-12-2023 09:11:59	Break Glass Account issued	ABR855696	Steve	20-12-2023 09:11:59

Page 1 of 1 (1 items) 1 Page size: 25

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.



Instructions

STATUS:

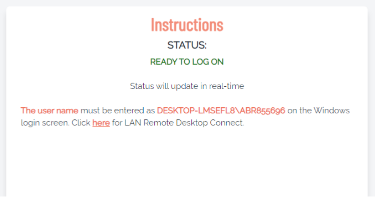
WAITING FOR ENDPOINT

Status will update in real-time

The user name must be entered as DESKTOP-LMSEFL8\ABR855696 on the Windows login screen. Click here for LAN Remote Desktop Connect.

You can activate the account by either of these options:

- Reboot and wait 30 seconds for the account to be active.
- Enter the credentials on the Windows login screen. If it fails, wait 10 seconds and re-enter the password.
- If you can log on to the endpoint: Invoke About and log out.



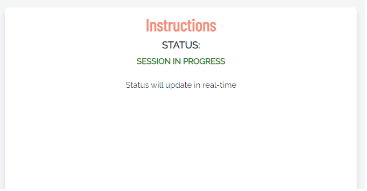
Instructions

STATUS:

READY TO LOG ON

Status will update in real-time

The user name must be entered as DESKTOP-LMSEFL8\ABR855696 on the Windows login screen. Click here for LAN Remote Desktop Connect.

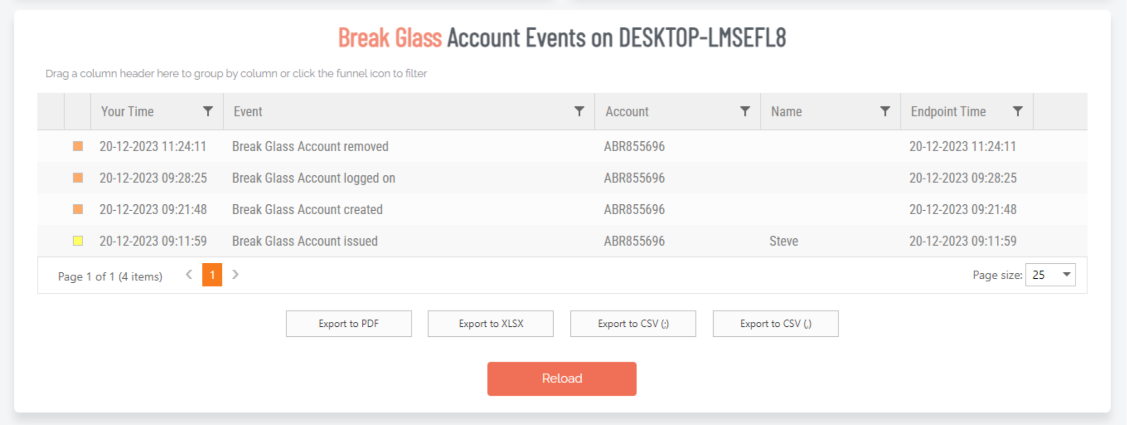


Instructions

STATUS:

SESSION IN PROGRESS

Status will update in real-time



Break Glass Account Events on DESKTOP-LMSEFL8

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

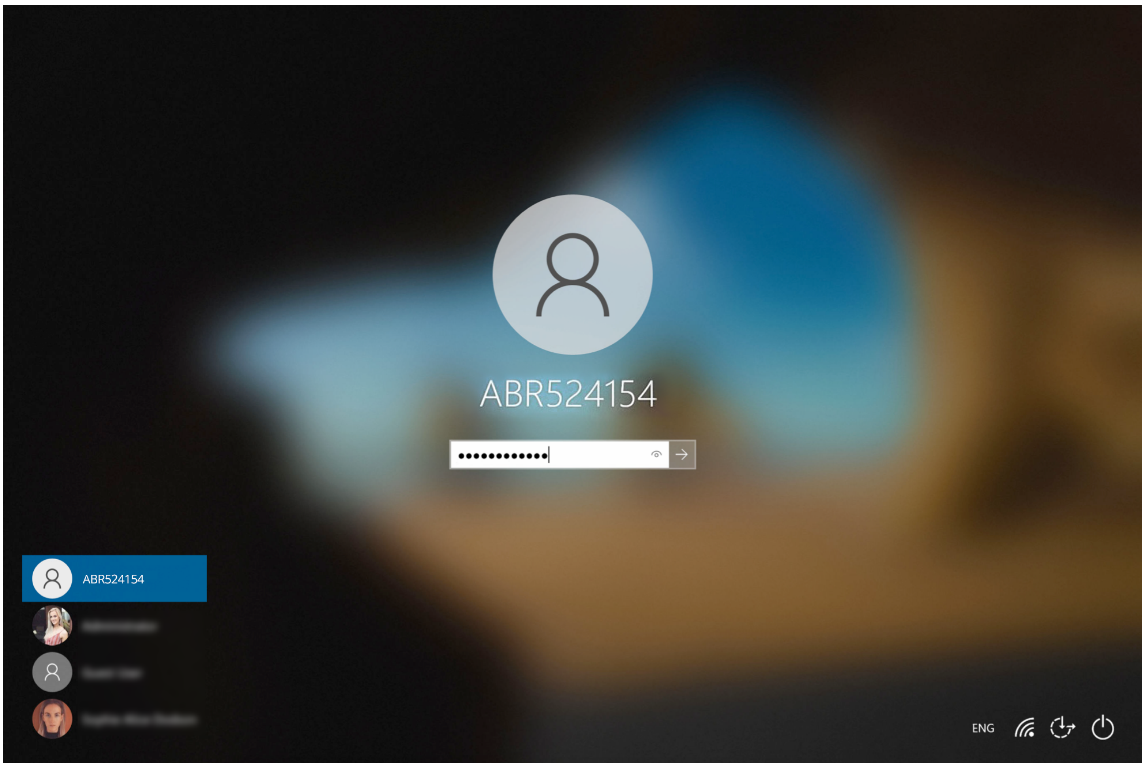
	Your Time	Event	Account	Name	Endpoint Time
🟧	20-12-2023 11:24:11	Break Glass Account removed	ABR855696		20-12-2023 11:24:11
🟧	20-12-2023 09:28:25	Break Glass Account logged on	ABR855696		20-12-2023 09:28:25
🟧	20-12-2023 09:21:48	Break Glass Account created	ABR855696		20-12-2023 09:21:48
🟨	20-12-2023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

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, and the account will appear in the bottom-left of the Windows log on screen along with the other accounts available on the endpoint:



b. If enabled, you can select **Other User** in the Windows log in screen and enter the generated Break Glass account *User* and *Password* into the fields. Remember to prefix the User credential with the device name (e.g. DESKTOP-LMSEFL8\ABR524154).

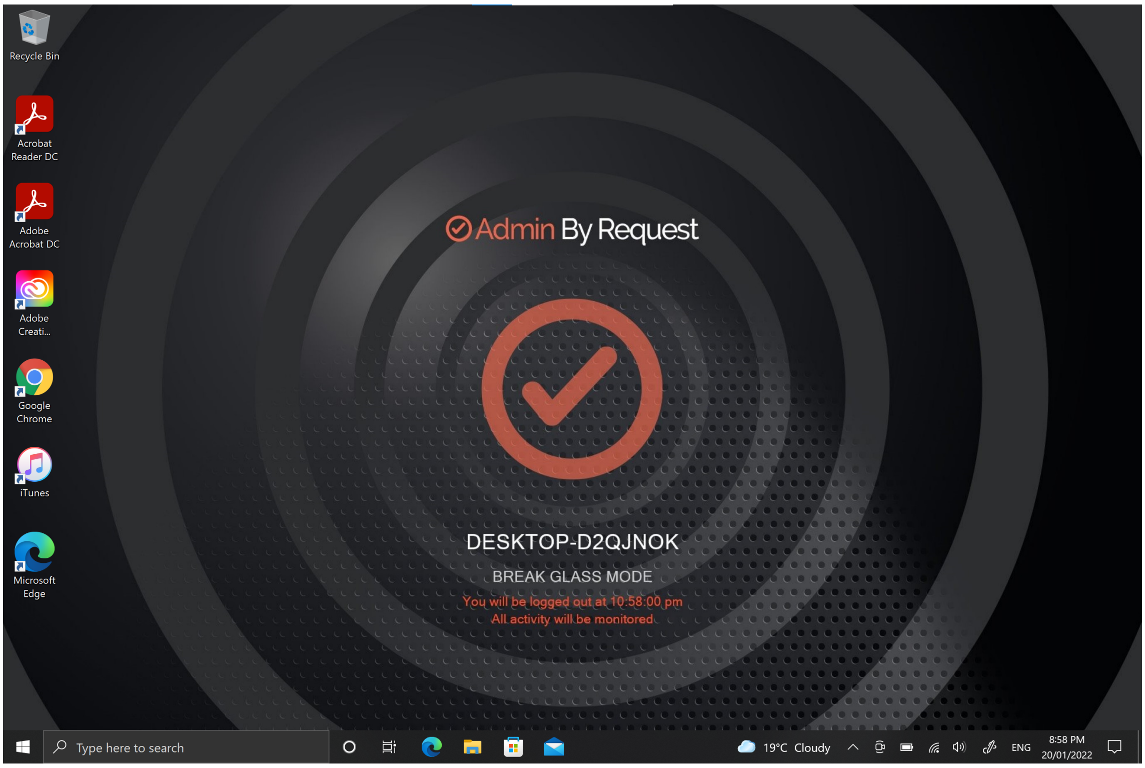
> **NOTE:**
> This may fail on the first attempt; if so, wait 10 seconds and then try again.

c. A third method to activate the account is by logging in to another account on the endpoint, selecting the Admin By Request icon from the bottom 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 on the built-in screensaver:



Admin By Request

DESKTOP-D2QJNOK

BREAK GLASS MODE

You will be logged out at 10:58:00 pm

All activity will be monitored

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.

Refer to Features > Break Glass / LAPS for more information on the feature.

Portal Administration for Windows

Introduction

This topic describes several key areas of the Admin Portal that can be used to manage *Windows Settings* and *Windows Sub Settings*. Fields that can be set and/or 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

Menu selection: **Settings > Workstation Settings > Windows 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 file that triggers User Account Control (UAC). The user is able to run the program sandboxed, without being local administrator. Only the process (not the user) has administrator rights. When enabled, the Explorer right-click icon is replaced by an Admin By Request icon.

Setting	Type	Description
Allow Run As Admin	Toggle On | Off Default: **On**	**On** - Allows users to elevate privileges for a selected file. Enables *Require approval* and *Require reason*. Disables *Block Run As Admin*. **Off** - Denies users the ability to elevate privileges for a selected file. Enables *Block Run As Admin*, which is how users with admin credentials can still elevate privileges.
Block Run As Admin (enabled only if *Allow Run As Admin* is Off)	Toggle On | Off Default: **Off**	**On** - Denies users the ability to execute *Run As Admin* even if administrator credentials are available (i.e. no UAC window is presented). **Off** - Allows users with administrator credentials to execute *Run As Admin* (i.e. UAC window pops-up asking for admin credentials).
Require approval	Toggle On | Off Default: **Off**	**On** - Sends a request to the IT team, which must be approved before elevation is granted. Makes *Require reason* mandatory (i.e. must be On). **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 *Require reason* optional (i.e. can be either On or Off).
Require reason	Toggle On | Off Default: **Off**	**On** - Extends the UAC window and asks the user to enter email address, phone number and reason. Reason must comprise at least *two words*. This information is stored in the Auditlog. **Off** - No reason is required by the user, but details of the actions performed are stored in the Auditlog.
Save	Button	Saves customization and changes to any fields. Note that reloading any defaults does not take effect until **Save** is clicked.

Admin Session Settings

Menu selection: **Settings > Workstation Settings > Windows 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 tray or desktop icon to request a protected administrator session, which makes the user a temporary member of the local administrator's group for a limited period of time under full audit.

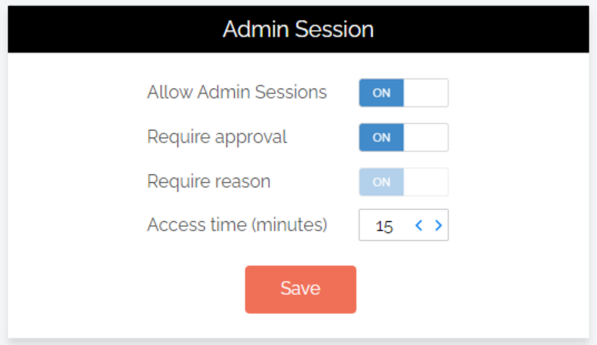
Setting	Type	Description
Allow Admin Sessions	Toggle On | Off Default: **On**	**On** - Allows users to effectively become a local administrator for the number of minutes specified in *Access time (minutes)*. Enables *Require approval*, *Require reason* and *Access time (minutes)*. **Off** - Denies users the ability to become a local administrator. Hides all other options under Admin Session.
Require approval	Toggle On | Off Default: **Off**	**On** - Sends a request to the IT team, which must be approved before the request is granted. Makes *Require reason* mandatory (i.e. must be On). **Off** - Allows the user to become a local administrator as soon as the request is made. Makes *Require reason* optional (i.e. can be either On or Off).
Require reason	Toggle On | Off Default: **Off**	**On** - Extends the UAC window and asks the user to enter email address, phone number and reason. This information is stored in the Auditlog. **Off** - No further information is required by the user, but user and computer details are stored in the Auditlog.
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 > Windows 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:



Admin Session

Allow Admin Sessions: ON
Require approval: ON
Require reason: ON
Access time (minutes): 15

3. Click **Save** when done.

Admin Rights Setting

Menu selection: **Settings > Workstation Settings > Windows 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: **Off**	**On** - Admin privileges are removed for all users except those appearing in the *Excluded accounts* list.. **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.

Tray Tools Settings

Menu selection: **Settings > Workstation Settings > Windows Settings > App Control > TRAY TOOLS**

Settings Table - Tray Tools

Tray Tools are items that appear when users click the Admin By Request system tray icon. As well as executable files, these tools could be web links with instructions, Control Panel applets or program shortcuts.

Minimum requirements

Tray Tools require Admin By Request version 7.1 or newer. Control Panel tools require Windows 10 version 2004 (build 19041) or newer.

New Tray Tool

Click button **New Tray Tool** to create a new entry in the tray tools menu.

Setting	Type	Description
Application	Text	The caption used for the system tray menu item. Enter the text to be used for the name or caption. Does not have to match the executable *File* name. Note that any webhooks you have created appear in a selection list when you click this field. The list is for convenience only and simply "pastes" the webhook caption into the field - no other fields are populated.
File	Text	The name of the executable file, including it's full path. You can also specify a web address (i.e. URL) in this field, in which case the *Run As Admin* toggle should be **Off** for security reasons.
Parameters	Text	Text values entered here are appended to the *File* as parameters during execution.
Run As Admin	Toggle On | Off Default: **On**	**On** - Allows the executable file named in *File* to be Run As Admin (i.e. run as an administrator). **Off** - Does not allow the executable file named in *File* to be Run As Admin. This should be the option selected if the entry in *File* is a web address.
Menu Separator	Toggle On | Off Default: **Off**	**On** - Inserts a line above this menu item. Allows tray tool menu items to be grouped. **Off** - No line is inserted.
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 Windows Workstation Global Settings page.

Quick add list

The *Quick add list* is a preset list of common Control Panel applets. It is a selection list, accessed by clicking the drop-down arrow at the right of the field. You can add other Control Panel applets by creating a tool that runs control.exe followed by a .cpl file.

> **NOTE:**
> If all entries in the *Quick add list* have already been added as tray tools, the *Quick add list* field does not appear at all.

Pre-Approval Settings

Menu selection: **Settings > Workstation Settings > Windows Settings > App Control > PRE-APPROVE**

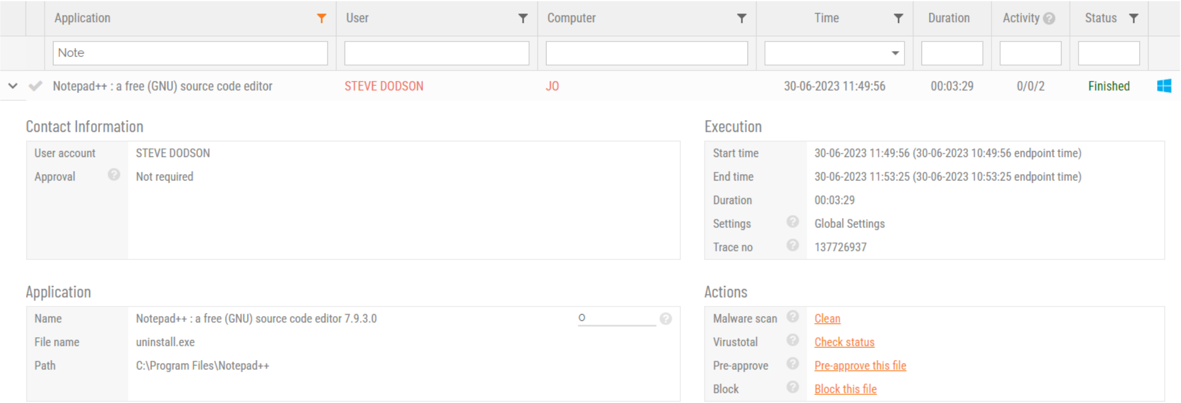
Pre-Approval (known sometimes as Whitelisting) refers to the method of working out which applications are trusted and frequently used, and adding them to a list that automatically allows users to elevate those applications when they need to. This is essentially the opposite of Blocklisting/Blacklisting – 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).

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:



Application	User	Computer	Time	Duration	Activity	Status
Note						
Notepad++ : a free (GNU) source code editor	STEVE DODSON	JO	30-06-2023 11:49:56	00:03:29	0/0/2	Finished

Contact Information

User account	STEVE DODSON
Approval	Not required

Execution

Start time	30-06-2023 11:49:56 (30-06-2023 10:49:56 endpoint time)
End time	30-06-2023 11:53:25 (30-06-2023 10:53:25 endpoint time)
Duration	00:03:29
Settings	Global Settings
Trace no	137726937

Application

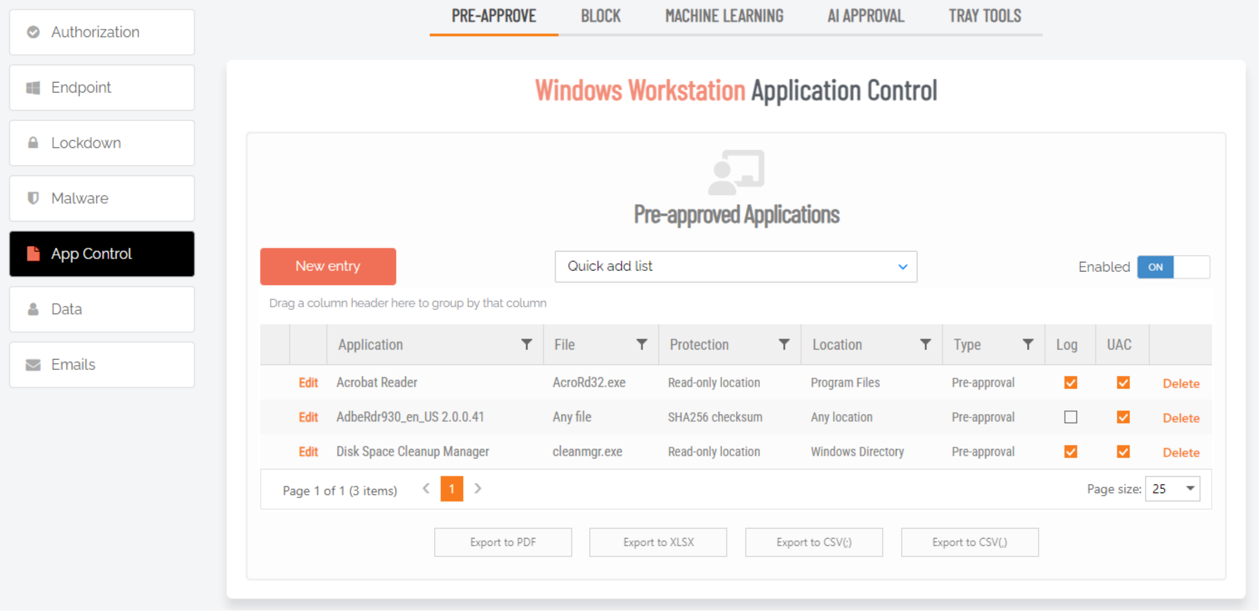
Name	Notepad++ : a free (GNU) source code editor 7.9.3.0
File name	uninstall.exe
Path	C:\Program Files\Notepad++

Actions

Malware scan	Clean
Virustotal	Check status
Pre-approve	Pre-approve this file
Block	Block this file

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:



Windows Workstation Application Control

Pre-approved Applications

Enabled ON

Drag a column header here to group by that column

		Application	File	Protection	Location	Type	Log	UAC	
	Edit	Acrobat Reader	AcroRd32.exe	Read-only location	Program Files	Pre-approval	☑	☑	Delete
	Edit	AdbeRdr930_en_US 2.0.0.41	Any file	SHA256 checksum	Any location	Pre-approval	□	☑	Delete
	Edit	Disk Space Cleanup Manager	cleanmgr.exe	Read-only location	Windows Directory	Pre-approval	☑	☑	Delete

Page 1 of 1 (3 items) 1 Page size: 25

Settings Table - Pre-Approve

Pre-approved applications are EXE, MSI, MSC or CPL files that are pre-approved to run with elevated privileges (i.e. **Run as administrator**) 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-aproval list, the difference is:

- The application is auto-approved; the approval flow is bypassed
- A reason is not required, as the application is known to be good
- You have the option to not log to the Auditlog (trivial data)
- If *Run As Admin* is disabled, a pre-approved application will still run
- A pre-approved application will overrule *Deny elevating system files*
- You can force applications to always run elevated (legacy applications)

New entry

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

Setting	Type	Description
Log to auditlog (hidden if *User confirmation* is Off)	Toggle On | Off Default: **Off**	**On** - .Relevant details about the application are logged. **Off** - No logging is performed for this application.
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 UAC window. **Off** - The user does not need to confirm elevation on the endpoint before execution. Hides the *Log to auditlog* field.

Setting	Type	Description
Type	Selection Default: **Run As Admin application pre-approval**	**Run As Admin application pre-approval** - Pre-approve this application for Run As Admin. **Run As Admin vendor pre-approval (digital certificate)** - Pre-approve all applications based on the specified *Vendor* digital certificate. Selecting this option enables the *Vendor* field and hides all other fields. **Run As Admin location pre-approval (all files in folder tree)** - Pre-approve all applications in the specified folder, including any sub-folders. Selecting this option enables the *Directory* field and hides all other fields. **Force running application elevated (legacy application)** - .Pre-approve this application to run elevated regardless of any other conditions.
Vendor (enabled when *Run As Admin vendor pre-approval (digital certificate)* is selected)	Read-only selection (via Button)	Use the **Browse** button to select a valid Vendor certificate file.
Protection	Selection Default: **File must be located in read-only directory**	Prevent users from bypassing pre-approval by file renaming. **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. **File must match digital certificate** - Vendor digital certificate of a file. Recommended if you have a copy of the file. **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. **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.
File location	Selection Default: **Program Files or subfolder**	**Program Files or subfolder** - The Program Files folder, typically either *C:\Program Files* or *C:\Program Files (x86)*.

Setting	Type	Description
		Windows directory or subfolder - The Windows system folder, typically *C:\Windows\System32*. **Custom read-only location** - Shows an additional field labeled *Directory* if selected.
Directory (enabled when other selections are in effect): • *Run As Admin location pre-approval (all files in folder tree)* • *Custom read-only location*	Text	A read-only location where the application to be added is stored. Can include the following environment variables: • %PROGRAMFILES% • %WINDIR% • %USERPROFILE% • %APPDATA% If the directory entered is not on the local machine, a UNC path can be used. The endpoint software will automatically translate drive letters to UNC path.
Application name	Text	The name of the application. Mandatory, although used for convenience only to help identify applications in the list.
File name	Selection (via Browse Button)	Use the **Browse** button to open an operating system *File open* dialog box. Locate and select a file with one of the following extensions: • exe • msi • msc • cpl
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 Windows Workstation Global Settings page.

Quick add list

The *Quick add list* is a preset list of common applications. It is a selection list, accessed by clicking the drop-down arrow at the right of the field.

> **NOTE:**
> If all entries in the *Quick add list* have already been added and are visible in the list of applications, the *Quick add list* field does not appear at all.

Enabled toggle

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

Machine Learning

The idea behind Machine Learning Auto-Approval is to kill two birds with one stone by allowing customers to build a Pre-Approved list as their employees use the software. This removes the need for enterprises to spend considerable amounts of time and effort figuring out and manually configuring which applications should be pre-approved ahead of time.

The way it works is, it allows you to create a simple rule that says:

"If approval for elevation of an application is granted X times, that application is now automatically approved for incoming requests from then on."

This allows the system to handle creating the list of applications that are safe for approval as applications are used.

For more information, including step-by-step procedures, refer to Features > Machine Learning.

Privacy Settings

Menu selection: **Settings > Workstation Settings > Windows 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 is a 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.
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	**On** - Record phone numbers associated with a user. **Off** - Do not record phone numbers.

Setting	Type	Description
	Default: **On**	
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

Menu selection: **Settings > Tenant Settings > Groups**

Settings Table - Entra ID

The *Entra ID Connector* allows endpoints to retrieve Entra ID (previously Azure AD) groups for sub-settings.

> **NOTE:**
> If you are using on-premise 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 sub-setting groups. Example values:

Tenant	**acme.onmicrosoft.com**
Application ID	**xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx**
Secret Key	**azVqedkQlVX9bHLBZjGCQZ6+iZIh4goI7u53i9WlZN8=**

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. **Off** - The Entra ID Connector is disabled and endpoints will use sub-settings as described under "Sub-Settings", rather than using Entra ID rules.

Setting	Type	Description
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: • **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. Unhides *National Service*, which is where the actual geographic instance is selected. **Off** - Disables selection of a physically isolated instance of Azure.
National Service (hidden if *National Cloud* is Off)	Selection Default: **US Government L4 / GCC High**	The geographic instance selected: • **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.

Entra ID SSO (Single Sign On)

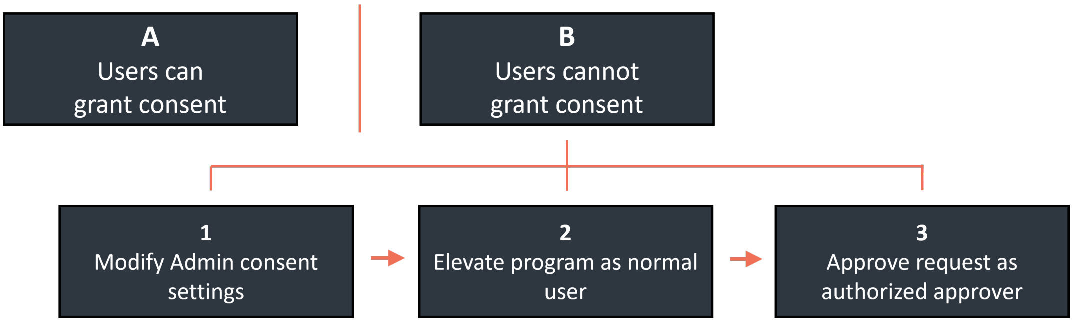
There are two methods that can be used to setup Admin By Request SSO in Entra ID, depending on whether or not users are allowed to grant consent to applications that might request access to data:

A. Users are permitted to grant consent
B. Users are not permitted to grant consent

Further, for the more complex case B, there are three tasks that must be done:

1. Modify Admin consent settings
2. Elevate program as normal user
3. Approve request as authorized approver

These methods and tasks are illustrated in the following chart (this chart reads as "Either A or B. If B, then do all three tasks in order"):



A
Users can grant consent

B
Users cannot grant consent

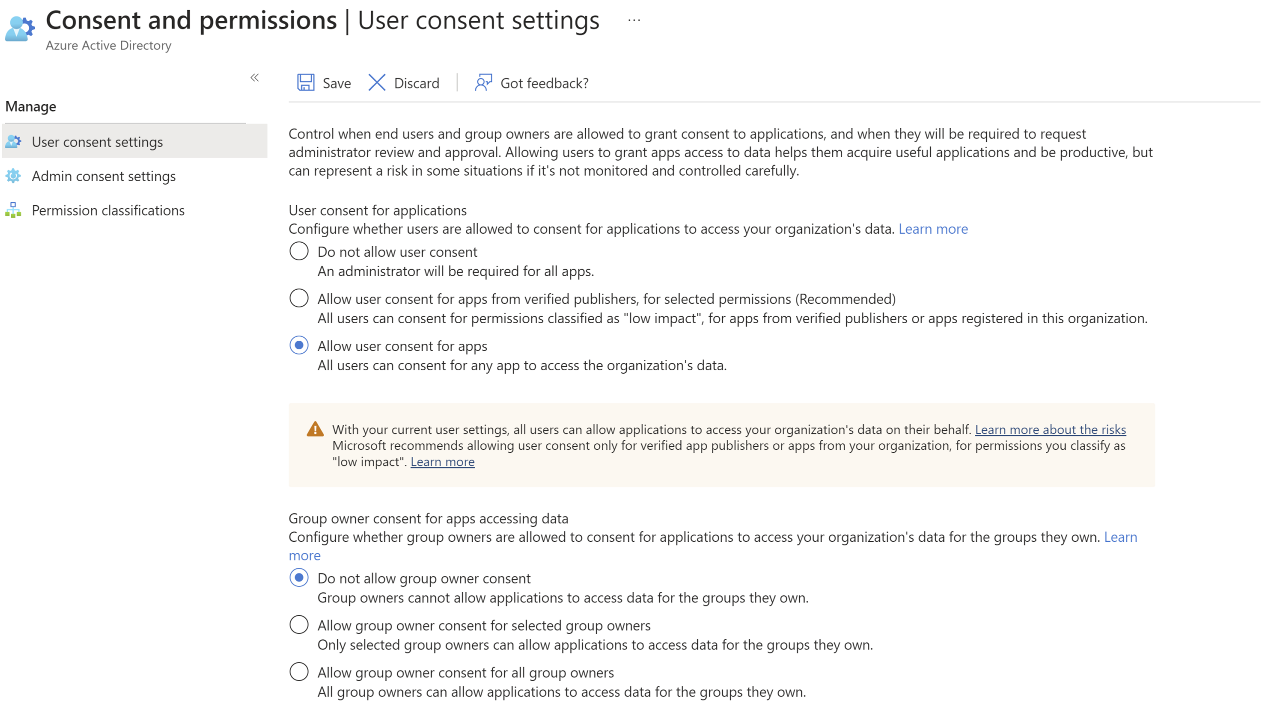
1
Modify Admin consent settings

2
Elevate program as normal user

3
Approve request as authorized approver

A. Users are permitted to grant consent

The first method requires that a user be allowed to grant consent to apps in Azure AD, as indicated in the screenshot below.



Consent and permissions | User consent settings ...
Azure Active Directory

Control when end users and group owners are allowed to grant consent to applications, and when they will be required to request administrator review and approval. Allowing users to grant apps access to data helps them acquire useful applications and be productive, but can represent a risk in some situations if it's not monitored and controlled carefully.

User consent for applications
Configure whether users are allowed to consent for applications to access your organization's data. Learn more

○ Do not allow user consent
An administrator will be required for all apps.

○ Allow user consent for apps from verified publishers, for selected permissions (Recommended)
All users can consent for permissions classified as "low impact", for apps from verified publishers or apps registered in this organization.

● Allow user consent for apps
All users can consent for any app to access the organization's data.

⚠ With your current user settings, all users can allow applications to access your organization's data on their behalf. Learn more about the risks
Microsoft recommends allowing user consent only for verified app publishers or apps from your organization, for permissions you classify as "low impact". Learn more

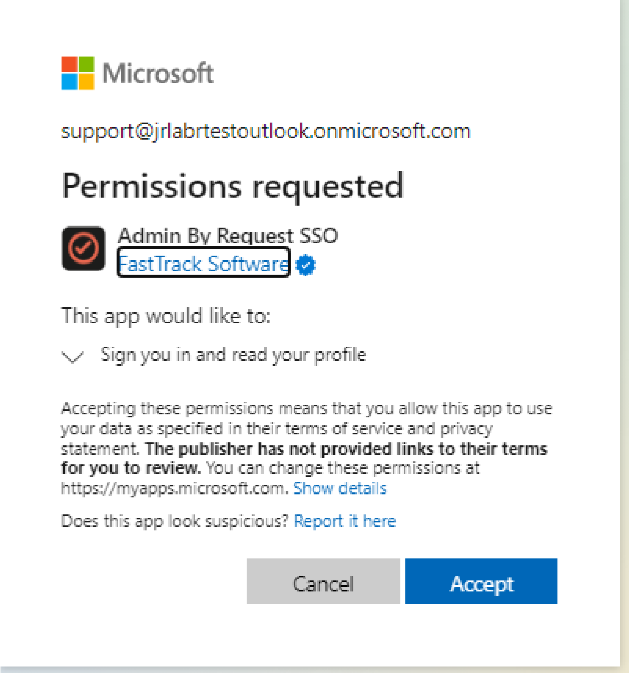
Group owner consent for apps accessing data
Configure whether group owners are allowed to consent for applications to access your organization's data for the groups they own. Learn more

● Do not allow group owner consent
Group owners cannot allow applications to access data for the groups they own.

○ Allow group owner consent for selected group owners
Only selected group owners can allow applications to access data for the groups they own.

○ Allow group owner consent for all group owners
All group owners can allow applications to access data for the groups they own.

The **first time** Admin By Request requires SSO from an endpoint, a Microsoft *Permissions requested* dialog appears:



support@jrlabrtestoutlook.onmicrosoft.com

Permissions requested

Admin By Request SSO
FastTrack Software

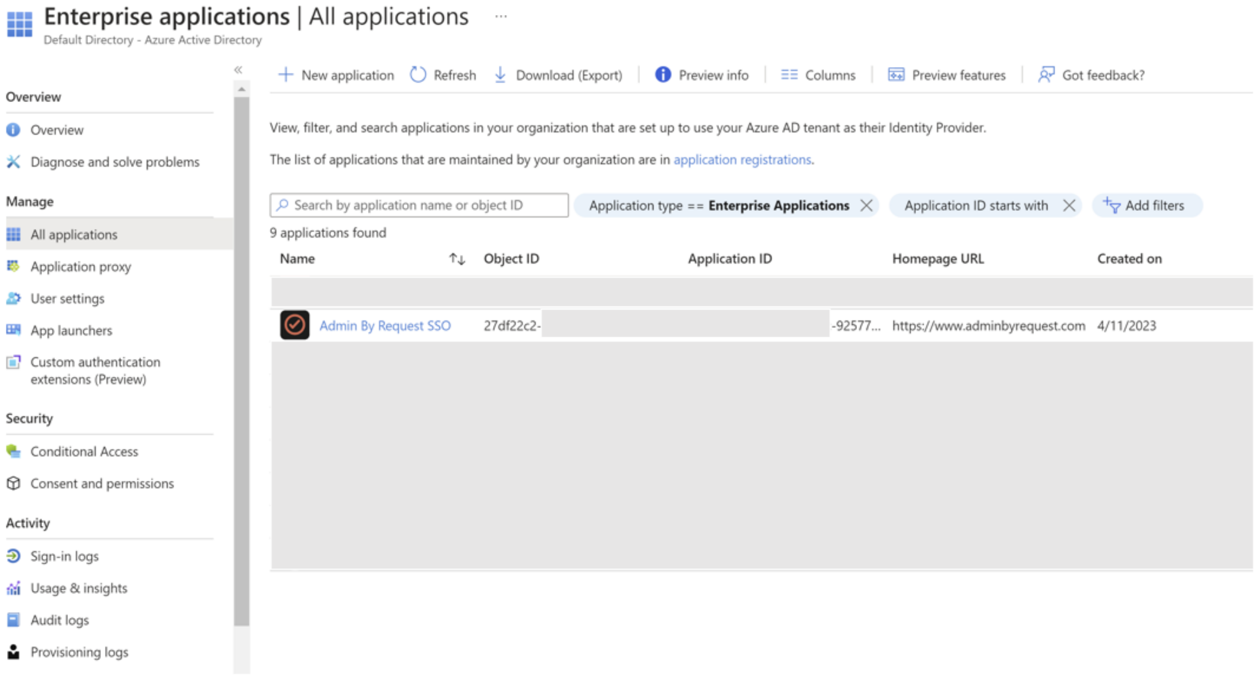
This app would like to:

Sign you in and read your profile

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. **The publisher has not provided links to their terms for you to review.** You can change these permissions at https://myapps.microsoft.com. Show details

Does this app look suspicious? Report it here

When the **first user accepts**, an Azure AD application is created for *Admin By Request SSO*. This application is now ready for any other user in the enterprise:



Enterprise applications | All applications

Default Directory - Azure Active Directory

View, filter, and search applications in your organization that are set up to use your Azure AD tenant as their Identity Provider.

The list of applications that are maintained by your organization are in application registrations.

Application type == **Enterprise Applications**

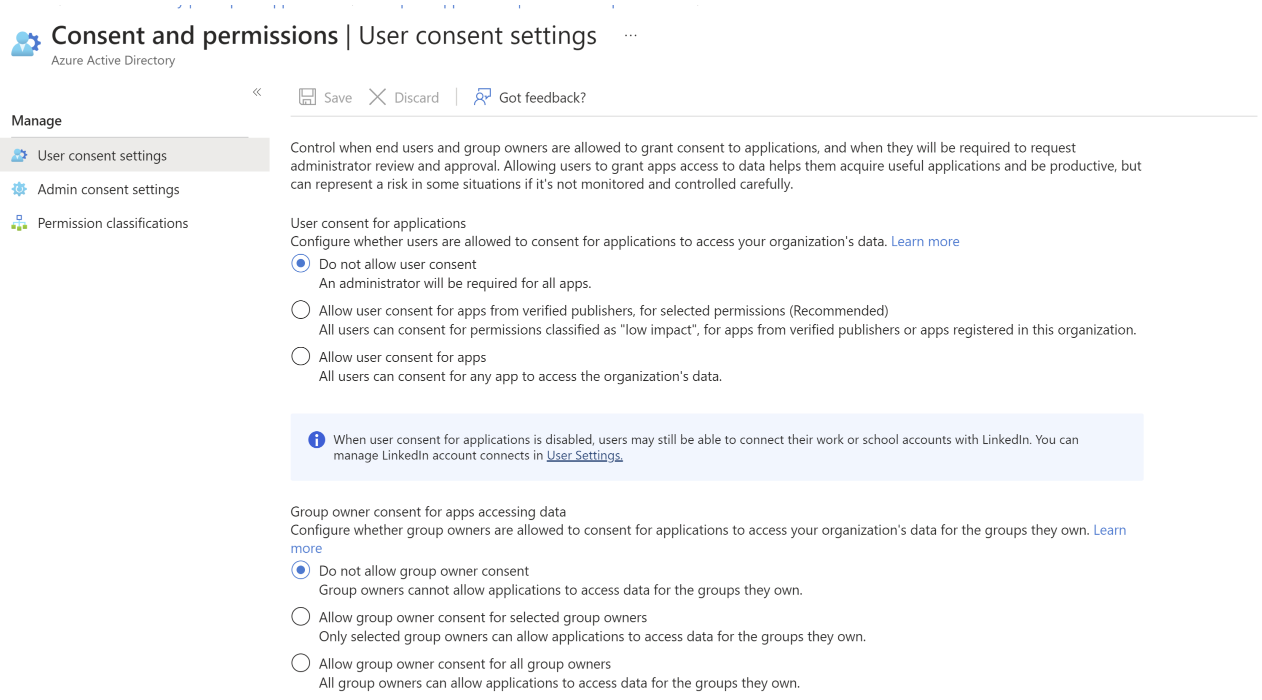
Application ID starts with

9 applications found

Name	Object ID	Application ID	Homepage URL	Created on
Admin By Request SSO	27df22c2-[redacted]	-92577...	https://www.adminbyrequest.com	4/11/2023

B. Users are not permitted to grant consent

The second method is more complex and is needed when users are not permitted to grant consent to apps in Azure AD, as indicated in the screenshot below:



Consent and permissions | User consent settings ...
Azure Active Directory

Control when end users and group owners are allowed to grant consent to applications, and when they will be required to request administrator review and approval. Allowing users to grant apps access to data helps them acquire useful applications and be productive, but can represent a risk in some situations if it's not monitored and controlled carefully.

User consent for applications
Configure whether users are allowed to consent for applications to access your organization's data. Learn more

● Do not allow user consent
An administrator will be required for all apps.

○ Allow user consent for apps from verified publishers, for selected permissions (Recommended)
All users can consent for permissions classified as "low impact", for apps from verified publishers or apps registered in this organization.

○ Allow user consent for apps
All users can consent for any app to access the organization's data.

When user consent for applications is disabled, users may still be able to connect their work or school accounts with LinkedIn. You can manage LinkedIn account connects in User Settings.

Group owner consent for apps accessing data
Configure whether group owners are allowed to consent for applications to access your organization's data for the groups they own. Learn more

● Do not allow group owner consent
Group owners cannot allow applications to access data for the groups they own.

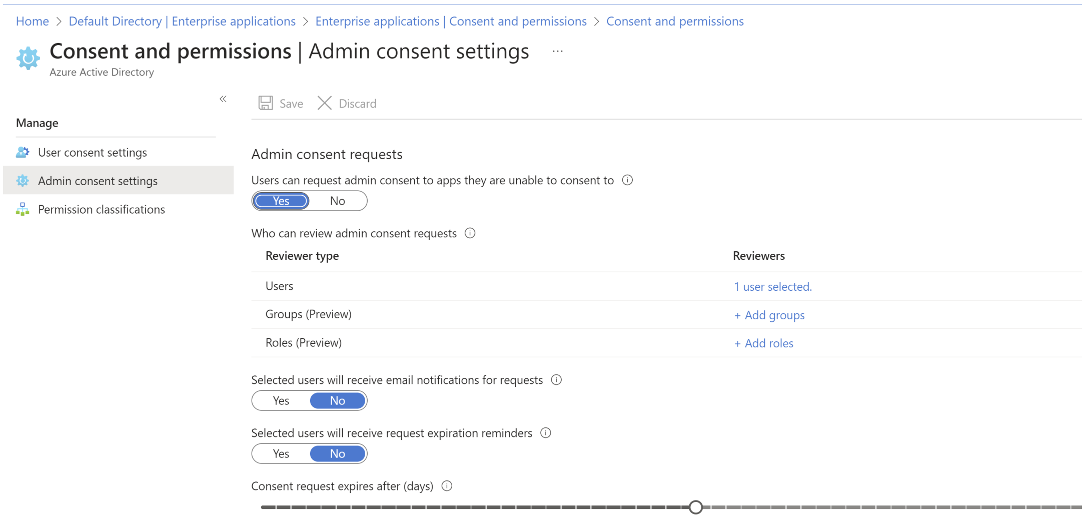
○ Allow group owner consent for selected group owners
Only selected group owners can allow applications to access data for the groups they own.

○ Allow group owner consent for all group owners
All group owners can allow applications to access data for the groups they own.

In this case, the following tasks must be completed:

1. Modify Admin consent settings:

   Admin consent settings must be modified so that users can request admin consent to apps they are normally unable to consent to:



Home > Default Directory | Enterprise applications > Enterprise applications | Consent and permissions > Consent and permissions

Consent and permissions | Admin consent settings ...
Azure Active Directory

Admin consent requests

Users can request admin consent to apps they are unable to consent to ⓘ
[✓ Yes] No

Who can review admin consent requests ⓘ

Reviewer type	Reviewers
Users	1 user selected.
Groups (Preview)	+ Add groups
Roles (Preview)	+ Add roles

Selected users will receive email notifications for requests ⓘ
Yes [✓ No]

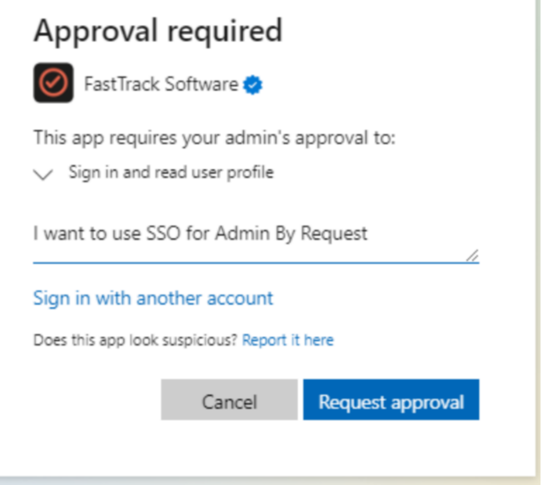
Selected users will receive request expiration reminders ⓘ
Yes [✓ No]

Consent request expires after (days) ⓘ

Determine which *Users*, *Groups* and/or *Roles* will be permitted to approve consent requests. To ensure approval requests are handled efficiently, those able to review requests for approval for a given application should be specified at this point.

2. Elevate a program as a normal user:

   The **first user** to initiate SSO validation from an endpoint is presented with an *Approval required* dialog:



Approval required

FastTrack Software

This app requires your admin's approval to:

Sign in and read user profile

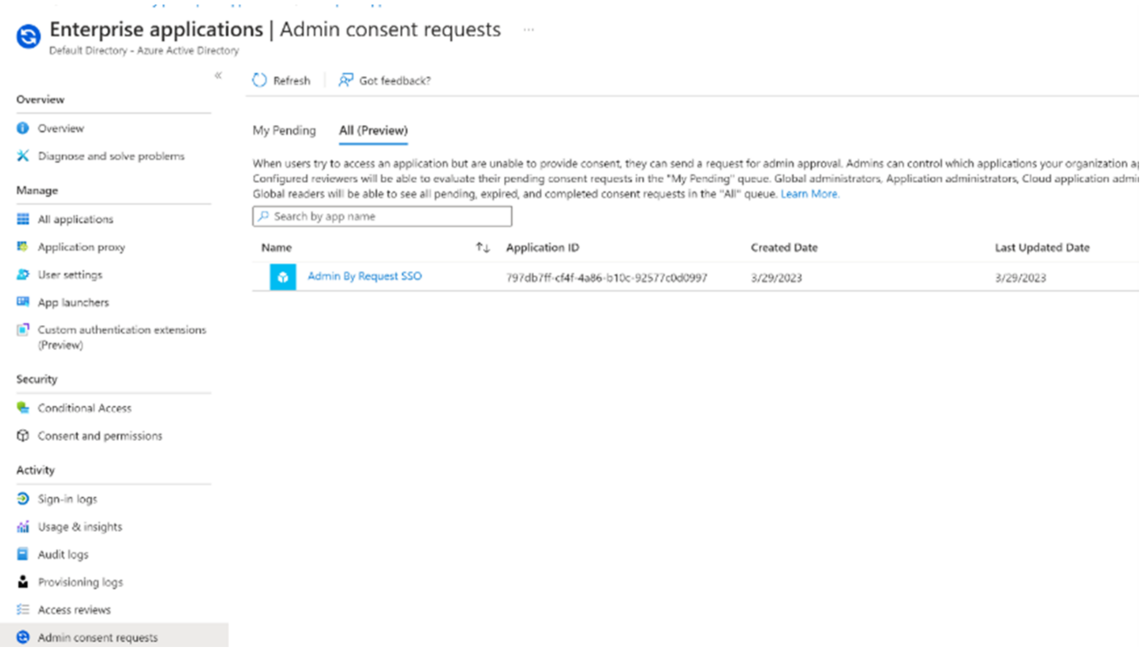
I want to use SSO for Admin By Request

Sign in with another account
Does this app look suspicious? Report it here
Cancel
Request approval

   To ensure first use is controlled, login as an ordinary user and create a consent request for the application by elevating a program. Enter the reason why you want this and click **Request approval**.

3. Approve the request as an authorized approver:

   Once the first approval request is made, go to your **AAD tenant > Enterprise Applications | Admin consent requests > All (Preview)** as one of the Users/Groups/Roles specified earlier. The following shows one request in the list:



Enterprise applications | Admin consent requests

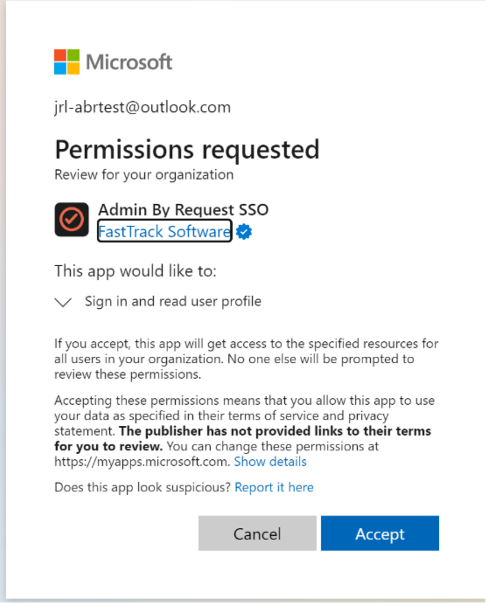
Default Directory - Azure Active Directory

When users try to access an application but are unable to provide consent, they can send a request for admin approval. Admins can control which applications your organization a Configured reviewers will be able to evaluate their pending consent requests in the "My Pending" queue. Global administrators, Application administrators, Cloud application admi Global readers will be able to see all pending, expired, and completed consent requests in the "All" queue. Learn More.

Name	Application ID	Created Date	Last Updated Date
Admin By Request SSO	797db7ff-cf4f-4a86-b10c-92577c0d0997	3/29/2023	3/29/2023

   For the request shown, click **Admin By Request SSO** to open it.

Finally, click **Accept** to approve it:



Microsoft

jrl-abrtest@outlook.com

Permissions requested

Review for your organization

Admin By Request SSO
FastTrack Software

This app would like to:

Sign in and read user profile

If you accept, this app will get access to the specified resources for all users in your organization. No one else will be prompted to review these permissions.

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. **The publisher has not provided links to their terms for you to review.** You can change these permissions at https://myapps.microsoft.com. Show details

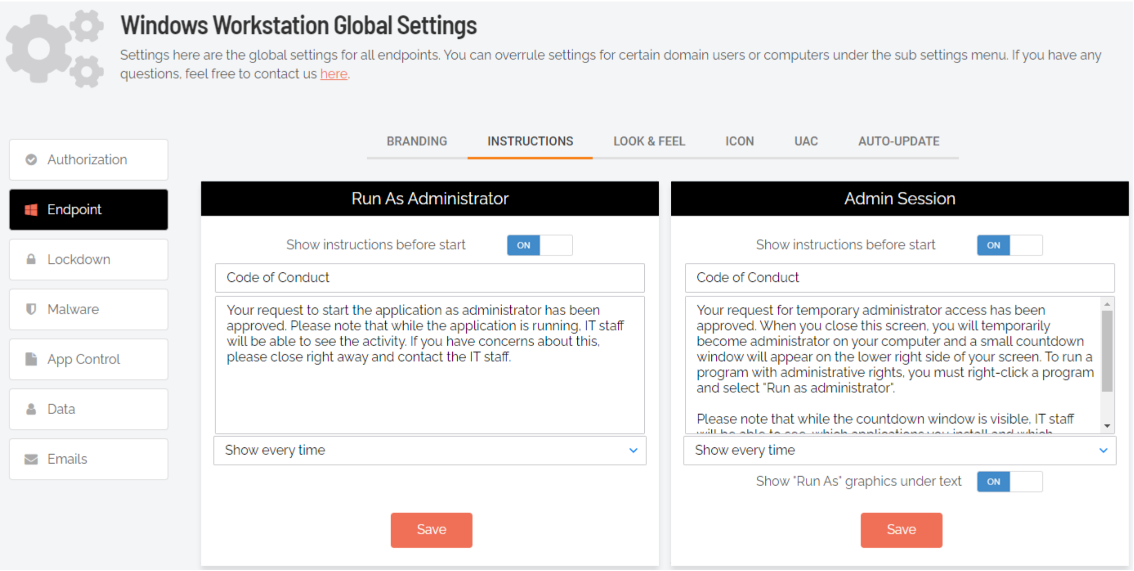
Does this app look suspicious? Report it here

Once accepted, all users can run the application.

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:



Windows Workstation 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.

Run As Administrator

Show instructions before start: ON

Code of Conduct

Your request to start the application as administrator has been approved. Please note that while the application is running, IT staff will be able to see the activity. If you have concerns about this, please close right away and contact the IT staff.

Show every time

Admin Session

Show instructions before start: ON

Code of Conduct

Your request for temporary administrator access has been approved. When you close this screen, you will temporarily become administrator on your computer and a small countdown window will appear on the lower right side of your screen. To run a program with administrative rights, you must right-click a program and select 'Run as administrator'.

Please note that while the countdown window is visible, IT staff

Show every time

Show 'Run As' graphics under text: ON

Offline Computers

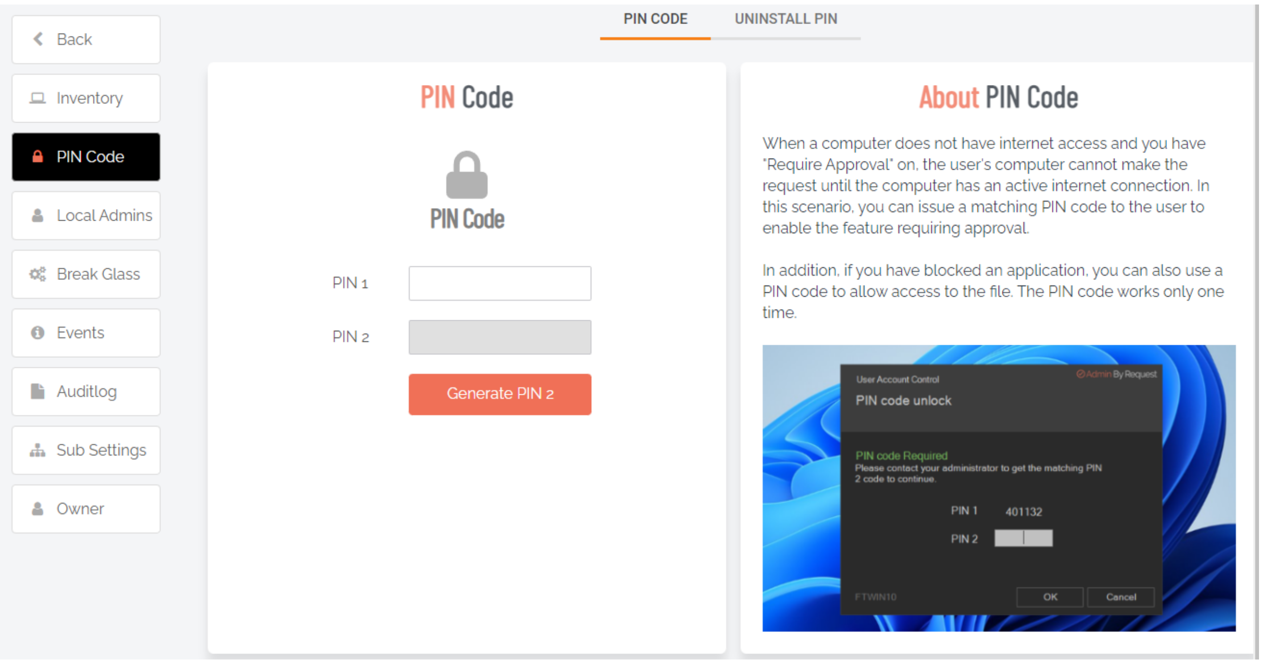
Admin By Request works the same whether the computer is online or offline. Portal settings, domain groups and OUs are cached on the client and all data going the other way are queued, so the user experience is exactly the same when a computer is away from your LAN or even when it has no internet connection.

PIN Code

Computers work the same online or offline – except of course, if you require approval and the computer is offline. Then no one will know the user has a pending request until the computer has an internet connection, at which time it will flush its upload queue. This would rarely be a real-world problem, but there are examples, where a computer is offline for a long period of time with no option to get online.

A good example is our customer Red Cross, which has workers going offline for weeks to a village in Africa. This is not a problem in itself, because the computer will just collect data and flush the queue later – but if approval is required, the user is stuck. If the user makes a request and approval is required, the user is informed that they have to either wait and queue the request until there is internet access, or seek internet access now (for example by connection sharing on a phone).

Or - request a PIN code in case of urgency and internet connectivity is impossible. If the user requests a PIN code, the user will see a 6 digit “PIN 1” code and must call, say, your Help Desk over the phone and get the matching 6 digit “PIN 2”. PIN 2 is a one-time PIN code that is hashed from PIN 1, customer id and computer name. Therefore, in the odd chance the same PIN 1 appears on a different computer, PIN 2 is different.



PIN Code

PIN Code

PIN 1

PIN 2

About PIN Code

When a computer does not have internet access and you have "Require Approval" on, the user's computer cannot make the request until the computer has an active internet connection. In this scenario, you can issue a matching PIN code to the user to enable the feature requiring approval.

In addition, if you have blocked an application, you can also use a PIN code to allow access to the file. The PIN code works only one time.

User Account Control

PIN code unlock

PIN code Required
Please contact your administrator to get the matching PIN 2 code to continue.

PIN 1 401132

PIN 2

FTWIN10

Policies for Windows

Settings in the Admin By Request client application are controlled in the portal under “Windows Settings” (**Portal > Settings > Windows Settings**). You can also define sub settings based on Computer or User Groups and/or OU.

It is highly recommended that you configure settings in the portal instead of using Group Policy Objects. If, for what-ever reason, you still want to overrule settings wholly or in part, you can set Policy keys either by using an ADMX file or by setting registry keys using GPO or by other means. Policy settings always overrule web settings.

> **IMPORTANT:**
> Please note we do not recommend that you use group policy 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 or a copy of an ADMX file, please feel free to contact us.

Supplementary Technical Information

This section provides more information on the following:

- Local Administrator's Group
- Entra ID / Azure Active Directory
- Sub-Settings
- Blocking
- Tampering
- User Account Control

The Local Administrator's Group

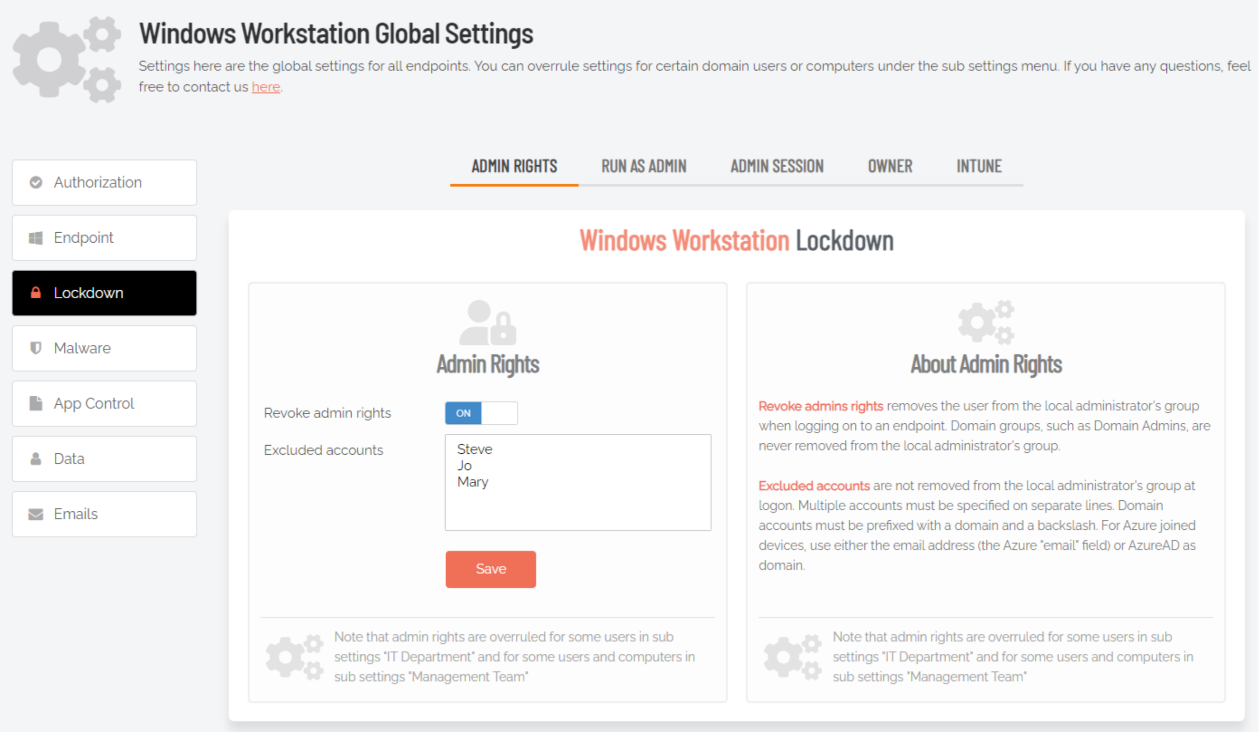
If the computer is in a domain, the Domain Users group will be removed from the local administrator's group right away. That is all that happens initially. When a user logs on, the user is removed from the local administrator's group, unless:

- You have unchecked the "Revoke admins rights" in the portal settings (see screenshot below)
- The user is in the list of excluded accounts in the portal settings
- The user is member of a group that is the local administrator's group (such as domain admins)

The reason all users are not removed right away is to only remove accounts that are interactive user accounts and not accidentally remove service accounts used to deploy software or similar.

Domain groups (except Domain Users) are not removed from the local administrator's group. This means that if a domain user logs on and is member of a domain group that is in the local administrator's group (for example, a Help Desk domain group), the user is always local administrator. In this case the tray icon is red and, mousing over it, you can see the tool tip saying "You are logged on as administrator".

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



Windows Workstation 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.

Windows Workstation Lockdown

Admin Rights

Revoke admin rights: ON

Excluded accounts:
Steve
Jo
Mary

Note that admin rights are overruled for some users in sub settings 'IT Department' and for some users and computers in sub settings 'Management Team'

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.

Note that admin rights are overruled for some users in sub settings 'IT Department' and for some users and computers in sub settings 'Management Team'

Entra ID / Azure AD and computers outside domains

The software works exactly the same for computers without a domain or for computers joined to Azure AD. For Azure AD, you can set up a connector in the portal settings. You do not need to do this for Azure AD, unless you need to use sub-settings, in which case you can set up the connector to create sub-settings based on Azure AD groups.

Sub-Settings

The portal has two levels of settings:

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

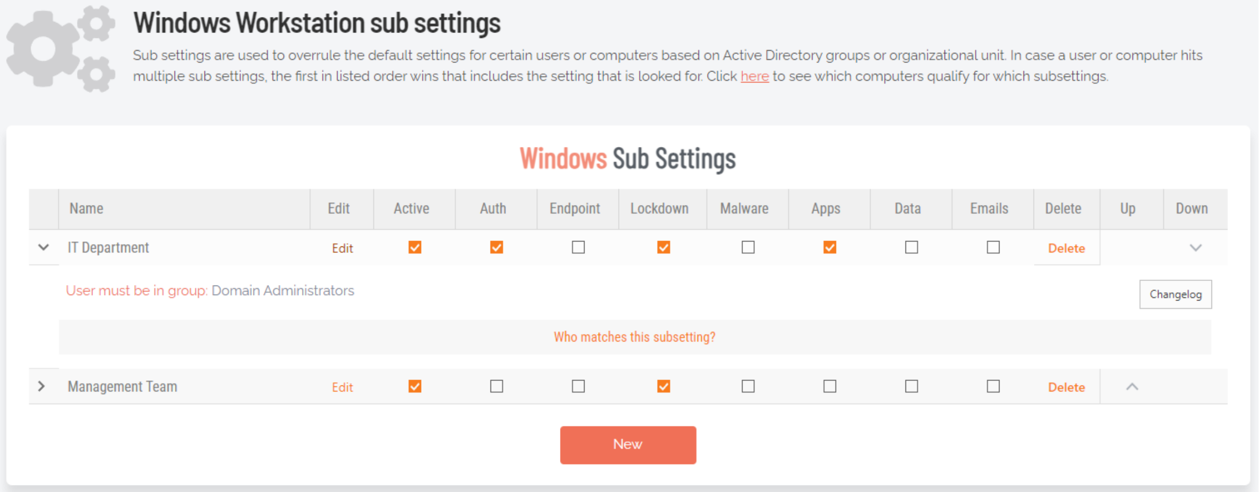
Settings here are the global settings for all endpoints. You can overrule settings for certain domain users or computers under the sub-settings menu.

Sub settings will *overrule* 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

A common scenario would be to require approval for all users – except users in the IT Department, who are allowed to elevate without permission:



Windows Workstation sub settings

Sub settings are used to overrule the default settings for certain users or computers based on Active Directory groups or organizational unit. In case a user or computer hits multiple sub settings, the first in listed order wins that includes the setting that is looked for. Click here to see which computers qualify for which subsettings.

Windows Sub Settings

	Name	Edit	Active	Auth	Endpoint	Lockdown	Malware	Apps	Data	Emails	Delete	Up	Down
⌄	IT Department	Edit	☑	☑	□	☑	□	☑	□	□	Delete		⌄
›	Management Team	Edit	☑	□	□	☑	□	□	□	□	Delete	⌃	

User must be in group: Domain Administrators

Entra ID / Azure AD and computers outside domains

The software works exactly the same for computers without a domain or for computers joined to Azure AD. For Azure AD, you can set up a connector in the portal settings. You do not need to do this for Azure AD, unless you need to use sub-settings, in which case you can set up the connector to create sub-settings based on Azure AD groups.

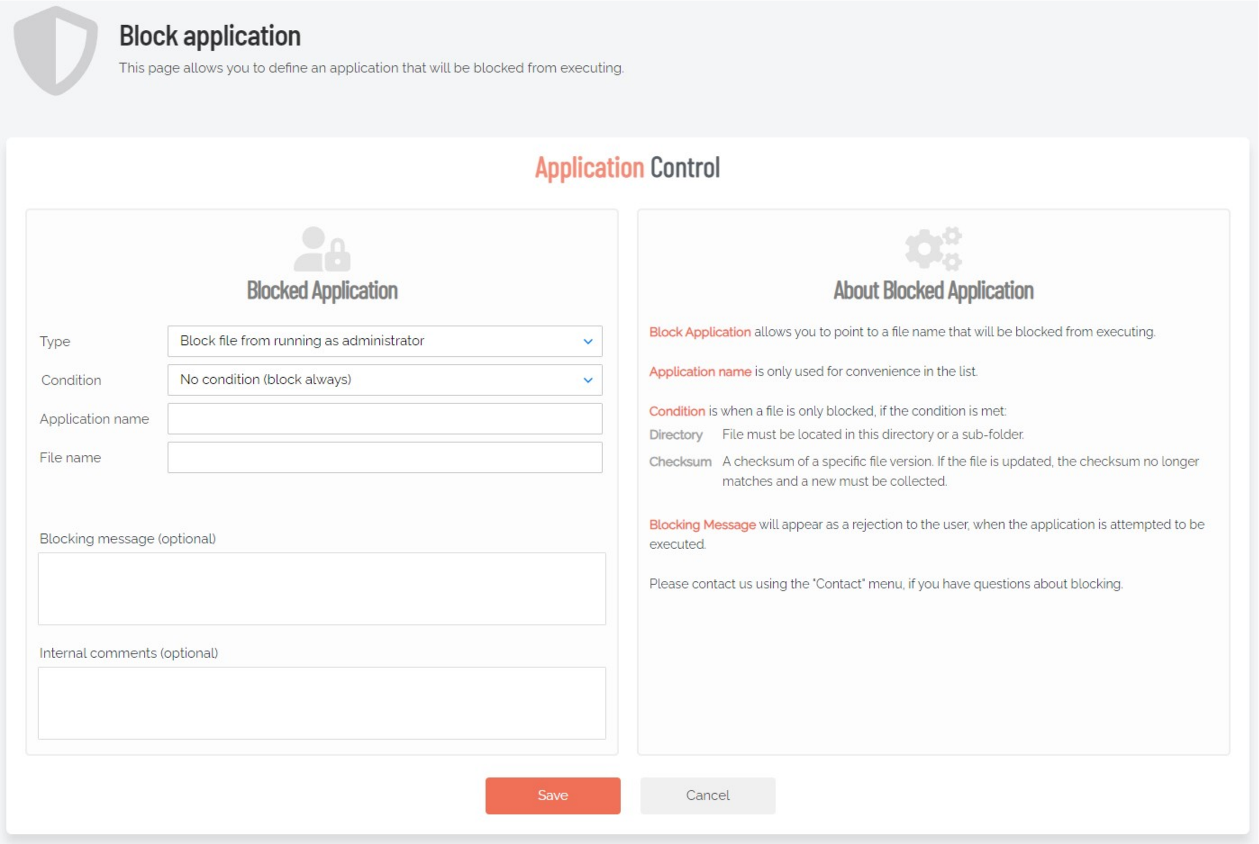
Blocking

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:



Block application

This page allows you to define an application that will be blocked from executing.

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.

You can also block users from elevating any Windows system file, which prevents users from running cmd.exe, regedit.exe, mmc.exe, etc as administrator.

Tampering

The software has built-in measures to avoid tampering with the software to become permanent administrator. The users and groups administration will be removed entirely from Computer Management during an administrator session. Even if the user still manages to tamper the local administrator's group, the administrator's group is snapshotted before the session starts and restored after the session ends.

If the user tries to add other users or groups to the administrator's group, these will simply be removed at the end of the session. If the user tries to uninstall Admin By Request during a session, Windows Installer will show an error message saying that Admin By Request cannot be uninstalled during an active session. If the user tries to tamper policy keys, these are also snapshotted and restored after sessions.

User Account Control

User Account Control (UAC) is still enforced (if enabled) to maintain the extra layer of security. If the user needs to run an application during an Admin Session, the user still has to envoke "Run as administrator" directly or indirectly and enter own credentials. This is intentional to avoid reducing the security level. Admin By Request does not replace or tap into UAC for the reasons stated in the previous section.

Admin By Request does not replace User Account Control, like some other solutions do. This is a design choice. Replacing Windows system files or components is dangerous and can lead to future problems because of Windows Updates, which could ultimately break your OS installs to the extent that computers can no longer boot. This is especially true with Windows 10 feature updates that often change basic functioning of the operating system. A significant advantage to the Admin By Request endpoint software is that it does not change or replace any system files or components and only uses what is already built into Windows. Because of this, it also does not consume any resources at all, unless the user invokes the software.

Windows Subsystem for Linux

Windows Subsystem for Linux (WSL) can be used with ABR installed on the endpoint and ABR handles this as it does other applications.

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 page 57 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.

Term	Definition
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.
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 and endpoint protection.

Term	Short for	Definition
ADMX	Administrative Template	A group policy template in Windows. Group policy tools use Administrative Templates to populate policy settings in the user interface. They have the extension .admx.
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	Microsft 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.
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	With FIDO Authentication, users sign in with phishing-resistant credentials, called "Passkey" on the next page. 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. Passkeys are more secure than passwords and SMS OTPs, simpler for consumers to use, and easier for service providers to deploy and manage.
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.

Term	Short for	Definition
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 30 June, 2023	8.0 12 December, 2022	Initial document release.
1.1 22 August, 2023	8.1 3 July, 2023	Included 8.1 features: • Support for Amazon WorkSpaces • Users able to delete desktop shortcuts • PIN Code MFA capability when offline • Support for Adobe installers • Support for in-app updating of MS Visual Studio
1.2 24 November, 2023	8.1 3 July, 2023	Clarified the difference between Standard and Admin users, including tray icon color. Added Diagnostics, Support Assist and Proxy Server sections to User Interface chapter. Added box and arrow charts to provide a clear overview of sections following that require choices or a sequence of tasks. Added "Creating an Intune package" as an installation option. Updated "Using the .msi installation file" as an uninstallation option. Removed "Policies for Windows" chapter and added a summary Policies section to Portal Administration.
1.3 22 December, 2023	8.1 3 July, 2023	Added Break Glass section.. Added multiple Settings Tables to chapter Portal Administration.
1.4 16 February 2024	8.2 15 January 2024	Added further Settings Tables for Admin Rights and Entra ID. Restructured User Interface chapter. Fixed pagination.
1.5 11 March 2024	8.2 15 January 2024	Added Settings Table for Windows Settings > Data > PRIVACY. Fixed a problem in chapter "The Windows Client User Interface", section *Requesting Assistance*, where the description of how assistance works was incorrect.

Index