Secure Remote Access (SRA)

# Remote Support: IT Admin Guide

## Document Information

| | |
|---|---|
| Code: | **PM-SUP-ITAG** |
| Version: | **2.1** |
| Date: | **16 March 2026** |

Admin By Request
ZERO TRUST PLATFORM

# Copyright © 2026 Admin By Request



# Contact Admin By Request

+64 21 023 57020
marketing@adminbyrequest.com
adminbyrequest.com
Unit C, 21-23 Elliot St, Papakura, NZ

# Table of Contents

# Remote Support Overview

## What is Remote Support?

Remote Support is part of the Secure Remote Access product by Admin By Request, that allows you to share screens and remotely control devices inside of your Admin By Request inventory, while using all of the well-known features of the Admin By Request ecosystem, such as: inventory, auditlog, settings and sub-settings, approval flows etc.

Remote Support allows either end users or IT admins to initiate a secure, just-in-time, remote support session – allowing them to share and control the end-user's device – and tear everything down once the session is done – eliminating any access points for bad actors.

This document covers getting started with Product Enrollment and Remote Support. It also describes key settings that can be administered from the portal.

**NOTE**
At the time of writing, Remote Support is available to **Windows and Mac** clients. Access to Linux clients is expected later in 2026.

### Related information

- Unattended Access
- Vendor Access

## Prerequisites

In order to use the full power of Remote Support, there are a number of requirements, listed under the following headings (not all are necessarily required - review those relevant to your environment):



### A. General requirements

Before starting, make sure you have the following:

- Access to the portal at **https://www.adminbyrequest.com/Login**
- Admin By Request for **Windows 8.4.0+** on each Windows endpoint
- Admin By Request for **Mac 5.2+** on each macOS endpoint

### B. Data location

Your data is stored in a data center that is located in one of the geographic locations listed below. These are in Europe, the USA, the UK and Asia.

To determine your data location, go to page Tenant Settings > Data in the portal and click the **RETENTION** tab.

Note the geographic location shown in field **Data Location** - it will be one of the following:

- **EU West, Netherlands** (Europe)
- **US East, Virginia** (USA)
- **US West, California** (USA)
- **London, United Kingdom** (UK)
- **EU Central, Germany** (Europe)
- **Singapore** (Asia)

To determine the *API prefix* for your data center, go to page Settings > Tenant Settings > Data > API KEYS in the portal and check which API prefix is shown under **About API Keys**. The data center API URL (also known as the API prefix) will be one of the following:

- **https://dc1api.adminbyrequest.com** (Europe - Netherlands)
- **https://dc2api.adminbyrequest.com** (US East)
- **https://dc3api.adminbyrequest.com** (UK)
- **https://dc4api.adminbyrequest.com** (Europe - Germany)
- **https://dc5api.adminbyrequest.com** (US West)
- **https://dc6api.adminbyrequest.com** (Asia)

Make a note of your prefix - among other things, this is the domain used when an API Key is created.

You can also see your API prefix on the API web pages (e.g. Public API > Auditlog API). However, a small script runs in the background that determines to which data center you are attached, so JavaScript must be enabled in your browser for this to work.

## C. IP addresses and API URLs

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

If your data is located in Europe (Netherlands):

- IP: **104.45.17.196**
- DNS: **api1.adminbyrequest.com**
- DNS: **macapi1.adminbyrequest.com**

If your data is located in the USA (East):

- IP: **137.117.73.20**
- DNS: **api2.adminbyrequest.com**
- DNS: **macapi2.adminbyrequest.com**

If your data is located in the UK:

- IP: **85.210.211.164**
- DNS: **api3.adminbyrequest.com**
- DNS: **macapi3.adminbyrequest.com**

If your data is located in Europe (Germany):

- IP: **9.141.94.162**
- DNS: **api4.adminbyrequest.com**
- DNS: **macapi4.adminbyrequest.com**

If your data is located in the USA (West):

- IP: **172.184.188.29**
- DNS: **api5.adminbyrequest.com**
- DNS: **macapi5.adminbyrequest.com**

If your data is located in Asia (Singapore):

- IP: **52.230.54.129**
- DNS: **api6.adminbyrequest.com**
- DNS: **macapi6.adminbyrequest.com**

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

## D. Cloud gateway

1. If you are using *Secure Remote Access*, you need to allow your browsers access to the following cloud gateways:
   - **cloudgatewayeu1.accessbyrequest.com** (Europe - Netherlands)
   - **cloudgatewayus1.accessbyrequest.com** (US East)
   - **cloudgatewayuk1.accessbyrequest.com** (UK)
   - **cloudgatewaygermany1.accessbyrequest.com** (Europe - Germany)
   - **cloudgatewayuswest1.accessbyrequest.com** (US West)
   - **cloudgatewaysingapore1.accessbyrequest.com** (Asia)

   They are called over **WSS** (Websockets Secure) on port **443** from the browser.

   Further, if you wish to remotely access endpoints using *Unattended Access* and *Remote Support*:

   - Outbound MQTT broker connectivity via Websockets - port **443** - for the following:
     - If your data is located in Europe (Netherlands):
       Ten nodes (**FastTrackHubEU1.azure-devices.net** to **FastTrackHubEU10.azure-devices.net**)
     - If your data is located in the USA (East):
       Ten nodes (**FastTrackHubUS1.azure-devices.net** to **FastTrackHubUS10.azure-devices.net**)
     - If your data is located in the UK:
       Ten nodes (**FastTrackHubUK1.azure-devices.net** to **FastTrackHubUK10.azure-devices.net**)
     - If your data is located in Europe (Germany):
       Ten nodes (**FastTrackHubGermany1.azure-devices.net** to **FastTrackHubGermany10.azure-devices.net**)
     - If your data is located in the USA (West):
       Ten nodes (**FastTrackHubUSWest1.azure-devices.net** to **FastTrackHubUSWest10.azure-devices.net**)
     - If your data is located in Asia:
       Ten nodes (**FastTrackHubSingapore1.azure-devices.net** to

**FastTrackHubSingapore10.azure-devices.net**)

- For *Remote Support*, RDP needs to be enabled on port **3389** on the device.

2. Cloudflare connectivity:
   - UDP outbound - port **7844** for the following:
     - **region1.v2.argotunnel.com**
     - **region2.v2.argotunnel.com**
   - If your firewall supports Server Name Indication (SNI), you need to allow the following URLs (UDP outbound - port **7844**):
     - **cftunnel.com**
     - **h2.cftunnel.com**
     - **quic.cftunnel.com**

     Refer to https://developers.cloudflare.com/cloudflare-one/connections/connect-networks/deploy-tunnels/tunnel-with-firewall/ for more information on Cloudflare's "tunnel with firewall" configuration.
3. The endpoint needs to be enrolled with an Admin By Request Secure Remote Access license (see Product Enrollment).
4. For Windows endpoints, RDP needs to be enabled on port **3389** on each device.

**NOTE**
Remote Support does not require RDP; rather, it relies on a VNC server that is spun up "just-in-time".

# macOS-specific behavior

- When Remote Support is first used on macOS, the user can be prompted to approve privacy permissions such as screen recording and audio/microphone capture.
- Some permissions can be distributed by MDM, but user consent is still required for certain privacy prompts on macOS.
- If a user is currently signed in at the endpoint, the workflow can require user logout before the session is established.

**IMPORTANT**
For Mac unattended-style login workflows, passwordless sign-in is not currently available. Operators can land at the login screen and need valid endpoint credentials (or a break-glass account) to continue.

## Identity prerequisite for group-based subsettings on macOS

If you use Okta groups to drive subsettings on macOS, platform SSO with Okta is required.

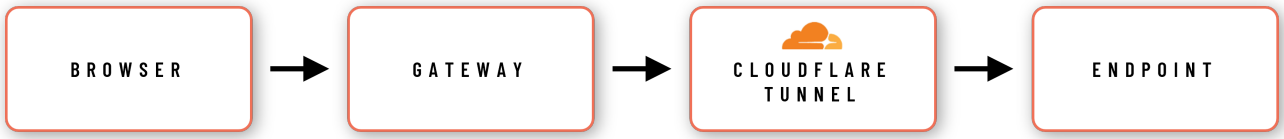
# How does Remote Support work?

Remote Support is based on the same gateway concept as the Unattended Access gateway, which is also part of the Admin By RequestSecure Remote Access product. It allows a just-in-time setup between the gateway and the endpoint by establishing a secure Cloudflare tunnel.

Once the tunnel is established, a just-in-time server session is created on the endpoint – allowing for screen sharing and remote control via the browser.

Once the session is terminated or expires, the tunnel and the server session are terminated, leaving the endpoint in the same state as before the remote support session.

The setup is fully cloud-based and does not require any on-premise setup besides what's mentioned in the prerequisites:




The process flow for a Remote Support session can be initiated either by an IT administrator via the portal (admin-initiated) or by an end user at the endpoint (user-initiated).

## Process - Admin-initiated

The process by which an *administrator* establishes a remote support session is:

1. The administrator navigates to a specific endpoint in the **Admin By Request Portal** inventory and clicks the *Support* link associated with that endpoint. This action initiates a Remote Support connection.
2. The **Admin By Request client** on the endpoint receives an instruction from the **MQTT Broker** to fetch settings using the **Admin By Request API**.
3. The user at the endpoint is prompted that an administrator requests to initiate a Remote Support session. The user must approve the request for the session to continue.
4. Upon approving the request, the **Admin By Request client** opens a **Cloudflare Tunnel** via an outbound UDP call on port 7844 using the QUIC Protocol.
5. The **Admin By Request client** creates a just-in-time VNC server on the endpoint and instructs the **Admin By Request API** that the endpoint is awaiting a connection.
6. The **Gateway** is instructed to forward the VNC connection through the tunnel opened by the endpoint.
7. A secure WebSocket connection is established between the administrator's browser and the **Gateway**. The response stream from the VNC connection is routed back to the browser using this secure connection.

**KEY POINTS**

- Once the session is terminated – or expires – the session server and the tunnel are terminated.
- The session is logged in the audit log in the Admin By Request portal, allowing for the IT admin to access documentation about each remote support session – as well as download a recording of each session (if recording is enabled).
- Based on the settings, each Remote Support session can be adapted with various security and compliance features like: Multi-Factor Authentication (MFA), view-only access, session expiration and session recording.

## Process - User-initiated

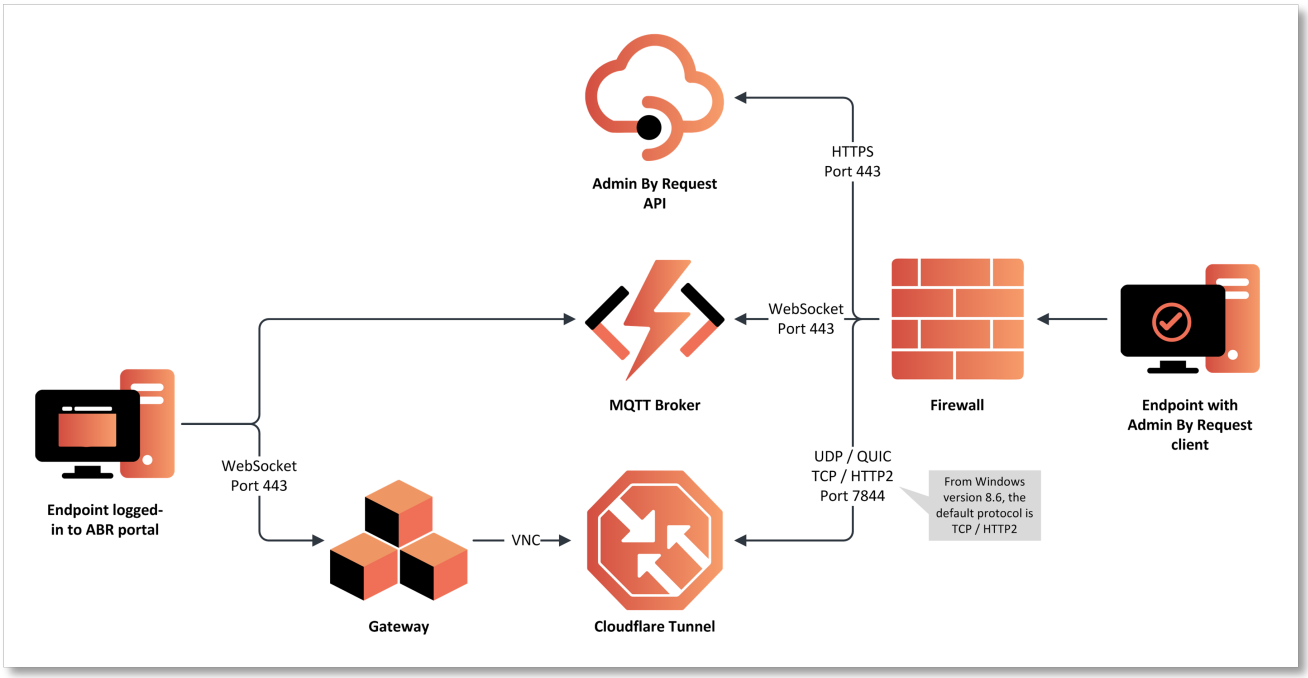
The process by which a *user* establishes a remote support session is:

1. The user requests a Remote Support session from the **Admin By Request client** running on their endpoint.
2. An administrator accepts the request from the **Admin By Request portal**.
3. The **Admin By Request client** on the endpoint receives an instruction from the **MQTT Broker** to fetch settings using the **Admin By Request API**.
4. The user at the endpoint is prompted that an administrator requests to initiate a Remote Support session.
5. Upon accepting the request, the **Admin By Request client** opens a **Cloudflare Tunnel** via an outbound UDP call on port 7844 using the QUIC Protocol.
6. The **Admin By Request client** creates a just-in-time VNC server on the endpoint and instructs the **Admin By Request API** that the endpoint is awaiting a connection.
7. The **Gateway** is instructed to forward the VNC connection through the tunnel opened by the endpoint.
8. A secure WebSocket connection is established between the administrator's browser and the **Gateway**. The response stream from the VNC connection is routed back to the browser using this secure connection.

### KEY POINTS

- The end user requests a Remote Support session from their endpoint, providing a reason for the request if necessary.
- The IT admin approves (or denies) the request via the Admin By Request portal.

Both admin-initiated and user-initiated processes are illustrated in the following diagram:



# Getting Started with Remote Support

## How do I get started?

The first thing is to make sure that the Admin By Request client software is installed on all the endpoints to which you might want to connect in remote support mode.

If you are already using Endpoint Privilege Management (EPM), then the client is already installed on the endpoints showing in the portal Inventory. Skip the installation procedures and go to "Enrolling devices" below.

If not (i.e. this is your first use of Admin By Request), then follow the installation procedures to install the client on one or more endpoints.

### Installing a single endpoint

- Windows
- Mac

### Installing multiple endpoints

- Using msiexec
- Via Intune package

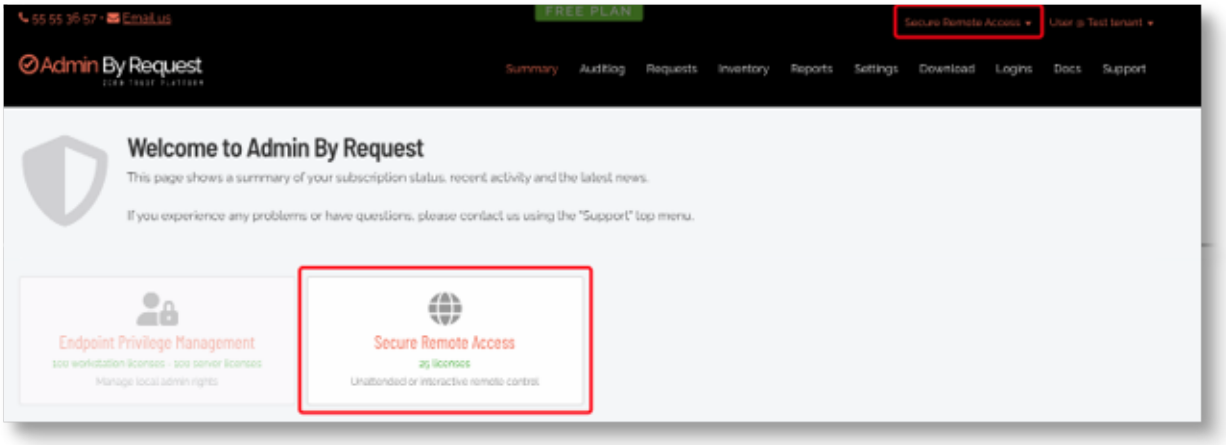
### Enrolling devices

The second thing is to make sure devices are enrolled. In order to access a device using Remote Support, the device needs to be enrolled with the Admin By Request Secure Remote Access product (see "Product Enrollment" on page 20).

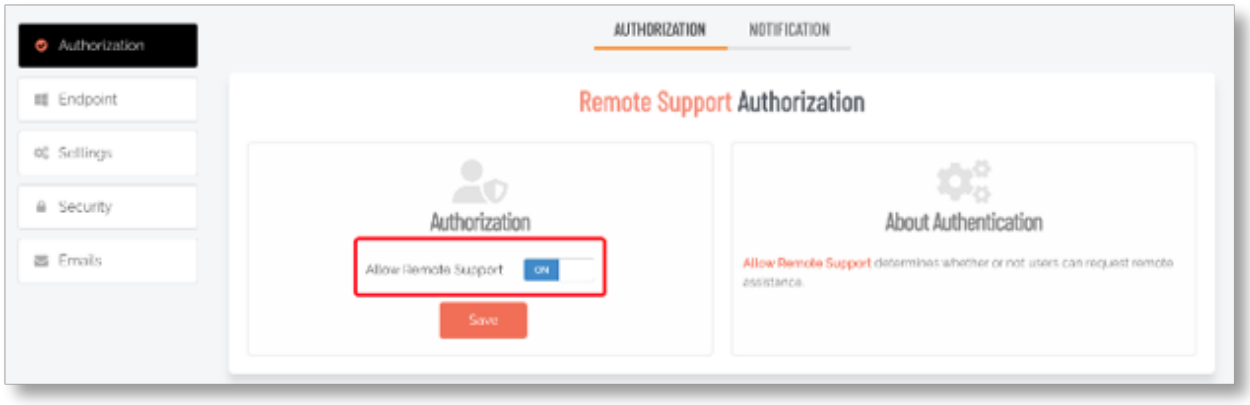
After the device is enrolled, the settings scope needs to allow Remote Support sessions.

To allow Remote Support sessions:

1. Navigate to the Admin By Request portal
2. Ensure that the **Secure Remote Access** view is selected either on the *Summary* page or via the product selector in the menu:



3. From the Settings menu, select **Remote Support Settings**.
4. Under the **AUTHORIZATION** tab, ensure that "Allow Remote Support" is set to **On**:




This ensures that devices falling within this settings scope have the ability to request a Remote Support session (or have one requested by a portal user).

### Mac enrollment and permissions

- If a Mac endpoint is not enrolled in Secure Remote Access, SRA-specific prompts are not shown.
- After enrollment, restart the endpoint so the client can fetch SRA components and apply the relevant permission flow.
- With MDM, some permissions can be configured centrally. However, macOS user consent is still required for privacy permissions such as screen recording and audio/microphone capture.
- For these privacy prompts, approval by the signed-in user is sufficient; elevation is not always required.

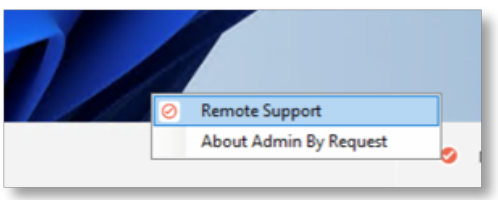
**NOTE**
On first connection, the signed-in user can be asked to log out before the remote control session starts.

## Requesting Remote Support (end user initiated)

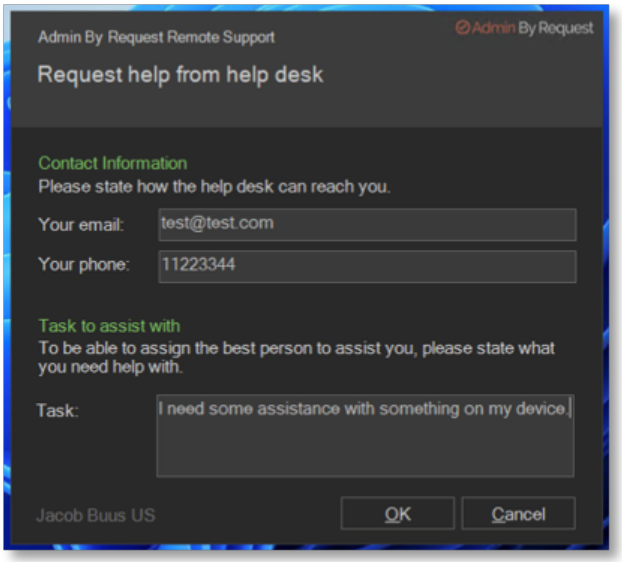
### Windows

To request a Remote Support session as an end user, the end user does the following:

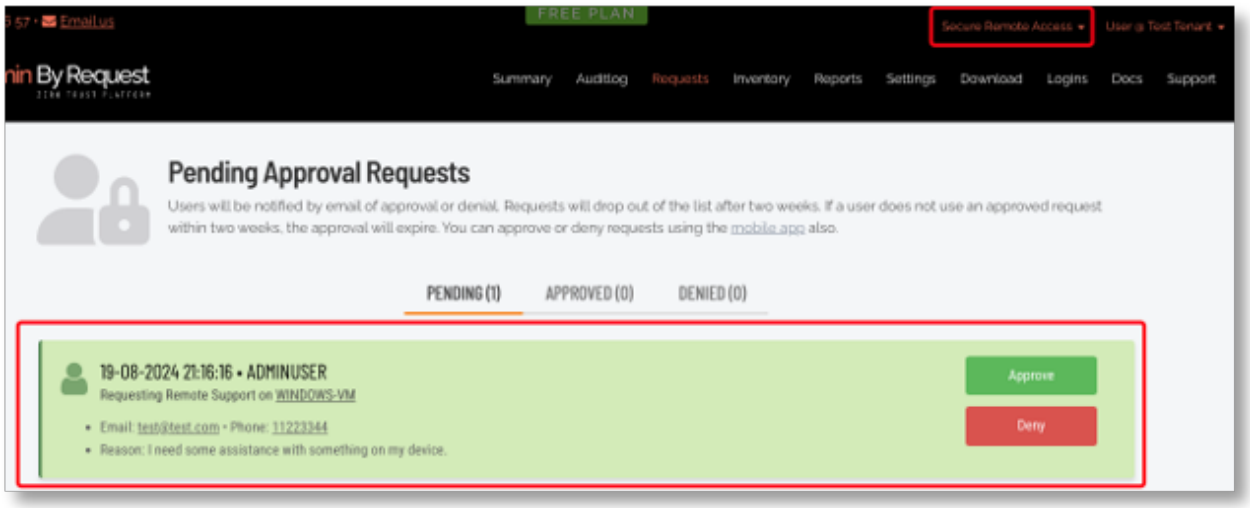
1. From the endpoint with the Admin By Request client installed, navigate to the Admin By Request tray icon (or use the desktop icon if this has been enabled - see "Set desktop icon" on page 26).
2. Right-click the icon and select the **Remote Support** item:



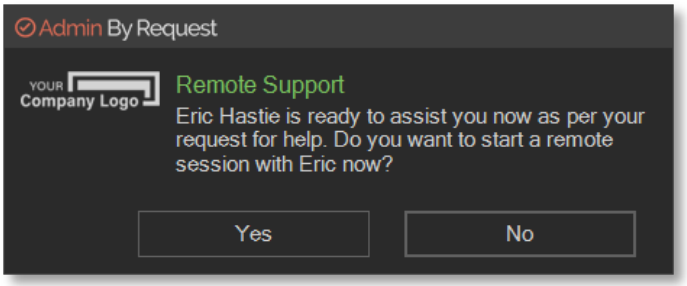
3. This prompts the user for contact information as well as a reason for the Remote Support request:




4. All Remote Support requests awaiting approval can be found by the portal admin in the Admin By Request portal under "Requests" with the "Secure Remote Access" view selected in the product selector:

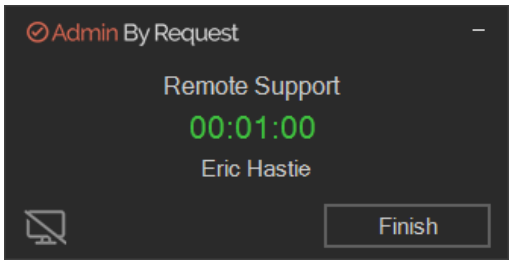



5. The portal admin can now approve or deny the request. If the request is approved, the end user is prompted to allow the connection:



6. By clicking **Yes**, the secure tunnel and just-in-time server session is initialized, and the portal user is connected to a Remote Support session – sharing the screen and input directly in the browser (if enabled - see "Specify View Only for portal admin" on page 29).

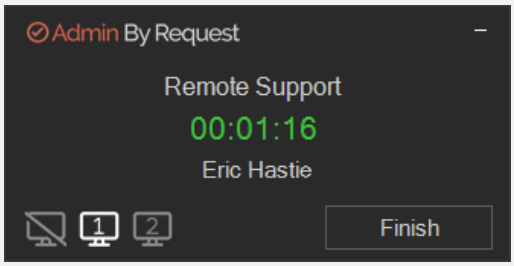
   Once the session starts, a timer appears in the lower, right corner of the screen, showing the amount of time used so far during the session:



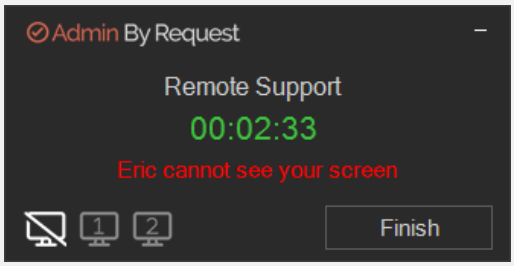

   Click the **Hide** icon at any time to hide the screen from the remote person.

**NOTE**

If the endpoint has multiple monitors, the monitor currently being viewed is indicated (**Monitor 1** in this example). Click a monitor icon to switch the view to that screen:



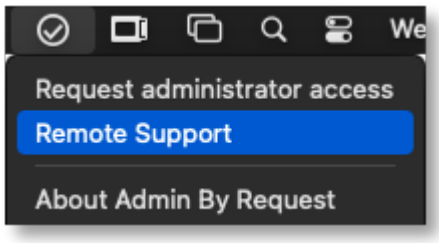

To hide a screen, simply click the **Hide** icon:



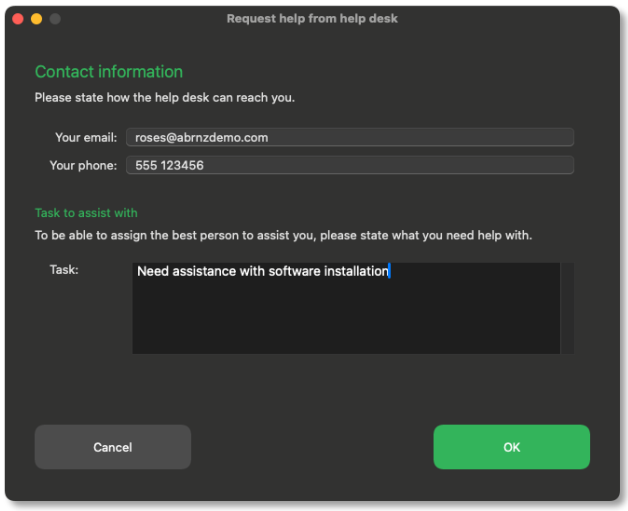
## Mac

To request a Remote Support session as an end user, the end user does the following:

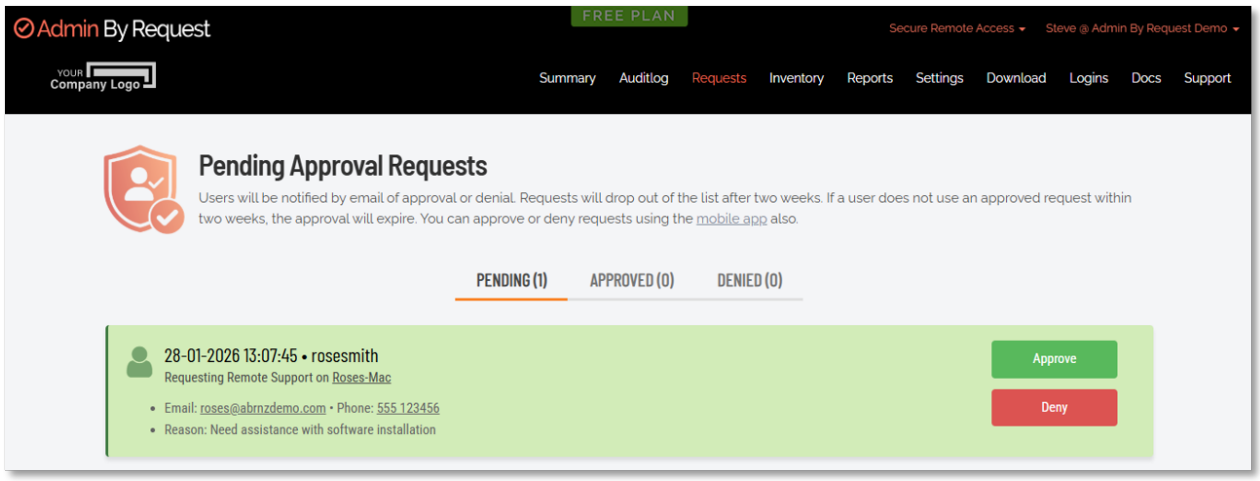
1. From the endpoint with the Admin By Request client installed, navigate to the Admin By Request menu bar.
2. Select **Remote Support**:



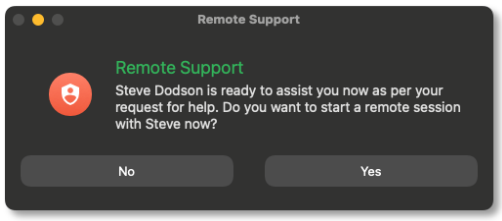

3. This prompts the user for contact information as well as a reason for the Remote Support request:




4. Click **OK** to submit the request and **OK** again to acknowledge the notification.
5. All Remote Support requests awaiting approval can be found by the portal admin in the Admin By Request portal under "Requests" with the "Secure Remote Access" view selected in the product selector:

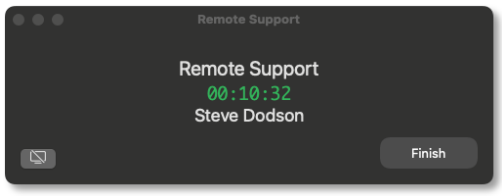


6. The portal admin can now approve or deny the request. If the request is approved, the end user is prompted to allow the connection:




7. By clicking **Yes**, the secure tunnel and just-in-time server session is initialized, and the portal user is connected to a Remote Support session – sharing the screen and input directly in the browser (if enabled - see Specify View Only for portal admin).

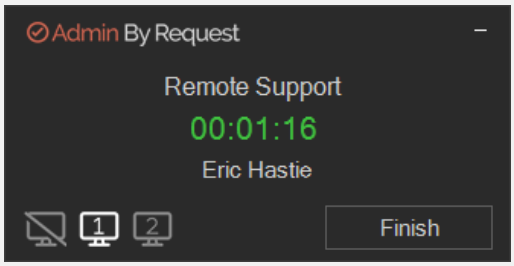
   Once the session starts, a timer appears in the lower, right corner of the screen, showing the amount of time used so far during the session:



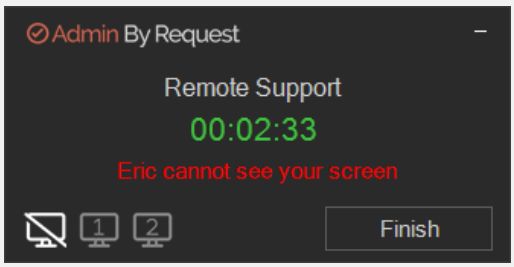

   Click the **Hide** icon at any time to hide the screen from the remote person.

**NOTE**

If the endpoint has multiple monitors, the monitor currently being viewed is indicated (**Monitor 1** in this example). Click a monitor icon to switch the view to that screen:




To hide a screen, simply click the **Hide** icon:

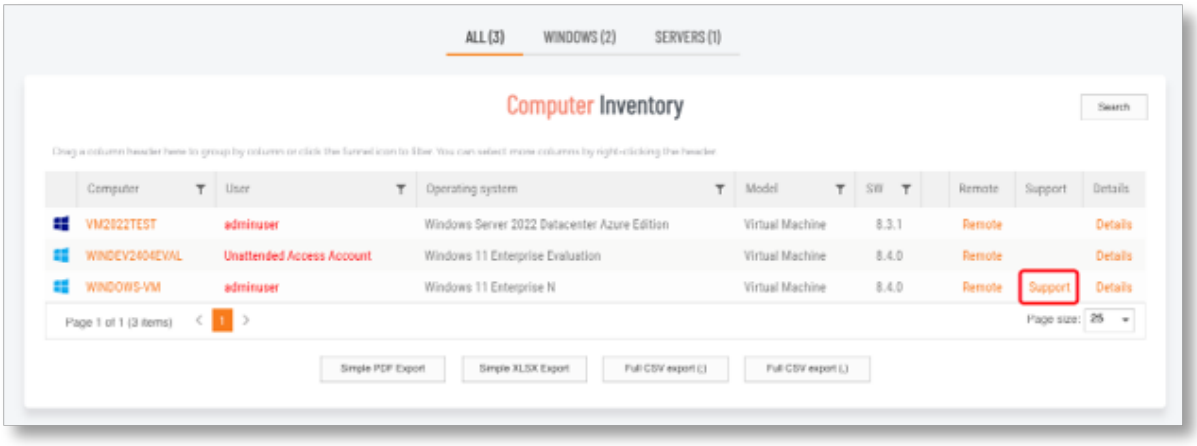


# Starting Remote Support (IT admin initiated)

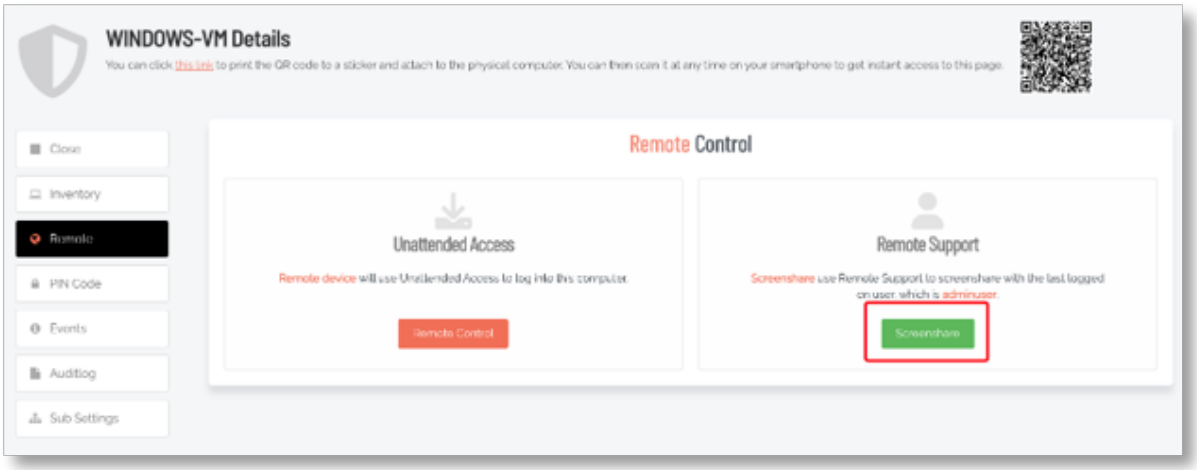
## Windows

To start a Remote Support session as a portal administrator, the following sequence occurs:

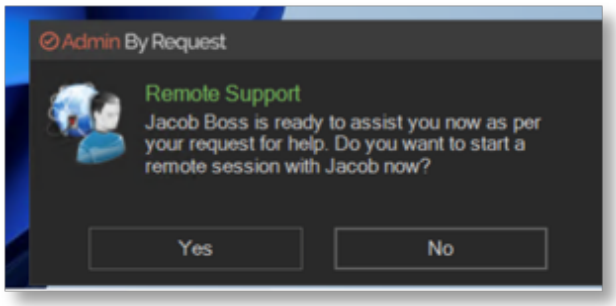
1. The portal admin identifies the target device in the Inventory and then either:
   a. clicks **Support** from the Inventory list:




   b. or, clicks the **Screenshare** button in the Remote Support panel (after drilling down into inventory details for the endpoint):



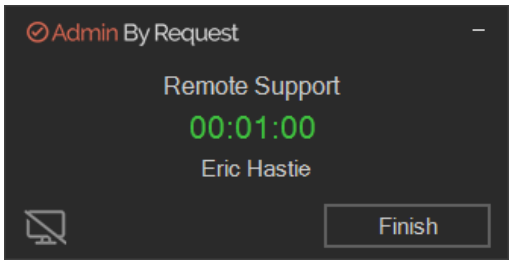

2. After either is clicked, the end-user receives a pop-up asking to accept the incoming connection:




3. If the end user clicks **Yes**, the secure tunnel and just-in-time server session is initialized, and the portal admin is now connected to a Remote Support session – sharing the screen and input (if enabled - see "Specify View Only for portal admin" on page 29) directly in the browser.

4. If the end user clicks **No**, the portal admin request to start a Remote Support session is denied. In any case, all request details are logged in the Auditlog.

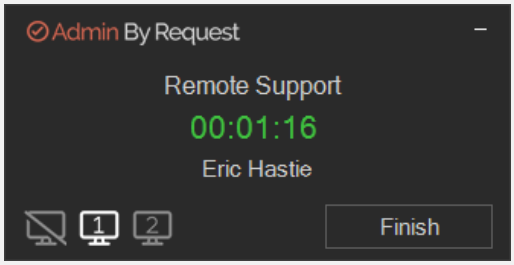
   Once the session starts, a timer appears in the lower, right corner of the screen, showing the amount of time used so far during the session:



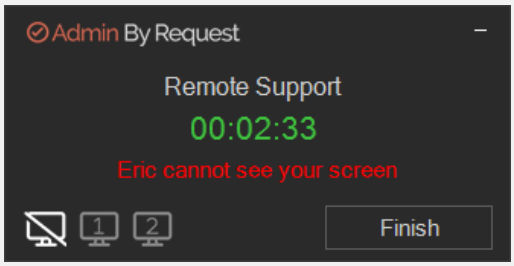

   Click the **Hide** icon at any time to hide the screen from the remote person.

**NOTE**

If the endpoint has multiple monitors, the monitor currently being viewed is indicated (**Monitor 1** in this example). Click a monitor icon to switch the view to that screen:



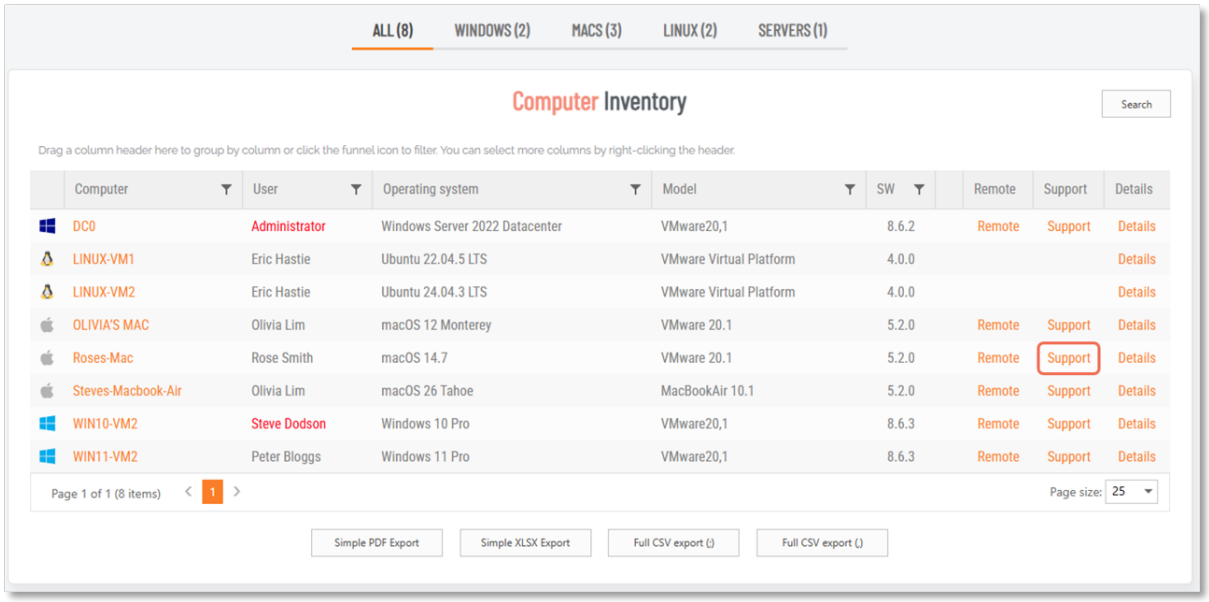

To hide a screen, simply click the **Hide** icon:



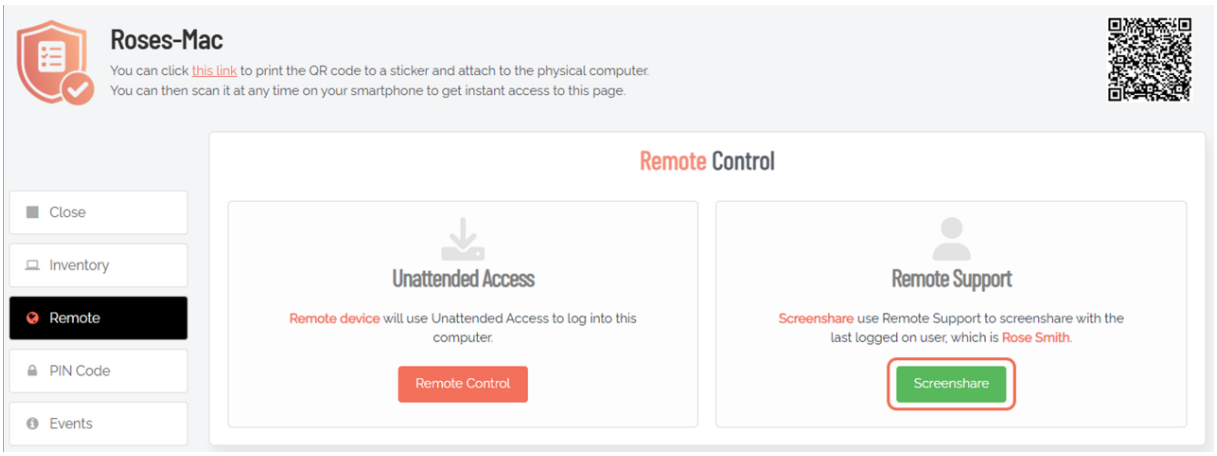
## Mac

To start a Remote Support session as a portal administrator, the following sequence occurs:

1. The portal admin identifies the target device in the Inventory and then either:
   a. clicks **Support** from the Inventory list:

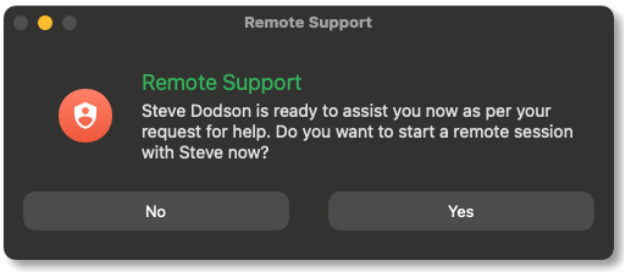



   b. or, clicks the **Screenshare** button in the Remote Support panel (after drilling down into inventory details for the endpoint):



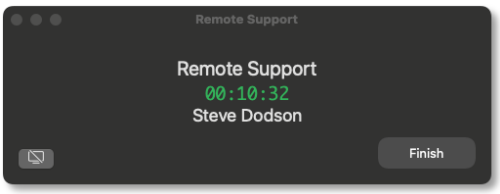

2. A connection is initiated and the permissions at the endpoint are checked:
   - If Admin By Request already has permission to do **Screen & System Audio Recording**, a connection is established and the remote support session begins.
   - If Admin By Request does not have permission, a **Remote Support Permissions Required** prompt appears at the endpoint. The endpoint user must click **Open Settings** and grant permission before the remote support session can continue.

3. The end-user receives a pop-up asking to accept the incoming connection:




4. If the end user clicks **Yes**, the secure tunnel and just-in-time server session is initialized, and the portal admin is now connected to a Remote Support session – sharing the screen and input (if enabled - see "Specify View Only for portal admin" on page 29) directly in the browser.
5. If the end user clicks **No**, the portal admin request to start a Remote Support session is denied. In any case, all request details are logged in the Auditlog.

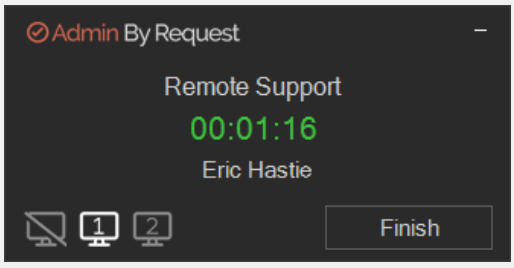
   Once the session starts, a timer appears in the lower, right corner of the screen, showing the amount of time used so far during the session:



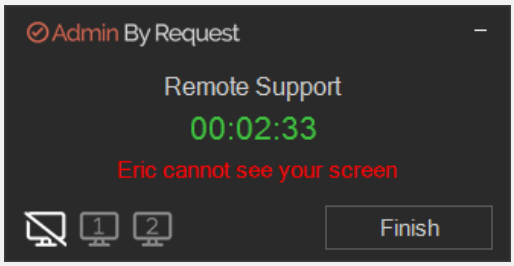

   Click the **Hide** icon at any time to hide the screen from the remote person.

**NOTE**

If the endpoint has multiple monitors, the monitor currently being viewed is indicated (**Monitor 1** in this example). Click a monitor icon to switch the view to that screen:




To hide a screen, simply click the **Hide** icon:



# Unattended behavior for Remote Support

Under **Remote Support Settings > Security > Unattended**, behavior changes as follows:

- **On**: the remote support session can start without an endpoint approval popup.
- **Off**: the endpoint user is asked to approve the remote support session.

This is commonly used for kiosk or shared devices where local interaction is not practical.

**NOTE**

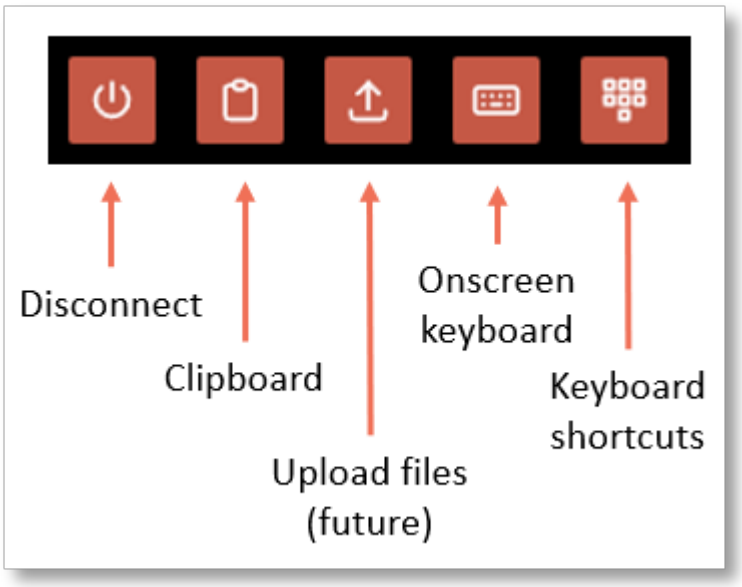
- This feature requires Mac 5.2 or newer and is not yet supported on Windows.
- There is a warning in the portal about the potential data protection exposure created when this setting is **ON**:

> Note that this feature is intended for factory machines or similar where there is no user at the other end. Use in other contexts may raise privacy or data protection concerns and could be subject to applicable laws.

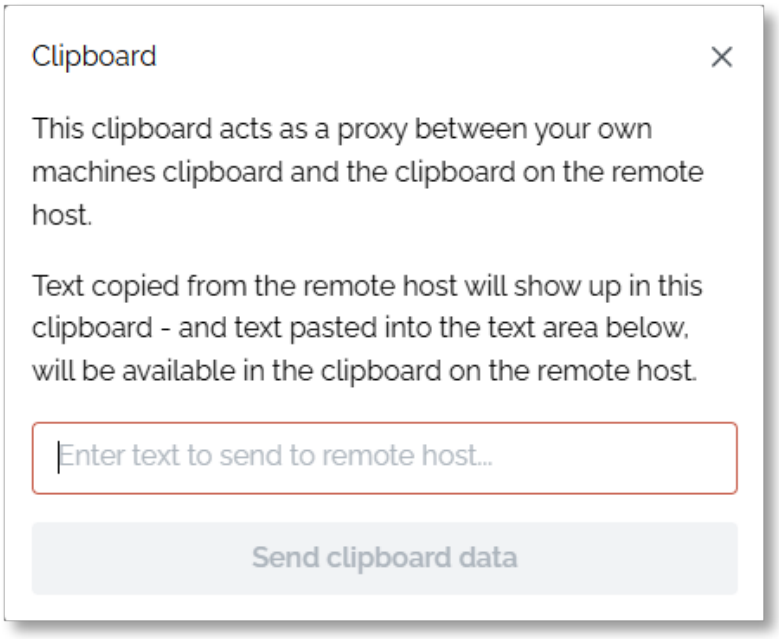
# During a session

Using the remote desktop via the browser is the same as if you were working with it directly, except that there will be a difference in performance, depending on the speed of your connection between the browser and the remote endpoint.

While a remote session is running, an action bar is available for performing some basic tasks:



Most of these are self-explanatory. However, the clipboard works as follows:




**NOTE**
Uploading files is not available at the time of writing.

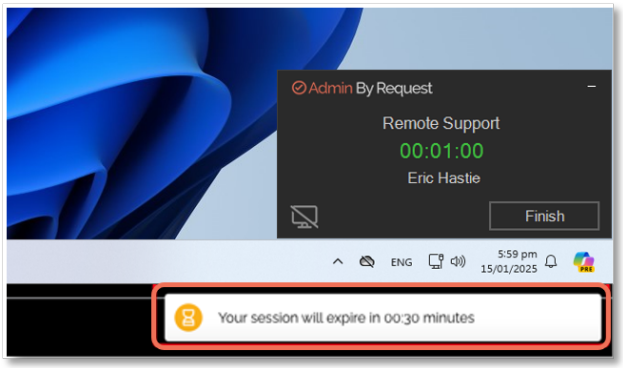
## Ending the session

A Remote Support session can end in a number of ways:

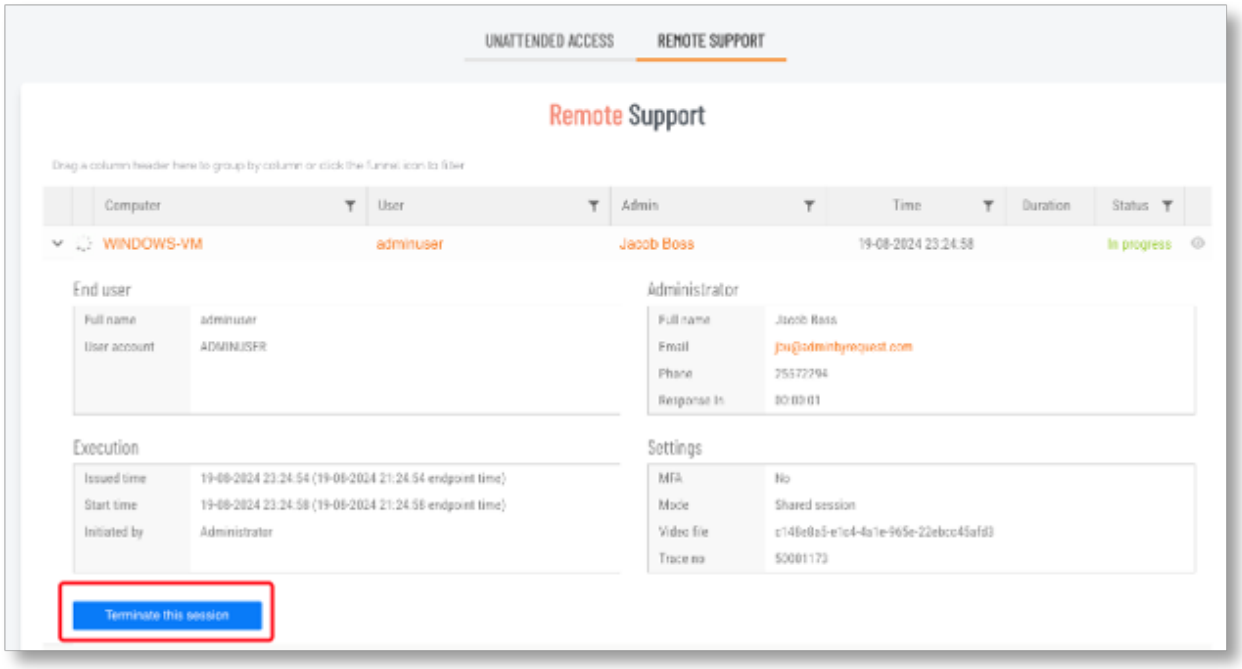
- Either party can end the session by pressing the **Finish** button in the timer window.
- The IT admin (i.e. the user working via a browser) can press the **Disconnect** icon in the action bar of the browser:

*Continued ...*

- If session expiration is enabled (see "Set session expiry" on page 29), the session will be terminated after the set amount of time. When the remaining time gets below 2 minutes, a countdown alert appears:




- By pressing the **Terminate this session** from the auditlog details of an ongoing Remote Support session:




## What next?

Check out "Basic Settings for Remote Support" on page 26 for details on how to setup the following:

- A desktop icon
- Session recordings
- MFA for extra security
- View-only for the portal admin
- Session expiry

# Product Enrollment

## What is Product Enrollment?

Product enrollment is the mechanism of determining which Admin By Request licenses – and hence product capabilities – should be available to specific endpoints.

## How does it work?

In a real-world scenario, a company might have 100 endpoints and the following Admin By Request licenses:

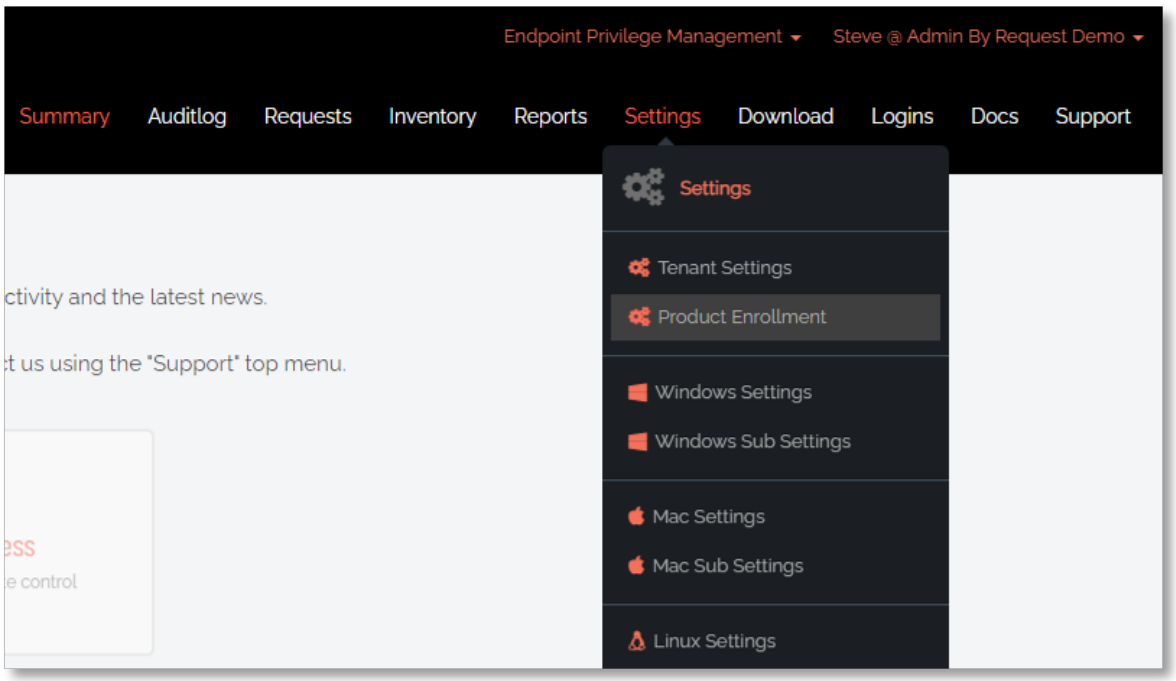
- 100 Endpoint Privilege Management (EPM) licenses
- 50 Secure Remote Access (SRA) licenses

Product enrollment allows the customer to determine which endpoints are activated with an EPM license, an SRA license – or both.

Once an endpoint gets a specific license, the corresponding functionality is instantly available on that endpoint. For example, if an endpoint gets a Secure Remote Access license then this device can now use both Unattended Access and Remote Support.

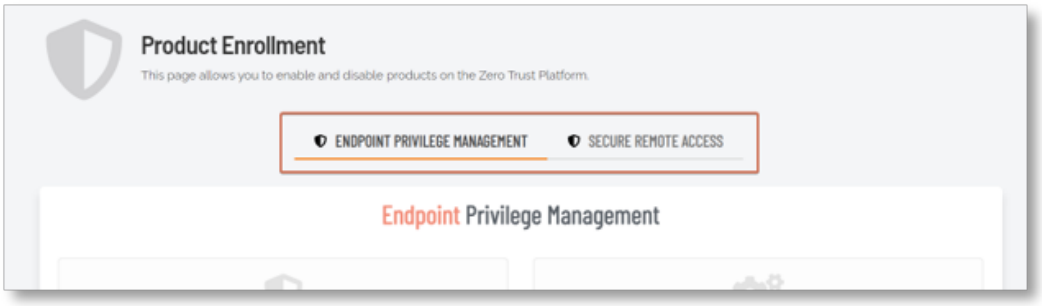
## Getting started with Product Enrollment

All product enrollment takes place from the Product Enrollment menu in the portal (**Settings > Product Enrollment**):




This menu is available from both EPM and SRA views.

The Product Enrollment page provides a way to assign licenses for specific Admin By Request products. The specific product is selected via tabs at the top – currently **ENDPOINT PRIVILEGE MANAGEMENT** and **SECURE REMOTE ACCESS** are available:




From each product tab, it's possible to determine the scope of enrollment for that product, as well as get an overview of the current license usage based on the selection.

## Platform Scope

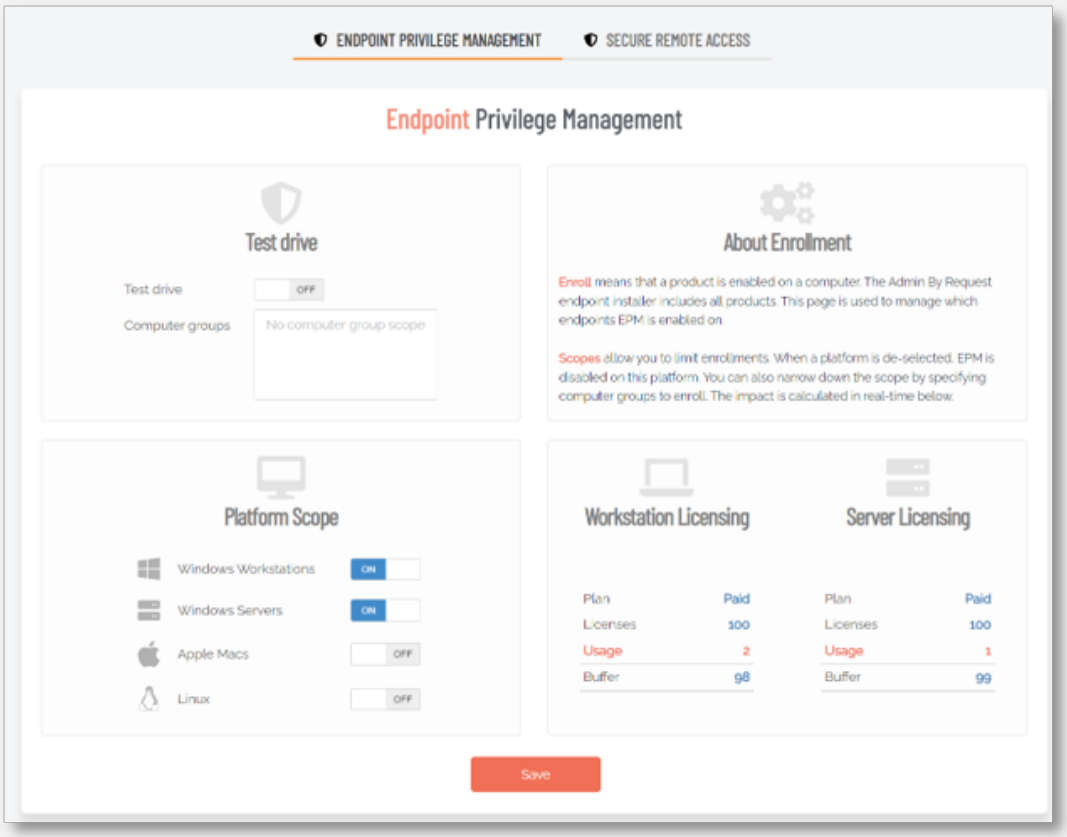
The Platform Scope allows for quickly setting up which inventory groups should have the current product license assigned.

In Example 1, the tenant is set up to have all Windows Workstations and Windows Servers enrolled with the Endpoint Privilege Management product – while Apple Macs and Linux devices won't be able to utilize the EPM functionality.

In Example 2, only Windows Servers and Discovered Devices can be connected remotely via Secure Remote Access.

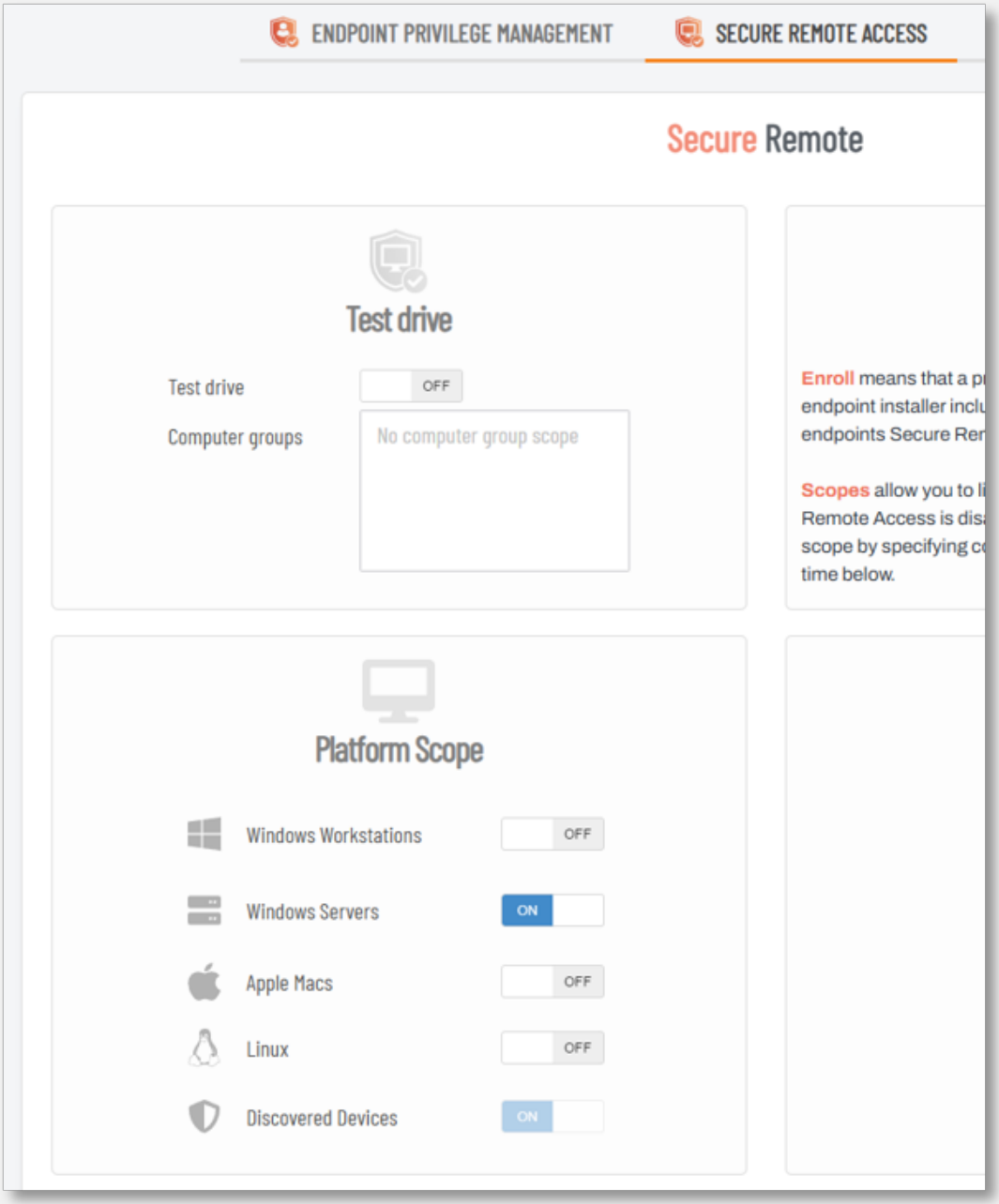
*Continued ...*

## Example 1




*Continued ...*

Example 2




# Licensing overview

The license overview box shows how many licenses are actually used by the current enrollment settings – and how many licenses are left in the pool of purchased licenses.

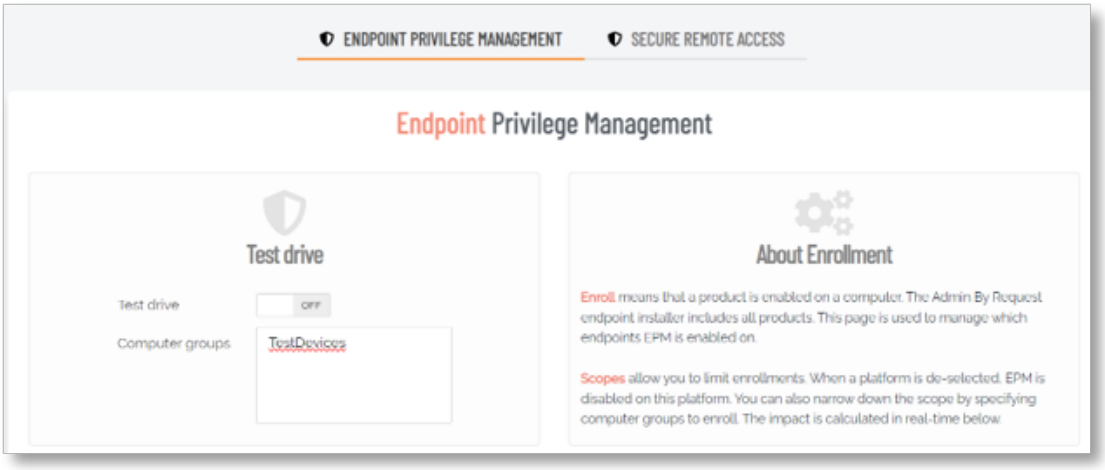
In the example above, the tenant has 100 licenses for both Workstation and Server – and the current selected enrollment uses 2 Workstation licenses and 1 Server license – leaving the tenant with a buffer of 98 for Workstation and 99 for Server Edition.

# Test Drive

The Test Drive mode allows a portal user to cherry pick which devices are enrolled with the selected product. This can either be done by specifying a computer group scope or by manually picking devices.

## Scope by computer groups

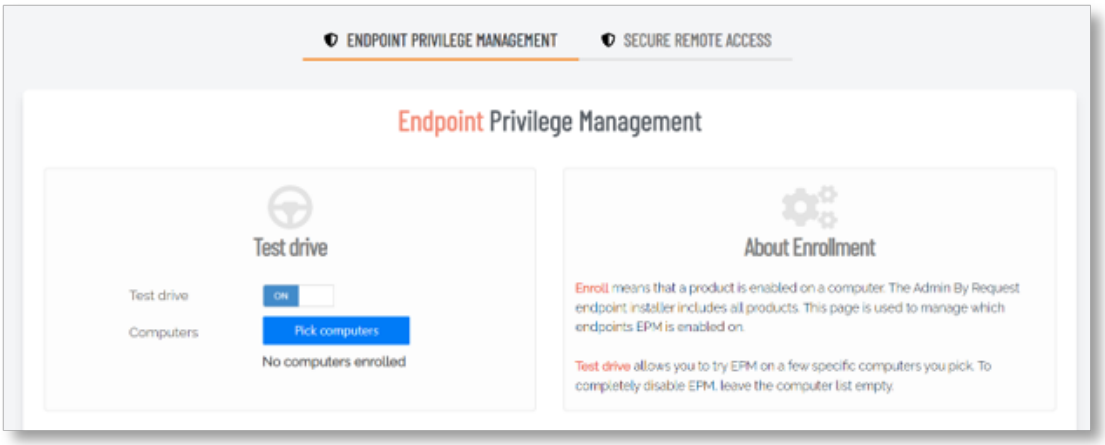
To apply the scope only to devices within specific computer groups, enter the group names into the "Computer groups" box:




In this example, the enrollment will affect only devices in the group "TestDevices".

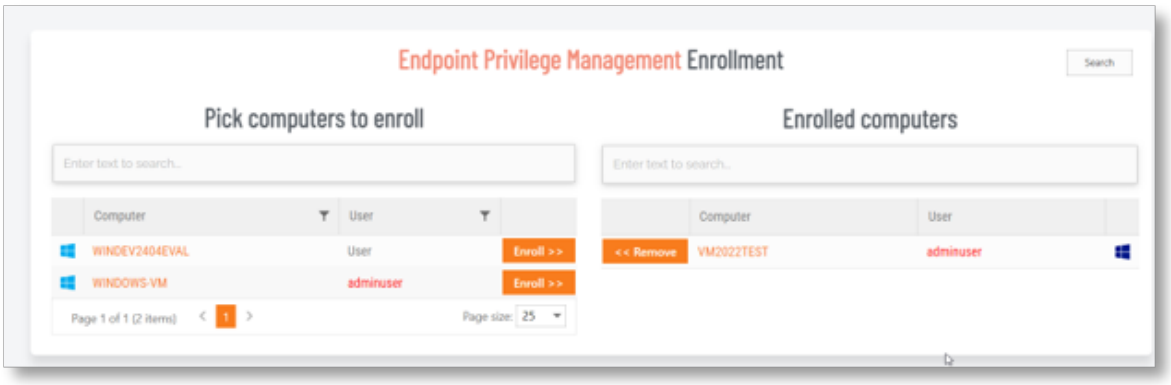
## Scope by manual selection

To manually pick which devices should be enrolled, the Test Drive switch can be turned **On**:




*Continued ...*

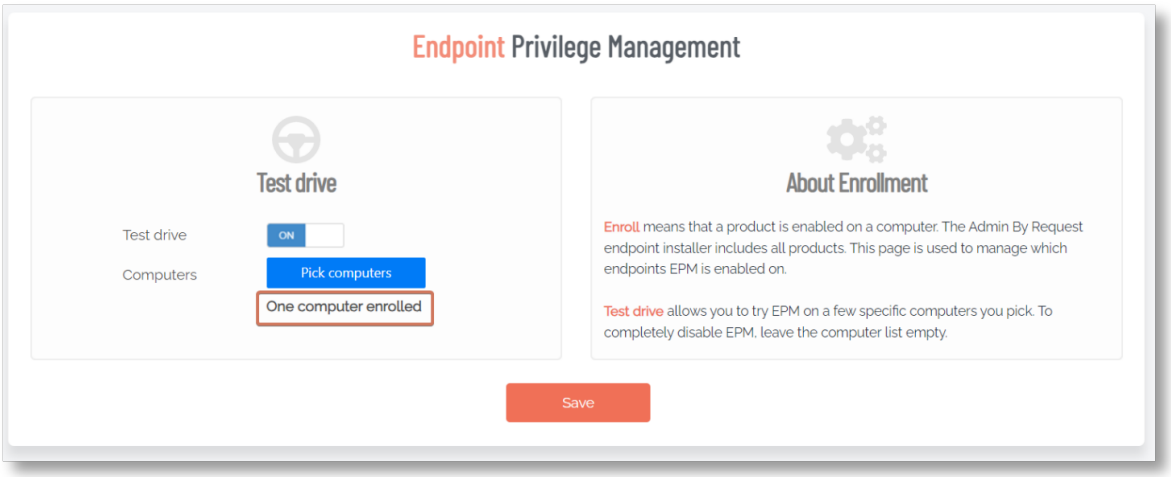
The **Pick computers** button is now available and allows for manual selection of the devices to enroll into the selected product:




In this example, the device named **VM2022TEST** has been enrolled with Endpoint Privilege Management, while the devices on the left have not.

To enroll devices, click the **Enroll >>** button for the specific device. To remove a device, click the **<< Remove** button for the device.

Going back to the enrollment page now shows the following license usage for the tenant:




Allowing for test driving Endpoint Privilege Management for the single selected device.

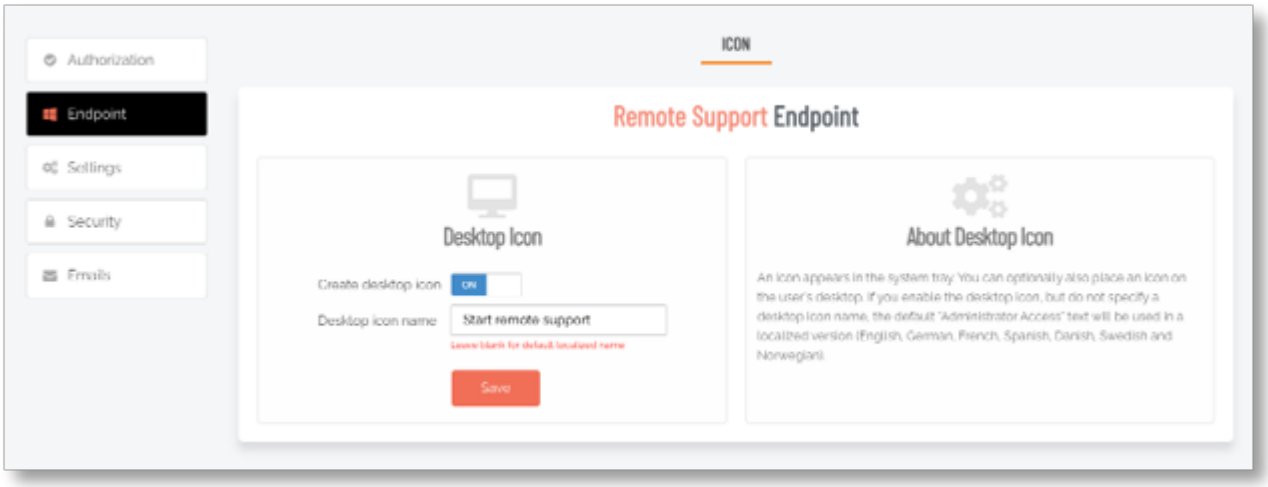
Please be aware that turning test drive on or off will cause licenses to be removed from non-selected devices. Only use the test drive feature if you manually want to pick the devices to enroll.

# Basic Settings for Remote Support

## Set desktop icon

To create a desktop icon on devices that support Remote Support, navigate to the Remote Support Settings and select the "Endpoint" tab.

From here, the "Create desktop icon" setting can be enabled or disabled:



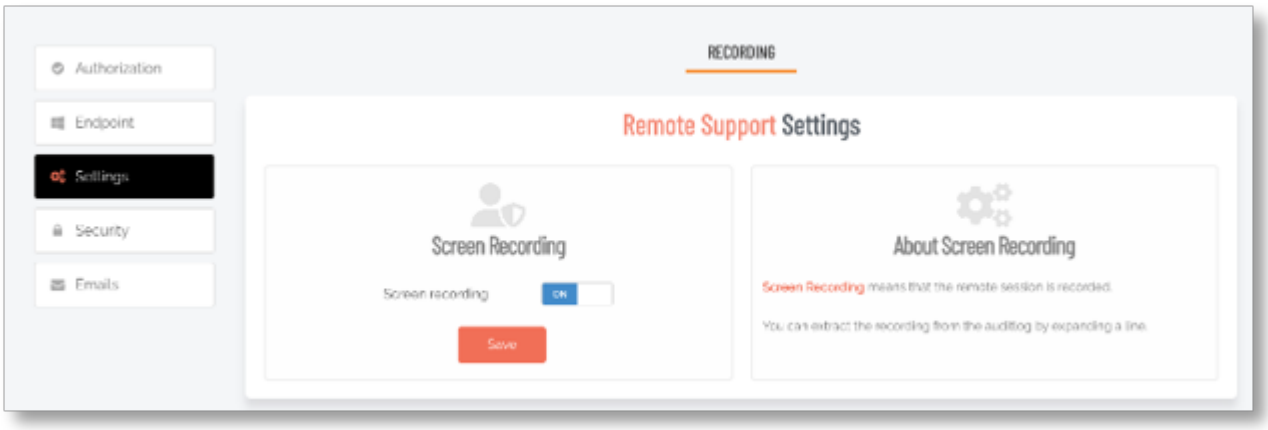

Enabling the setting will create a desktop icon on the affected devices with the supplied desktop icon name. If no name is supplied, a default localized name is used:


Note that a Tray Tool menu item is always created for Remote Support.

Refer to "Endpoint" on page 32 (ICON) for more information.

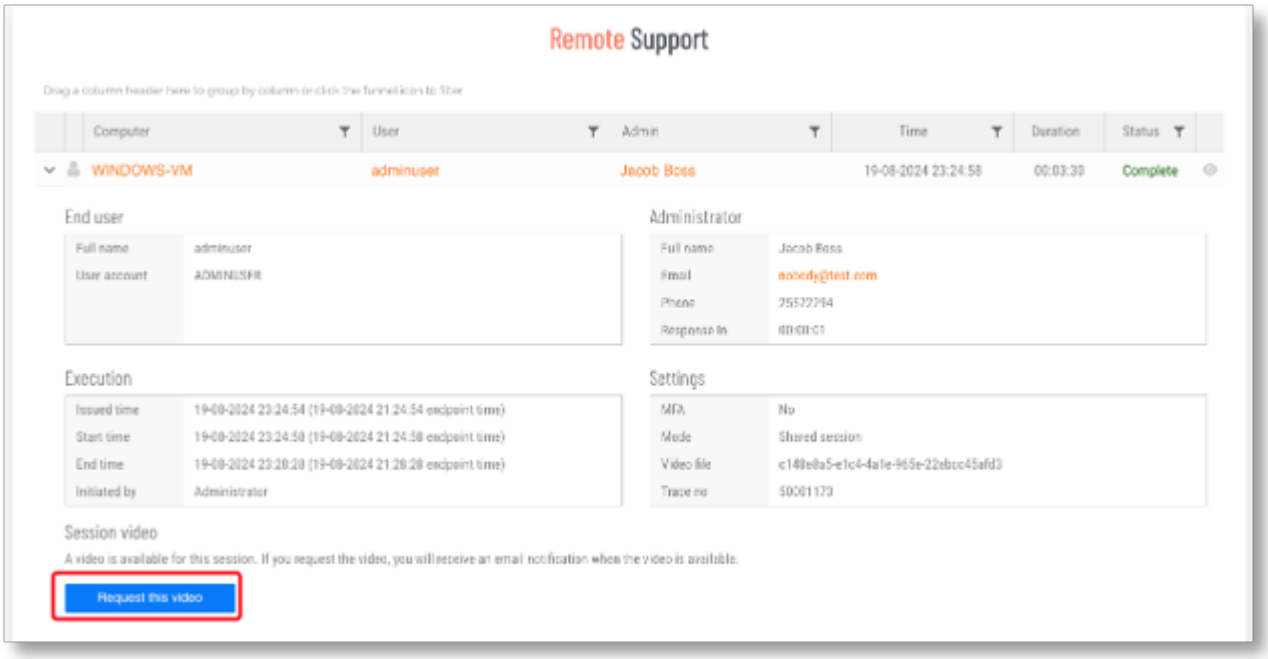
# Enable session recording

Session recordings can be enabled or disabled from the "Settings" tab under the Remote Support Settings:




Enabling the session recordings creates a screen recording of all Remote Support sessions done under this setting scope.

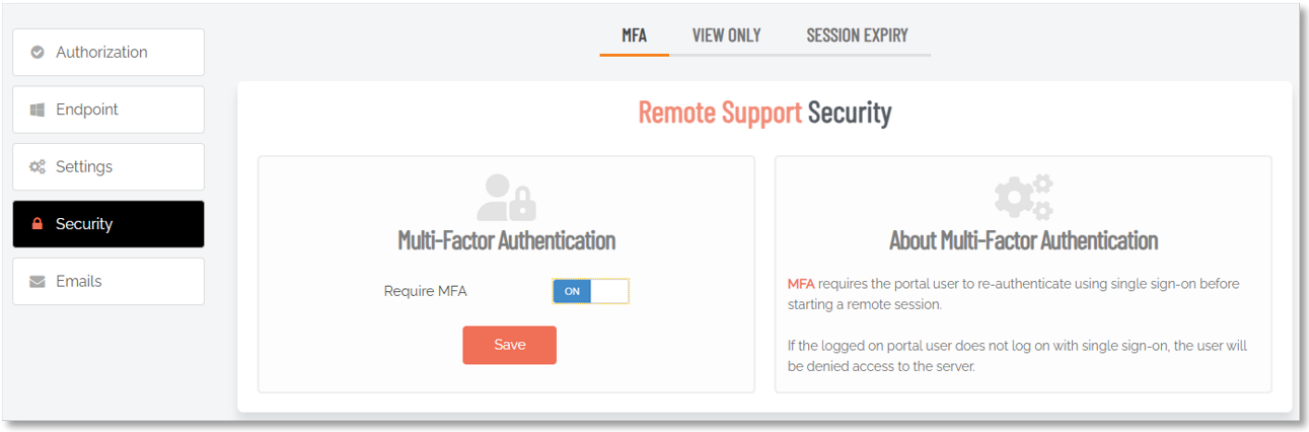
Recordings can be requested via the auditlog after a session has ended by clicking the **Request this video** button under the auditlog entry:



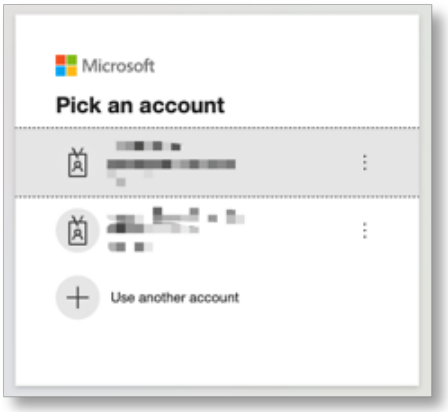

Refer to "Settings" on page 32 (RECORDING) for more information.

# Require Multi-Factor Authentication

Enabling the "Require MFA" setting will require the portal user to re-authenticate using MFA before being able to start any Remote Support session (both end-user and portal user initiated):




With MFA enabled, the portal user will be met with the Microsoft account login screen:



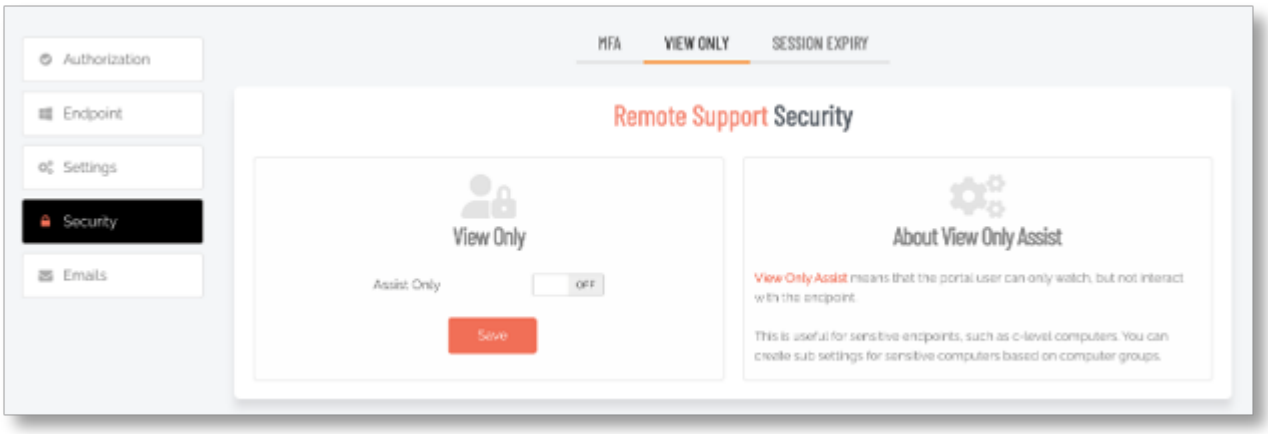

This is a required step before being able to proceed to initiating the Remote Support session with the endpoint.

**NOTE**
Using the MFA setting requires the portal user to be signed into the portal using SSO.

Refer to "Security" on page 33 (MFA) for more information.

# Specify View Only for portal admin

To have Remote Support sessions be view-only (meaning that the portal admin can only view the screen but not control mouse or keyboard), the **View Only** setting can be enabled:

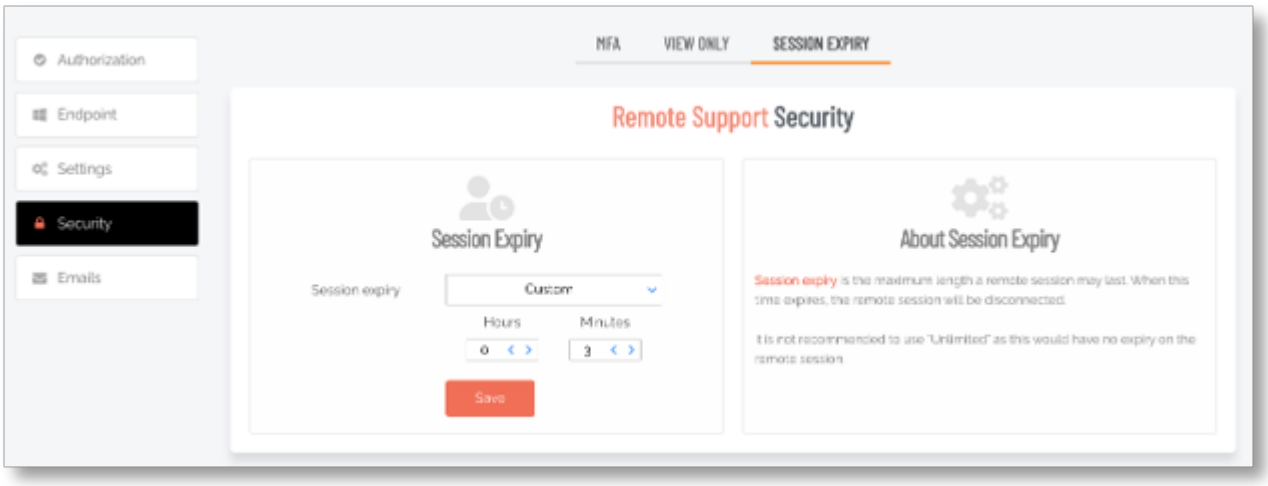



Upon enabling this setting, all Remote Support session made from this setting scope will be screensharing only but with no control over mouse or keyboard. This is particularly useful when supporting sensitive endpoints like e.g. C-level devices.

Refer to "Security" on page 33 (VIEW ONLY) for more information.

# Set session expiry

To prevent sessions from being “forgotten” and therefor run forever, the session expiry setting can be used:




By setting a session expiry setting, all Remote Support sessions that fall under this setting scope will automatically be disconnected after the selected amount of time has expired.

The connected users will get a countdown warning when the remaining time gets below 2 minutes.

To disable session expiration, select “Unlimited” as the expiration value.

Refer to "Security" on page 33 (SESSION EXPIRY) for more information.

# Portal Administration for Remote Support

## Introduction

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

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

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

To change any of the settings in the portal, log in to the portal and select the setting from the menu.

## In this topic

# Remote Support Settings

Portal menu: **Secure Remote Access > Settings > Remote Support Settings**

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

## Authorization

Portal menu: **Secure Remote Access > Settings > Remote Support Settings > Authorization**

### AUTHORIZATION tab

*Remote Support* allows users to remotely assist other users with issues. It is often combined with the EPM feature *Support Assist* to perform installs without logging the user out and without giving the user admin rights.

*Remote Support* requires Windows endpoint software **8.4+** and is part of the Secure Remote Access product suite.

| Setting | Type | Description |
|---|---|---|
| Allow Remote Support | Toggle<br>On \| Off<br>Default: **On** | **On** - Allows computers to be accessed remotely, provided a user is present (i.e. remote user must confirm).<br>Note that supporting user might only be able to watch and not take control (see Security settings (VIEW ONLY tab)).<br>**Off** - Computers cannot be accessed remotely regardless of whether a user is present or not.<br>Note that *Unattended Access* might still be possible, depending on Unattended Access settings. |
| **Save** | Button | Saves customization and changes to any fields.<br>Note that reloading any defaults does not take effect until **Save** is clicked. |

### NOTIFICATION tab

Email notification to administrators is available when *Require approval* is checked under Authorization.

Notifications can be sent for the following scenarios:

- Each new request for approval (*Run As Admin*) or admin session access (*Admin Session*)
- When malware is detected (Workstation Settings > [OS] Settings > Malware)
- When unattended remote access is requested (*Unattended Access*)
- When either an end user or portal admin initiates a *Remote Support* session.

As with other request types, new requests for approval always appear under **Requests > Pending** in the Portal top menu. This is the case for both Endpoint Privilege Management and Secure Remote Access.

The *Notification* setting enables and configures **additional email notification** for new requests. If multiple email addresses are specified, they must be on separate lines.

**NOTE**
Phone notification is separate and happens automatically via push notifications to phones with the mobile app installed.

| Setting | Type | Description |
|---|---|---|
| Send email notifications | Toggle<br>On \| Off<br>Default: **Off** | **On** - Additional email notifications are sent to the email addresses listed in *Email addresses*.<br>**Off** - Email notifications are not sent. |
| Email addresses | Text | Standard email address format. Use a new line for each address. |
| **Save** | Button | Saves customization and changes to any fields.<br>Note that reloading any defaults does not take effect until **Save** is clicked. |

## Endpoint

Portal menu: **Secure Remote Access > Settings > Remote Support Settings > Endpoint**

### ICON tab

An icon for Remote Support appears in the system tray at install time.

This setting lets you optionally also place an icon on the user's desktop. If you enable the desktop icon, but do not specify a desktop icon name, the default "Administrator Access" text will be used in a localized version (English, German, French, Spanish, Danish, Swedish and Norwegian).

| Setting | Type | Description |
|---|---|---|
| Create desktop icon | Toggle<br>On \| Off<br>Default: **On** | **On** - Place icon on the desktop.<br>**Off** - Do not place icon on the desktop. Only the tray tool icon will be available.<br>. |
| Desktop icon name | Text | Label to use for the icon. If left blank, **Administrator Access** is used as the label. |
| **Save** | Button | Saves customization and changes to any fields.<br>Note that reloading any defaults does not take effect until **Save** is clicked. |

## Settings

Portal menu: **Secure Remote Access > Settings > Remote Support Settings > Settings**

### RECORDING tab

Screen recording means that the remote session is recorded.

Files are stored locally and can be requested in the auditlog by expanding the relevant line.

| Setting | Type | Description |
|---|---|---|
| Screen recording | Toggle<br>On \| Off<br>Default: **Off** | **On** - Screen recording is enabled.<br>**Off** - Screen recording is disabled. |
| **Save** | Button | Saves customization and changes to any fields.<br>Note that reloading any defaults does not take effect until **Save** is clicked. |

## Security

Portal menu: **Secure Remote Access > Settings > Remote Support Settings > Security**

### MFA tab

MFA (Multi-Factor Authentication) requires the portal user to re-authenticate with single sign-on when connecting remotely to an endpoint.

If the logged-on portal user does *not* log on with SSO (single sign-on), the user will be denied access to the endpoint.

| Setting | Type | Description |
|---|---|---|
| Require MFA | Toggle<br>On \| Off<br>Default: **On** | **On** - The logged-on portal user must authenticate via SSO when connecting remotely to an endpoint.<br>**Off** - Portal user does not need to authenticate via SSO to remotely connect. |
| **Save** | Button | Saves customization and changes to any fields.<br>Note that reloading any defaults does not take effect until **Save** is clicked. |

### VIEW tab

View Only means that the portal user can watch, but not interact with the endpoint.

This is useful for sensitive endpoints, such as c-level computers. You can create sub settings for sensitive computers based on computer groups.

| Setting | Type | Description |
|---|---|---|
| Assist Only | Toggle<br>On \| Off<br>Default: **On** | **On** - The portal user can only watch, but not interact with the endpoint.<br>**Off** - Portal user can take control of screen and keyboard during a session. |
| **Save** | Button | Saves customization and changes to any fields.<br>Note that reloading any defaults does not take effect until **Save** is clicked. |

### SESSION EXPIRY tab

Session expiry is the maximum length a remote session may last. When this time expires, the remote session will be disconnected.

**NOTE**
Selecting **Unlimited** is not recommended, as this would result in no expiry on the remote session.

| Setting | Type | Description |
|---|---|---|
| Session expiry | Selection<br>Default: **4 hours** | Select a value between **15 minutes** and **Unlimited**.<br>**Custom** is also available - if selected, choose the required number of **Hours** and **Minutes**. |
| **Save** | Button | Saves customization and changes to any fields.<br>Note that reloading any defaults does not take effect until **Save** is clicked. |

## Emails

Portal menu: **Secure Remote Access > Settings > Remote Support Settings > Emails**

Emails go out when *Require approval* is turned **On** under . You can create your own email templates here with information specific to your company, such as a Help Desk phone number and custom instructions.

| Setting | Type | Description |
|---|---|---|
| Email template | Selection<br>Default: **Run As Admin: Approved email** | **Run As Admin \| Admin Session: Approved email** - Loads a template that advises *the user* (i.e. requester) that the request for access has been approved.<br>**Run As Admin \| Admin Session: Denied email** - Loads a template that advises the request for access has been denied without giving a reason.<br>**Run As Admin \| Admin Session: Denied with reason** - Loads a template that advises the request for access has been denied and provides the reason.<br>**Admin notify: New request** - Loads a template that advises *the administrator* (i.e. person who approves or denies) that a request for access is waiting for attention.<br>**Admin notify: Malware detected** - Loads a template that advises *the administrator* that malware has been detected, including a link to the Auditlog. |
| Email sender | Text<br>Default: **Admin By Request Team** | The email address to be used as the sender for the email. Can be used with custom domains. Use the **Email address** button to set up custom domains.<br>Refer to Email Domain for more information on configuring an email address to be used as the sender for all user notifications. |
| Email subject | Text | Text that will appear in the subject line of emails. |

| Setting | Type | Description |
|---|---|---|
| | Default: **Admin By Request** | |
| **Get default** | Button | Loads the default *Email template* for the option selected.<br>**NOTE:**<br>• Default email templates are created by Admin By Request. Contact us if you wish to customize a default email template.<br>• Using this button will **overwrite** any customization you might have done in the *Template body*. |
| **Email address** | Button | Switches to Email Domain in Tenant Settings in the portal, allowing you to use a custom domain as the sender.<br>This allows sending email from domains other than @adminbyrequest.com.<br>**NOTE:**<br>This is optional, but you cannot add an email sender field of e.g. "tom@mydomain.com" *unless* you have first set up the custom email domain "mydomain.com" via the *Email Domain* setting in the portal (**Settings > Tenant Settings > Email Domain**). |
| Template body | Formatted text | The body of the email to be sent.<br>Includes three views:<br>• **Design**: WYSIWYG view of content. Enter and format body text here.<br>• **HTML**: The same content in HTML format. Can also be edited if necessary and changes will be reflected in Design and Preview.<br>• **Preview**: What the recipient sees. Read only - switch to Design view to make changes.<br>**Dynamic content tags**<br>Tags can be used in the body, which are place holders in curly braces. These are replaced with actual request values when emails are sent.<br>The following tags are available:<br>• {UserFullName} Name of requesting user<br>• {UserEmail} Email address of requesting user<br>• {UserPhone} Phone number of requesting user<br>• {UserReason} Reason the requesting user gave<br>• {DenyReason} Admin's reason for denial (only used for denial with reason)<br>• {ComputerName} Name of requesting computer<br>• {AdminUserName} Name of administrator receiving notification (only for admin notify) |
| **Save** | Button | Saves customization and changes to any fields. |

| Setting | Type | Description |
|---|---|---|
| | | Note that reloading any defaults does not take effect until **Save** is clicked. |

You can set up an email notification to your ticketing system and embed the tags below for dynamic content.

| Setting | Type | Description |
|---|---|---|
| Ticket system email | Text | The email address to which emails intended for your ticket system will be sent.<br>For example: **itsupport@mycompany.com** |
| Email sender | Text<br>Default: **Admin By Request Team {ID}** | The email address to be used as the sender for the email. Can be used with custom domains. Use the **Email address** button to set up custom domains. |
| Email subject | Text<br>Default: **Admin By Request** | Text that will appear in the subject line of emails. |
| **Get default** | Button | Loads the default *Email template* for the option selected.<br>**NOTE:**<br>• Default email templates are created by Admin By Request. Contact us if you wish to customize a default email template.<br>• Using this button will **overwrite** any customization you might have done in the *Template body*. |
| **Email address** | Button | Switches to Email Domain in Tenant Settings in the portal, allowing you to use a custom domain as the sender.<br>This allows sending email from domains other than @adminbyrequest.com.<br>**NOTE:**<br>This is optional, but you cannot add an email sender field of e.g. "tom@mydomain.com" *unless* you have first set up the custom email domain "mydomain.com" via the *Email Domain* setting in the portal (**Settings > Tenant Settings > Email Domain**). |
| Template body | Formatted text | The body of the email to be sent to the ticketing system.<br>Includes three views:<br>• **Design**: WYSIWYG view of content. Enter and format body text here.<br>• **HTML**: The same content in HTML format. Can also be edited if necessary and changes will be reflected in Design and Preview.<br>• **Preview**: What the recipient sees. Read only - switch to Design view to make changes. |

| Setting | Type | Description |
|---|---|---|
| | | **Dynamic content tags**<br>Tags can be used in the body, which are place holders in curly braces. These are replaced with actual request values when emails are sent.<br>The following tags are available:<br>• {ID} Unique auditlog trace no<br>• {APIID} ID for looking up this entry through the public Auditlog API<br>• {Status} Requested, Approved, Denied, Started, Finished<br>• {UserFullName} Name of the requesting user<br>• {UserEmail} Email address of requesting user<br>• {UserPhone} Phone number of requesting user<br>• {UserReason} Reason the requesting user gave<br>• {DenyReason} Admin's reason for denial<br>• {ComputerName} Name of requesting computer<br>• {AdminUserName} Admin approving or denying request<br>• {InstallList} Installed programs<br>• {UninstallList} Uninstalled programs<br>• {AuditlogURL} URL to this entry in the auditlog<br>• {RequestURL} URL to this entry in requests<br>**Ticket ID**<br>You can find a ticket by its ticket ID using the **Search** button in the Auditlog.<br>**Voided text**<br>If a line has one or more tags and all tags in the line are empty, the entire line is automatically removed. |

# Sub Settings

Portal menu: **Secure Remote Access > Settings > Remote Support Sub Settings**

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.

## Overruling a global setting

As with sub-settings for EPM servers and workstations, SRA sub-settings mirror their respective global settings, with the addition of an **Overrule global settings** switch.

The following table lists the settings and sub-settings structure for both Unattended Access and Remote Support:

| Unattended Access | Remote Support |
|---|---|
| Authorization | Authorization |
| Settings | Endpoint |
| Security | Settings |
| Gateways | Security |
| Emails | Emails |

Each of these can be on or off, which is controlled by a *Global Settings Overrule*:

| Setting | Type | Description |
|---|---|---|
| Overrule global settings | Toggle<br>On \| Off<br>Default: **On** | **On** - This setting will overrule its associated global setting.<br>The global setting fields are then undimmed and become available for editing.<br>**Off** - This setting will not overrule its associated global setting.<br>The global setting fields remain dimmed. |

## Scope for sub-settings

The key to sub-settings is to define and activate their **Scope**.

In the portal sub-settings, Scope is the second-top menu item, immediately below the **< Back** button.

| Setting | Type | Description |
|---|---|---|
| Active | Toggle<br>On \| Off<br>Default: **Off** | **On** - Sub-settings are active for the set named in *Sub settings name*.<br>**Off** - Sub-settings are not active .for the set named in *Sub settings name*. |
| Sub settings name | Text | The name assigned to this set of sub-settings. |
| Portal user in group | Text | A list of groups into which users are placed, with multiple groups on separate lines. |
| Computer in group | Text | A list of groups into which computers are placed, with multiple groups on separate lines. |
| Computer in OU | Text | A list of organizational units into which computers are placed, with multiple OUs on separate lines. |
| Network scope | Toggle<br>On \| Off<br>One entry for each Gateway<br>Default: **Off** | **On** - Scope is active for this gateway.<br>**Off** - Scope is not active for this gateway.<br>Network scope means that these sub settings only apply to the selected gateway combination. A gateway represents an on-premise LAN - if no toggles are on, there is no network scope. |
| **Save** | Button | Saves customization and changes to any fields.<br>Note that reloading any defaults does not take effect until **Save** is clicked. |

## About sub-settings scope

Note the following:

- *Tiering* can be achieved by setting up a gateway on each tier and set portal user and sub settings network scopes.
- Computer scope does not work for discovered devices, because the server endpoint software is required to collect groups and OUs.
- Entra ID / Azure AD groups require you to set up the Entra ID Connector.
- All scopes must be met. If multiple user groups and computer Organizational Units (OUs) are specified, the user must be member of at least one of the groups and the computer in one of the OU locations.

In the portal text fields, multiple groups or OUs (Organizational Units) must be specified on separate lines. OUs can be specified as either:

- The bottom name, e.g. **Sales**. Any OU named Sales will match.
- Path from root using backslashes, e.g. **\US\Florida\Sales**.
- The fully distinguished name, e.g. **C=US,ST=Florida,OU=Sales**.

# Document History

| Document | Product | Changes |
|---|---|---|
| 6 September 2024<br>**1.0** | August 2024 | Initial document release. |
| 4 October 2024<br>**1.1** | August 2024 | Adjusted api URLs in *Prerequisites* section of chapter "Overview" so they point to the correct data center locations. |
| 29 November 2024<br>**1.2** | August 2024 | Added process flow steps and diagram to chapter "Remote Support Overview". |
| 20 January 2025<br>**1.3** | January 2025 | Added descriptions of screen-hide and multiple monitor capabilities to chapter "Getting Started with Remote Support".<br>Updated session timer screenshots to reflect change of button name from **Done** to **Finish**. |
| 20 February 2025<br>**1.4** | February 2025 | Updated *Prerequisites* in chapter "Overview" to increase number of outbound MQTT broker nodes from two to ten for each data center. |
| 24 February 2025<br>**1.5** | February 2025 | Corrected UDP / QUIC port number. |
| 25 February 2025<br>**1.5.1** | February 2025 | Corrected UDP / QUIC port number - both processes, steps 4 & 5, pages 3 & 4. |
| 4 March 2025<br>**1.5.2** | February 2025 | Removed the prerequisite for RDP needing to be enabled on port 3389. |
| 22 December 2025<br>**1.6** | February 2025 | Added how to determine your data location to *Data Location* section in chapter "Remote Support Overview".<br>Added note to the same chapter advising access is available only from Windows clients at this time. |
| 16 February 2026<br>**2.0** | February 2026 | Updated procedures to accommodate new features in Mac 5.2.<br>Added installation of endpoint client as first task in chapter "Getting Started". |
| 16 March 2026<br>**2.1** | February 2026 | Modified procedures for connecting remotely to endpoints in chapter "Getting Started". |

# Index

# N



# O



# P



# R



# S



# T



# V