Secure Remote Access (SRA) | Vendor Access

Vendor Access: IT Admin Guide

Document Information

Code:	**PM-VEN-ITAG**
Version:	**1.2**
Date:	**24 February 2025**

Admin By Request

ZERO TRUST PLATFORM

Copyright © 2025 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

Vendor Access Overview

What is Vendor Access?

Vendor Access is a feature of Admin By Request's Secure Remote Access product that allows *external* users, such as third-party vendors, to be given *secure access to internal devices*. This access is managed entirely through their local Internet browser app - there is no need for any additional locally installed software.

Related information

- Unattended Access
- Remote Support

Prerequisites

The main prerequisite for *Vendor Access* applies to Single Sign-On, where **SSO must be enabled for each user** who will login to the *Vendor Access* page (https://access.work).

Additional requirements depend on whether or not you are using Cloudflare's managed service as a gateway, or hosting your own on-premise gateway. These requirements are covered below and are the same as those outlined in the *Unattended Access* and *Remote Support* IT Admin Guides.

Prerequisites are listed under these headings:

- Data location
- Cloud gateway (managed service)
- On-premise gateway (self-hosted)

Data location

Your data is stored in a data center that is located in one of two geographic locations - one in Europe and one in the USA.

To determine your data center, go to page Tenant Settings > API Keys in the portal and check which API prefix is shown under **About API Keys**. The API prefix will be one of the following:

- **https://dc1api.adminbyrequest.com** (Europe)
- **https://dc2api.adminbyrequest.com** (USA)

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.

Cloud gateway (managed service)

- Access to the portal at **https://www.adminbyrequest.com/Login**
- Admin By Request for **Windows 8.4.0+** on each client
- Admin By Request API - port **443** for the following:
  - **api1.adminbyrequest.com** (if your data is located in Europe)
  - **api2.adminbyrequest.com** (if your data is located in the USA)
  - **api.adminbyrequest.com**
- Outbound MQTT broker connectivity via Websockets- port **443** for the following:
  - If your data is located in Europe:
    ten nodes (**FastTrackHubEU1.azure-devices.net** to **FastTrackHubEU10.azure-devices.net**)
  - If your data is located in the USA:
    ten nodes (**FastTrackHubUS1.azure-devices.net** to **FastTrackHubUS10.azure-devices.net**)
- 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.

- The endpoint needs to be enrolled with an Admin By Request Secure Remote Access license (see Product Enrollment).
- For Windows endpoints, RDP needs to be enabled on port **3389** on each device.

On-premise gateway (self-hosted)

- Access to pull Docker images from **adminbyrequest.azurecr.io**
- Admin By Request API - port **443** for the following:
  - **connectorapi1.adminbyrequest.com** (if your data is located in Europe)
  - **connectorapi2.adminbyrequest.com** (if your data is located in the USA)
- Outbound MQTT broker connectivity via Websockets- port **443** for the following:
  - If your data is located in Europe:
    ten nodes (**FastTrackHubEU1.azure-devices.net** to **FastTrackHubEU10.azure-devices.net**)
  - If your data is located in the USA:
    ten nodes (**FastTrackHubUS1.azure-devices.net** to **FastTrackHubUS10.azure-devices.net**)
- 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.

- In order for the on-premise gateway to be able to discover devices on the network, these need to be available to the gateway on ports **3389** (RDP), **22** (SSH) or **5900/5901** (VNC).

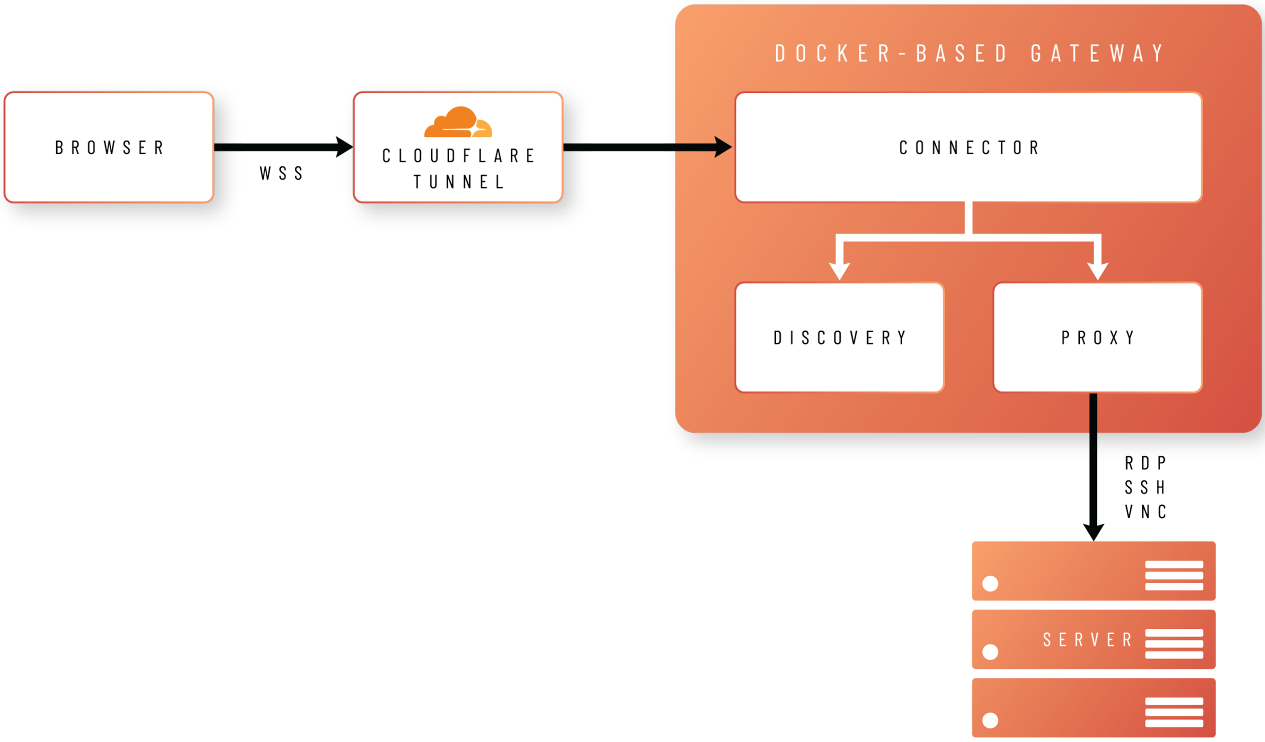
How does Vendor Access work?

Architecture

The idea behind *Vendor Access* is to allow users to connect to your remote endpoints using nothing but their browsers.

In order to achieve this, the browser creates a Secure WebSocket connection to a Docker-based gateway, hosted either in your own infrastructure (self-hosted) or as a managed service.

The connection is made via a secure Cloudflare tunnel, as shown in the following diagram:



The gateway comprises three different images:

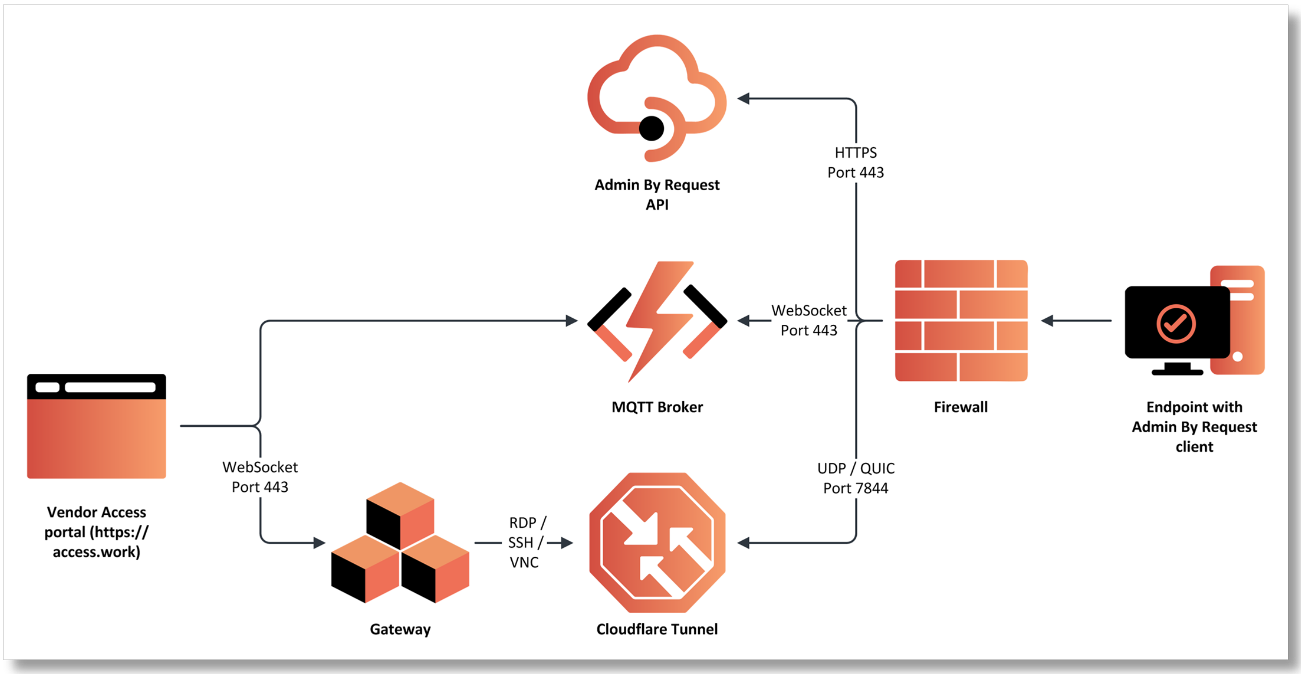
- **Connector**
  Handles validation and translation of the data between the portal and the proxy container, as well as managing logs, health checks and other data.
- **Proxy**
  Establishes a protocol connection between Admin By Request and your endpoint using either RDP, SSH or VNC.
- **Discovery**
  Handles automatic discovery of connectable devices running on the same network as the gateway.

Process

The process by which a user establishes a Vendor Access session is:

1. The user initiates a connection from **https://access.work**.
2. The **Admin By Request client** on the target endpoint receives an instruction from the **MQTT Broker** to fetch settings using the **Admin By Request API**.
3. The settings response instructs the **Admin By Request client** to open a **Cloudflare Tunnel** by making an outbound UDP call on port 7844 using the QUIC Protocol.
4. The **Gateway** is instructed to forward the RDP, SSH or VNC connection through the tunnel opened by the endpoint.
5. A secure WebSocket connection is established between the user's browser and the **Gateway**. The response stream from the RDP, SSH or VNC connection is routed back to the browser using this secure connection.

The process is illustrated in the following diagram:



What next?

This document describes how to get started with *Vendor Access*. It also provides a link to a 3-minute video of how to establish a session and explains key portal login settings relevant to Vendor Access users.

Using Vendor Access

Introduction

Vendor Access, also known as *access.work* (https://access.work), is a feature of Secure Remote Access that allows users to connect to devices through their browsers *without* needing access to the Admin By Request Portal.

Quick setup

To quickly start using access.work, do the following:

A. If you haven't already, enable *Unattended Access* and choose either a manged service or a self-hosted implementation (managed service is a quicker setup).
B. Make sure users that will sign-in with access.work are configured in the portal for SSO (.**Logins > Single Sign-on Setup**).
C. Head to access.work in your browser and sign in with SSO.

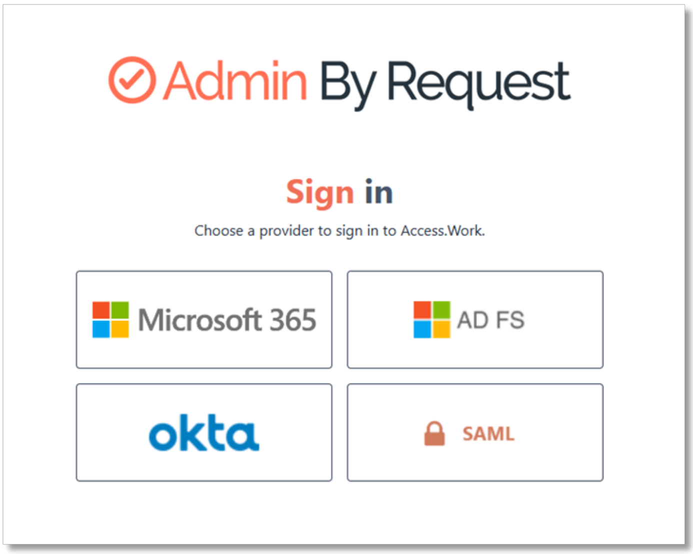
In more detail

These steps provide more information about analyzing your inventory computers, configuring remote access gateways and setting-up your users with the correct access:

1. Log in to the Admin Portal at https://www.adminbyrequest.com/Login and check your computer inventory.
2. Check your remote access gateways at **Secure Remote Access > Settings > Unattended Access Settings > Gateways > CLOUD**, including the computers that are accessible through them. You should be able to correlate computers in the inventory with computers you want accessible via remote access.
3. Go to **Logins > User Logins** and check that you have setup user logins correctly (i.e. with the appropriate access and via the appropriate gateway). Use the **Preview** link alongside a user in the list of users to make sure each can access only the computers expected.

> **NOTE**
> The **Preview** link appears only if a scope is created for the user (**SCOPE** tab). If no scope is created, the user will have access to all computers controlled by the gateway.

4. As a test user, go to access.work in a browser and log in using one of the SSO options:


Admin By Request

Sign in

Choose a provider to sign in to Access.Work.

5. Once logged-in, verify the available computers - these should match what you expect from step 3. If not, recheck the settings under **Logins > User Logins**, **EDIT** user, **SCOPE** tab, *Network Scope*.

   Don't forget to **Save** if making changes.
6. In the browser, refresh the list of remote computers and verify you can see the computers you expect to see.
7. Connect to a remote computer using the **Connect** button:
   - If a *key* icon is visible, credentials are required to log in.
   - A *locked* icon indicates that your request to access the computer remotely must be approved first.
   - An *unlocked* icon indicates access is pre-approved and no reason is required to connect and log in.

   Notifications and data input are handled entirely within the browser, although users might also receive notifications via their email clients if running.

   Admins can approve requests for remote access in the same way they do for other requests - if using the portal, the requests appear under the **Requests** menu (**PENDING** tab).
8. In the portal, use the **Auditlog** to check activity during a remote access session.

   If the *Recording* option is on (**Secure Remote Access > Settings > Unattended Access Settings**, **RECORDING** tab), you can replay a video of all actions taken by the user during the session

   In the Auditlog, locate and expand the relevant session, so you can request and view the session video.

Watch a demo

To watch a 3-minute overview of access.work, visit Using Vendor Access online.

Questions?

If you have any questions, don't hesitate to contact us or raise a support ticket (paid plans only - support tickets are *generally* not available under the free plan).

Logins

Introduction

The Portal User Logins page allows you to create additional user accounts for portal management. Initially, only the first administrator (i.e. the person whose email was used to sign up for the free plan) can modify the portal user list. That person can add new users to the portal with different roles, including the ability to also add new users if so required.

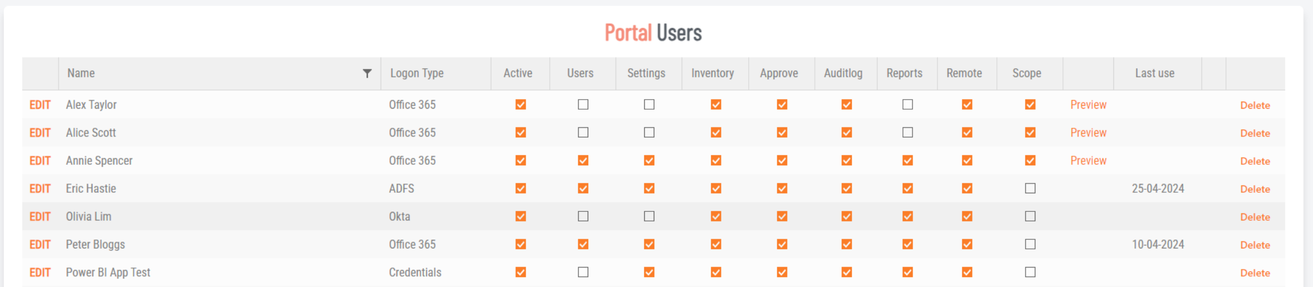
About Portal Users

Portal users (also known as Portal Admins) are users that can log in to the portal and access the areas you decide. You can define scopes to limit the resources a user can access.

For example, a manager who is not in IT could be set up to approve requests in his own sub-organization. In such a case, you can set up a scope based on users in an *Organizational Unit* or in groups.

Portal User Logins

Users with portal access are listed in the table; these users can log on to both the portal and the mobile phone app (see Mobile Application).



Portal Users

	Name	Logon Type	Active	Users	Settings	Inventory	Approve	Auditlog	Reports	Remote	Scope		Last use		
EDIT	Alex Taylor	Office 365	☑	□	□	☑	☑	☑	□	☑	☑	Preview			Delete
EDIT	Alice Scott	Office 365	☑	□	□	☑	☑	☑	□	☑	☑	Preview			Delete
EDIT	Annie Spencer	Office 365	☑	☑	☑	☑	☑	☑	☑	☑	☑	Preview			Delete
EDIT	Eric Hastie	ADFS	☑	☑	☑	☑	☑	☑	☑	☑	□		25-04-2024		Delete
EDIT	Olivia Lim	Okta	☑	□	□	☑	☑	☑	☑	☑	□				Delete
EDIT	Peter Bloggs	Office 365	☑	☑	☑	☑	☑	☑	☑	☑	□		10-04-2024		Delete
EDIT	Power BI App Test	Credentials	☑	□	☑	☑	☑	☑	☑	☑	□				Delete

The following column check boxes are matched with their corresponding settings under the *Rights* heading, which is available when clicking **New user** or **EDIT.**

- Users - Portal users admin
- Settings - Settings
- Inventory - Inventory
- Approve - Approve Requests
- Auditlog - Auditlog
- Reports - Reports
- Remote - Allow Remote Control
- Scope - Indicates if a scope is applied to this user

The *Preview* link is visible only when a scope exists for the user and indicates the computers to which the user has access.

Click **New user** or **EDIT** to access the settings table.

Adding or Updating Portal Users

Portal menu: **Logins > User Logins**

IMPORTANT

Vendor Access users who are not authorized to login to the portal must have setting "Limit to access.work" in the **Rights** panel set to **On**.

Account tab

Account heading

Click the **New user** button to create a new portal user, or click the **EDIT** link to update an existing user..

Setting	Type	Description
Account enabled	Toggle On | Off Default: **On**	**On** - .Account is active and user can log in to the portal.. **Off** - Account is disabled and user cannot log in.
Sign-on method	Selection Default: **Credentials**	**Credentials** - Authorize access to the portal with username and password. **Two factor (Credentials and SMS)** - Authorize access with username, password and an SMS code sent to a mobile phone. **Office 365 / Azure AD Single sign-on** - Authorize access with an account that has previously been configured in Azure AD for single sign-on (SSO). The following options are available only *after* Single Sign-on Setup (portal menu **Logins > Single Sign-on Setup**) has been completed for the respective option. **ADFS** - Authorize access with an account that has previously been configured in Active Directory Federation Services for SSO. **Okta** - Authorize access with an account that has previously been setup in Okta Identity Manager for SSO. **SAML** - Authorize access with an account that has previously been configured via a third party product under SAML 2.0 rules for SSO. Note that there can be multiple entries for the ADFS, Okta and SAML sign-on methods. Each domain configured will have an option.

Setting	Type	Description
Password (enabled only when either *Credentials* or *Two factor (Credentials and SMS)* is selected as Sign-on method)	Selection Default: **Send a set password email to user upon save**	**Keep current password** - Use the password currently set for this user. **I will enter a new password** - Use a new password entered by the portal admin adding or updating this user account. Selecting this option makes visible the *New password* field. **Send a set password email to user upon save** - Send an email to the user's *Email address* which advises that the user must set a new password on first login to the portal.
New password (enabled only when *I will enter a new password* is selected in the Password field)	Text	A new password, entered in clear text, to be used by the portal user being added or updated.
Full name	Text	The full name of the portal user.
Email address	Text	The email address of the portal user.
Phone number	Text	The phone number of the portal user.
Date format	Selection Default: **Auto-detect**	**Auto-detect** - Use the date format of the operating system. **United States (mm/dd/yyyy)** - Use the American date format (month/day/year). **Default (dd/mm/yyyy)** - Use the European date format (day/month/year).
Save	Button	Saves customization and changes to any fields. Note that reloading any defaults does not take effect until **Save** is clicked.

Rights heading

The setting *Limit to access.work* can be used for external users, to limit their access to the admin portal. As it applies only to remote access, this field is hidden until at least one on-premise gateway is configured.

Setting	Type	Description
Areas		
Auditlog	Toggle On | Off Default: **On**	**On** - User can access the portal Auditlog. **Off** - User cannot access the Auditlog.
Reports	Toggle On | Off Default: **On**	**On** - User can access Admin By Request reports. **Off** - User cannot access reports.

Setting	Type	Description
Settings	Toggle On | Off Default: **Off**	**On** - This user is authorized to make changes to settings (global and sub), unless *Read-only view* is **On**. Note that this does not apply to these portal user settings - that is controlled by *Portal users admin*. **Off** - User cannot make any changes to settings.
Mobile App	Toggle On | Off Default: **On**	**On** - User is authorized to install and use the Mobile Application. **Off** - User cannot use the mobile application.
Requests	Toggle On | Off Default: **On**	**On** - Allow user to view requests. To also allow the user to approve requests, make sure *Approve Requests* is **On**. **Off** - User cannot view requests. Selecting this option disables *Approve Requests*..
Inventory	Toggle On | Off Default: **On**	**On** - User is authorized to view inventory records. **Off** - User cannot view inventory.
Portal users admin	Toggle On | Off Default: **Off**	**On** - This user is authorized to add, update and delete other portal users, unless *Read-only view* is **On**. **Off** - User cannot administer portal user logins.
Read-only view	Toggle On | Off Default: **Off**	**On** - This setting lets the user view selected areas, but without the option to change any data. Note that rights still apply - the user can enable *Approve Requests*, *Create Support Ticket*, *Issue PIN Codes* and *Issue Break Glass* in read-only view. **Off** - User is a normal portal administrator, with the ability to change data.
Permissions		
Approve Requests	Toggle On | Off Default: **On**	**On** - Allow user to approve requests for elevated privileges. **Off** - User cannot approve requests.
Issue PIN Codes	Toggle On | Off Default: **On**	**On** - Allow user to issue PIN codes for uninstallation or other elevated privilege operations. **Off** - User cannot issue PIN codes.
Allow Remote Control	Toggle On | Off Default: **On**	**On** - Allow user to take remote control of servers or workstations via Admin By Request's *Unattended Access* feature. **Off** - User cannot take remote control of other computers via Admin By Request.
Create Support Ticket	Toggle On | Off Default: **On**	**On** - Allow user to create a support ticket via the admin portal (menu Support > New Support Ticket).

Setting	Type	Description
		Note that creating a support ticket is not available under the Free Plan. **Off** - User cannot create a support ticket.
Issue Break Glass	Toggle On | Off Default: **Off**	**On** - Allow user to create a one-time-use *Break Glass* account. **Off** - User cannot create Break Glass accounts.
Limit to access.work (visible when the tenant has one or more devices that are able to be remotely accessed)	Toggle On | Off Default: **Off**	**On** - Prevent user from logging-in to the admin portal at www.adminbyrequest.com. User can still log in to www.access.work. **Off** - Allow user to log in to the portal.
Communication		
Product Updates	Toggle On | Off Default: **On**	**On** - Authorized to receive product update emails. **Off** - Will not receive product update emails.

Scope tab

User Scope defines which computers the user can view in this context. Defining a scope for a user enables the **Preview** link on the users list. Clicking Preview shows the computers this user can see in the inventory.

Network Scope is used to hide computers for certain users. This is typically used for tiering. When you toggle a gateway off, all computers behind this gateway become invisible to the user.

The Network Scope section becomes available only when the tenant has one or more devices that are remote access capable. This means a device:

- has ABR Server Edition installed, or
- has been discovered by an on-premise gateway.

Discovered devices are only known by a name, unlike computers with Admin By Request Server Edition installed that can also be scoped using Operating System Scope and Domain Scope. With an on-premise gateway installed on your local network, you can use network scope to limit who can see and access computers on the network represented by that gateway.

Setting	Type	Description
Computer Type		
Windows Workstations	Toggle On | Off Default: **On**	**On** - User can see (and therefore connect to) Windows workstations. **Off** - User cannot see Windows workstations.
Windows Servers	Toggle On | Off Default: **On**	**On** - User can see Windows servers. **Off** - User cannot see Windows servers.
Apple Macs	Toggle On | Off	**On** - User can see computers running macOS.

Setting	Type	Description
	Default: **On**	**Off** - User cannot see computers running macOS.
Linux	Toggle On | Off Default: **On**	**On** - User can see computers running Linux. **Off** - User cannot see computers running Linux.
Discovered Devices	Toggle On | Off Default: **On**	**On** - User can see devices discovered by gateways. **Off** - User cannot see devices discovered by gateways.
Domain Scope		
Computer must be in OU	Text	A list of organizational units into which computers are placed, with multiple OUs on separate lines.
Computer must be in group	Text	A list of groups into which computers are placed, with multiple groups on separate lines.
Computer must be in domain	Text	A list of domains into which computers are placed, with multiple domains on separate lines.
End user must be in OU	Text	A list of organizational units into which users are placed, with multiple OUs on separate lines.
End user must be in group	Text	A list of groups into which users are placed, with multiple groups on separate lines.
End user must be in domain	Text	A list of domains into which users are placed, with multiple domains on separate lines.
Network Scope		
Computers without a gateway	Toggle On | Off Default: **On**	**On** - User can see all computers that are available for remote control, across all gateways. **Off** - User can see only those computers controlled by the relevant gateway.

Document History

Document	Product	Changes
1.0 14 February 2025	14 February 2025	Initial document release. Removed chapter "Using Vendor Access" from document *Unattended Access IT Admin Guide* and used it as the basis for this manual.
1.1 20 February 2025	14 February 2025	Updated *Prerequisites* in chapter "Overview" to increase number of outbound MQTT broker nodes from two to ten for each data center.
1.2 24 February 2025	14 February 2025	Corrected UDP / QUIC port number.

Index