Secure Remote Access (SRA) | Unattended Access

Unattended Access: IT Admin Guide

Document Information

Code:	**PM-UNA-ITAG**
Version:	**2.3**
Date:	**29 November 2024**

Admin By Request
ZERO TRUST PLATFORM

Copyright © 2024 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

Unattended Access Overview

What is Unattended Access?

Unattended Access is a feature of Secure Remote Access that allows you to connect remotely to your servers and network endpoints directly from your browser, using a lot of the well-known Admin By Request features like: inventory, auditlog, settings and sub-settings, approval flows, integrations etc.

The implementation of *Unattended Access* can use either a "Cloud" or an "On-premise" gateway, eliminating the need for VPN and jump servers, while still maintaining a secure and segregated setup.

This document covers getting started with Product Enrollment, Unattended Access and Vendor Access. It also describes key settings that can be administered from the portal.

Prerequisites

In order to use the full power of Unattended Access, there are a number of requirements:

Using 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:
  - **FastTrackHubEU1.azure-devices.net** (if your data is located in Europe)
  - **FastTrackHubUS1.azure-devices.net** (if your data is located in the USA)
- 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" on page 5).
- For Windows endpoints, RDP needs to be enabled on port **3389** on each device.

Using 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:
  - **FastTrackHubEU1.azure-devices.net** (if your data is located in Europe)
  - **FastTrackHubUS1.azure-devices.net** (if your data is located in the USA)
- 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).

Using Vendor Access

A further prerequisite applies to *Vendor Access*, where **SSO must be enabled for each user** who will login to the *Vendor Access* page (https://access.work).

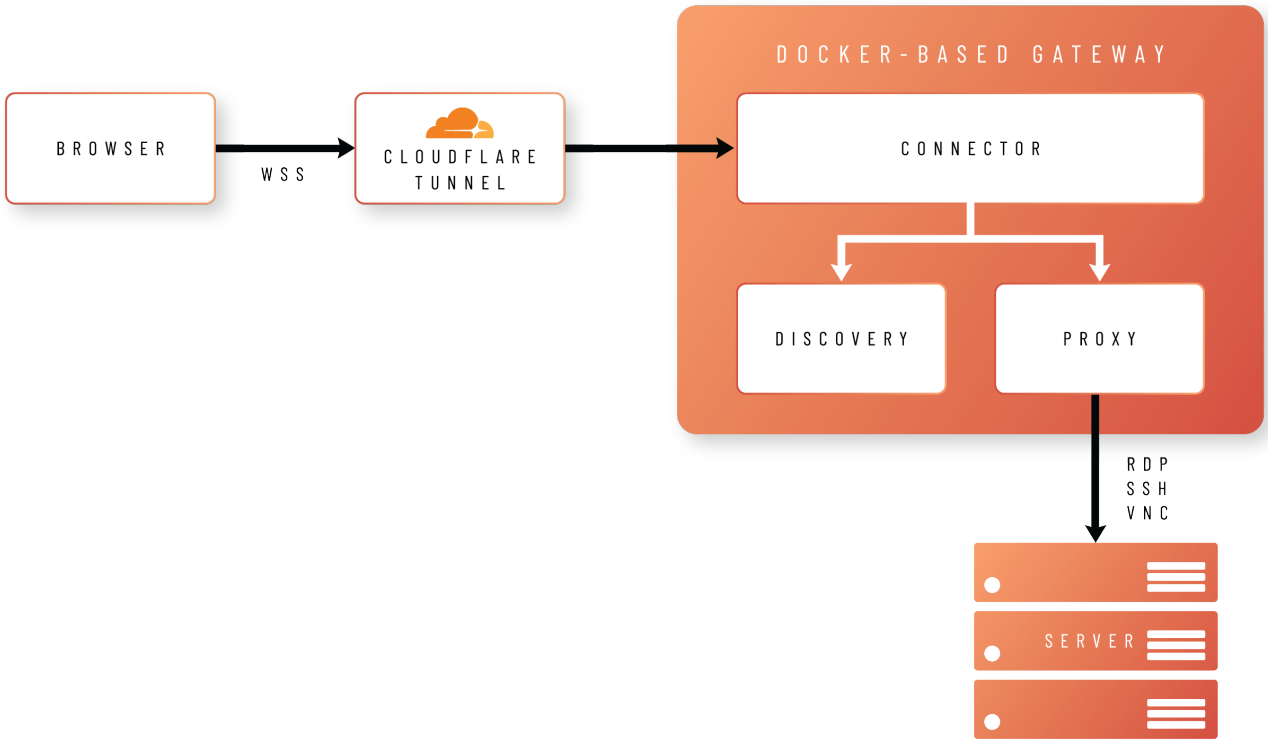
How does Unattended Access work?

Architecture

The idea behind *Unattended 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.

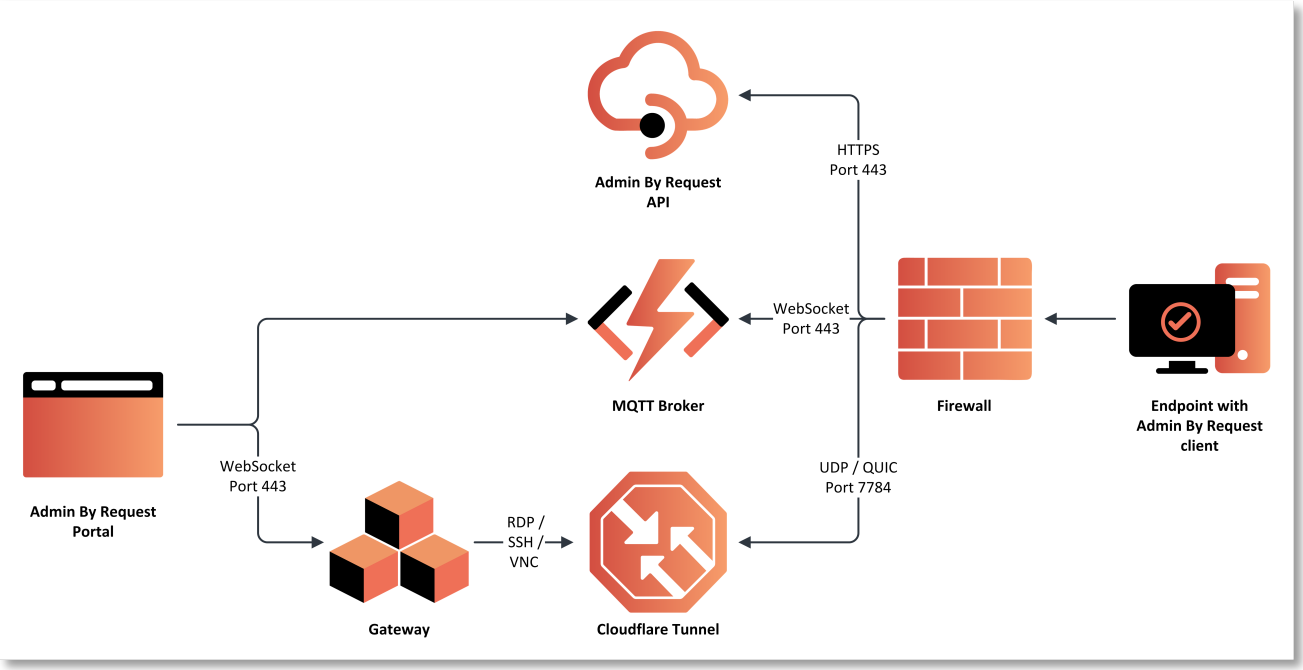
Process

The process by which a user (IT admin or standard user) establishes an unattended access session is:

1. The user initiates a connection from the **Admin By Request Portal**.
2. The **Admin By Request client** on the unattended 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 7784 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?

As well as outlining how to get started with *Unattended Access*, this document describes the customization options available and provides reference documentation for various settings that can be changed in the portal.

The next section covers licensing endpoints for Secure Remote Access via Product Enrollment. After that, Getting Started lists the initial steps for enabling *Unattended Access*, followed by the steps required for a managed cloud service, and then the steps required for a self-hosted implementation.

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:

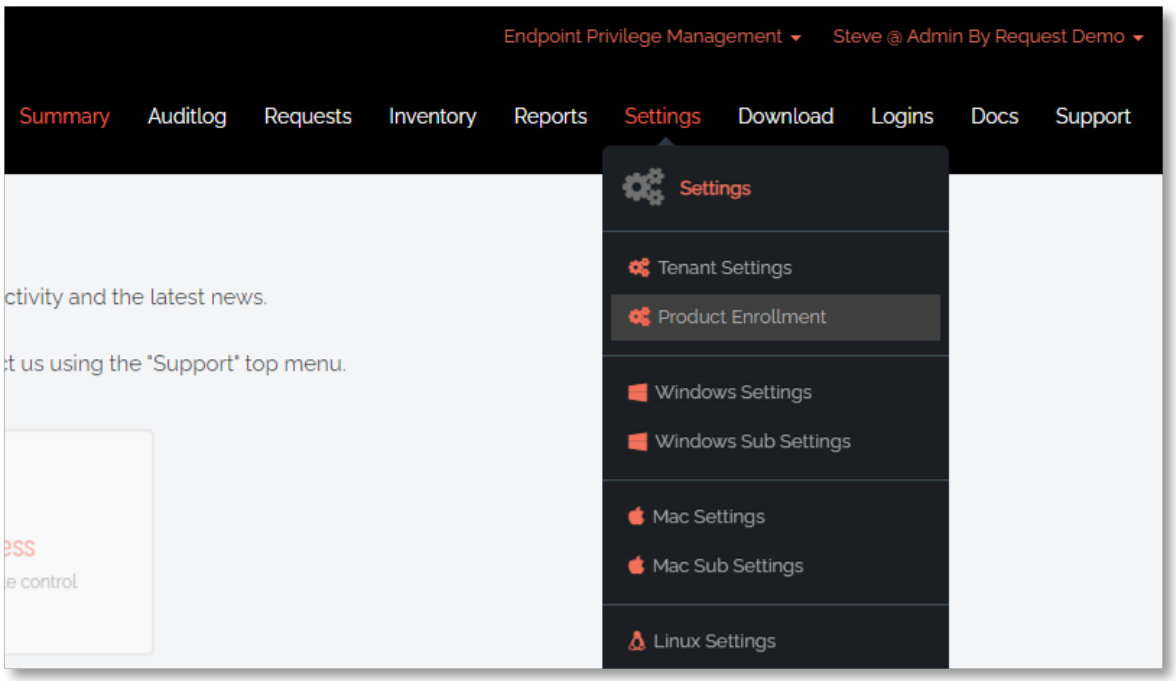
- 100 Endpoint Privilege Management (EPM) licenses
- 50 Secure Remote Access (SRA) licenses

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.

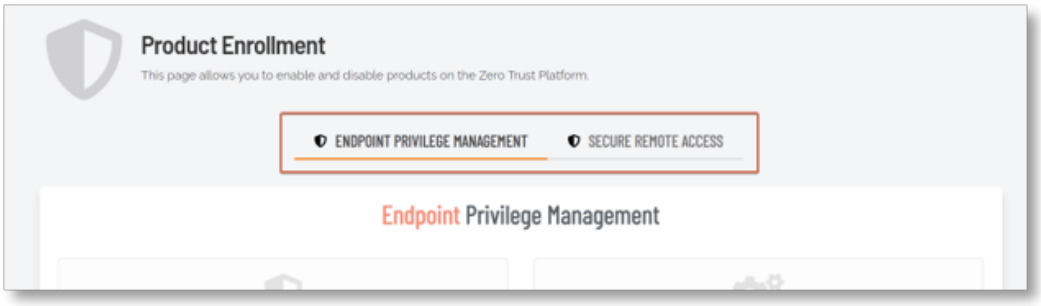
Getting started with Product Enrollment

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:

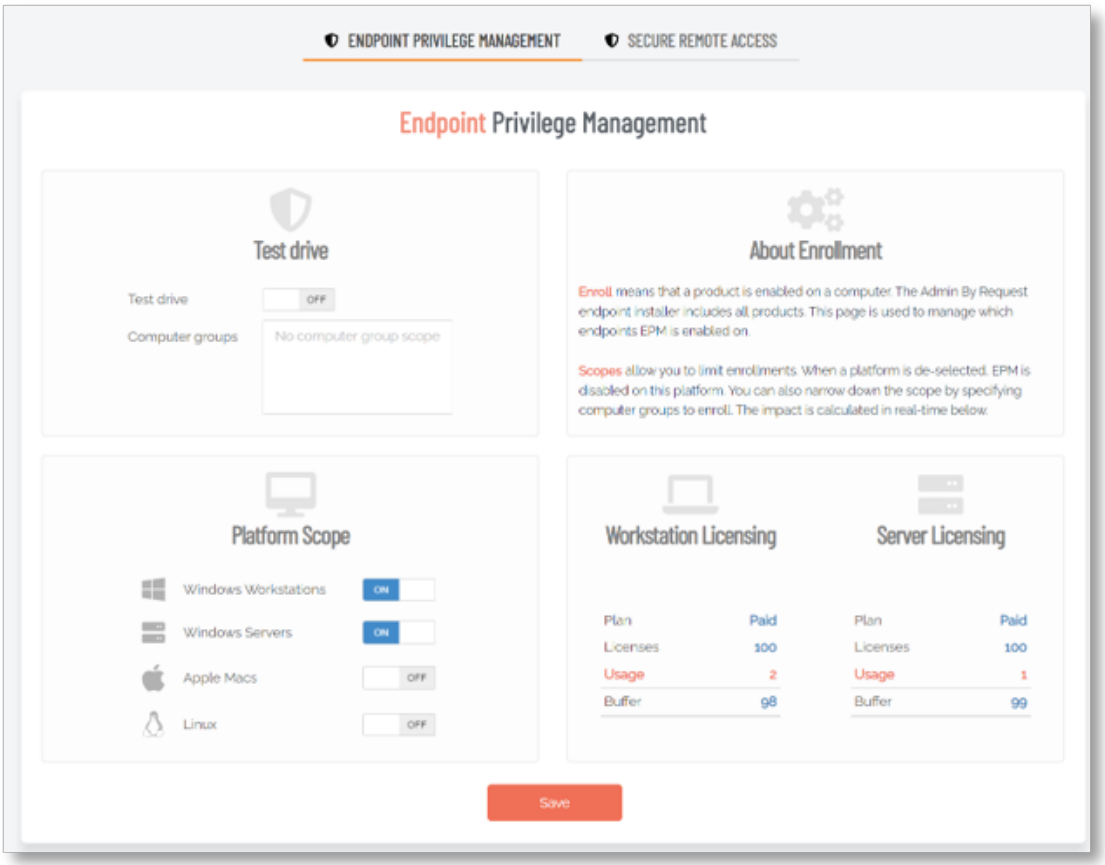


From each product tab, it's possible to determine the scope of enrollment for that product, as well as get an overview of the current license usage based on the selection.

Platform Scope

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

In the following example, 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:



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.

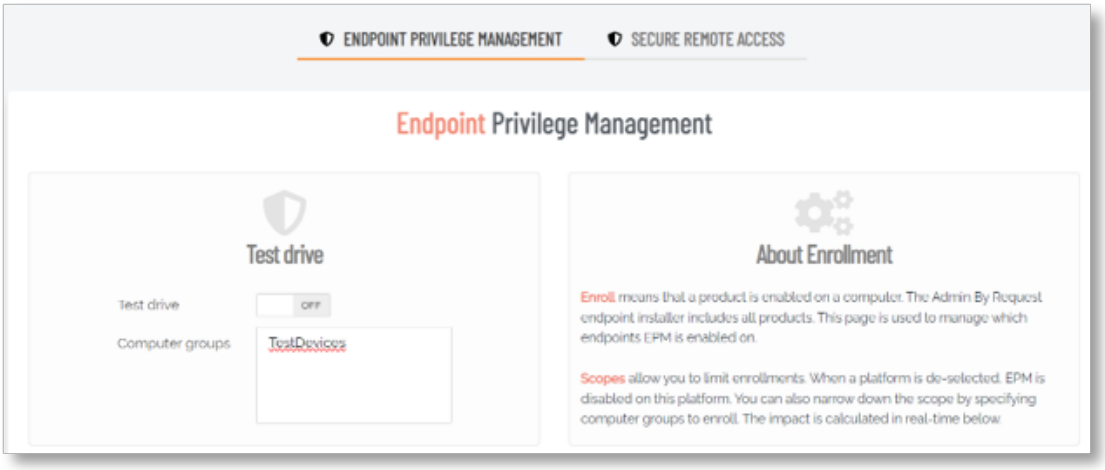
In the example above, the tenant has 100 licenses for both Workstation and Server – and the current selected enrollment uses 2 Workstation licenses and 1 Server license – leaving the tenant with a buffer of 98 for Workstation and 99 for Server Edition.

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

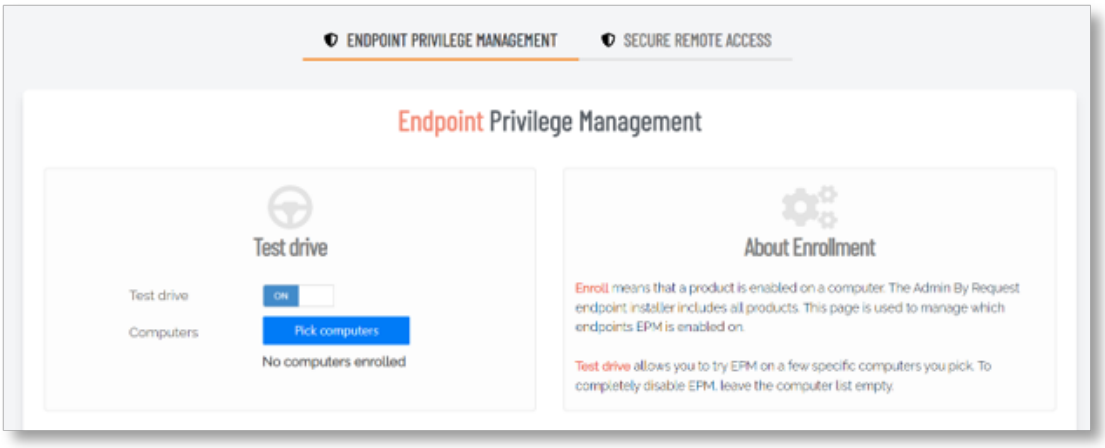
To apply the scope only to devices within specific computer groups, enter the group names into the "Computer groups" box:



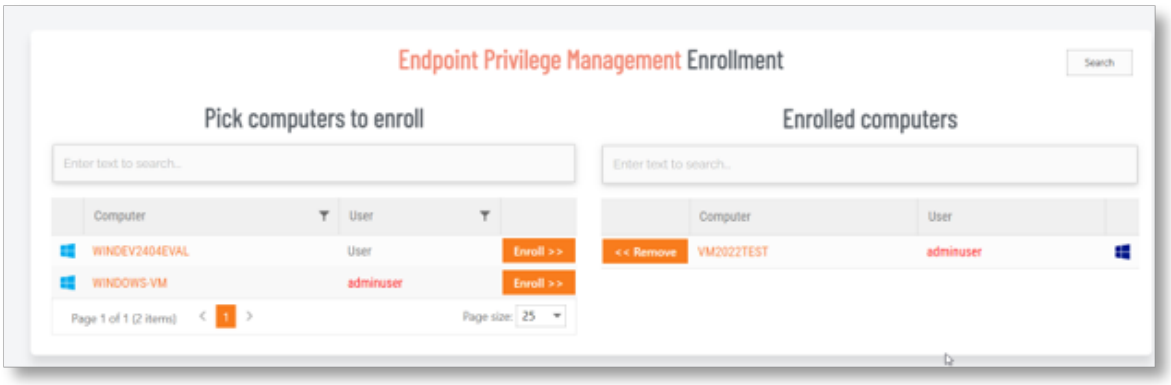
In this example, the enrollment will affect only devices in the group "TestDevices".

Scope by manual selection

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



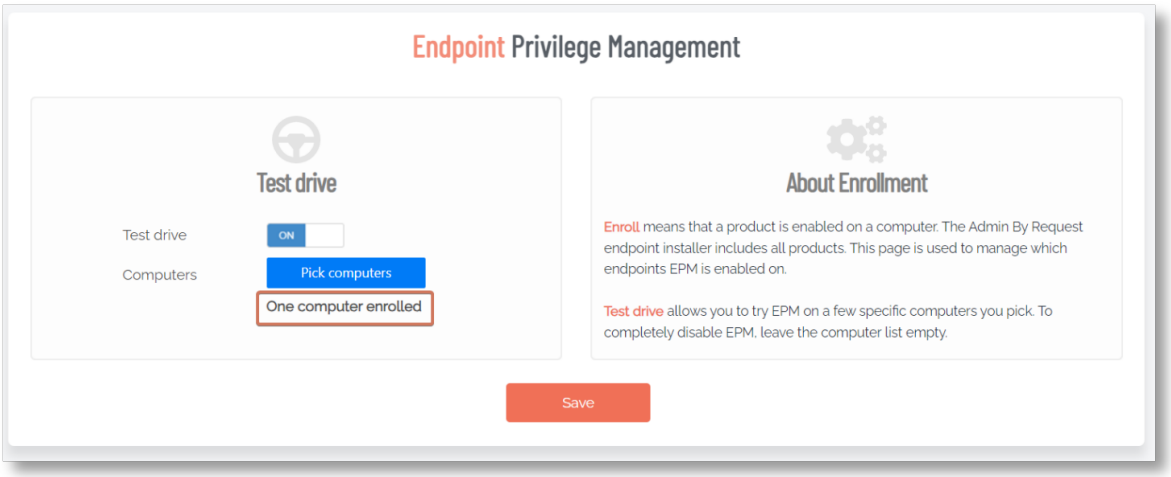
The **Pick computers** button is now available and allows for manual selection of the devices to enroll into the selected product:



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.

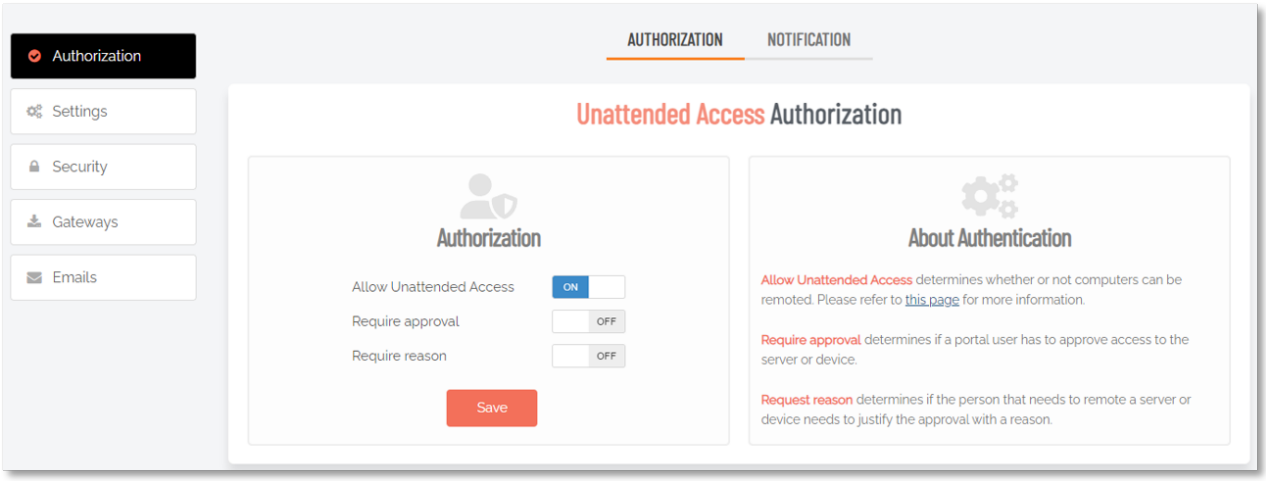
Please be aware that turning test drive on or off will cause licenses to be removed from non-selected devices. Only use the test drive feature if you manually want to pick the devices to enroll.

Getting Started with Unattended Access

How do I get started?

The very first thing is to make sure *Unattended Access* is turned on:

1. To enable Unattended Access, log in to the Admin By Request portal and head over to **Secure Remote Access > Settings > Unattended Access Settings**.
2. Select **Authorization** in the left menu and, from the **AUTHORIZATION** tab, ensure that *Allow Unattended Access* is turned **On**:



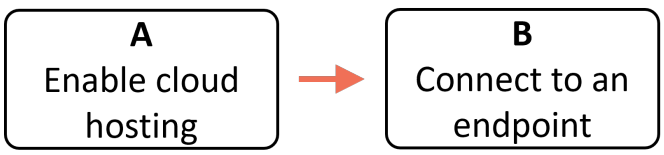
How do I setup a Managed Service?

A *managed service* is a way of operating Unattended Access so that your infrastructure allows an outbound connection to establish a secure tunnel from your respective endpoints and that these have the Admin By Request endpoint client installed.

Using Admin By Request's Managed Service for *Unattended Access* is the default. If you decide on this option when first enabling *Unattended Access*, no configuration is required; all you need to do is:

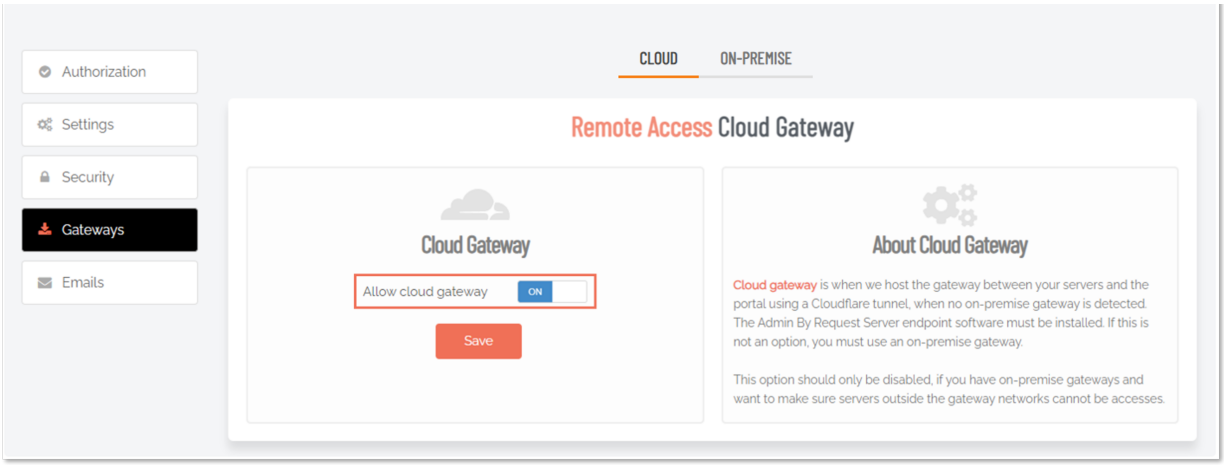
1. Ensure your endpoints have the Admin By Request endpoint client installed.
2. Connect to an endpoint (see next page).

If this is not the first time enabling *Unattended Access* and you have previously configured an on-premise gateway, the following tasks are needed to setup a managed service using a Cloudflare tunnel:



A. Enable cloud hosting

1. Ensure that your endpoints have the Admin By Request endpoint client installed
2. In the portal, go to **Secure Remote Access > Settings > Unattended Access Settings**.
3. Select the *Gateways* menu and, from the CLOUD tab, ensure that *Allow cloud gateway* is **On**:



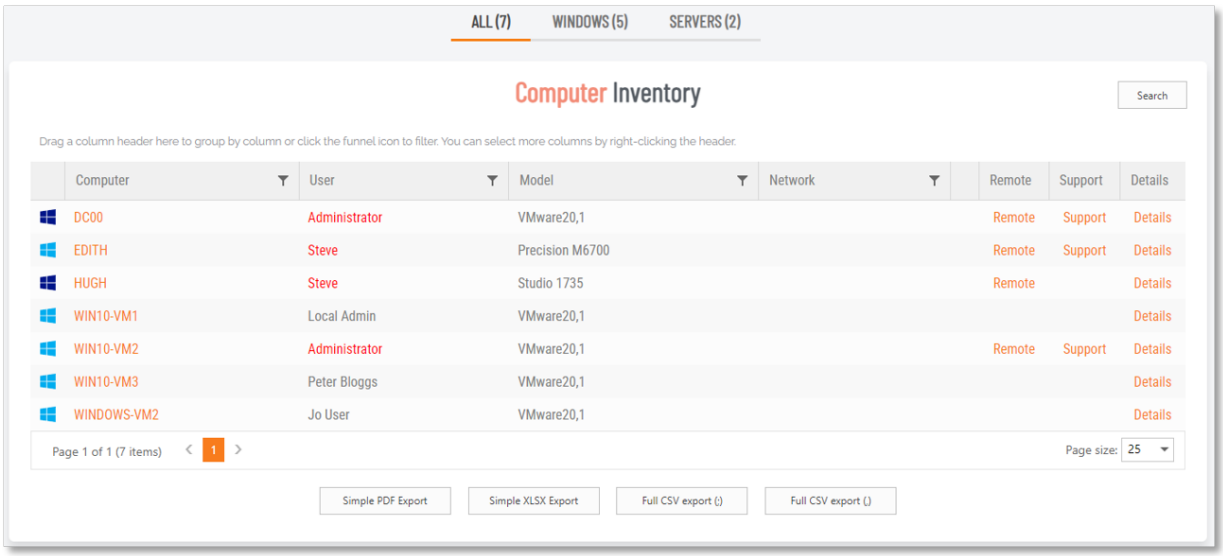
> **NOTE**
> The CLOUD tab becomes visible only when an on-premise gateway is created. If no on-premise gateway exists, Unattended Access will use the managed service option, which is enabled by default and requires no configuration.
>
> Configuring an on-premise gateway means disabling the cloud gateway (see "How do I setup a Self-hosted Implementation?" on the next page) which is why the CLOUD tab becomes available when a gateway is created.

That's it. The Admin By Request agent will now attempt to establish a secure tunnel via an outbound call - allowing connections directly via the managed gateway.

B. Connect to an endpoint

> **NOTE**
> In order to allow Admin By Request to connect to your endpoints, they need to allow traffic on the following ports:
>
> - RDP - **3389**
> - SSH - **22**
> - VNC - **5900** and **5901**

1. From the portal, head over to your Inventory and make sure you're in the Secure Remote Access view. Select an endpoint with the Admin By Request client installed:



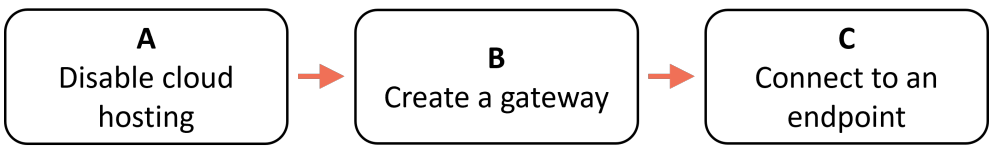
2. Click the **Remote** link for this endpoint, enter *User name* and *Password* and click **Connect**:

After a few seconds, the connection appears directly in your browser.

How do I setup a Self-hosted Implementation?

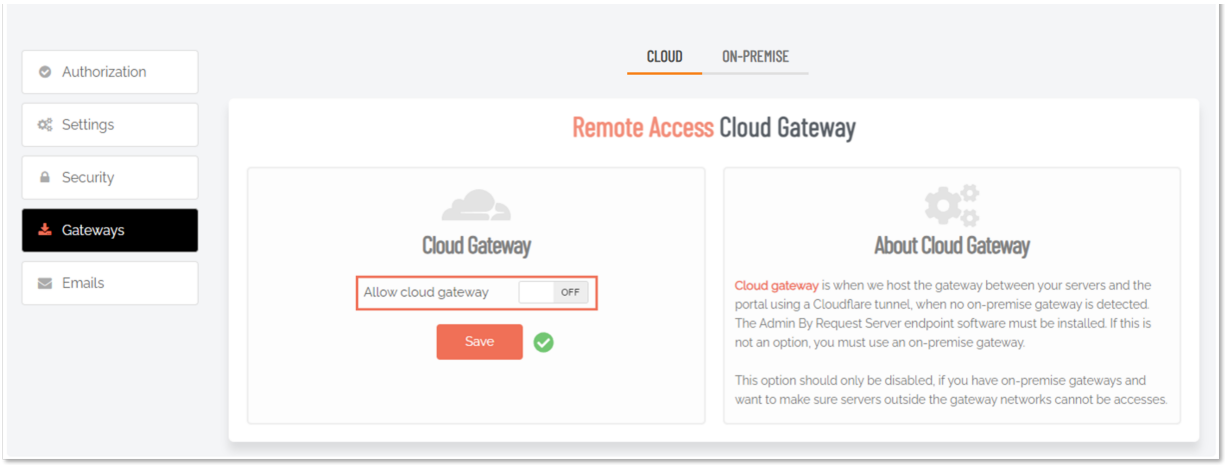
A *self-hosted implementation* means that you run Unattended Access on-premise inside your own infrastructure, including the ability to run Docker containers. To establish a secure tunnel, your infrastructure must also allow outbound connections to Cloudflare.

The following tasks are needed to setup a self-hosted implementation:



A. Disable cloud hosting

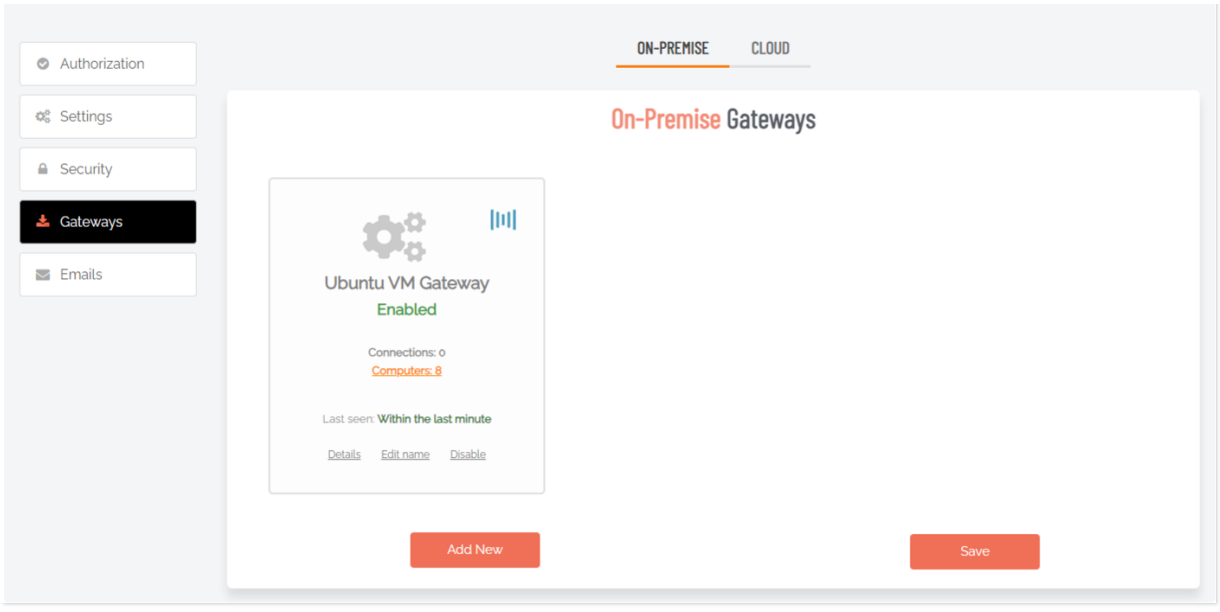
1. Ensure that your endpoints have the Admin By Request endpoint client installed.
2. In the portal, go to **Secure Remote Access > Settings > Unattended Access Settings**.
3. Select the Gateways menu and, from the CLOUD tab, ensure that *Allow cloud gateway* is **Off**:



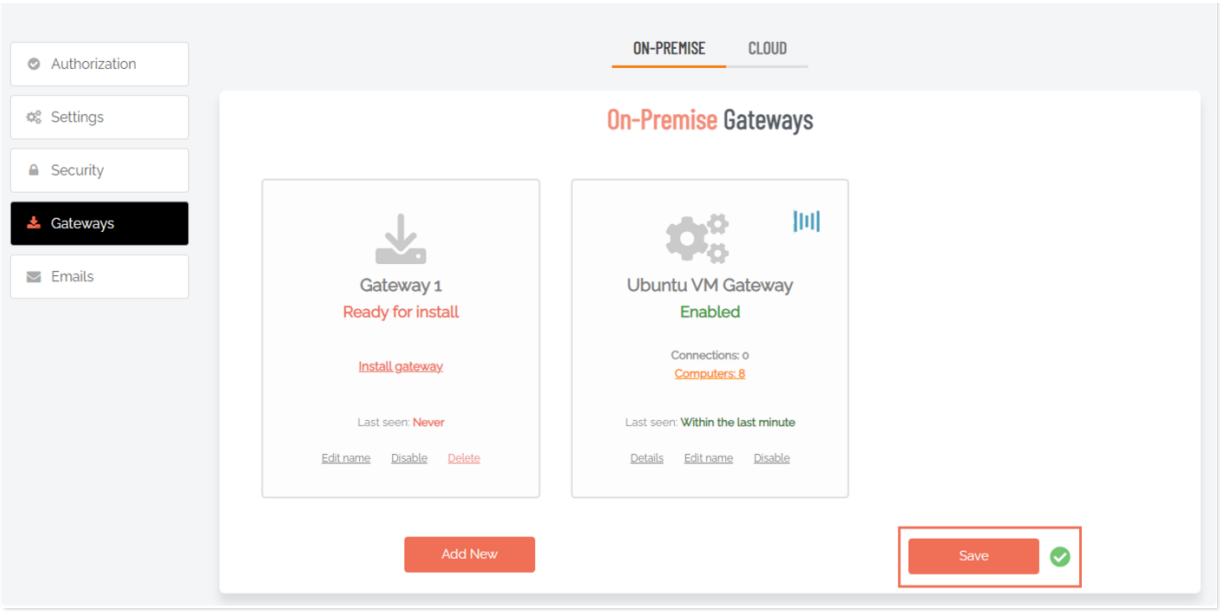
4. Click **Save** if making changes.

B. Create a gateway

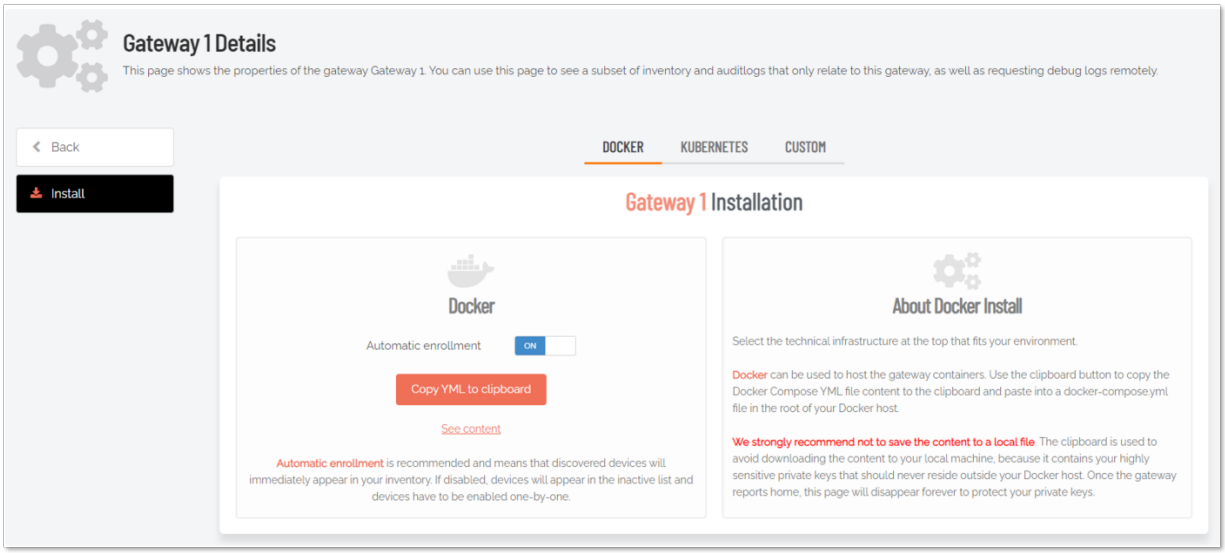
1. In the portal, from the Gateways menu, select the ON-PREMISE tab. This shows the current gateways for your tenant:



2. Click **Add New**, followed by **Save**. This will create a new Gateway with the default name *Gateway 1*:



3. Click the words **Install gateway**. This displays a view that allows access to the Docker compose file used for the installation:



The Docker compose file contains all the information necessary to orchestrate the Docker containers required to make *Unattended Access* work.

4. Click **Copy YML to clipboard** to copy the Docker compose file to your clipboard.
5. Add a new `docker-compose.yml` file to your Docker host, paste in the content and run the following command:

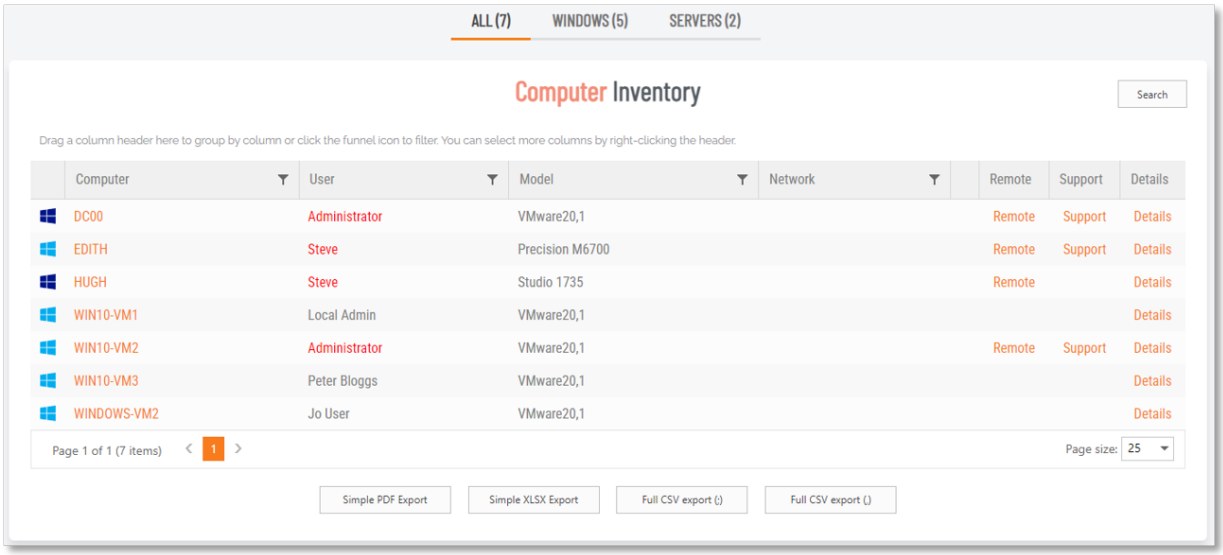
```
sudo docker compose up -d
```

This will spin up the containers and communicate back to the Admin By Request portal with all of the necessary information. Furthermore, a secure tunnel will be initiated between Cloudflare and the Connector container.

C. Connect to an endpoint

> **NOTE**
> In order to allow Admin By Request to connect to your endpoints, they need to allow traffic on the following ports:
> - RDP - **3389**
> - SSH - **22**
> - VNC - **5900** and **5901**

1. From the portal, head over to your Inventory and make sure you're in the Secure Remote Access view. Select an endpoint with the Admin By Request client installed:



2. Click the **Remote** link for this endpoint, enter *User name* and *Password* and click **Connect**:

After a few seconds, the connection appears directly in your browser.

Upgrading Unattended Access On-Premise (Self-hosted)

An environment variable was introduced from version 2.0.9 that needs to be present in order for your gateway to function properly. The variable is called **AUTH__TOKEN** and, if missing in your environment, you can add it to your Docker setup to enable the next `docker compose pull` to complete successfully.

AUTH__TOKEN needs to be set for all three images: *Connector*, *Proxy* and *Discovery*. The value of the AUTH__TOKEN variable can be anything you choose - it just needs to be the same across the different services. We recommend setting it to a UUID value or something of similar complexity.

In the case of a Docker compose file, the change would look like this:

docker-compose.yml

```yaml
version: "3"

services:
  connector:
    image: adminbyrequest.azurecr.io/remote-access/connector
    container_name: "connector"
    ports:
      - "8000:80"
    environment:
      - TOKEN__SECRET=123123123
      - TOKEN__PRIVATEKEY=324234324234
      - TOKEN__INITIALIZATIONVECTOR=90879087897
      - API__URL=url
      - API__KEY=239048239048902384
      - API__PRIVATEKEY=234+90823490+8239804
      - API__INITIALIZATIONVECTOR=230498239048
      - AUTH__TOKEN=xxxx
    volumes:
      - shared-data:/records
    restart: unless-stopped

  proxy:
    image: adminbyrequest.azurecr.io/remote-access/proxy
    container_name: "proxy"
    environment:
      - CONNECTOR_HOST=connector
      - AUTH__TOKEN=xxxx
    depends_on:
      connector:
        condition: service_healthy
    links:
      - connector
    volumes:
      - shared-data:/records
    restart: unless-stopped

  discovery:
    image: adminbyrequest.azurecr.io/remote-access/discovery
    container_name: "discovery"
    environment:
      - AUTH__TOKEN=xxxx
    network_mode: "host"
    depends_on:
      connector:
        condition: service_healthy
    restart: unless-stopped

    volumes:

    shared-data:
```

Once these changes have been made, you can run the following commands (in order):

```
sudo docker compose pull
sudo docker compose up -d
```

This will spin up the containers using the new image and the newly added AUTH__TOKEN variable.

> **NOTE**
> If you spin up a new gateway using the portal, you will not need to change anything manually. The required changes will be incorporated into the docker compose file generated by the portal.

Discovery

When using the self-hosted on-premise setup, the Discovery module is also available. The Discovery module automatically looks at the current network in which it is running and reports findings back to the portal about endpoints responding on ports **3389**, **22** or **5900/5901**.

This gives you the advantage of not having to manually map endpoints that are not running the Admin By Request endpoint client. This also has the benefit of mapping your network(s) automatically to your Admin By Request inventory, allowing you to connect to agent-less devices like routers, firewalls etc.

Refer to "Configuring Discovery" on page 17 for more information on Discovery.

Modifying Configurations

Configuring Discovery

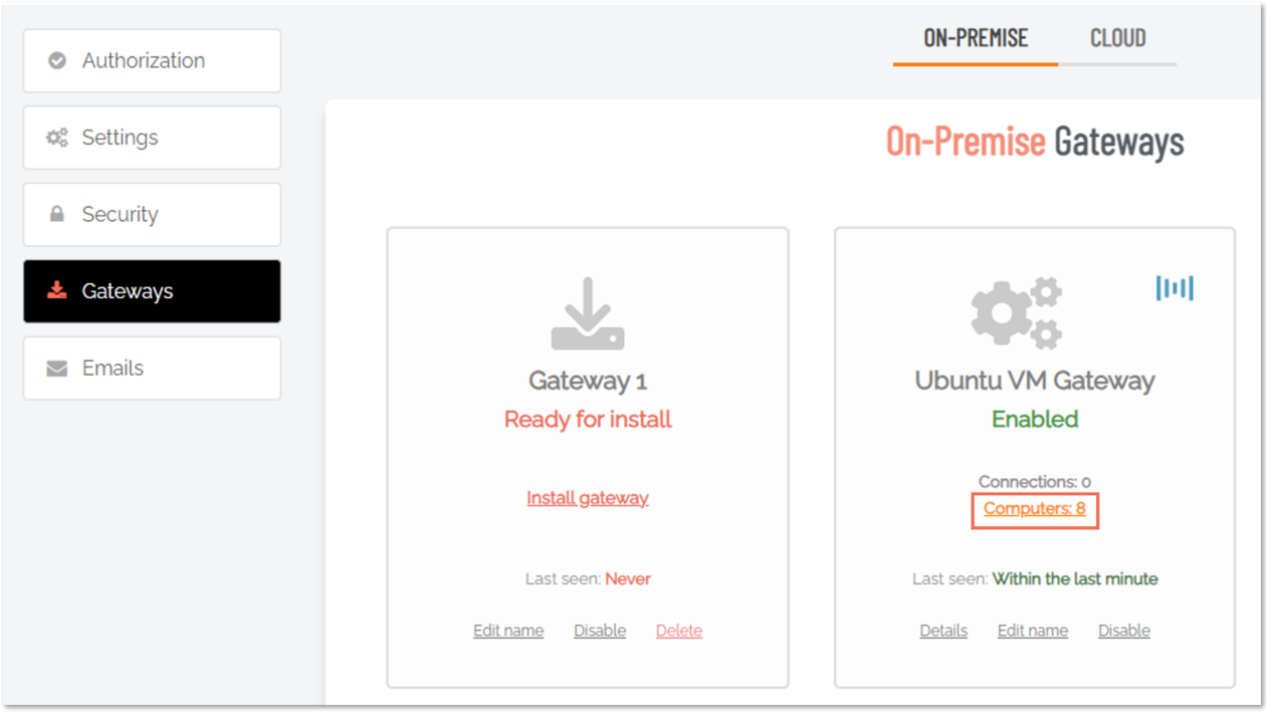
> **IMPORTANT**
> If you run your gateway behind a reverse proxy, you need to ensure that the end user's IP is forwarded to the gateway using the `X-Forwarded-For` header.

When using the self-hosted on-premise setup, the Discovery module is also available. The Discovery module automatically looks at the current network in which it is running and reports findings back to the portal about endpoints responding on ports **3389**, **22** or **5900/5901**.

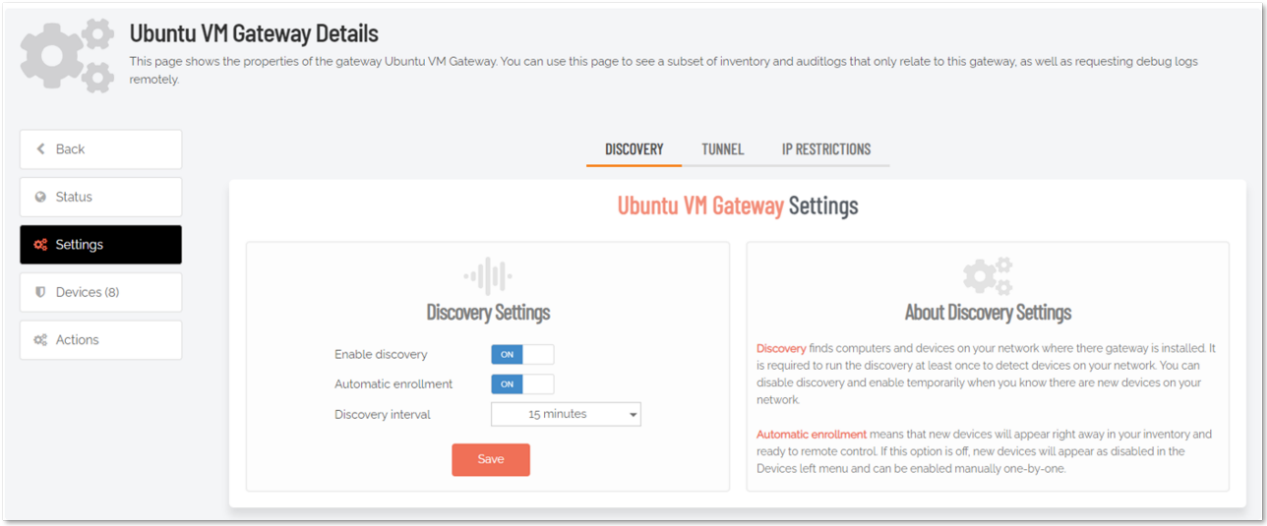
This gives you the advantage of not having to manually map endpoints that are not running the Admin By Request endpoint client. This also has the benefit of mapping your network(s) automatically to your Admin By Request inventory, allowing you to connect to agent-less devices like routers, firewalls etc.

The Discovery service can be configured by going to the details view of a gateway and accessing the Settings menu:

1. In the portal, go to **Secure Remote Access > Settings > Unattended Access Settings**.
2. Select the **Gateways** menu and click the **Computers (n)** link:



3. This action opens the *Devices (n)* menu, which is the default and shows a list of devices the gateway can access. Select the **Settings** menu to view Discovery Settings for the selected gateway:



The discovery service runs at the selected interval (every 15 minutes in this case). If automatic enrollment is *enabled*, the discovered devices will automatically be added as active endpoints to your inventory. If automatic enrollment is *disabled*, devices will be shown as inactive devices within your inventory.

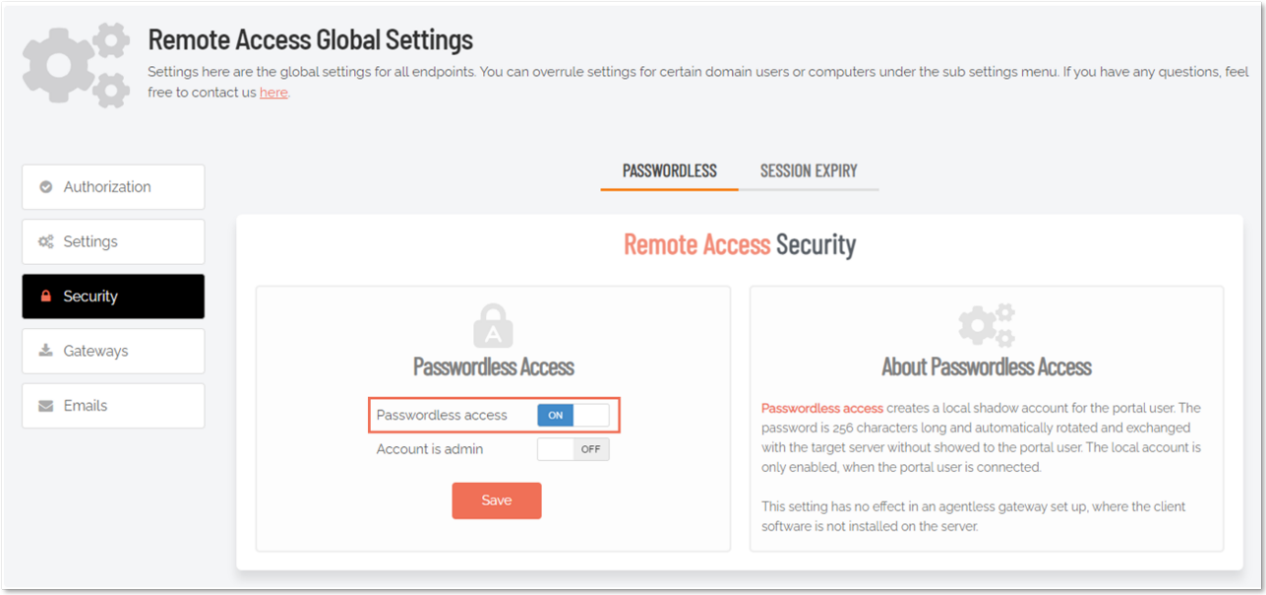
> **NOTE**
> Refer to "Settings" on page 39 for more information on configuring discovery settings.

Password-less

If you do not wish to let users connect to your remote endpoints using username and password, the Admin By Request Server agent allows you to connect password-less by using a *Just-In-Time* account that gets created for a specific session and then gets disabled immediately afterwards.

To enable password-less accounts for endpoints running the agent:

1. In the portal, go to **Secure Remote Access > Settings > Unattended Access Settings** and select the **Security** menu.
2. Turn on **Password-less access**:



3. Don't forget to click **Save**.

Now, if you select an endpoint with the Admin By Request client installed, you wont be prompted to enter username and password, but will instead be signed in using a *Just-In-Time* account.

What if I don't want to use Docker compose?

You can use the on-premise *Unattended Access* setup without Docker compose. In order to make the setup work without docker compose, you will need to spin-up containers using the following Docker images:

- **Connector**: `adminbyrequest.azurecr.io/remote-access/connector`
- **Proxy**: `adminbyrequest.azurecr.io/remote-access/proxy`
- **Discovery**: `adminbyrequest.azurecr.io/remote-access/discovery`

From the downloaded Docker compose file, you can see the necessary environment variables for the containers. These are also available from the Gateway installation page under the *Custom Setup* tab (see "Install" on page 38).

Furthermore, the following needs to apply:

- Your endpoint needs to be reachable via RDP, SSH or VNC from the Proxy container.
- The Proxy container needs to be reachable from the Connector container.
- The Connector container needs to allow HTTPS-traffic.
- If you wish to use the discovery functionality, the Discovery container needs to be reachable from the Connector container.

Once spun up, the Proxy container will automatically register with the Connector container, which will automatically register with the Admin By Request portal, allowing you to use the same connection flow described in "How does Unattended Access work?" on page 2.

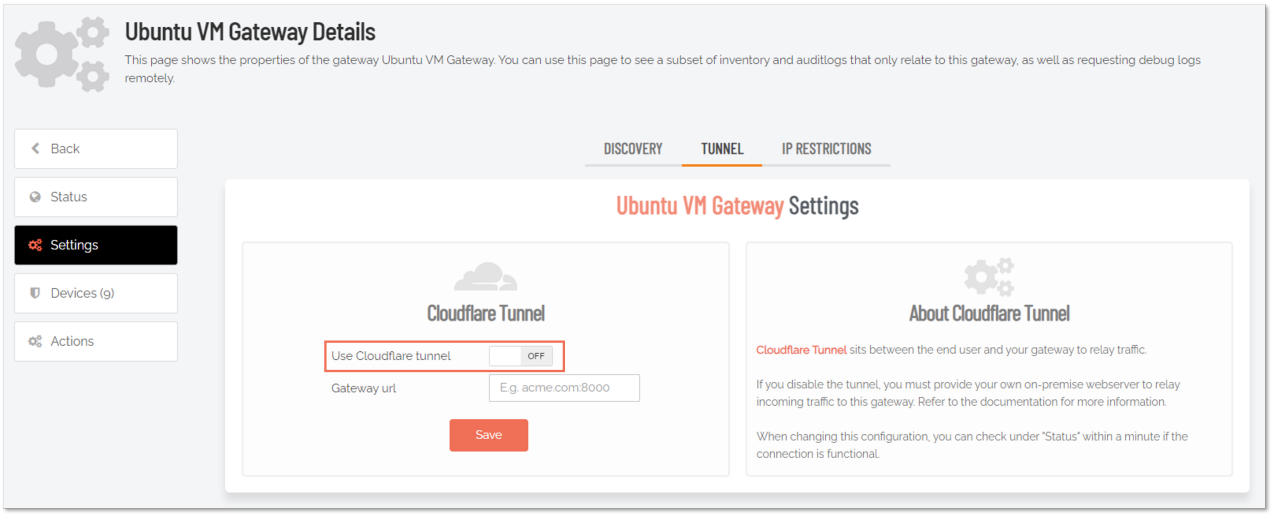
What if I don't want to use Cloudflare tunnels?

You can also use the *Unattended Access* setup without using Cloudflare tunnels. In this scenario, you need to have a webserver, HTTP proxy or reverse proxy configured that can direct traffic to the Connector container on the Docker host.

A way to accomplish this would be to spin up something like **Traefik** (https://traefik.io/traefik/) within the Docker host and use this as the receiving endpoint for the Secure WebSocket communication.

In order to configure the Admin By Request portal to disable tunnels and setup a custom domain or IP to point the traffic to, you need to do the following:

1. In the portal, go to **Secure Remote Access > Settings > Unattended Access Settings** and select the **Gateways** menu.
2. Click the **Details** link to go to the properties view of the gateway you want to configure and select the **Settings** menu.
3. Click the **TUNNEL** tab. From here you can disable the *Use Cloudflare tunnel* option:



   Disabling the *Use Cloudflare tunnel* option makes the *Gateway URL* field visible, which is where you can enter the URL of your own gateway.
4. Enter the address of your webserver, reverse proxy or similar and click **Save**.

All connection requests will be directed to that URL – and the Connector will not be instructed to set up a Cloudflare tunnel.

Auditlog

All sessions with *Unattended Access* are documented in the Auditlog, regardless of the setup in use. The Auditlog shows which users have connected to which endpoints, as well as the session duration and gateway used.

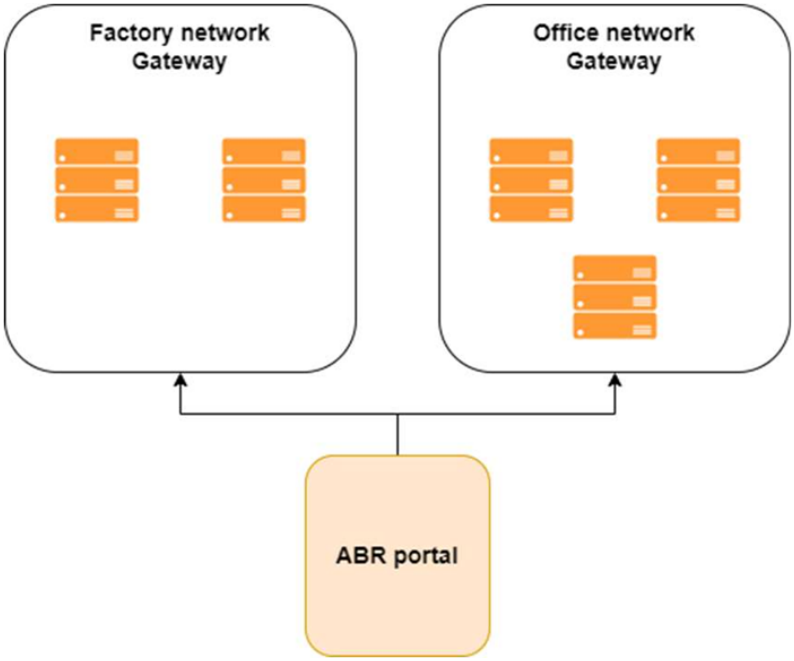
Refer to "Supplementary Technical Info" on page 23 for more information about the Auditlog.

Multi-Gateway Setup

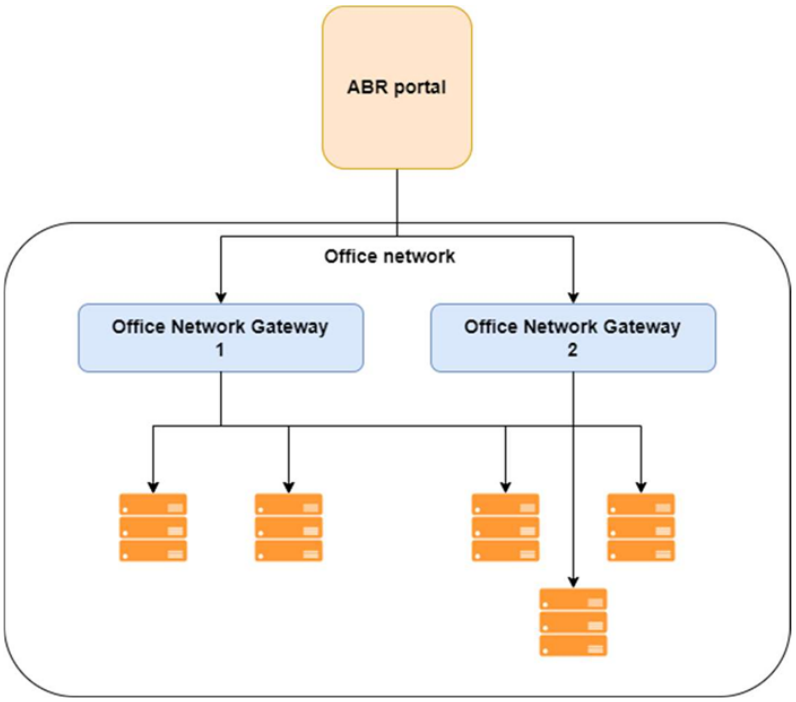
In order for the on-premise gateway to allow connections to your remote endpoints, there needs to be a direct connection path. This means that the user needs to be able to connect to the Connector, the Connector needs to be able to connect to the Proxy container and the Proxy container needs to be able to connect to your endpoint on any of the supported ports.

If you have multiple segregated networks, you simply create and spin up a gateway per network, location, subnet or however your setup is segregated. Each gateway will establish a connection with the portal and make itself available without further configuration.

The endpoint you choose to connect to will simply handle the connection via the gateway(s) available to it:



You can even spin up multiple gateways on the same network if you want to scale for better performance. In this case, the portal will simply select the gateway with the fewest active connections whenever a remote session is requested:



Each gateway will deliver discovery information, allowing you to map your entire network(s) to the Admin By Request inventory, as well as remote connecting directly each endpoint.

Gateway details

Besides the inventory, each gateway will also show information about the devices available for the specific gateway, active connections, auditlogs, callbacks made by the gateway, logs and much more:

Supplementary Technical Info

Unattended Access Auditlog

All sessions with *Unattended Access* are documented in the Auditlog, regardless of the setup in use. The Auditlog shows which users have connected to which endpoints, as well as the session duration and gateway used.

If the endpoint has the Admin By Request Server agent installed, the auditlog will also contain detailed information about which software has been used as well as all of the other things recorded by the classic Admin By Request auditlog.

Besides this, you also have the option to enable video recording of each session to be used as additional documentation.

To enable video recording:

1. In the portal, go to **Secure Remote Access > Settings > Unattended Access Settings** and select the **Settings** menu.
2. On the **RECORDING** tab, enable *Screen recording*.

A Word about Security

There are security mechanisms built in to the *Unattended Access* setup.

When clicking the **Remote Control** button for a device in the Inventory (**Inventory > [Device] > Details > Properties**), the following flow is initiated:

1. A one-time unique transfer token is coupled with the initiating user's IP address.
2. The transfer token is sent to the Connector.
3. The Connector uses the transfer token to call back the Admin By Request portal to verify that the request is valid and actually initiated by the current user.
4. If the transfer token is valid, the Admin By Request portal issues a connector token. This token contains information about the endpoint and credentials, as well as settings for the remote session.
5. The Connector receives the connector token and verifies its validity.
6. If the token is valid, the arguments are sent to the Proxy, which will in turn attempt to establish a connection to the endpoint.

Furthermore, the information supplied in the Docker compose file can only be spun up for a short period of time. Once the gateway has been spun up, it will be locked to the server's IP address.

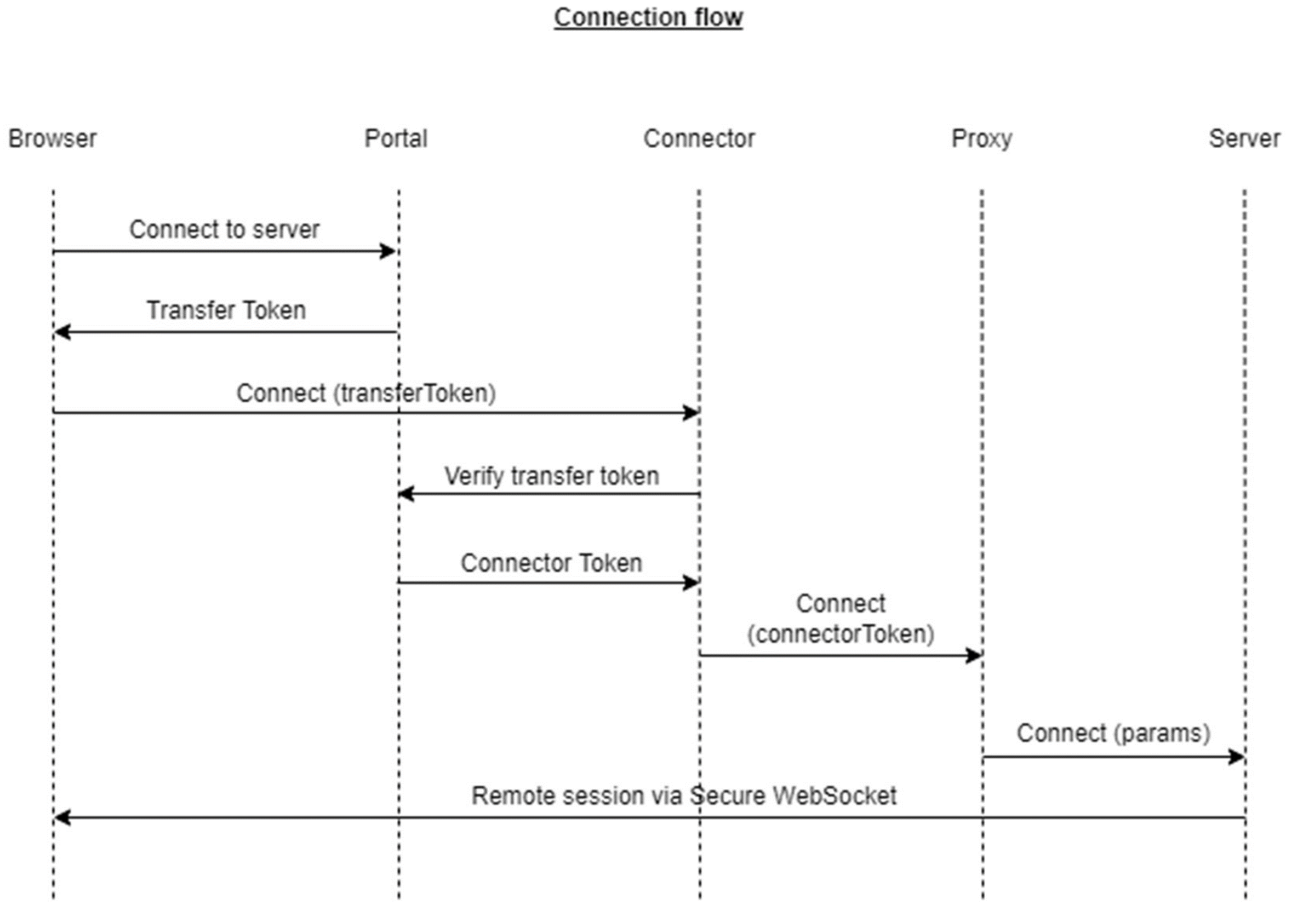
The connector token is encrypted using a secret only known by the Connector and the Admin By Request portal. The token values are also HMAC-validated by verifying a signed hash value of the connection properties.

All connections made by browsers are via Secure WebSockets and the gateways are "pull-configuration" only.

Technical Flows

Connection Flow

The following diagram shows the technical flow when a user requests to access a remote endpoint.



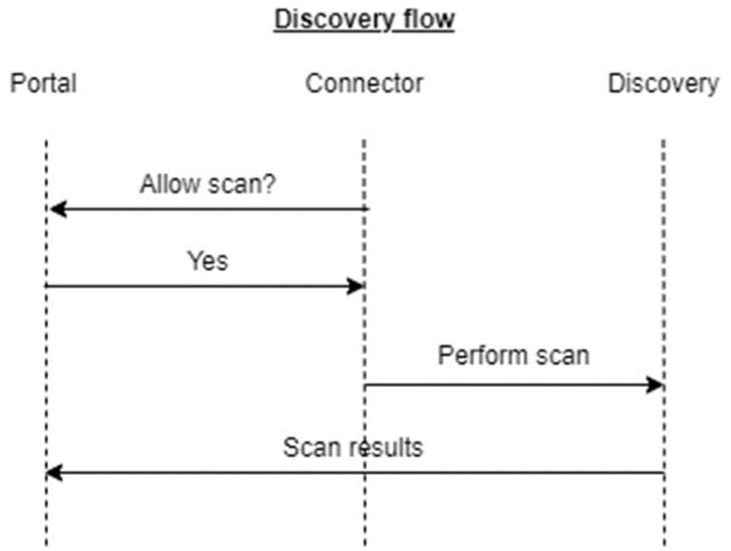
During this process, the following happens:

1. The Admin By Request portal assigns a one-time transfer token that's coupled with the user's IP address.
2. The transfer token is delivered from the browser to the Connector to inform that a request to connect to an endpoint is present.
3. The Connector validates the transfer token by sending it back to the portal alongside the user's IP address. If token and IP address match, the portal issues a connector token that contains the necessary information to connect to the endpoint.
4. When the Connector receives the token, it'll start by decrypting the values. Once decrypted, the values are HMAC-validated to ensure that no tampering has occurred.
5. If decryption and HMAC validation succeeds, the connection parameters are passed along to the Proxy, which initiates the connection to the endpoint with the requested protocol.
6. The connection stream is delivered back to the browser via Secure WebSocket.

If the gateway is configured with Cloudflare tunnels, then all communication is sent via the unique secure tunnel for that gateway.

Discovery Flow

The following diagram shows the discovery flow:

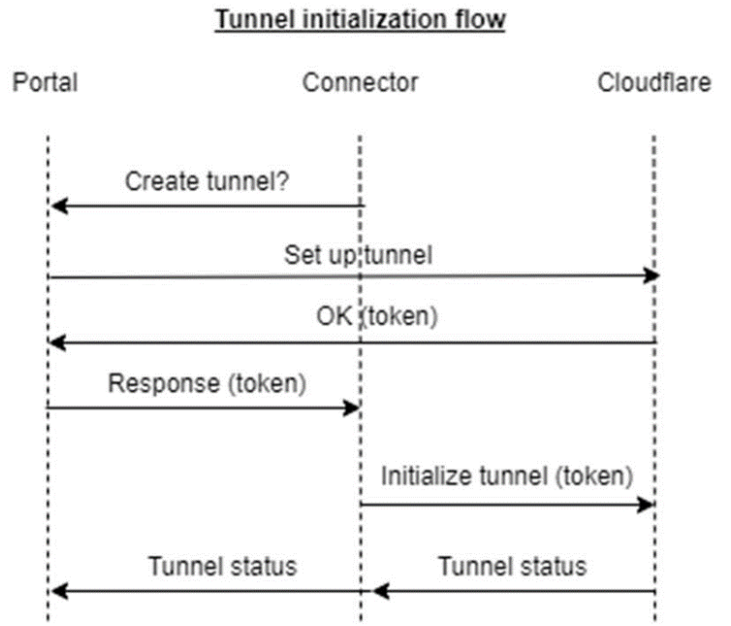


The Connector asks the portal repeatedly if a discovery scan should be allowed to run. Based on the settings within the portal, this might eventually return a positive result.

Upon receiving a positive result, the Connector asks the Discovery container to run the discovery process. This returns a collection of discovered devices, which will in turn be returned to the portal to be ingested into the Inventory.

Tunnel Initiation Flow

The following diagram shows the tunnel initiation flow:



Upon spinning up the Connector container, the portal is asked repeatedly if a tunnel should be initialized. If the portal settings allow for a tunnel to be created, the portal calls Cloudflare to set up the tunnel and receive a unique tunnel token back.

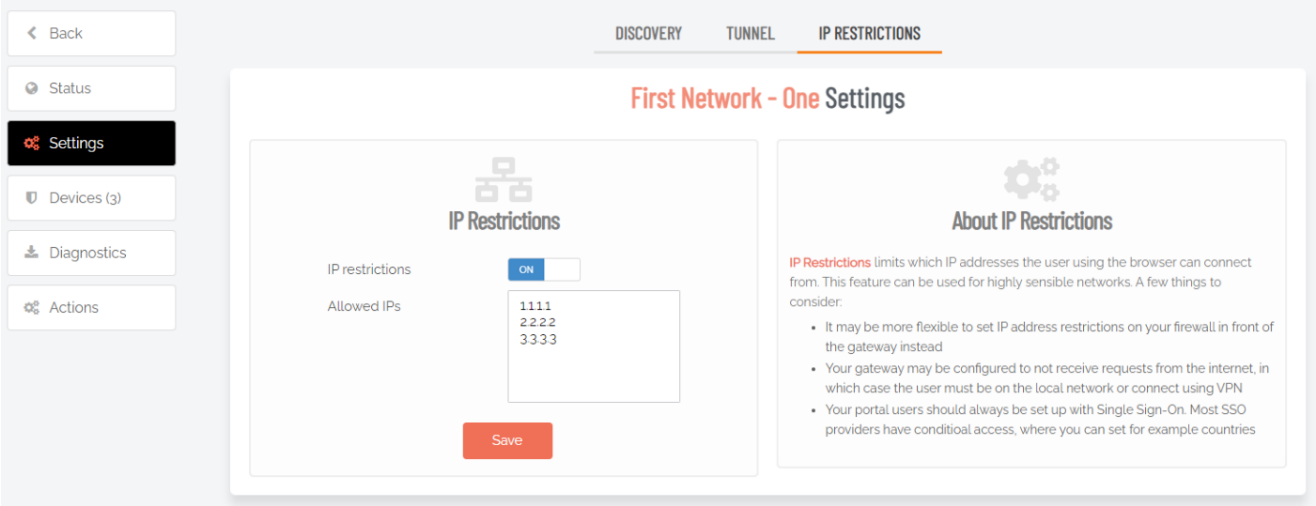
This token is returned to the Connector, which then initializes the tunnel to Cloudflare. Once the tunnel has been established, a status call is made to ensure connectivity. This status is returned to the portal, notifying it that the tunnel is ready for use.

Limiting Access

Besides how the *Unattended Access* solution grants access to various endpoints inside the infrastructure, limiting and securing access is of the highest importance. We recommend that customers at the very least:

a. Enable SSO with conditional access for users with remote access privileges.
b. Consider restricting the access to gateways based on the IP addresses that should be allowed to connect via each one.

We recommend that IP address restrictions are made within your own infrastructure, but restrictions can also be set via the portal by going to the gateway details and selecting **Secure Remote Access > Settings > Unattended Access Settings > Gateways > ON-PREMISE > [Gateway] > Settings > IP RESTRICTIONS**:



From here, IP restrictions can be enabled, allowing you to enter the IP addresses you want to allow the ability to access endpoints via the selected gateway.

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.

> **NOTE**
> At A, if you want to use access.work alongside on-premise gateways in a self-hosted implementation, these gateways need to be running *Unattended Access* v2.1.0 or later.

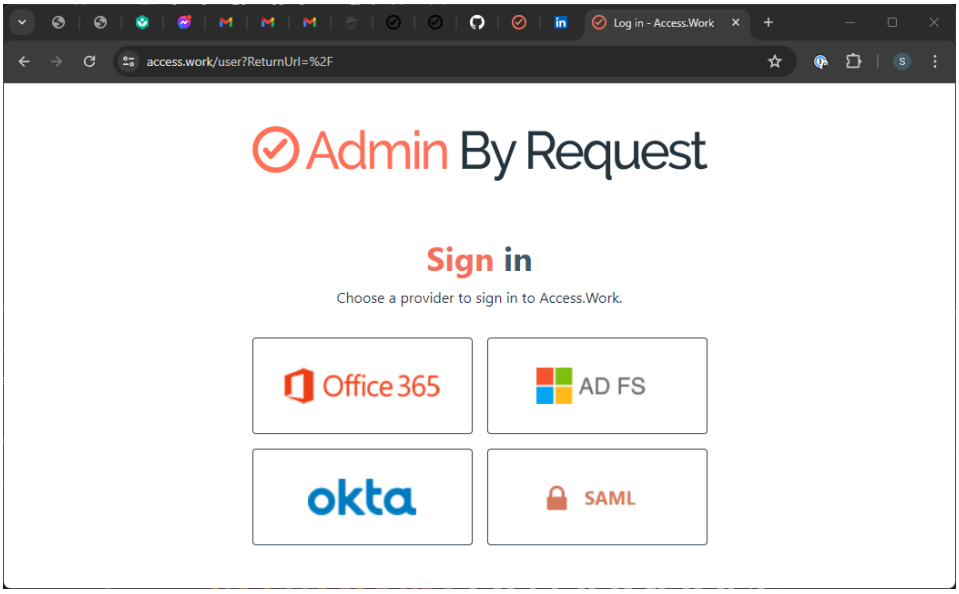
In more detail

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:



5. 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 not available under the free plan).

Portal Administration for Unattended Access

Introduction

This topic describes several key areas of the Admin Portal that can be used to manage *Unattended Access Settings* and *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

Unattended Access Settings

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

AUTHORIZATION tab

Unattended Access is a feature that allows portal admins to remote control computers using only a browser and without requiring a user to be present at the remote computer.

Allow Unattended Access is the overall setting that determines whether or not the feature is enabled.

Setting	Type	Description
Allow Unattended Access	Toggle On | Off Default: **On**	**On** - Allows computers to be accessed remotely without a user present. Unhides *Require approval* and *Require reason* fields. **Off** - Computers cannot be accessed remotely without a user present. Hides *Require approval* and *Require reason* fields. Note that *Remote Support* might still be possible, depending on Remote Support settings.
Require approval (hidden if *Allow Unattended Access* is Off)	Toggle On | Off Default: **Off**	**On** - Sends a request to the IT team, which must be approved before remote access to the server or device is granted. Makes *Require reason* mandatory (i.e. must be On). **Off** - Allows remote access to the server or device without approval. Makes *Require reason* optional (i.e. can be either On or Off).
Require reason (hidden if *Allow Unattended Access* is Off)	Toggle On | Off Default: **Off**	**On** - A reason for remote access must be provided, and it must comprise at least *two words*. This information is stored in the Auditlog. **Off** - No reason is required for remote access, 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.

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 On | Off Default: **Off**	**On** - Additional email notifications are sent to the email addresses listed in *Email addresses*. **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. Note that reloading any defaults does not take effect until **Save** is clicked.

Settings

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

RESOURCES tab

Enable or disable file sharing.

Setting	Type	Description
Allow file sharing	Toggle On | Off Default: **On**	**On** - Allows the upload of files to the server in the cloud. **Off** - Disables the ability to upload files to the server. If file upload is a concern, this setting should be disabled (i.e. set to Off). .
Save	Button	Saves customization and changes to any fields. Note that reloading any defaults does not take effect until **Save** is clicked.

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

Security

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

PASSWORDLESS tab

Used to connect to endpoints passwordless. This setting creates a local shadow account for the portal user. The password is 256 characters long and is automatically rotated and exchanged with the target server with no visibility to the portal user. The local account is enabled only when the portal user is connected.

This setting has no effect in an agentless set up, where the client software is not installed on the server.

Setting	Type	Description
Passwordless access	Toggle On | Off Default: **Off**	**On** - Passwordless access is enabled - a local admin account that is an alias of the logged-in portal user will be created every hour. Unhides *Account is admin* field. **Off** - Passwordless access is disabled.
Account is admin (hidden if *Passwordless access* is Off)	Toggle On | Off Default: **Off**	**On** - The rotating account will have admin-level access.. **Off** - The rotating account will not have admin-level access.
Save	Button	Saves customization and changes to any fields. Note that reloading any defaults does not take effect until **Save** is clicked.

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 On | Off Default: **On**	**On** - The logged-on portal user must authenticate via SSO when connecting remotely to an endpoint. **Off** - Portal user does not need to authenticate via SSO to remotely connect.
Save	Button	Saves customization and changes to any fields. 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 Default: **4 hours**	Select a value between **15 minutes** and **Unlimited**. **Custom** is also available - if selected, choose the required number of **Hours** and **Minutes**.
Save	Button	Saves customization and changes to any fields. Note that reloading any defaults does not take effect until **Save** is clicked.

Gateways

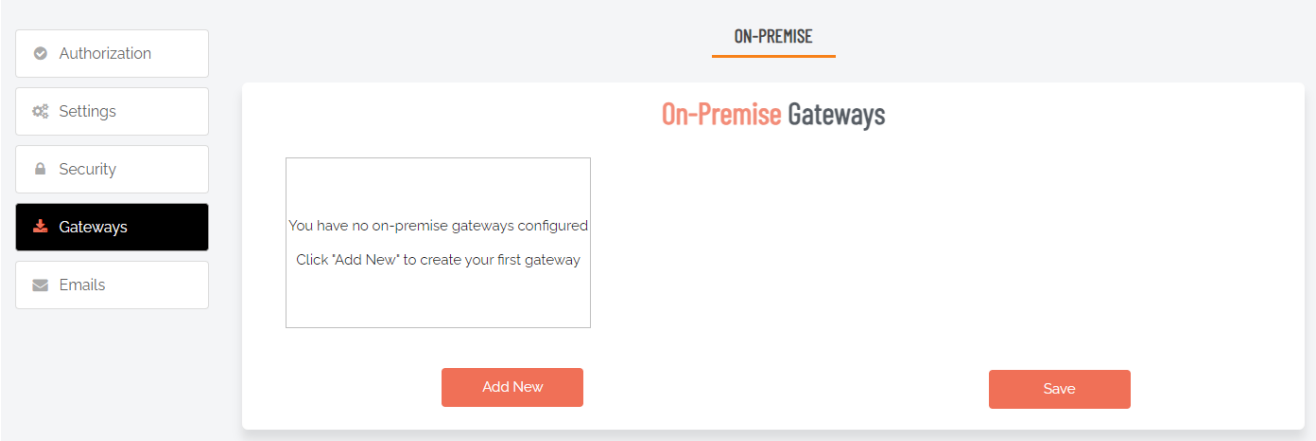
Portal menu: **Secure Remote Access > Settings > Unattended Access Settings > Gateways**

The Gateways menu provides both dashboard and detailed information views. The default view is the "Gateway Dashboard" on the next page, which provides an overview of existing gateways and links and buttons for further information.

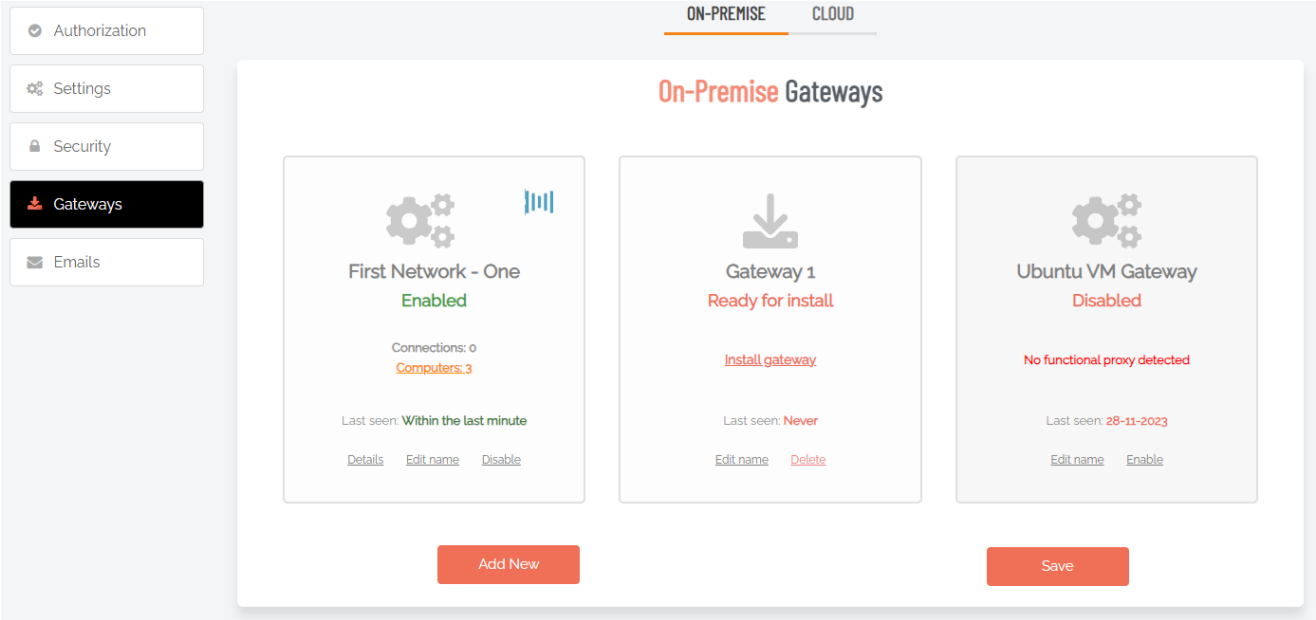
Additional views are: "New Gateway" on page 37 and "Existing Gateway" on page 39.

Gateway Dashboard

First use (i.e. no gateways configured):



Example dashboard showing three gateways:



CLOUD tab

Cloud hosting is when Admin By Request hosts the gateway between your servers and the portal using a *Cloudflare* tunnel. Cloud hosting is the default for *Unattended Access* and is used when no on-premise gateway is detected. In fact, when first enabling *Unattended Access*, the CLOUD tab will not even be visible, since it is enabled by default and requires no configuration.

If configuring an on-premise gateway, the CLOUD tab becomes visible, allowing you to disable it in favor of the on-premise gateway.

Cloud hosting requires installation of the Admin By Request Server endpoint software. If this is not an option or you have devices on which you cannot install the endpoint software, you must use an on-premise gateway.

This option should only be disabled if you have on-premise gateways and want to make sure servers *outside* the gateway networks cannot be accessed.

Setting	Type	Description
Allow cloud gateway	Toggle On | Off Default: **On**	**On** - Allows the remote access gateway to be hosted by Admin By Request in the cloud. **Off** - The remote access gateway cannot be hosted in the cloud.
Save	Button	Saves customization and changes to any fields. Note that reloading any defaults does not take effect until **Save** is clicked.

ON-PREMISE tab

On-premise gateways are used to create a create a traffic gateway from the Admin By Request portal to your internal network. You can set up multiple gateways on multiple networks and limit access to specific users and groups via portal user scopes and sub settings.

Gateway computers, accessed via link *Computers (n)*, are the devices that can be remote controlled through this gateway. Note the following:

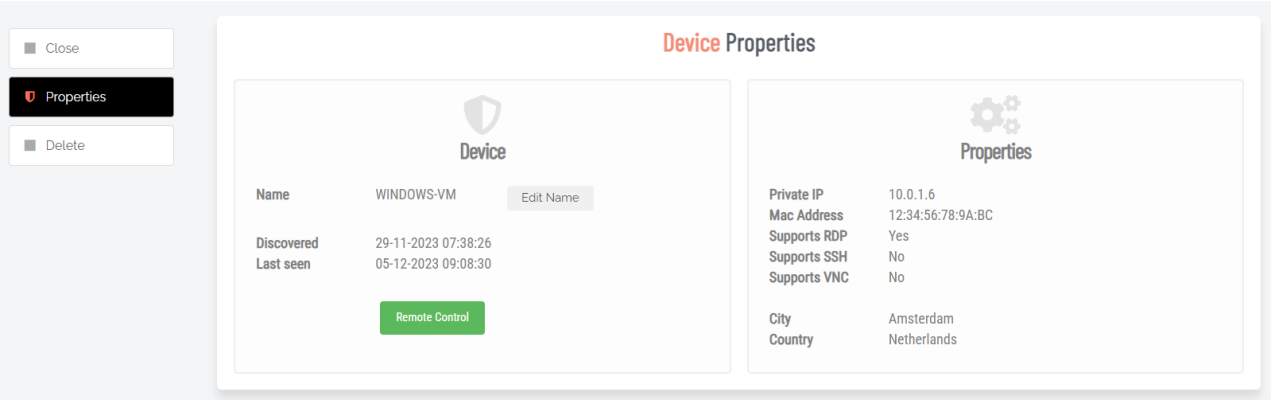
- Computers will appear based on discovery.
- If computers appear that are not supposed to be made available for remote control, they can be deleted from the list.
- If computers have been deleted by mistake, they can be restored under the "Deleted" tab.
- Offline computers are computers that were not seen in last discovery.

Setting	Type	Description
Gateway	Dashboard	Displays information about existing gateways and provides links and buttons for updating, drilling down further and creating new gateways.
Computers (n)	Link (drill-down)	Clicking the drill-down link opens an inventory-style list of all devices accessible via this gateway. Devices can be entered manually or they can be discovered. Devices can be **ACTIVE** or **INACTIVE** and are displayed in the corresponding tab: • **ACTIVE**: able to be connected to via Unattended Access and consume a license. • **INACTIVE**: are not able to be connected via Unattended Access and do not consume a license. Use the Disable/Enable links to make a device active/inactive respectively. Use the **Search** button to search for devices in large lists and the **Export** buttons to export data in the format shown.

Setting	Type	Description
Details	Link (drill-down)	Shows the current status of the gateway, including Internet and LAN availability. Use the **Run discovery now** button to renew discovery of connected devices.
Edit name	Link	Opens the gateway name field in edit mode, allowing the name to be changed. Click the small *Save* icon to update.
Disable	Link	Disables the gateway. Click **Save** to confirm.
Add New	Button	Creates a new gateway and labels it **Gateway 1**, **Ready for install**. Edit the name if necessary and click **Save** to save the new gateway. Note that there are more steps required: once a gateway has been created, it must be installed. Refer to "New Gateway" on the next page for information on how to install a gateway.
Save	Button	Saves customization and changes to any fields. Note that reloading any defaults does not take effect until **Save** is clicked.

To remotely access a device:

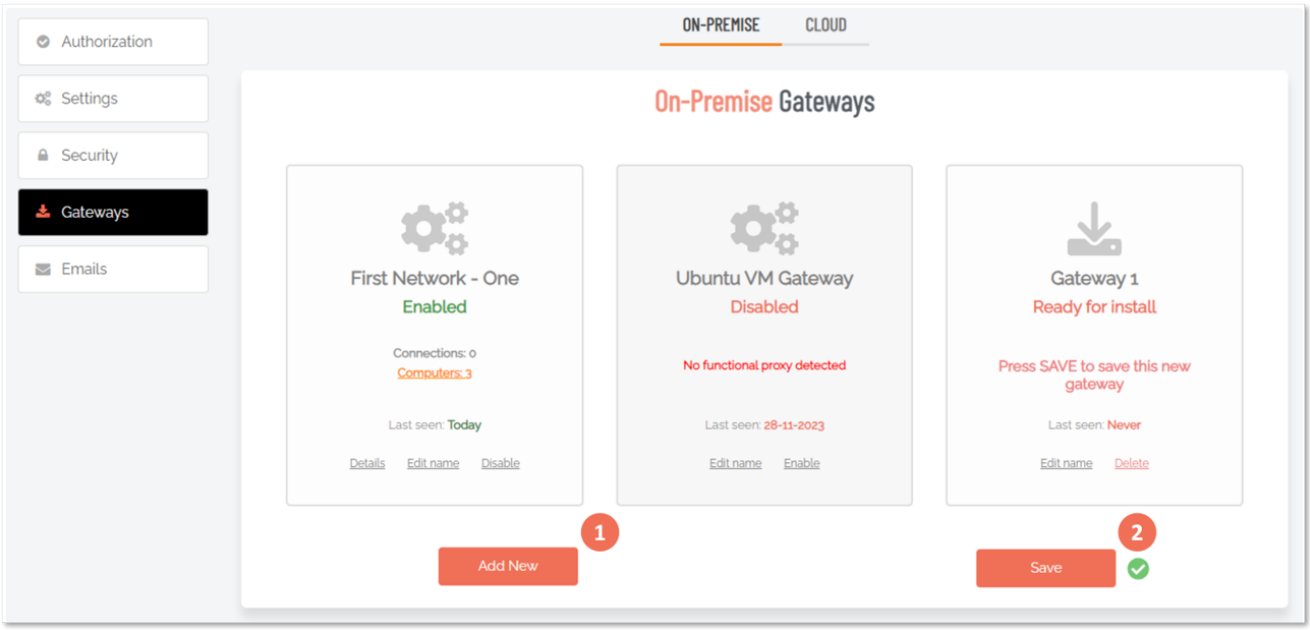
1. In the portal, go to **Secure Remote Access > Settings > Unattended Access Settings** and select menu **Gateways**.
2. Click **Computers (n)** for the gateway connected to the device.
3. In the list of computers, click the device you wish to connect to (either the Computer or Details column).
4. Click button **Remote Control**:



5. Provide your credentials to login remotely:

6. The connection should now appear directly in your browser.

New Gateway



To add a new gateway:

1. From the Gateway Dashboard, click **Add New**.
2. Click **Save**.
3. Click link Install gateway (see below).

Back

Returns to the Dashboard.

Install

Once a gateway has been created (and saved), it is ready to be installed, which is initiated by clicking link **Install gateway** from the Dashboard. This opens the **Install** menu for the new gateway.

DOCKER tab

> **NOTE**
> Select the technical infrastructure that corresponds to your environment. The Install menu opens by default at the DOCKER tab, but KUBERNETES and CUSTOM are also available.

Docker can be used to host the gateway containers. Use the clipboard button **Copy YML to clipboard** to copy the Docker Compose YML file content to the local computer's clipboard and paste it into a `docker-compose.yml` file in the root of your Docker host.

> **IMPORTANT**
> We strongly recommend not to save the content to a local file. We use the clipboard to avoid downloading the content to your local machine because it contains your highly sensitive private keys that should never reside outside your Docker host. Once the gateway reports home, this page will disappear forever to protect your private keys.

Setting	Type	Description
Automatic enrollment	Toggle On | Off Default: **On**	**On** - Discovered devices appear immediately in the ACTIVE list and the inventory. Automatic enrollment is recommended. **Off** - Discovered devices appear in the INACTIVE list and devices will need to be enabled one-by-one.
Copy YML to clipboard	Button	Copies the required YML code to the local computer's memory.
See content	Link	Displays the YML code in a scrollable window.

KUBERNETES tab

Kubernetes is typically highly customized on your side and we therefore only provide a simple yml file compilation in a single file.

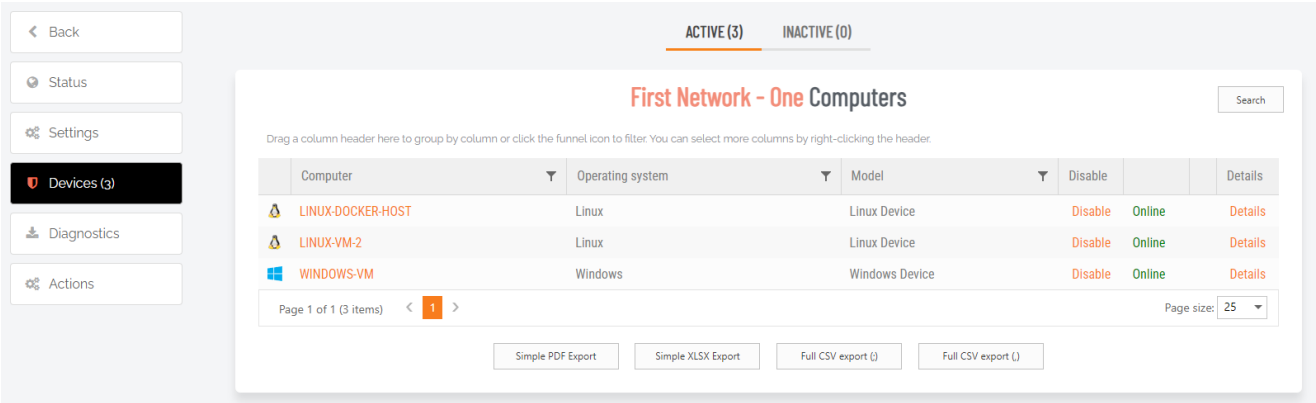
Parameter names and values in the Kubernetes settings table are the same as for the DOCKER tab.

CUSTOM tab

In a custom setup, you will need the secret keys listed in the yml file. Please contact us for more information, if necessary.

Parameter names and values in the Custom settings table are the same as for the DOCKER tab.

Existing Gateway



Back

Returns to the Dashboard.

Status

Shows the current status of the gateway, including Internet and LAN availability.
Use the **Run discovery now** button to renew discovery of connected devices.

Settings

DISCOVERY tab

Discovery finds computers and devices on your network where the gateway is installed. It is necessary to run discovery at least once to detect devices on your network. Once initial discovery is complete, you can disable it and enable temporarily when you know there are new devices on the network.

Automatic enrollment means that new devices appear right away in your inventory and are ready for remote control. If this option is off, new devices appear as *Disabled* in the **Devices (n)** menu - disabled devices can be enabled manually one-by-one.

Setting	Type	Description
Enable discovery	Toggle On | Off Default: **On**	**On** - The discovery service is enabled and will check for new devices at the frequency set in *Discovery interval*. **Off** - The discovery service is disabled - no new devices will be found when they are attached to the network.
Automatic enrollment	Toggle On | Off Default: **On**	**On** - Discovered devices appear immediately in the ACTIVE list and the inventory. Automatic enrollment is recommended. **Off** - Discovered devices appear in the INACTIVE list and devices will need to be enabled one-by-one.
Discovery interval	Selection Default: **15 m**	How often the discovery service checks for new devices. There are ten options, ranging from 5 minutes to weekly.
Save	Button	Saves changes made to this setting.

TUNNEL tab

Cloudflare Tunnel sits between the end user and your gateway to relay traffic.

If you disable the tunnel, you must provide your own on-premise webserver to relay incoming traffic to this gateway. Refer to "What if I don't want to use Cloudflare tunnels?" on page 20 for more information.

When changing this configuration, you can check under **Status** within a minute if the connection is functional.

Setting	Type	Description
Use Cloudflare tunnel	Toggle On | Off Default: **On**	**On** - A Cloudflare-hosted tunnel will be created for traffic. **Off** - A Cloudflare tunnel will not be used. You must configure your own webserver to relay traffic.
Save	Button	Saves changes made to this setting.

IP RESTRICTIONS tab

IP Restrictions limits which IP addresses the user's browser can connect from. This feature can be used for highly sensitive networks. A few things to consider:

- It may be more flexible to set IP address restrictions on your firewall in front of the gateway instead.
- Your gateway may be configured to not receive requests from the internet, in which case the user must be on the local network or connect using VPN.
- Your portal users should always be set up with Single Sign-On. Most SSO providers have conditional access, where you can set, for example, countries from which access is allowed.

Setting	Type	Description
IP restrictions	Toggle On | Off Default: **Off**	**On** - Limits the IP addresses from which browsers can connect. Shows the *.Allowed IPs* field. **Off** - There are no IP restrictions. Hides the *.Allowed IPs* field.
Allowed IPs	Text	A list of IP addresses that are permitted to access the gateway. Note that no computer will be able to connect to the gateway if *IP restrictions* is on and there are no entries in the list.
Save	Button	Saves changes made to this setting.

Devices (n)

Clicking the drill-down link opens an inventory-style list of all devices accessible via this gateway. Devices can be entered manually or they can be discovered.

Devices can be **ACTIVE** or **INACTIVE** and are displayed in the corresponding tab:

- **ACTIVE**: able to be connected to via Unattended Access and consume a license.
- **INACTIVE**: are not able to be connected via Unattended Access and do not consume a license.

Use the Disable/Enable links to make a device active/inactive respectively.
Use the **Search** button to search for devices in large lists and the **Export** buttons to export data in the format shown.

> **NOTE**
> Gateway computers are those that can be remote controlled through this gateway. Computers appear based on discovery. If computers appear that are not supposed to be made available for remote control, they can be *disabled*, which moves them to the INACTIVE tab. Any computers currently disabled can be *enabled*, which moves them to the ACTIVE tab. Offline computers are computers that were not seen in the last discovery.

Diagnostics

CALLBACKS tab

Displays a log-style view of gateway callback events. Includes columns for:

- Time - date and time the activity occurred.
- Call - the type of event.
- Data - the raw data in JSON form.

Rows can be sorted according to a column by clicking the column title (click again to reverse the sort), and data can be filtered by clicking a column's filter icon. Columns can also be rearranged by clicking, holding and dragging a column to another position.

Use the **Refresh** button to get the latest diagnostics.

LOGS tab

Click the **Request Logs** button to retrieve log files. Takes up to 60 seconds.

Actions

PURGE DEVICES tab

Purge devices removes devices that are *offline* in the **Devices (n)** ACTIVE or INACTIVE tabs.

> **NOTE**
> Purged devices are effectively removed from the inventory, although they will automatically re-appear if they are discovered at a later time.

DELETE GATEWAY tab

Delete gateway deletes the gateway. Any computers in the **Devices (n)** menu that are not discovered by other gateways will not be accessible until a new gateway discovers these.

> **IMPORTANT**
> Deleting a gateway can lead to inaccessible devices.

Emails

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

Emails go out when *Require approval* is turned **On** under Authorization. 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 Default: **Approved email**	**Approved email** - Loads a template that advises *the user* (i.e. requester) that the request for access has been approved. **Denied email** - Loads a template that advises the request for access has been denied without giving a reason. **Denied with reason** - Loads a template that advises the request for access has been denied and provides the reason. **Administrator notify** - Loads a template that advises *the administrator* (i.e. person who approves or denies) that a request for access is waiting for attention.
Email sender	Text 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. 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 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. **NOTE:** • Default email templates are created by Admin By Request. Contact us if you wish to customize a default email template. • 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. This allows sending email from domains other than @adminbyrequest.com. **NOTE:**

Setting	Type	Description
		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. Includes three views: • **Design**: WYSIWYG view of content. Enter and format body text here. • **HTML**: The same content in HTML format. Can also be edited if necessary and changes will be reflected in Design and Preview. • **Preview**: What the recipient sees. Read only - switch to Design view to make changes. **Dynamic content tags** 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. The following tags are available: • {UserFullName} Name of requesting user • {UserEmail} Email address of requesting user • {UserPhone} Phone number of requesting user • {UserReason} Reason the requesting user gave • {DenyReason} Admin's reason for denial (only used for denial with reason) • {ComputerName} Name of requesting computer • {AdminUserName} Name of administrator receiving notification (only for admin notify) • {AuditlogURL} URL to this entry in the auditlog • {RequestURL} URL to this entry in requests
Save	Button	Saves customization and changes to any fields. 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. For example: **itsupport@mycompany.com**

Setting	Type	Description
Email sender	Text 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.
Email subject	Text 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. **NOTE:** • Default email templates are created by Admin By Request. Contact us if you wish to customize a default email template. • 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. This allows sending email from domains other than @adminbyrequest.com. **NOTE:** 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. Includes three views: • **Design**: WYSIWYG view of content. Enter and format body text here. • **HTML**: The same content in HTML format. Can also be edited if necessary and changes will be reflected in Design and Preview. • **Preview**: What the recipient sees. Read only - switch to Design view to make changes. ### Dynamic content tags 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. The following tags are available: • {ID} Unique auditlog trace no

Setting	Type	Description
		• {APIID} ID for looking up this entry through the public Auditlog API • {Status} Requested, Approved, Denied, Started, Finished • {UserFullName} Name of the requesting user • {UserEmail} Email address of requesting user • {UserPhone} Phone number of requesting user • {UserReason} Reason the requesting user gave • {DenyReason} Admin's reason for denial • {ComputerName} Name of requesting computer • {AdminUserName} Admin approving or denying request • {InstallList} Installed programs • {UninstallList} Uninstalled programs • {AuditlogURL} URL to this entry in the auditlog • {RequestURL} URL to this entry in requests **Ticket ID** You can find a ticket by its ticket ID using the **Search** button in the Auditlog. **Voided text** 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 > Unattended Access 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

Unattended Access	Remote Support
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 On | Off Default: **On**	**On** - This setting will overrule its associated global setting. The global setting fields are then undimmed and become available for editing. **Off** - This setting will not overrule its associated global setting. 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 On | Off Default: **Off**	**On** - Sub-settings are active for the set named in *Sub settings name*. **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 On | Off One entry for each Gateway Default: **Off**	**On** - Scope is active for this gateway. **Off** - Scope is not active for this gateway. 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. 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
1.0 15 January 2024	2.0.1 15 January 2024	Initial document release
1.1 12 February 2024	2.0.9 12 February 2024	Updated Overview diagram "How does *Unattended Access* work?" Added documentation on new environment variable AUTH__TOKEN.
1.2 20 February 2024	2.0.9 12 February 2024	Resized images. Fixed broken cross-references. Added "sudo" to docker commands.
1.3 10 April 2024	2.0.9 12 February 2024	Added settings tables in chapter "Settings": • Security > MFA • Gateways > Add New > Kubernetes • Gateways > Add New > Custom Updated images and content to highlight that CLOUD tab is not visible until an on-premise gateway is created.
1.4 14 May 2024	2.1.0 24 April 2024	Added "access.work" chapter.
2.0 26 August 2024	26 August 2024	Renamed "Remote Access" to "Unattended Access" and brought under the new product *Secure Remote Access* umbrella. Renamed "access.work" to "Vendor Access".
2.1 6 September 2024	26 August 2024	Updated section *Prerequisites* in chapter "Overview".
2.2 4 October 2024	26 August 2024	Adjusted api URLs in *Prerequisites* section of chapter "Overview" so they point to the correct data center locations.
2.3 29 November 2024	26 August 2024	Added process flow steps and diagram to chapter "Unattended Access Overview".

Index

L

M

N

O

P

R

S

T

U

V