Document Code: **PM-RA-ITAG**

Document Version: **1.3**

Document Date: **10 April 2024**

Remote Access: IT Admin Guide

Install and manage Remote Control gateways

Admin By Request

Remote Access Product Version: **2.0.9**

Contact Admin By Request

1390 Market Street, Suite 200
San Francisco, CA 94102

Phone and Email:
adminbyrequest.com/contact

www.adminbyrequest.com
linktr.ee/adminbyrequest

Table of Contents

Remote Access Overview

What is Remote Access?

Remote Access is an addition to Admin By Request Server Edition that will allow 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 Remote Access eliminates the need for VPN and jump servers, while still maintaining a secure and segregated setup.

Prerequisites

Remote Access has two primary ways of operating (i.e. two possible setups):

1. Used as a managed cloud service via Admin By Request.
2. Used as a self-hosted implementation inside your own infrastructure via Docker.

The prerequisites for the Remote Access product vary depending on the desired setup.

1. Remote Access as a managed service

The only requirement for using Remote Access as a managed service is that your infrastructure allows an outbound connection to establish a secure tunnel from your respective endpoints and that these have the Admin By Request Server agent installed.

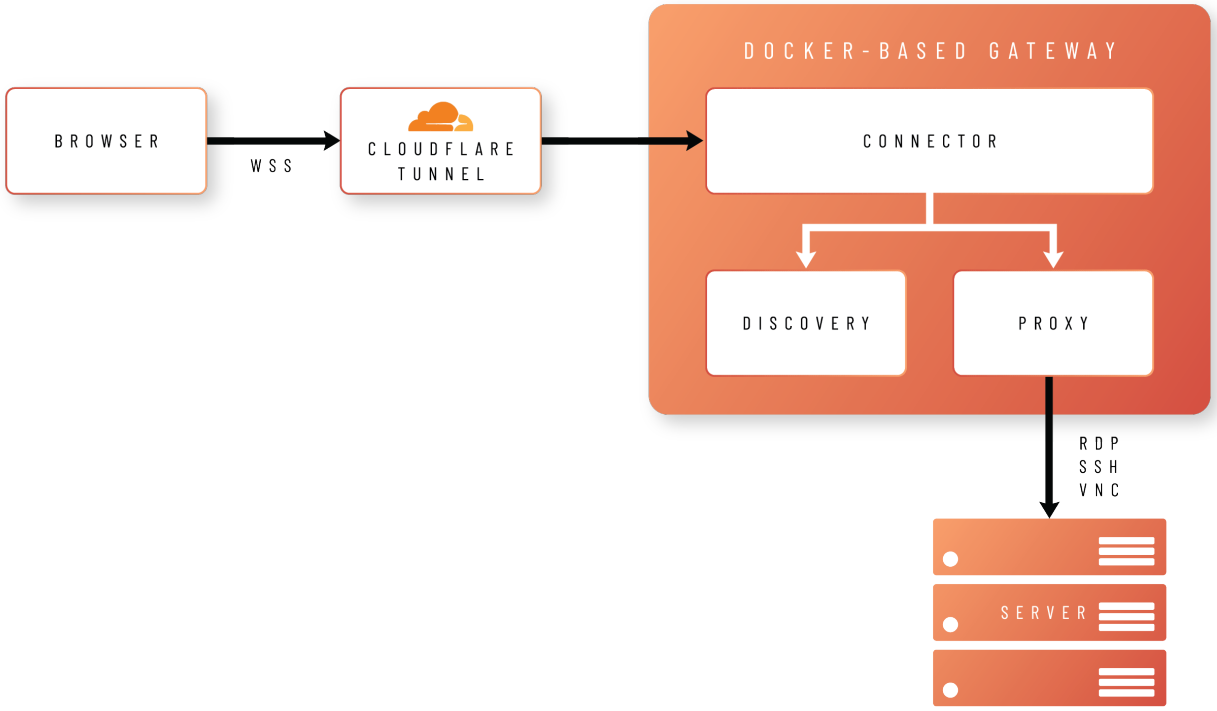
2. Remote Access as a self-hosted implementation

In order to run Remote Access on-premise inside your own infrastructure, you will need to be able to run a few Docker containers as well as allow outbound connections to Cloudflare in order to establish a tunnel.

How does Remote Access work?

The idea behind Remote 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 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.

What next?

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

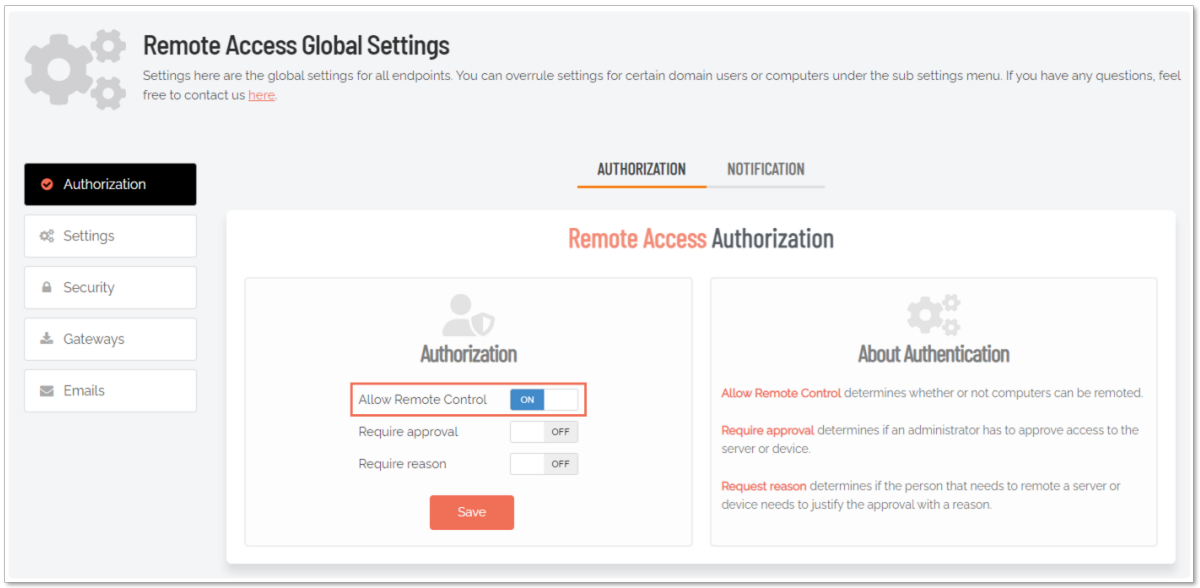
The next section covers the initial steps for enabling Remote Access, followed by the steps required for a managed cloud service, and then the steps required for a self-hosted implementation.

Getting Started with Remote Access

How do I get started – General

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

1. In order to enable remote access, simply log into the Admin By Request portal and head over to **Settings > Server Settings > Remote Access Settings**.
2. From the AUTHORIZATION tab, ensure that *Allow remote control* is turned **On**:



How do I get started – Managed Service?

A *managed service* is a way of operating Remote 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 Server agent installed.

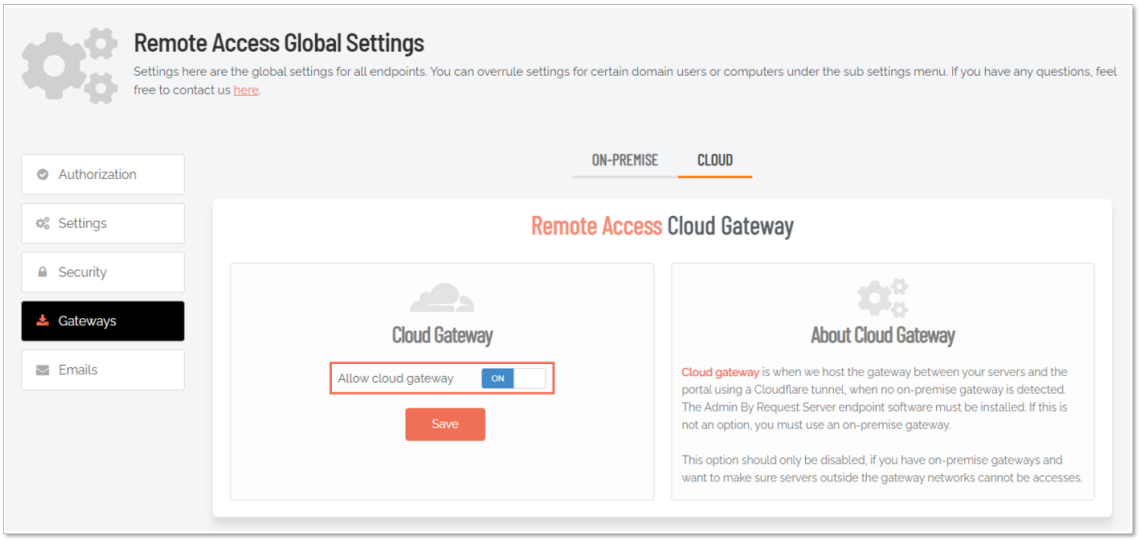
Using Admin By Request's Managed Service for remote access is the default. If you decide on this option when first enabling Remote Access, no configuration is required; all you need to do is:

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

If this is not the first time enabling Remote 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 Server agent installed
2. In the portal, go to **Settings > Server Settings > Remote Access Settings**.
3. Select the Gateways menu and, from the CLOUD tab, ensure that *Allow cloud gateway* is **On**:



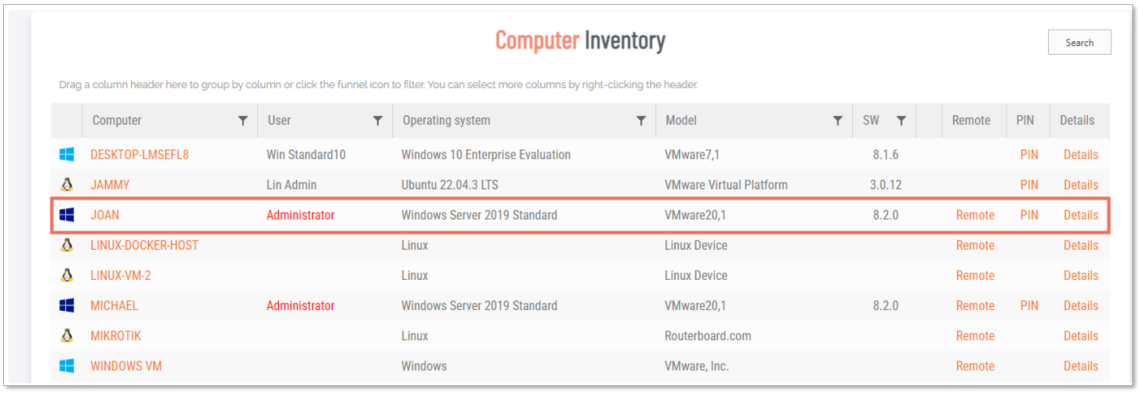
> **NOTE:**
> The CLOUD tab becomes visible only when an on-premise gateway is created. If no on-premise gateway exists, Remote Access will use the managed service option, which is enabled by default and requires no configuration.
>
> Configuring an on-premise gateway means disabling the cloud gateway (see "How do I get started – 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.

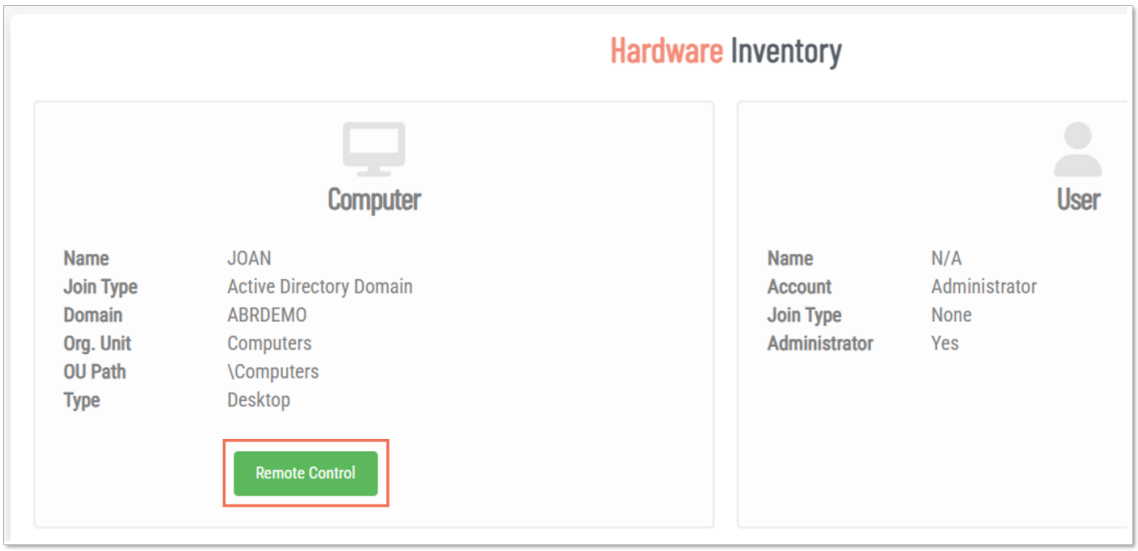
B. Connect to an endpoint

> **NOTE:**
> In order to allow Admin By Request to connect to your endpoints, these endpoints 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 select an endpoint with the Admin By Request Server agent installed:



2. Click the **Remote** link for this server and then, on the Hardware Inventory screen, click **Remote control**:



3. Enter *User name* and *Password* and click **Sign in**:

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

How do I get started – Self-hosted Implementation?

A *self-hosted implementation* means that you run Remote 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.

IMPORTANT:
With the release of the 2.0.9 version of Remote Access, we have introduced a new environment variable that needs to be present in order for the gateway to function properly.

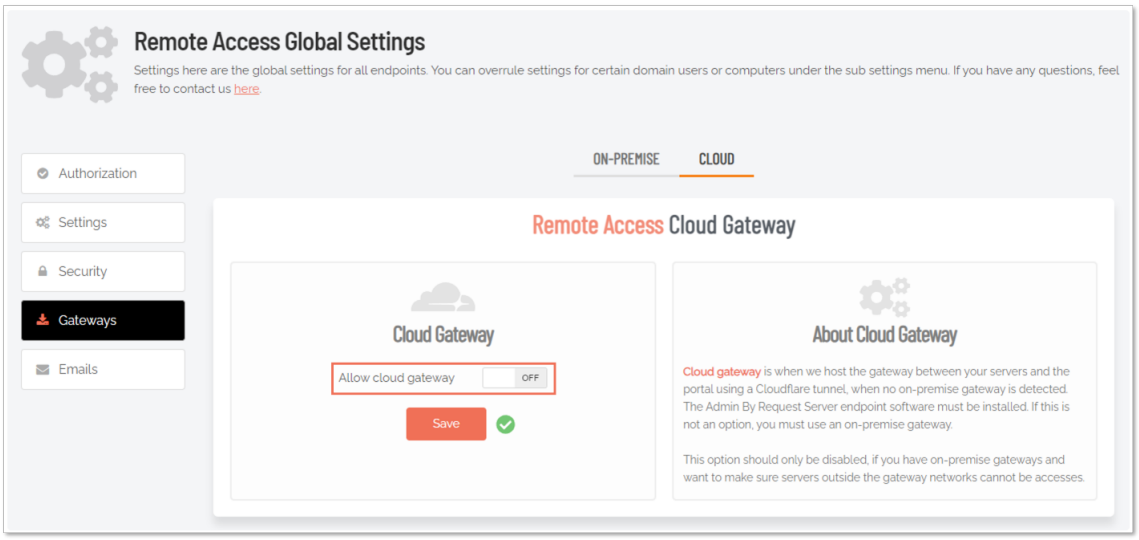
The new variable is called AUTH__TOKEN and, If you're upgrading your on-premise gateway from 2.0.1 to the latest version, you will need to add this environment variable to your Docker setup.

Please refer to "Upgrading Remote Access On-Premise (Self-hosted)" on page 10 for more information.

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

A. Disable cloud hosting

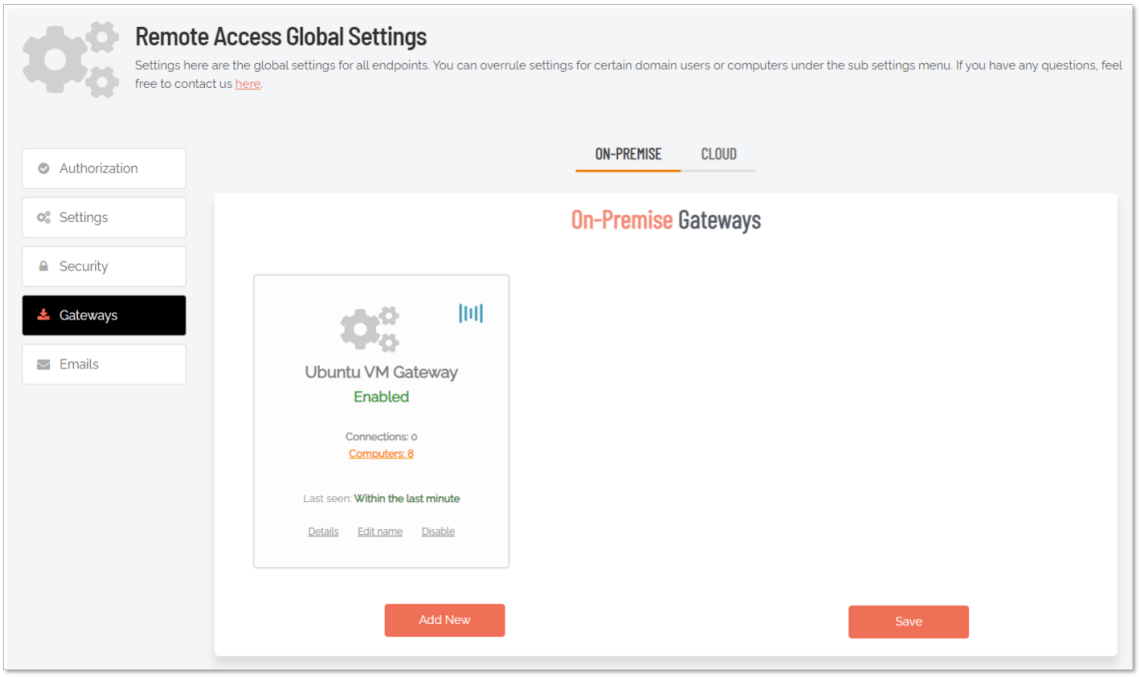
1. Ensure that your endpoints have the Admin By Request Server agent installed.
2. In the portal, go to **Settings > Server Settings > Remote Access Settings**.
3. Select the Gateways menu and, from the CLOUD tab, ensure that *Allow cloud gateway* is **Off**:



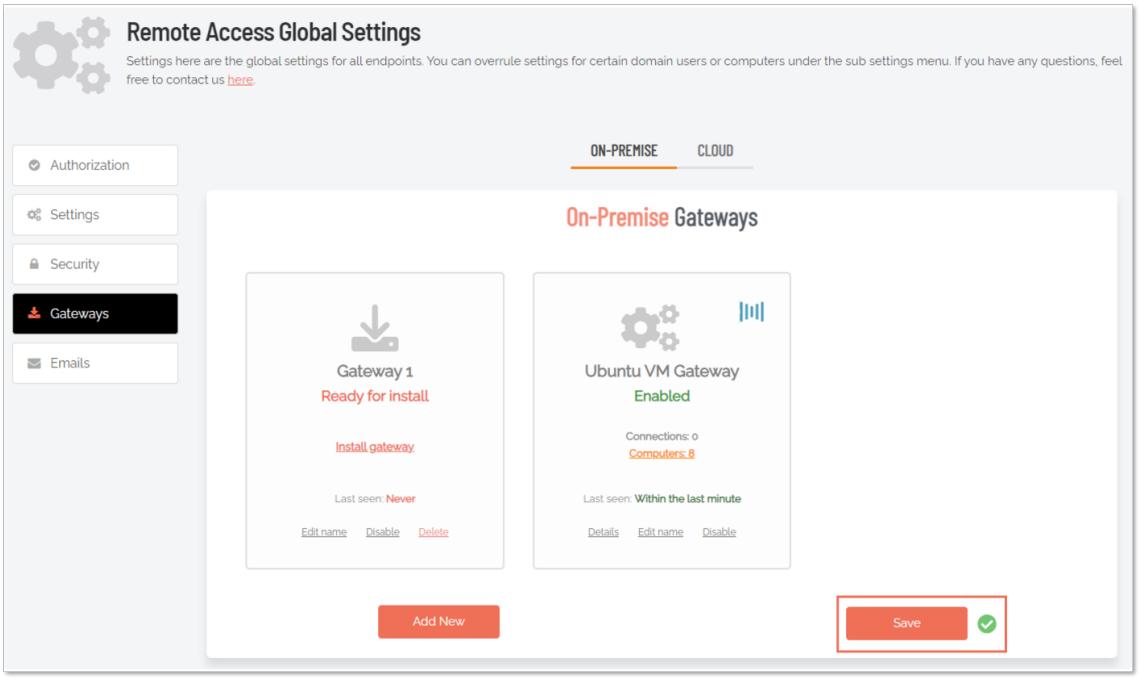
4. Click **Save** if making changes.

B. Create a gateway

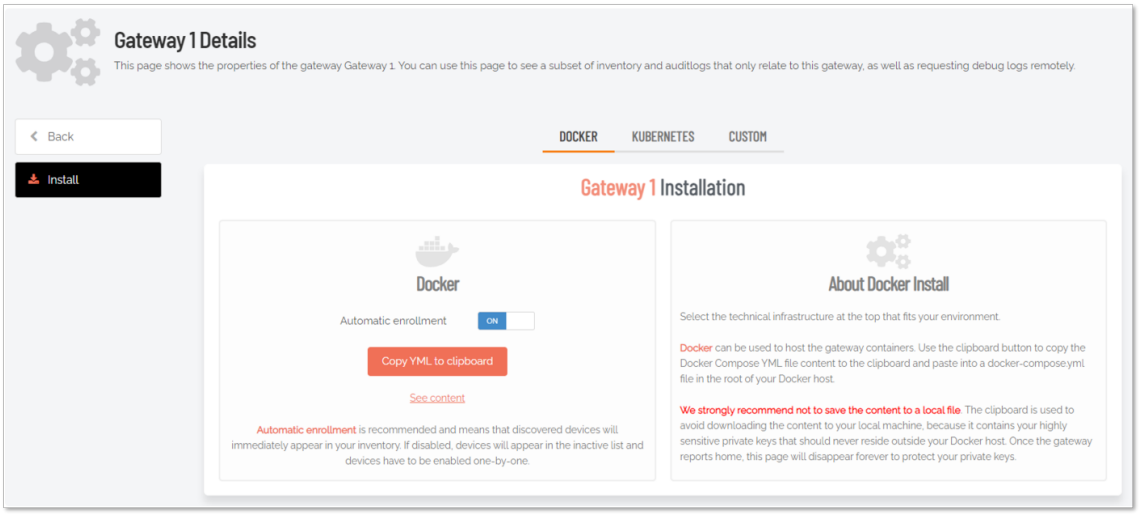
1. In the portal (Remote Access Global Settings), from the Gateways menu, select the ON-PREMISE tab. This shows the current gateways for your tenant:



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 Remote 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:

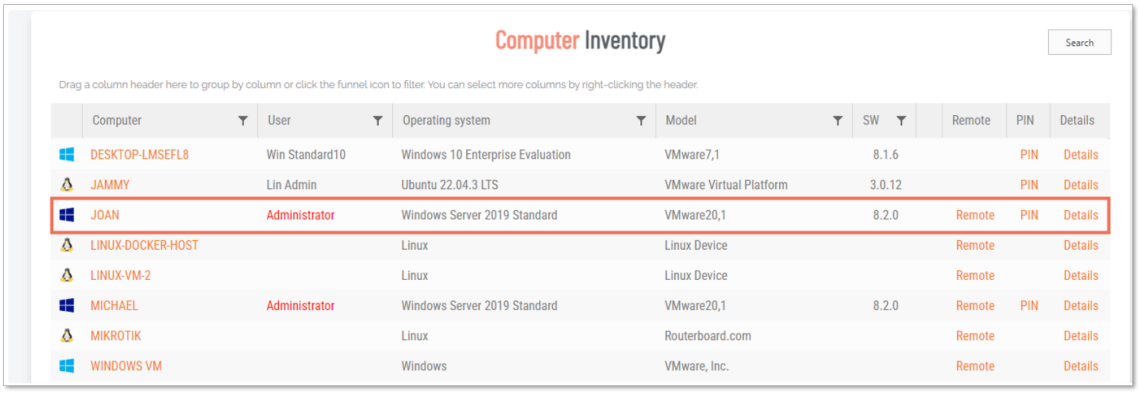
```
sudo docker compose up -d
```

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.

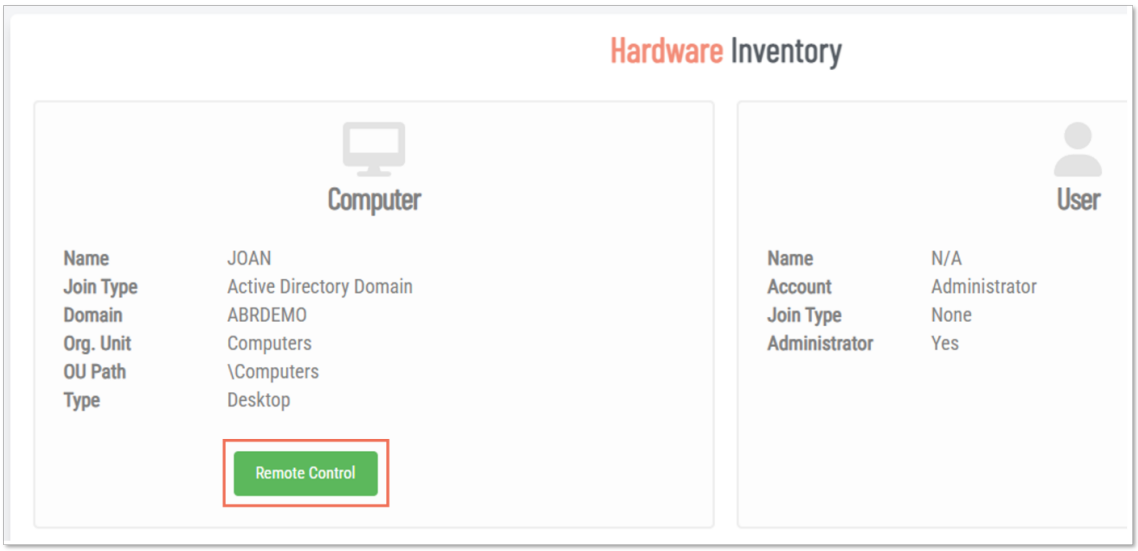
C. Connect to an endpoint

> **NOTE:**
> In order to allow Admin By Request to connect to your endpoints, these endpoints 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 select an endpoint with the Admin By Request Server agent installed:



2. Click the **Remote** link for this server and then, on the Hardware Inventory screen, click **Remote control**:



3. Enter *User name* and *Password* and click **Sign in**:

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

Upgrading Remote Access On-Premise (Self-hosted)

A new environment variable has been introduced from version 2.0.9 that needs to be present in order for your gateway to function properly. The new variable is called **AUTH__TOKEN** and you can add this environment variable 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 Server agent. 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 the next page for more information on Discovery.

Modifying Configurations

Configuring Discovery

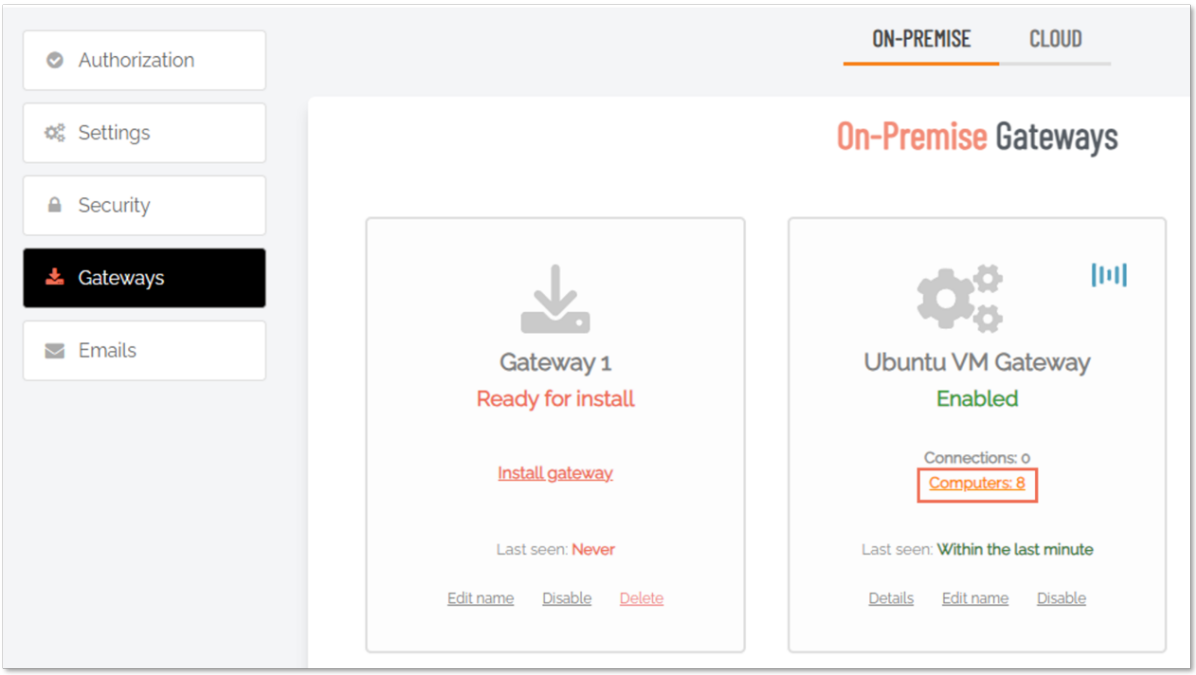
> **IMPORTANT:**
> If you run your gateway behind a reverse proxy, you need to ensure that the end user's IP is forwarded to the gateway using the `X-Forwarded-For` header.

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**.

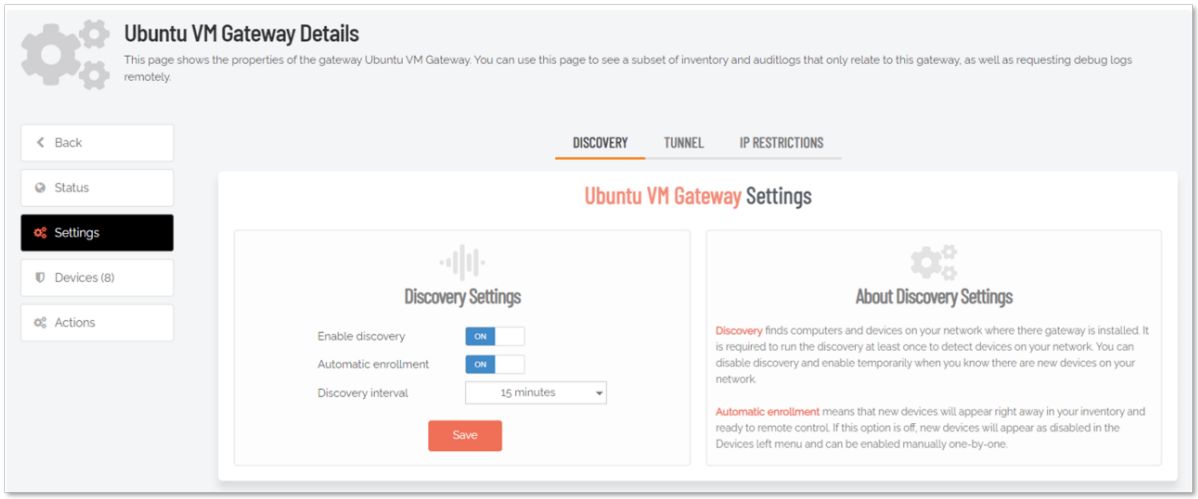
This gives you the advantage of not having to manually map endpoints that are not running the Admin By Request Server agent. This also has the benefit of mapping your network(s) automatically to your Admin By Request inventory, allowing you to connect to agent-less devices like routers, firewalls etc.

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 **Settings > Server Settings > Remote 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.

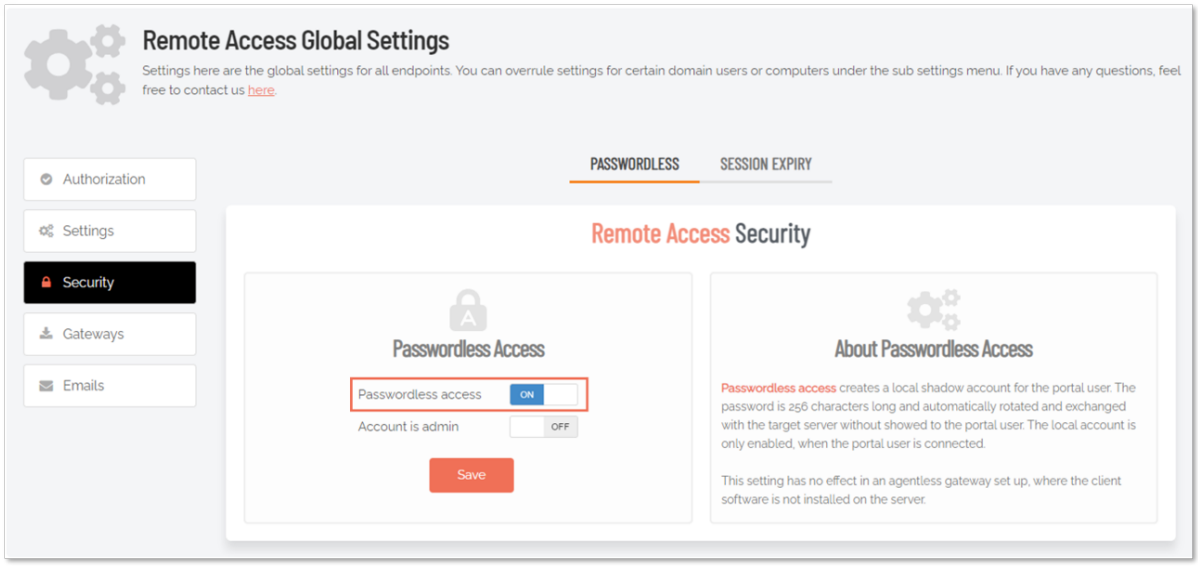
> **NOTE:**
> Refer to "Settings" on page 31 for more information on configuring discovery settings.

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 **Settings > Server Settings > Remote 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 Server agent 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 Remote 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 29).

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 Remote Access work?" on page 1.

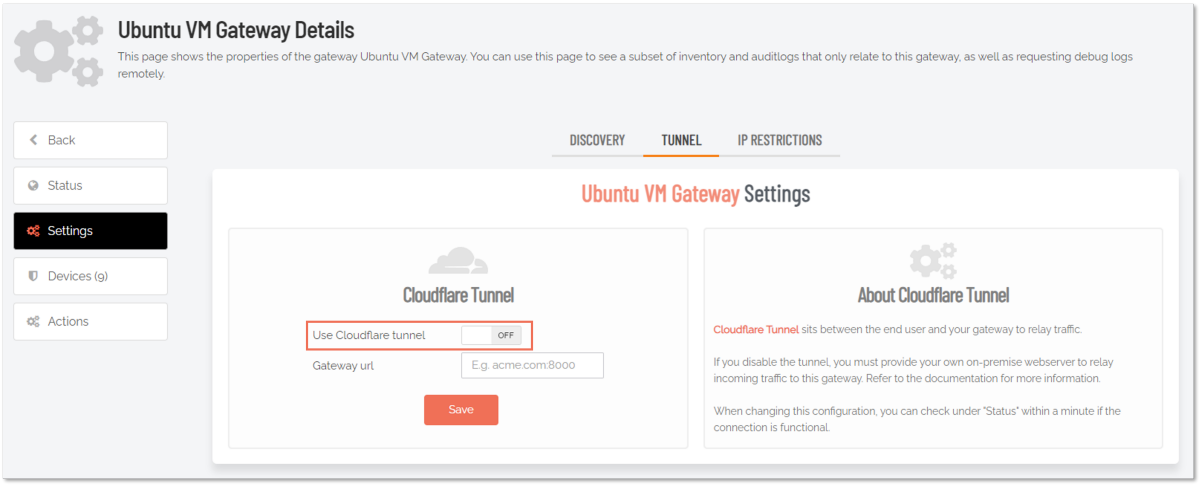
What if I don't want to use Cloudflare tunnels?

You can also use the Remote 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 **Settings > Server Settings > Remote 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 Remote 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.

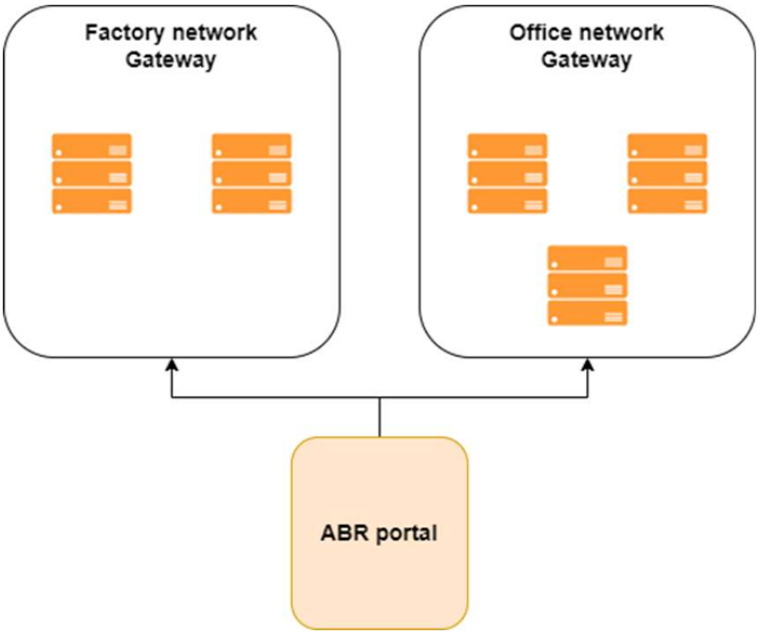
Refer to "Remote Access Auditlog" on page 18 for more information about the Auditlog.

Multi-Gateway Setup

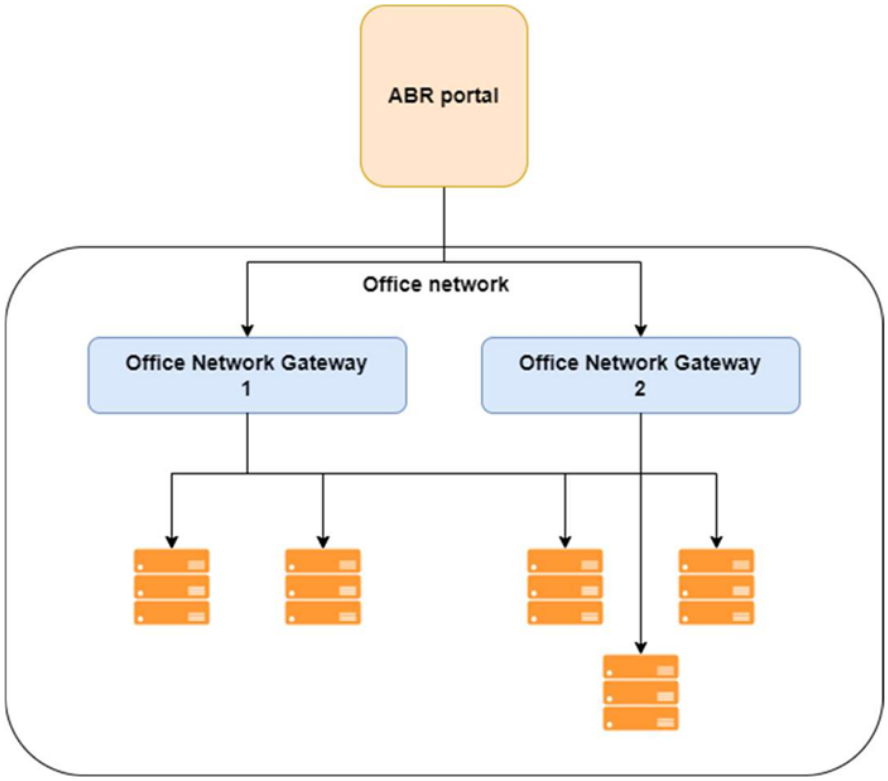
In order for the on-premise gateway to allow connections to your remote endpoints, there needs to be a direct connection path. This means that the user needs to be able to connect to the Connector, the Connector needs to be able to connect to the Proxy container and the Proxy container needs to be able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

Remote Access Auditlog

All sessions with Remote 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 **Settings > Server Settings > Remote 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 Remote 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.

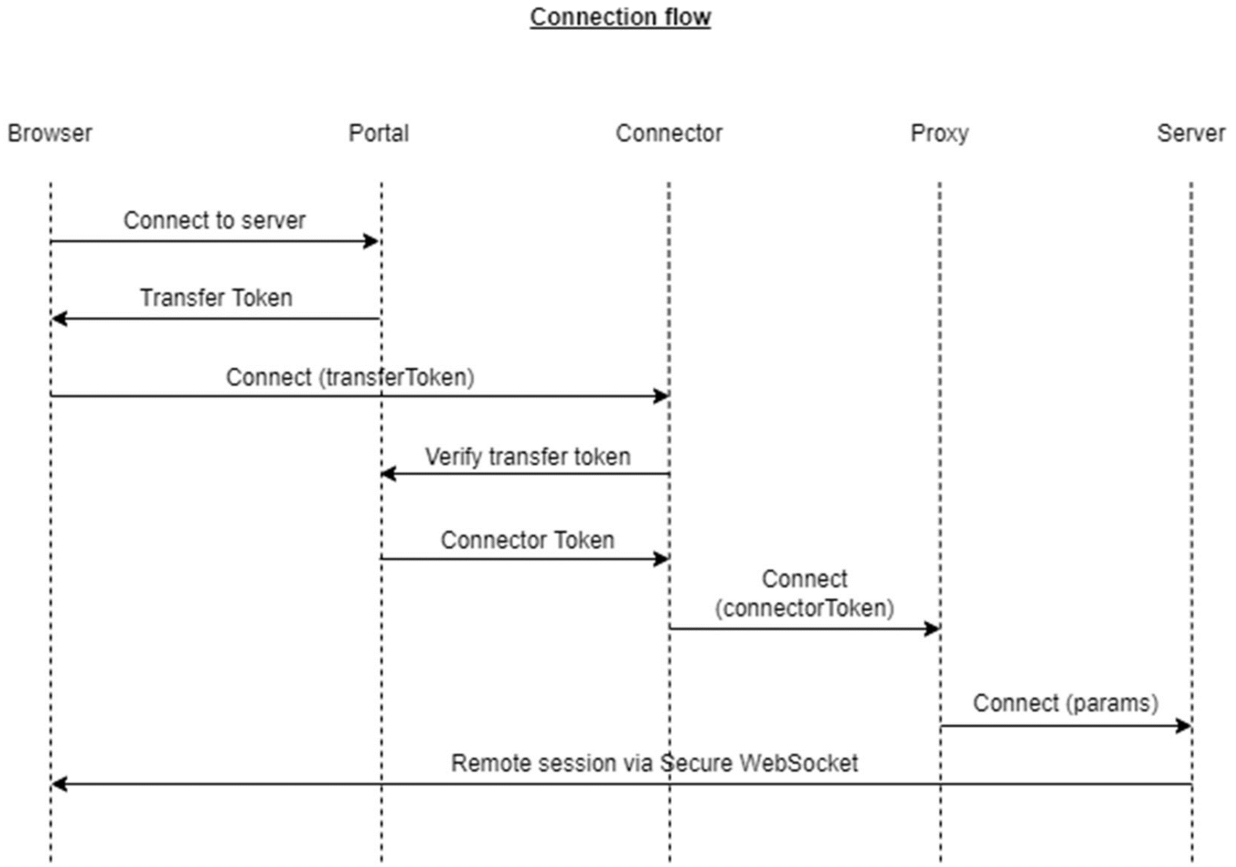
The connector token is encrypted using a secret only known by the Connector and the Admin By Request portal. The token values are also HMAC-validated by verifying a signed hash value of the connection properties.

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.



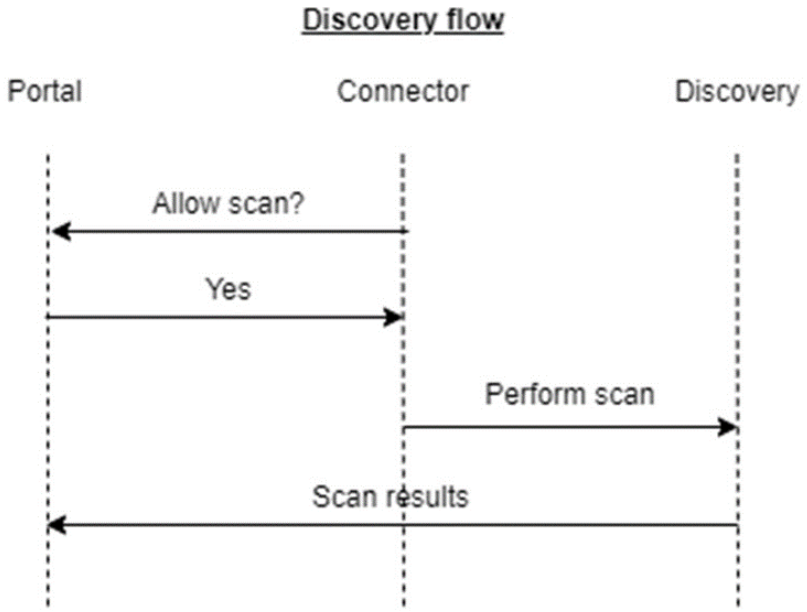
During this process, the following happens:

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:

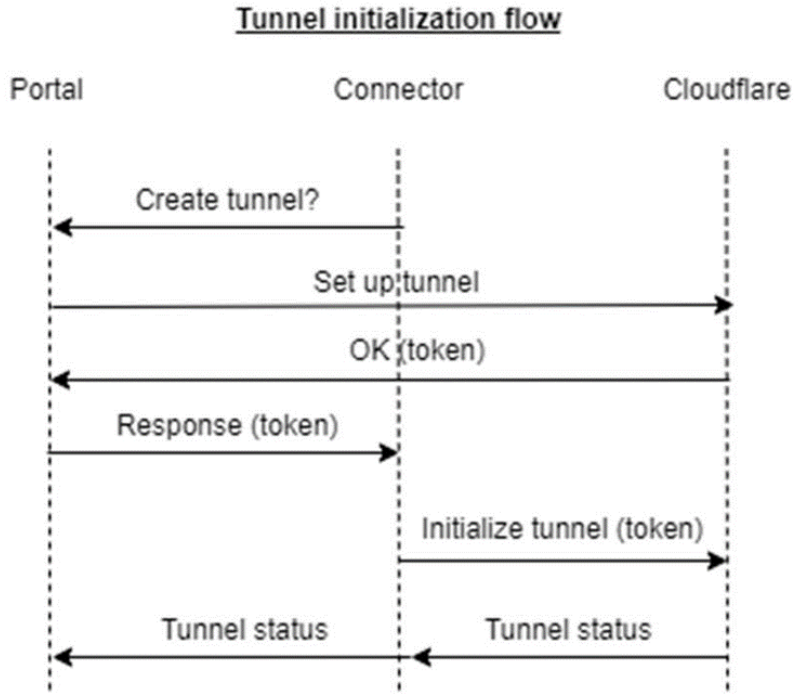


The Connector asks the portal repeatedly if a discovery scan should be allowed to run. Based on the settings within the portal, this might eventually return a positive result.

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.

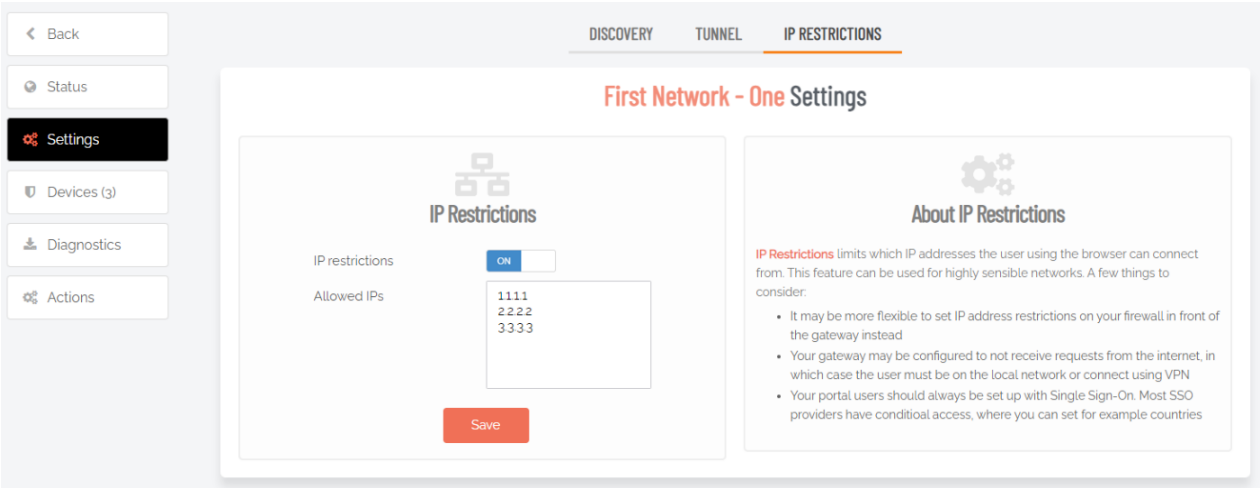
This token is returned to the Connector, which then initializes the tunnel to Cloudflare. Once the tunnel has been established, a status call is made to ensure connectivity. This status is returned to the portal, notifying it that the tunnel is ready for use.

Limiting Access

Besides how the Remote 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 **Settings > Server Settings > Remote Access Settings > Gateways > [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.

Settings

Remote Access Global Settings

Portal menu: **Settings > Server Settings > Remote Access Settings**

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

Authorization

Portal menu: **Settings > Server Settings > Remote Access Settings > Authorization**

Authorization tab

Allow Remote Control determines whether or not computers can be remotely accessed.

Setting	Type	Description
Allow Remote Control	Toggle On | Off Default: **Off**	**On** - Allows computers to be accessed remotely. Unhides *Require approval* and *Require reason* fields. **Off** - Computers cannot be accessed remotely. Hides *Require approval* and *Require reason* fields.
Require approval (hidden if *Allow Remote Control* 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 Remote Control* 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 (for *Run As Admin*, *Admin Session*, or *Remote Access*).

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 remote access is requested (Server Settings > Remote Access)

As with other request types, new Remote Access requests for approval always appear under **Requests > Pending** in the Portal top menu. This *Notification* setting enables and configures a further 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. Refer to the Admin By Request documentation site (left menu **Portal > Mobile Application**) for more information on the mobile application.

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: **Settings > Server Settings > Remote 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 desktop is recorded, when an on-premise gateway is used.

Setting	Type	Description
Screen recording	Toggle On | Off Default: **Off**	**On** - Screen recording is enabled. **Off** - Screen recording is disabled.

Setting	Type	Description
		Files are stored locally on your on-premise gateway and can be requested in the auditlog by expanding the relevant line.
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: **Settings > Server Settings > Remote Access Settings > Security**

Passwordless tab

Used to connect to servers 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 a server.

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

Setting	Type	Description
Require MFA	Toggle On | Off Default: **On**	**On** - The logged-on portal user must authenticate via SSO when connecting remotely to a server.

Setting	Type	Description
		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

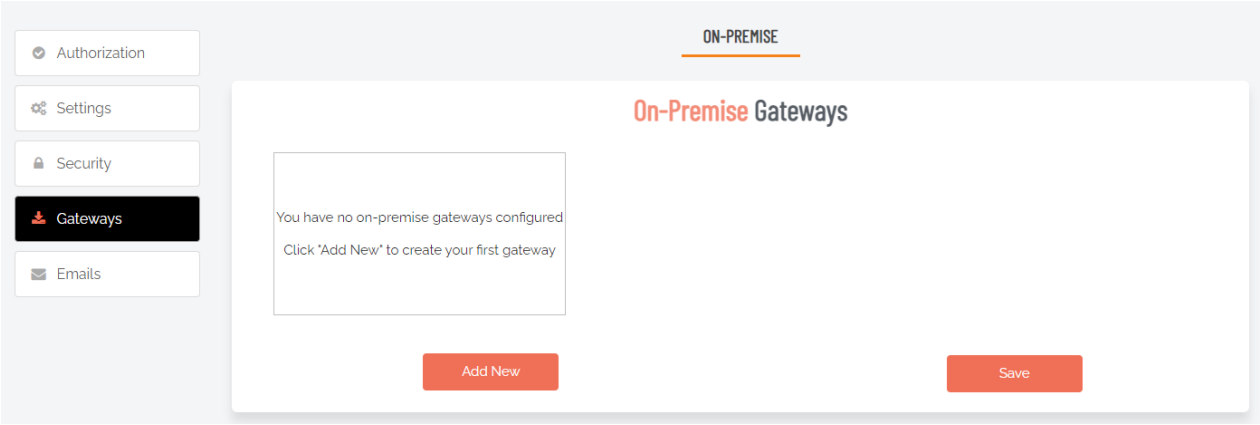
Portal menu: **Settings > Server Settings > Remote Access Settings > Gateways**

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.

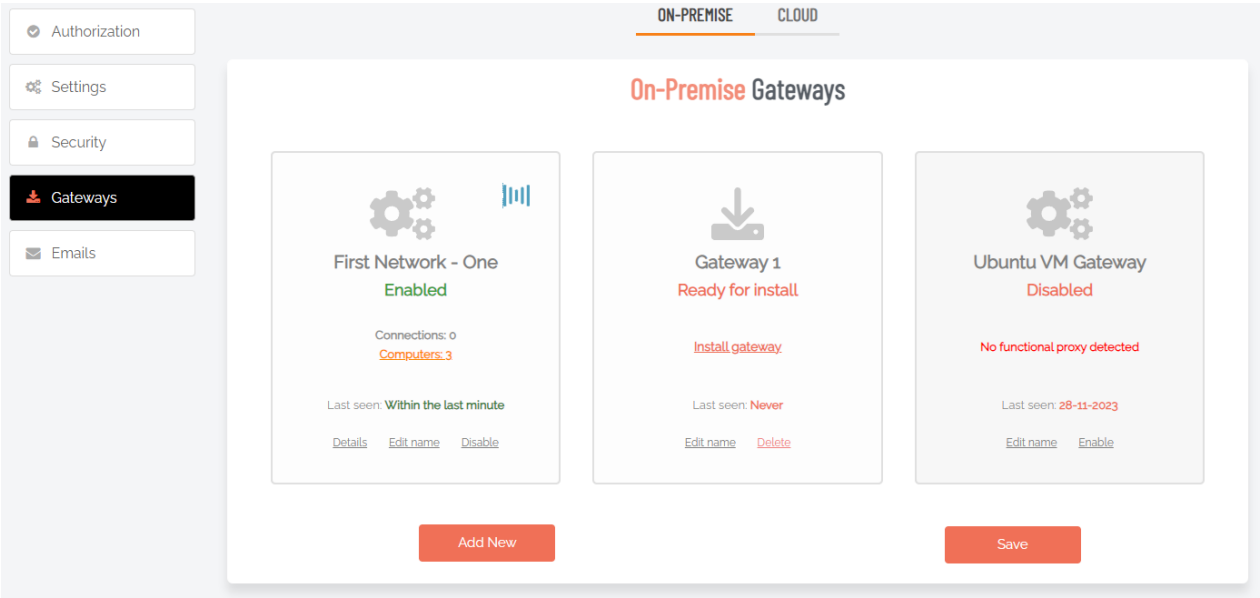
Additional views are: "New Gateway" on page 29 and "Existing Gateway" on page 30.

Gateway Dashboard

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



Example dashboard showing three gateways:



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:

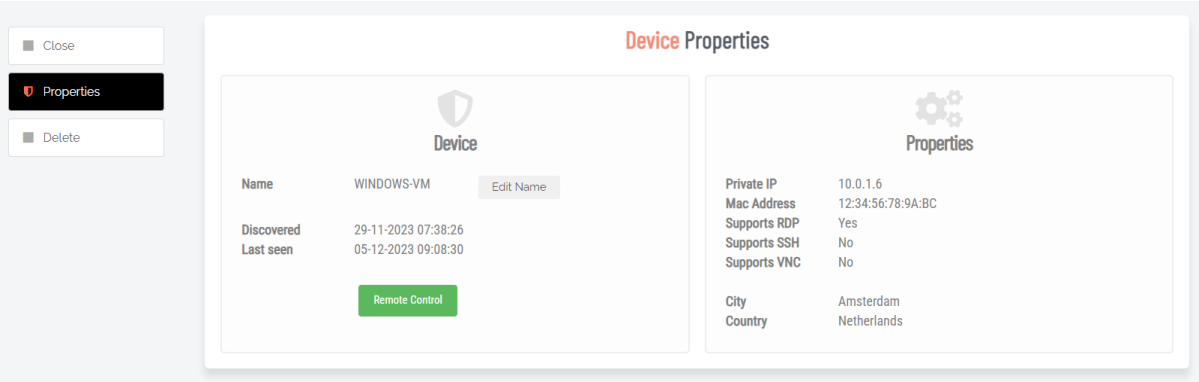
- Computers will appear based on discovery.
- If computers appear that are not supposed to be made available for remote control, they can be deleted from the list.
- If computers have been deleted by mistake, they can be restored under the "Deleted" tab.
- Offline computers are computers that were not 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 Remote Access and consume a license. • **INACTIVE**: are not able to be connected via Remote 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.
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 page 29 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 **Settings > Server Settings > Remote 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.

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 Remote Access and is used when no on-premise gateway is detected. In fact, when first enabling Remote 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.

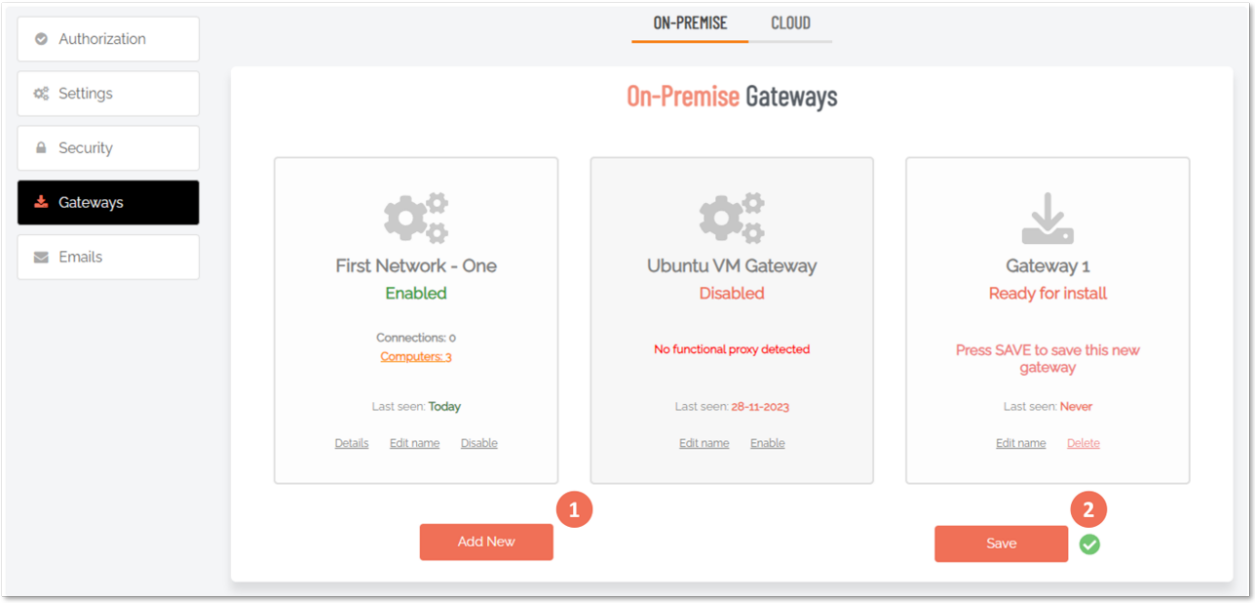
Cloud hosting requires installation of the Admin By Request Server endpoint software. If this is not an option or you have devices on which you cannot install the endpoint software, you must use an on-premise gateway.

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	**On** - Allows the remote access gateway to be hosted by Admin By Request in the cloud.

Setting	Type	Description
	Default: **On**	**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.

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.

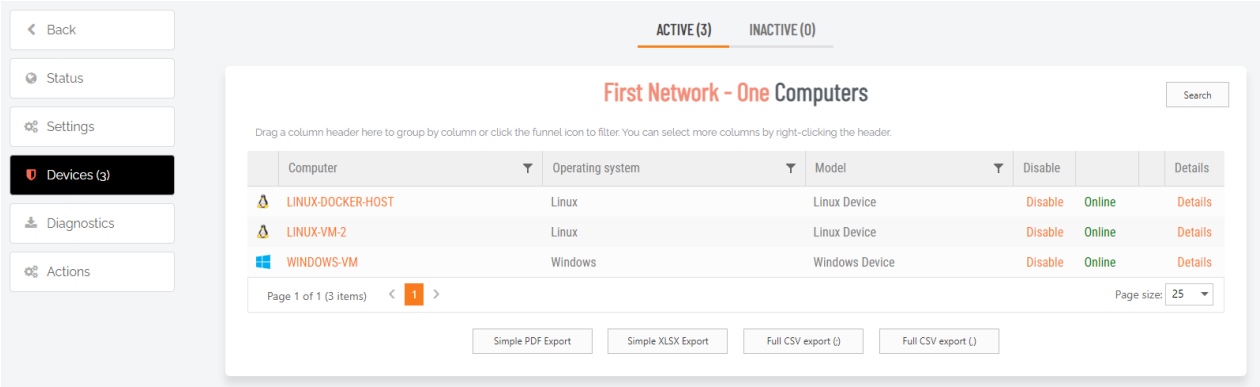
Parameter names and values in the Kubernetes settings table are the same as for the DOCKER tab.

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 14 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 Remote Access and consume a license.
- **INACTIVE**: are not able to be connected via Remote 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: **Settings > Server Settings > Remote Access Settings > Emails**

Request Emails tab

Emails go out when *Require approval* is turned **On** under "Authorization tab" on page 22. 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 the Admin By Request documentation site (left menu **Portal > Tenant Settings > 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.

Setting	Type	Description
		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. 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.

Ticketing System tab

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**
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

Setting	Type	Description
		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 • {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 • {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.
User requests approval	Toggle On | Off Default: **On**	**On** - Sends a notification for *User requests approval*. **Off** - Does not send a notification.
Admin approves user request	Toggle On | Off Default: **On**	**On** - Sends a notification for *Admin approves user request*. **Off** - Does not send a notification.
Admin denies user request	Toggle On | Off Default: **Off**	**On** - Sends a notification for *Admin denies user request*. **Off** - Does not send a notification.
User starts remote session	Toggle On | Off Default: **Off**	**On** - Sends a notification for *User starts remote session*. **Off** - Does not send a notification.
User finishes remote session	Toggle On | Off	**On** - Sends a notification for *User finishes remote session*.

Setting	Type	Description
	Default: **Off**	**Off** - Does not send a notification.
Save	Button	Saves customization and changes to any fields. Note that reloading any defaults does not take effect until **Save** is clicked.

Remote Access Sub Settings

Portal menu: **Settings > Server Settings > Remote 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 servers and workstations, Remote Access sub-settings follow the same structure used for global settings:

- Authorization
- Settings
- Security
- Gateways
- Emails

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

Setting	Type	Description
Global Settings Overrule	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.
Save	Button	Saves changes made to the overrule values entered.

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 portal 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 OUs 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.

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 Remote 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.

Index

M

N

O

P

R

S

T

U