



June 17, 2025

## Table of Contents

<b>1</b>	<b>Overview .....</b>	<b>4</b>
1.1	Netop Portal .....	4
1.2	Technical requirements – Portal website .....	4
1.3	Technical requirements - OnDemand Sessions web client .....	5
1.4	Technical requirements - OnDemand Sessions desktop application .....	5
<b>2</b>	<b>General .....</b>	<b>7</b>
2.1	Authentication .....	7
2.1.1	Forgot Password .....	9
2.2	User Interface .....	10
2.2.1	Filter Information .....	11
2.3	User Profile .....	13
2.3.1	Edit Profile Details .....	14
2.3.2	Change Your Password .....	14
2.3.3	Generate recovery codes .....	15
<b>3</b>	<b>How to remote control a device .....</b>	<b>17</b>
3.1	My devices – permanent devices (attended and unattended) .....	19
3.1.1	Target device – Host setup .....	19
3.1.2	Technician device .....	35
3.2	OnDemand Sessions .....	40
3.2.1	Browser Based Support Console – OnDemand Sessions .....	42
3.2.2	Start an OnDemand Session application on a Windows machine .....	50
3.2.3	Initiate an OnDemand Session remote connection .....	52
3.2.4	OnDemand Sessions Clipboard functionality .....	56
3.2.5	Start an OnDemand Session application on a macOS machine .....	58
3.2.6	Start an OnDemand Session application on an iOS device .....	67
<b>4</b>	<b>How to manage your account .....</b>	<b>88</b>
4.1	Manage Users .....	89
4.1.1	Create a new user .....	90
4.1.2	LDAP users - automatically added into the Portal at first login .....	99
4.1.3	Multiple accounts .....	99
4.1.4	View User Info .....	103
4.1.5	Edit the user .....	104
4.1.6	Remove user .....	106
4.1.7	Remove multiple users .....	107
4.1.8	Set up the default remote control action .....	108
4.2	Manage Groups .....	110

4.2.1	Create a new group .....	111
4.2.2	Attach users to user groups .....	111
4.2.3	Add Azure AD user groups .....	112
4.2.4	LDAP user groups .....	115
4.2.5	Attach devices to device groups.....	118
4.2.6	View group details.....	119
4.2.7	Edit Groups .....	120
4.2.8	Remove groups.....	120
4.3	Manage Devices .....	121
4.3.1	Edit devices .....	122
4.3.2	Remove devices .....	123
4.3.3	Favorite Devices .....	124
4.3.4	My Mobile Devices .....	125
4.3.5	Applications.....	126
4.4	Roles and Role assignments .....	128
4.4.1	View Predefined Roles .....	129
4.4.2	How to add a role .....	130
4.4.3	How to edit a role .....	130
4.4.4	How to copy a role .....	131
4.4.5	How to remove a role.....	132
4.4.6	Add role assignment .....	133
4.4.7	Edit role assignment.....	134
4.4.8	Create a schedule for a role assignment .....	136
4.4.9	Remove role assignments .....	142
4.4.10	Confirm Access role.....	142
4.4.11	Whitelisted applications role.....	147
4.4.12	Check permissions.....	150
4.5	Downloads - using Deployment Packages.....	152
4.5.1	Create a deployment package .....	153
4.5.2	Download and install the Host using default configuration .....	155
4.5.3	Download and install online installer using a custom Host configuration (Windows).....	158
4.5.4	Mass deploy the Host (Windows).....	159
4.5.5	Revoke deployment packages.....	159
4.5.6	Remove deployment packages.....	160
4.5.7	Pending state.....	160
5	Security .....	161
5.1	Enable Multi-Factor authentication .....	161

<b>5.2</b>	<b>Authentication .....</b>	<b>163</b>
5.2.1	LDAP authentication .....	163
5.2.2	ADFS/Azure AD authentication.....	164
<b>5.3</b>	<b>Enable logging .....</b>	<b>166</b>
5.3.1	Enabling audit logging .....	167
5.3.2	Retrieve Audit Logs .....	167
<b>6</b>	<b>Account Configuration .....</b>	<b>169</b>
6.1	Account details.....	169
6.2	Change the account owner.....	171
6.3	Change Portal logo .....	172
<b>7</b>	<b>How to contact the Netop support team.....</b>	<b>173</b>



# 1 Overview

This guide is intended to explain how to use the **Netop Portal**.

## 1.1 Netop Portal

The **Portal** has two primary functions:

- **Communication relay** – the **Portal** acts as a secure relay service to connect the **Guest** and **Host** modules.
- **Management console** - the **Portal** provides a browser-based interface that allows users to:
  - Manage access control
  - View connected devices (**Hosts**)
  - View audit logs
  - Create remote sessions using a lightweight support console

## 1.2 Technical requirements – Portal website

The **Portal** provides a browser-based interface. Here is a list of supported browsers and versions based on the operating system.

Operating System	Supported Browser
Windows	Chrome latest version, Firefox latest version, and Microsoft Edge based on Chromium and Internet Explorer 11.
macOS	Chrome latest version, Firefox latest version, and Safari latest version.
Linux	Chrome latest version, Firefox latest version.

## 1.3 Technical requirements - OnDemand Sessions web client

The **OnDemand Sessions** functionality in the **Portal** requires a web browser on the client-side. Here is a list of supported browsers and versions based on the operating system.

Operating System	Supported Browser
Windows	Chrome latest version, Firefox latest version, and Microsoft Edge based on Chromium
macOS	Chrome latest version, Firefox latest version, and Safari latest version.
Linux	Chrome latest version, Firefox latest version.

## 1.4 Technical requirements - OnDemand Sessions desktop application

The **OnDemand Sessions** functionality in the **Portal** requires an application to be executed on the device to be controlled. Here is a list of supported operating systems and platforms for that application.

Operating System	Supported Platforms
Windows	Platform: 32 & 64-bit Windows 11: Home, Pro Windows 10: Home, Pro, Enterprise and Education, IoT Windows 8.1: Professional, Enterprise Windows 7: Starter, Home Basic, Home Premium, Professional, Ultimate, Enterprise (SP 0,1) Windows Server 2019: Essentials, Standard, Datacenter Windows Server 2016: Standard, Datacenter Windows Server 2012 R2: Foundation, Essentials, Standard, Datacenter  <b>NOTE:</b> For Windows 8.1, 7, and Windows Server 2012 R2, the OnDemand Session desktop application works only if TLS 1.2 is enabled.

Operating System	Supported Platforms
macOS	macOS 12 Monterey macOS 11 Big Sur macOS 10.15 Catalina macOS 10.14 Mojave macOS 10.13 High Sierra
iOS	iOS 13 iOS 14 or higher

## 2 General

### 2.1 Authentication

To log into the **Portal**, use the link and the credentials you used to set up the trial account:

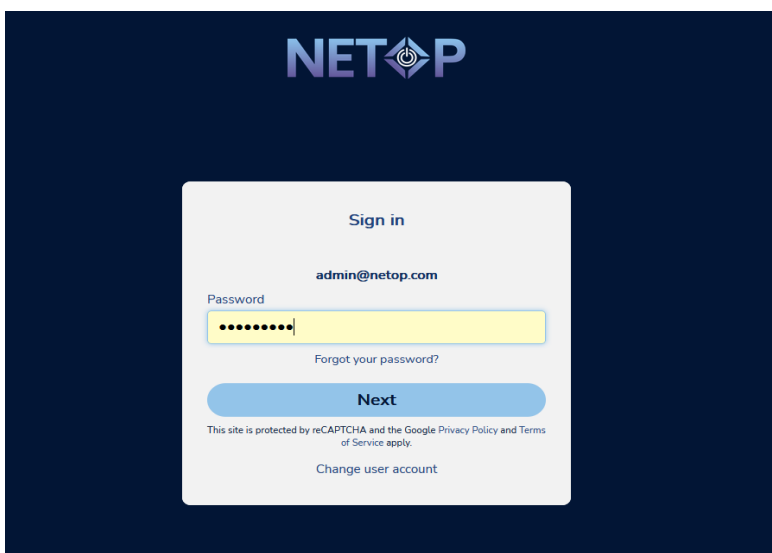
1. Specify the username and click on **Next**.



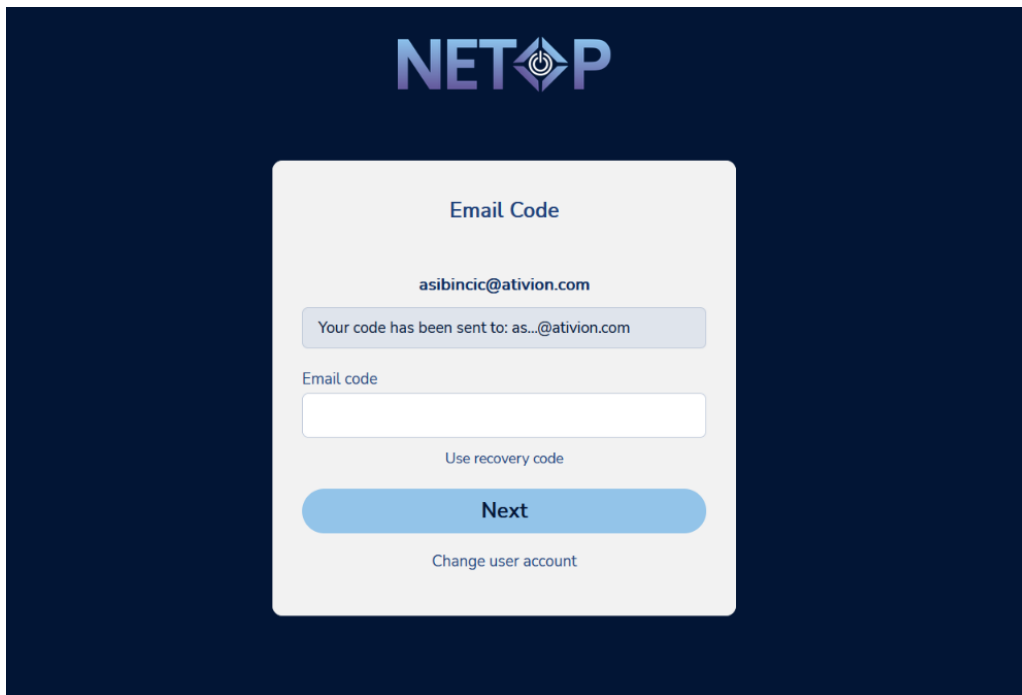
The screenshot shows the Netop Portal sign-in interface. At the top is the Netop logo. Below it is a white sign-in box. Inside the box, the text "Sign in" is at the top. Below that is a "Username" label followed by a text input field. Under the input field is a blue "Next" button. At the bottom of the box, there is a link "Sign up here" and a smaller link "Or find out more about our product". At the very bottom, in small text, it says "By signing in, you agree to the terms of Netop's [Acceptable Use Policy](#)."

2. Specify the password and click on **Next**.

If **multi-factor authentication** is enabled for your account, it is necessary that you specify the code sent to you via email as a second factor of authentication in the **Portal**.

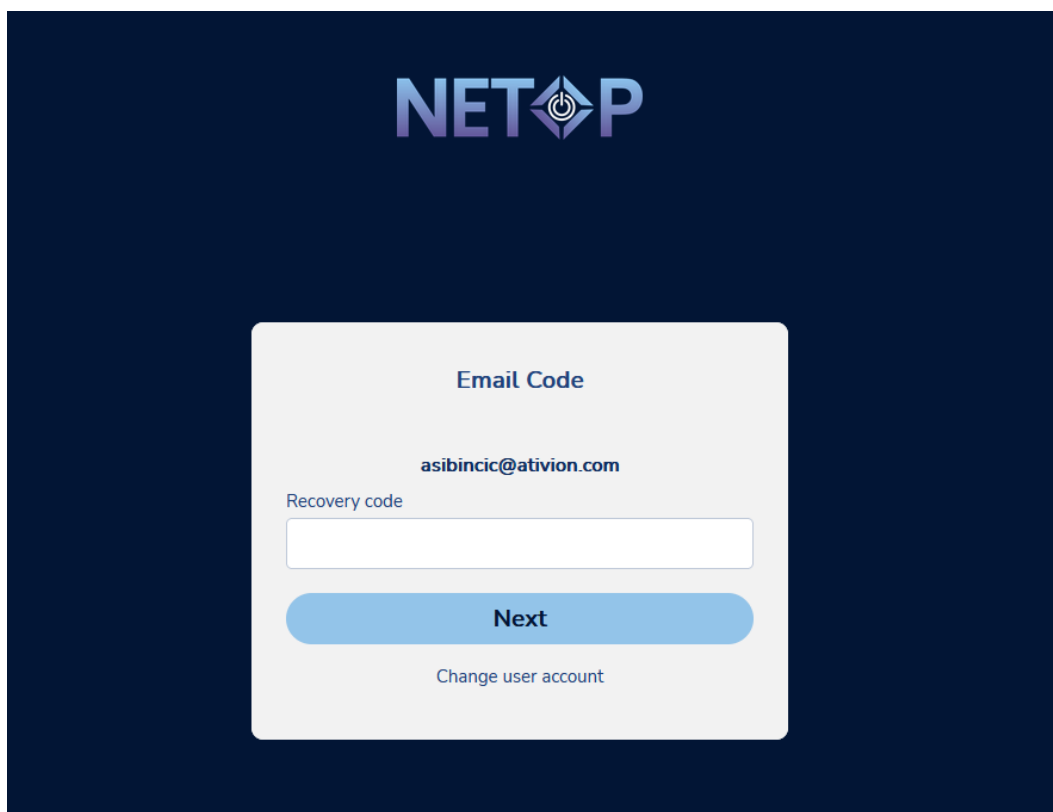


The screenshot shows the Netop Portal sign-in interface with the password field filled. The "Username" field now contains the text "admin@netop.com". The "Password" field is highlighted in yellow and contains ten dots, indicating a masked password. Below the password field is a link "Forgot your password?". The blue "Next" button is still present. At the bottom of the box, it says "This site is protected by reCAPTCHA and the Google Privacy Policy and Terms of Service apply." and a link "Change user account".



The screenshot shows the 'Email Code' screen of the Netop Portal. At the top is the 'NETOP' logo. Below it, the email address 'asibincic@ativion.com' is displayed. A message states: 'Your code has been sent to: as...@ativion.com'. There is an input field labeled 'Email code'. Below the input field is a link that says 'Use recovery code'. A large blue button labeled 'Next' is prominent, and at the bottom is a smaller link that says 'Change user account'.

If you do not have access to your e-mail account, you can use the recovery codes to sign in.



The screenshot shows the 'Email Code' screen of the Netop Portal, but for recovery codes. The email address 'asibincic@ativion.com' is displayed. Below it is an input field labeled 'Recovery code'. A large blue button labeled 'Next' is prominent, and at the bottom is a smaller link that says 'Change user account'.

Refer to the [Generate recovery codes](#) sub-chapter for details on how to generate recovery codes.

If **LDAP authentication** is set up for your account, authenticate in the **Portal** using the following username format: *domain identifier\LDAP username* and the domain password.

If **ADFS / Azure AD** is set up, the steps are the same as for **LDAP authentication**. The authentication is done on the customers' **ADFS / Azure AD** authentication page.

The **Portal** now uses the reCAPTCHA v2 invisible feature offered by Google as a means of protection against fraudulent attempts to logins, activities, spam, and abuse. The reCAPTCHA feature is designed to be friendly to humans. It uses advanced risk analysis techniques to differentiate humans and bots apart from each other in order to protect the Portal from spam.

### 2.1.1 Forgot Password

To reset your password, on the login page, specify your username and click on

the [Forgot your password?](#) button. In the **Recover password** window, specify the email address associated with your **Portal** account and click on the **Send** button. You receive an email with instructions on how to change your password.

**NOTE:** The forgot password functionality does not work for **LDAP, ADFS** or **Azure AD** authentication. To recover your domain password, contact your system administrator.

## 2.2 User Interface

The graphical interface has three main areas:

- **Menu sidebar (on the left)** - allows you to navigate through the **Portal**.

The sidebar menu can be collapsed to increase the usable area of your display, by clicking on the collapse button that can be found at the bottom of the sidebar menu.

**NETOP**

**DASHBOARD**

**ACCESS**

- My sessions
- My devices
- My mobile devices

**MANAGE**

- Users
- Devices
- Groups
- Applications
- Roles
- Role assignments

**Downloads**

**SECURITY**

- Account security
- Authentication
- Logs

**ACCOUNT**

- Configuration

**Devices & Users**

Devices		Users	
Total devices:	141	Total users:	28
Online devices:	2	Online users:	1
Pending devices:	0	ADFS / Azure AD users:	2
Device groups:	11	LDAP users:	3
		User groups:	10
		LDAP user groups:	2

**Account info**

Company	Netop
Expiration date	2026-12-02
Account owner	TEAM Account Owner galeham_portal@netop.com
Timezone	Europe/Bucharest

**Documentation**

- [Impero Connect Portal Quick Start Guide](#)
- [Impero Connect Portal User's Guide](#)
- [Browser-based Support Console User's Guide](#)
- [Mass deploy Portal components](#)

**Activity**

Not enough data available. Come back later to see an overview of your account.

[View more logs](#)

**Recent updates**

**NEW** April 7th, 2022

- We've refreshed the Impero Connect Portal user interface with new colors, updated icons, and small changes to page layouts.
- These changes align the user experience of the Connect Portal with other Impero products, making it easier for customers to navigate the full Impero product portfolio.
- The user interface updates don't change features or functions and have been designed to enhance the overall user experience.
- Custom logos can be uploaded to the Portal and have your Portal account reflect your unique brand or identity.
- Account owners can upload JPG, PNG and SVG files from the Configuration tab.

**January 28th, 2021**

- Netop Remote Control version 12.84 for Windows is now available.
- This new version addresses a security vulnerability in prior versions of the Windows based Guest, Host, Gateway, and Security Server modules.
- We recommend all users upgrade to the new version as soon as possible.
- Read the release notes [here](#).

**December 14th, 2020**



- **Title bar (on the upper side)** - allows you to perform general actions like **contacting support**, accessing the **My profile** page, **OnDemand** sessions, number of devices enlisted, number of users, and log off.
- **Content area (right of the menu bar)** - displays information such as devices and users, activity, account information, documentation, and recent updates.

The screenshot displays the Netop Portal Dashboard. On the left is a dark blue sidebar with the 'NETOP' logo and a menu categorized into ACCESS, MANAGE, SECURITY, and ACCOUNT. The main content area is titled 'DASHBOARD' and features several widgets. The 'Devices & Users' widget shows statistics for devices and users. The 'Account info' widget displays details like company, expiration date, and account owner. The 'Activity' widget shows a message about insufficient data. The 'Recent updates' widget lists updates from April 7th, 2022, and January 28th, 2021. The top right of the dashboard includes buttons for 'Contact Netop' and 'Purchase', along with status indicators for users, on-demand users, devices, and the current user 'Netop Admin1'.

Devices		Users	
Total devices:	141	Total users:	28
Online devices:	2	Online users:	1
Pending devices:	0	ADFS / Azure AD users:	2
Device groups:	11	LDAP users:	3
		User groups:	10
		LDAP user groups:	2

Company	Netop
Expiration date	2026-12-02
Account owner	TEAM Account Owner (devteam_portal@netop.com)
Timezone	Europe/Bucharest

**Recent updates**

**NEW April 7th, 2022**

- We've refreshed the Impero Connect Portal user interface with new colors, updated icons, and small changes to page layouts.
- These changes align the user experience of the Connect Portal with other Impero products, making it easier for customers to navigate the full Impero product portfolio.
- The user interface updates don't change features or functions and have been designed to enhance the overall user experience.
- Custom logos can be uploaded to the Portal and have your Portal account reflect your unique brand or identity.
- Account owners can upload JPG, PNG and SVG files from the Configuration tab.

**January 28th, 2021**

- Netop Remote Control version 12.84 for Windows is now available.
- This new version addresses a security vulnerability in prior versions of the Windows based Guest, Host, Gateway, and Security Server modules.
- We recommend all users upgrade to the new version as soon as possible.
- Read the release notes [here](#).

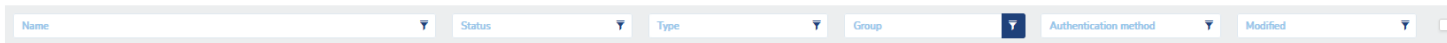
## 2.2.1 Filter Information

You can filter the information displayed in the content area by using the filters available on each column header (in case a listing is displayed). Using the filter improves the ability to locate specific items within the listings.

Clicking on the **Filter** icon on a column header displays an advanced filter, which allows you to select the filter criteria.

**NOTE:** When you filter by device group, you only see the device groups that you have permissions for.

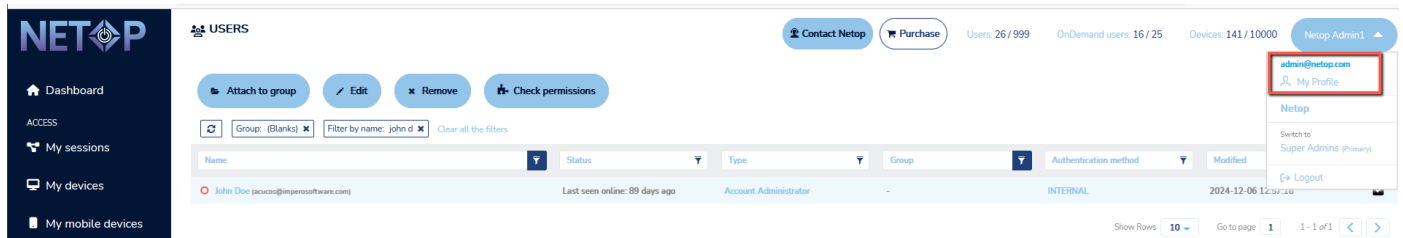
You can set multiple filters to a listing.



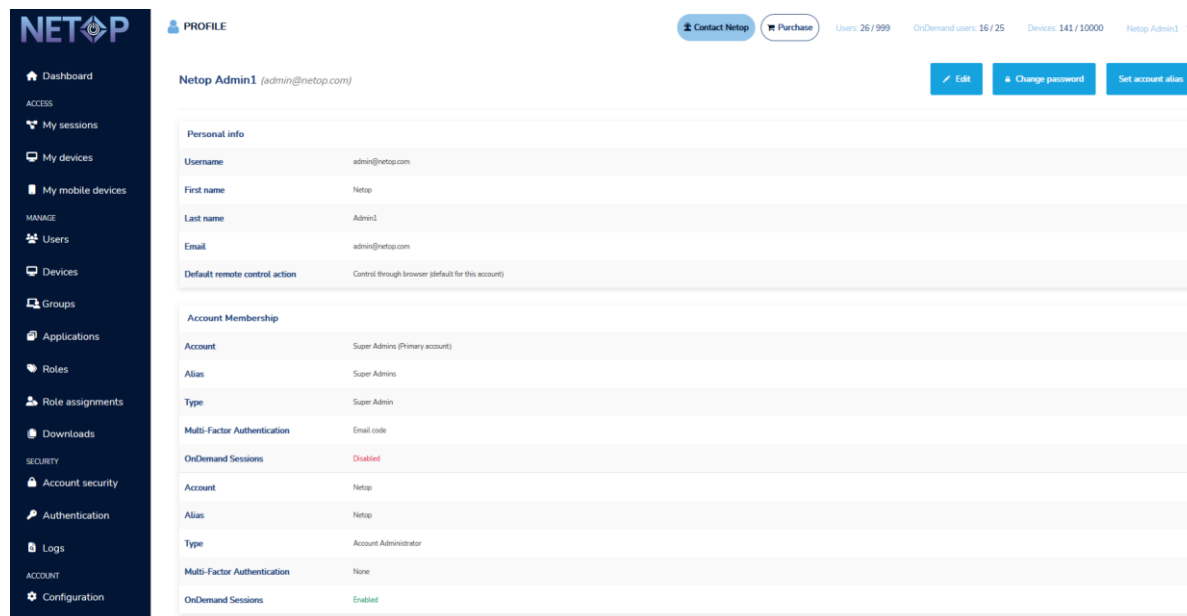
To remove a filter, from above the current listing, click on the filter you want to remove. You can also reload the current listing and clear all the filters.

## 2.3 User Profile

You can view your **Portal** profile details by clicking on the **Username** button in the title bar.



The **My Profile** tab displays information on the profile of the user currently logged in.



### 2.3.1 Edit Profile Details

You can change your profile details by clicking on the **Edit profile** button. The profile details become editable, except for the username which is non-editable.

Field	Description
First Name	User's first name.
Last Name	User's last name.
Email	The email address to which the user receives notifications from the <b>Portal</b> and the <b>multi-factor authentication</b> code (if enabled).
Email (MFA)	Enables or disables the multi-factor authentication for the User.
Default remote control action	<p>Possible options:</p> <ul style="list-style-type: none"> <li>• Control through Guest</li> <li>• Control through browser</li> </ul> <p>The option that you set here as the default remote control action is the one that is displayed in the <b>My devices</b> tab when you want to start a remote control session with a device.</p>

Make the profile updates that you want and click on the **Save** button to store the updates.

**NOTE:** **LDAP**, **ADFS** and **Azure AD** users cannot edit their **Portal** profile.

### 2.3.2 Change Your Password

To change your password, go to your profile and click on the **Change password** button.

**NOTE:** **LDAP**, **ADFS** and **Azure AD** users cannot change their password from within the **Portal**.

Specify and confirm a new password for your account.

A password is valid if it agrees with the following rules:

- minimum of 8 characters
- at least one uppercase letter
- at least one lowercase letter
- at least one numeric character

For the updates to take effect, click on the **Save** button.

### 2.3.3 Generate recovery codes

Recovery codes are used to log in to the **Portal** if you have **multi-factor authentication** enabled.

To generate the recovery codes:

1. Log in to the **Portal**.
2. Go to **My profile**.
3. Click on the **Generate new codes** button.

**NETOP**

**PROFILE**

1 / 5 1 / 2 43 / 50

[Edit](#) [Change password](#)

**Personal info**

Username	
First name	
Last name	
Email	
Type	Account Owner
Multi-Factor Authentication	Email code
OnDemand Sessions	Enabled
Default remote control action	Control through Guest (default for this account)

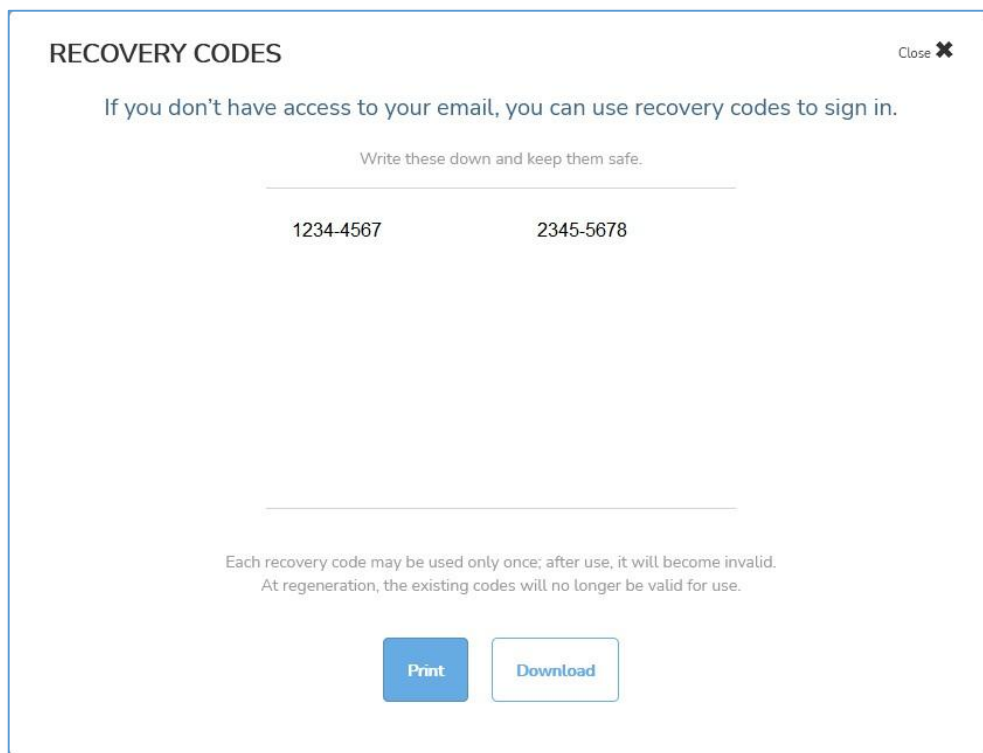
**Recovery codes**

If you don't have access to your email, you can use recovery codes to sign in. The codes come in sets of 10. Once you've used a recovery code to sign in, it will become invalid.

When clicking on Generate new codes, a new set is generated and the old one becomes invalid. Please make sure you keep the recovery codes safe because they are sensitive information.

[Generate new codes](#)

The recovery codes come in sets of 10. You can generate a new set at any point. When generating a new set of recovery codes, the previous set becomes automatically inactive. Also, after you've used a recovery code to sign in, the recovery code becomes inactive.



You can print the codes or download them on your computer. We recommend you keep the recovery codes safe due to their sensitive information.

### 3 How to remote control a device

The **My devices** and **My sessions** tabs list the online devices for which you have access permissions as defined by the applied role assignment(s).

Refer to the [Roles and Role assignments](#) sub-chapter for more information. If there is no device attached to the account, the options for installing the **Host** are displayed.

To remote control a device, users can:

- Use the **My devices** tab to connect to an installed **Host** through an installed **Guest (Support Console)** or by using the **Control through browser** option. For more information, refer to the [My devices – permanent devices \(attended and unattended\)](#) subchapter.
- Use the **My sessions** tab to connect to an **OnDemand Session** to temporarily access a Windows, macOS or iOS device through the browser option. For more information, refer to the **OnDemand Sessions** subchapter.
- Use the **My mobile devices** tab to connect to a **Host** mobile device. For more information, refer to the [My mobile devices](#) subchapter.

To connect to a **Host** device through the **Guest (Support Console)**, it is necessary that you download and install it on your device.

The **Guest (Support Console)** application can be installed on the following operating systems:

- Windows
- macOS
- Linux

## Supported actions depending on the Host

Host operating system	Actions
Windows	<ul style="list-style-type: none"> <li>- Remote Control</li> <li>- File transfer</li> <li>- Remote management (*)</li> <li>- Chat (*)</li> </ul>
Linux & macOS	<ul style="list-style-type: none"> <li>- Remote Control</li> <li>- File transfer</li> </ul>

\* **Guest** version 12.70 or higher is required

You can download the **Guest (Support Console)** application on your Windows device from the **My devices** tab.

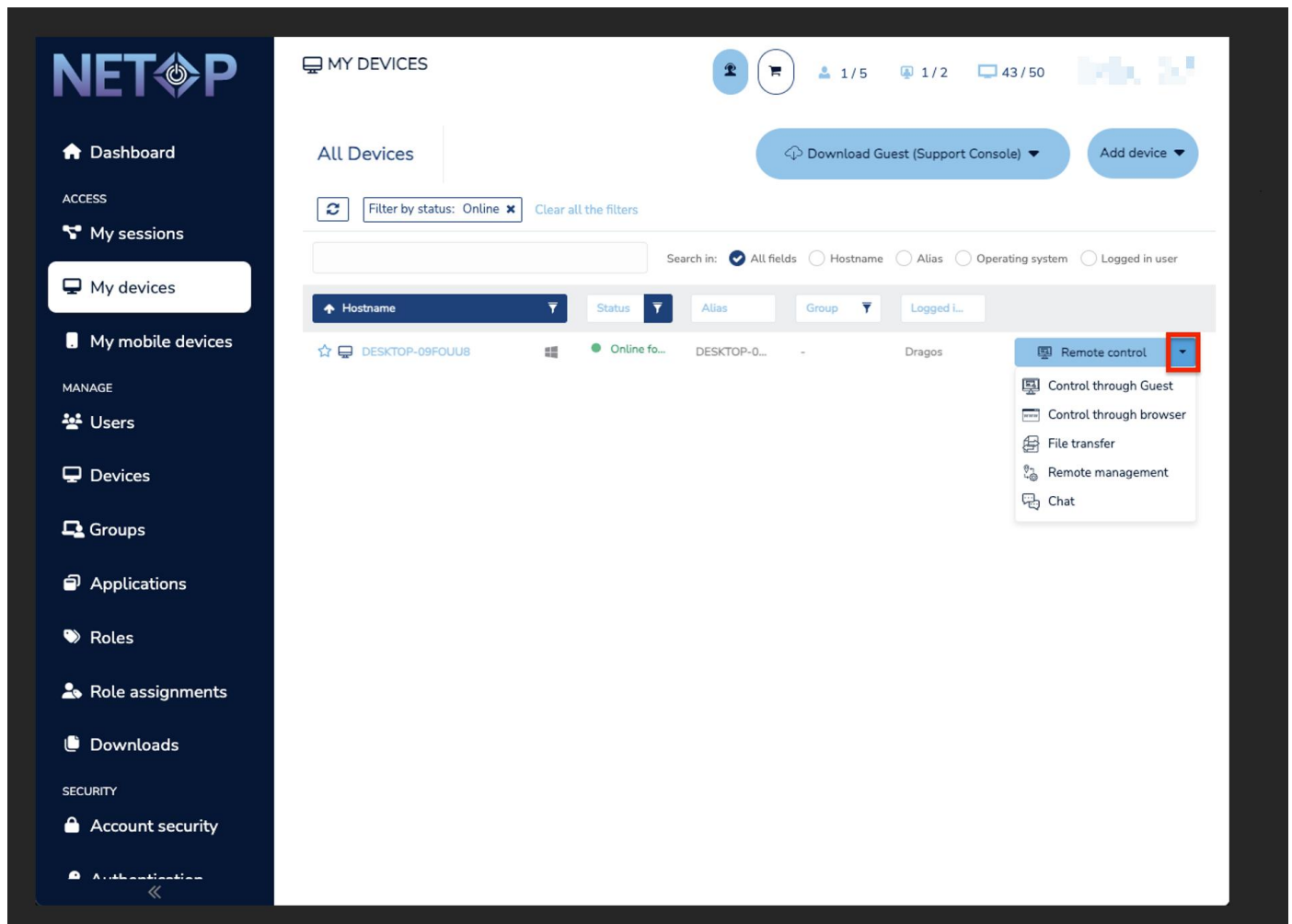


## 3.1 My devices – permanent devices (attended and unattended)

Through the **My devices** tab you can:

- Remote Control a **Host** device through the **Guest (Support Console)**
- Remote Control a **Host** device through the browser
- Use the File transfer feature
- Use the Remote management feature
- Use the Chat feature

To view or use these options click on the dropdown menu button near the **Remote control** button.



**NOTE:** Using either the **File transfer**, **Remote management**, **Chat feature**, or **Control through Guest** option, launches the **Guest (Support Console)** application.

### 3.1.1. Target device – Host setup

#### 3.1.1.1 Windows 7 or later

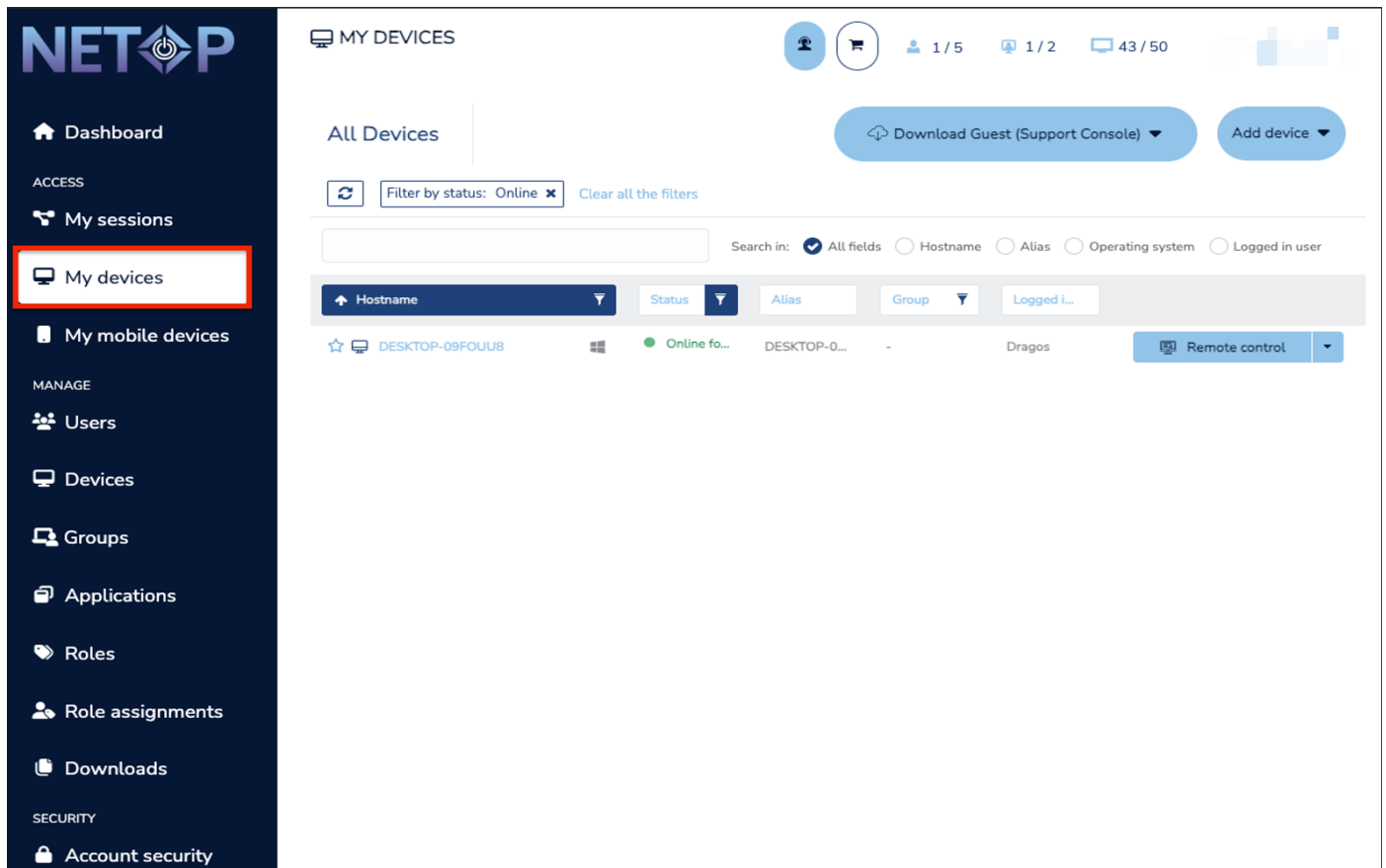
Depending on your needs, you can:

- [Install the Host on the device that you are on](#)
- [Install the Host on another device](#)
- [Automatically install the Host using a mass deployment tool](#)

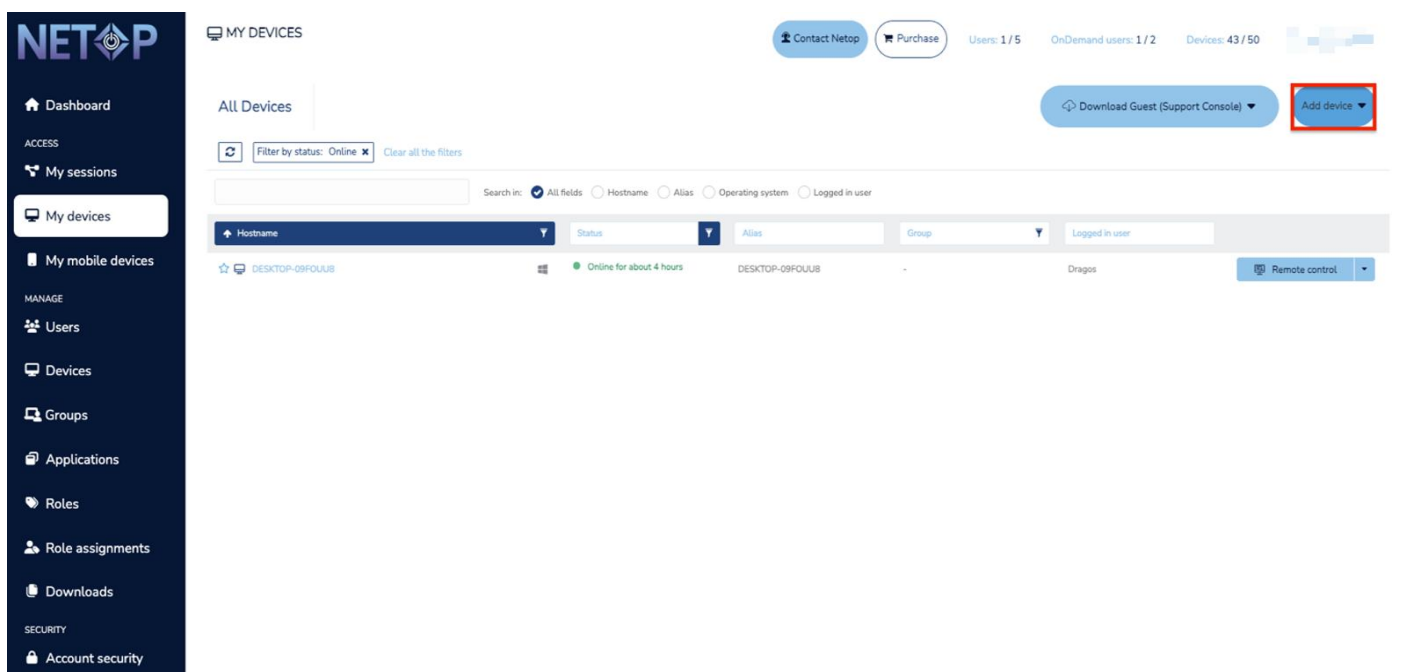
## Install the Host on the device that you are on

To install the **Host** on the device that you are on, proceed as follows:

1. Go to the **My devices** tab.



2. Click on the **Add device** button.



### 3. Click on the **Host installer** button.

The screenshot shows the 'MY DEVICES' page in the Netop Portal. The left sidebar contains navigation links for Dashboard, My sessions, My devices (selected), My mobile devices, Users, Devices, Groups, Applications, Roles, Role assignments, Downloads, and Account security. The main content area shows a list of devices under the 'All Devices' tab. A filter is set to 'Online'. A search bar is available with options for All fields, Hostname, Alias, Operating system, and Logged in user. A table lists devices with columns for Hostname, Status, Alias, Group, and Logged in user. The first device is 'DESKTOP-09FOU08' with status 'Online for about 4 hours'. A 'Remote control' button is visible for this device. In the top right corner, there are buttons for 'Contact Netop', 'Purchase', and 'Add device'. A dropdown menu is open, showing 'Host installer' (highlighted with a red box) and 'Host for other operating system'.

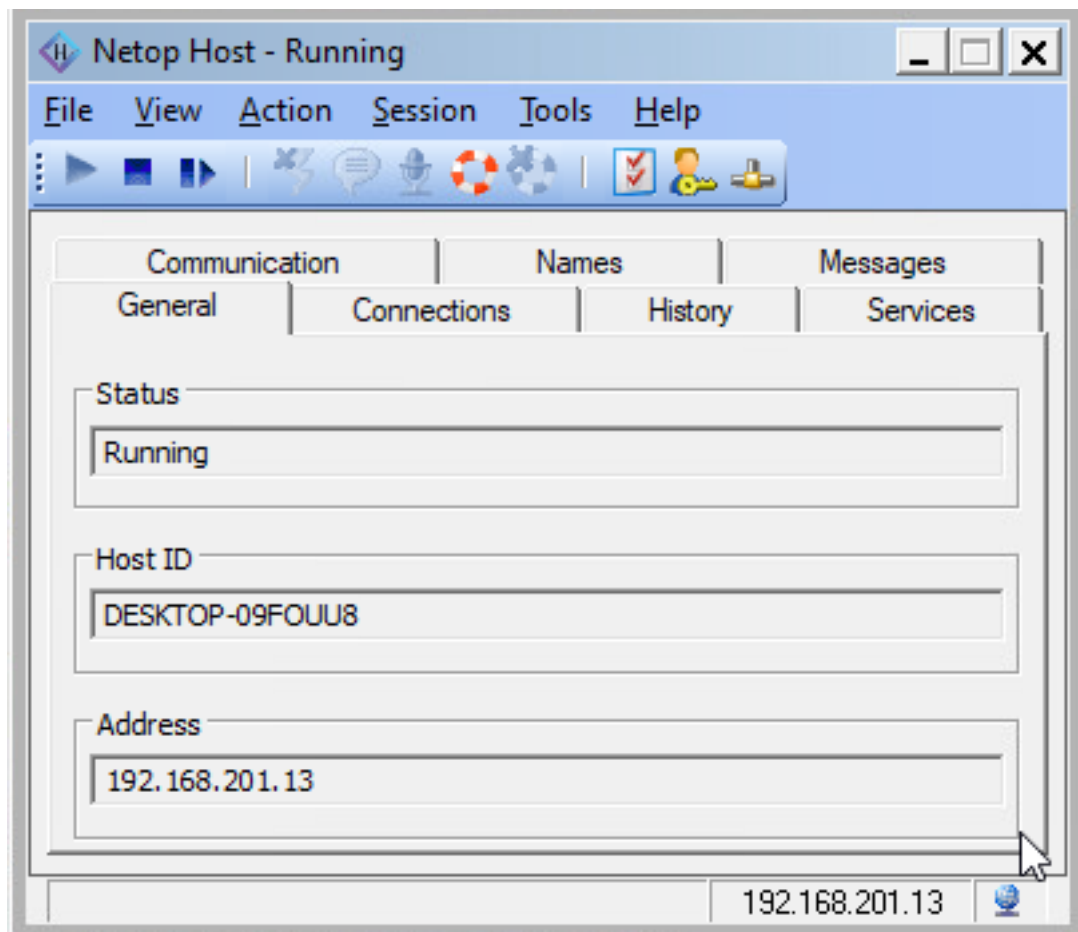
### 4. When there is more than one deployment package defined in your account, you are redirected to the **Downloads** page. Select the deployment package and click on the **Online installer** button for the download to start. Otherwise, the online installer is downloaded automatically.

The screenshot shows the 'DOWNLOADS' page in the Netop Portal. The left sidebar is the same as in the previous screenshot. The main content area shows a message: 'There is more than one valid deployment package in your account. If you want to add a device, select a deployment package, and then download and run the installer.' Below this, there is a table of deployment packages. The table has columns for Name, Enrollment state, Valid from, Valid to, and Devices. The first package is 'new test' with status 'Enrolled', valid from '2024-11-20', and 9 devices. The 'Online installer' button for this package is highlighted with a red box. The second package is 'new test 2' with status 'Pending', valid from '2024-11-20', and 0 devices. The third package is 'Trial Host' with status 'Enrolled', valid from '2019-11-21', and 34 devices. The 'Online installer' button for this package is also visible. At the bottom right, there are links for 'Show Rows', 'Go to page', and '1 - 3 of 3'.

### 5. Click on the downloaded executable file.

The installation process begins, and it only requires that you accept the **Acceptable Use Policy**.

6. When the installation process is finished, the **Host** automatically connects to the **Portal**.



### 3.1.1.2 macOS and Linux

#### 3.1.1.2.1 macOS

The **Host** for macOS window contains most of the **Host** for Windows window elements, but the **Host** for macOS is limited in functionality when compared to the Windows version and the setup is organized differently.

The **Host** for macOS enables a remote **Guest** to connect through the TCP/IP, TCP/IP (TCP), HTTP, WebConnect, WebConnect 3 and the **Portal** communication protocols to remote control the **Host** for a macOS device, transfer files between the computers, and run a typed text chat session between the computer users.

Prior to installation, verify that your computer meets the technical requirements. For more information, refer to the [macOS system](#)

[requirements](#) knowledge base article.

**NOTE:** To be able to install, make sure that the user logged on to the computer is a local admin account. Using a domain account with local admin privileges does not work.

You can download and install the **Netop** for the supported macOS versions from the files found on the **Netop** [download](#) page.

Open the relevant **.dmg** file downloaded from the **Netop** website and double-click on the resulting **.pkg** file to display the installation wizard that guides you through the **Netop** installation. Accept the license agreement and specify the licensee name and the **Netop** license number when prompted.

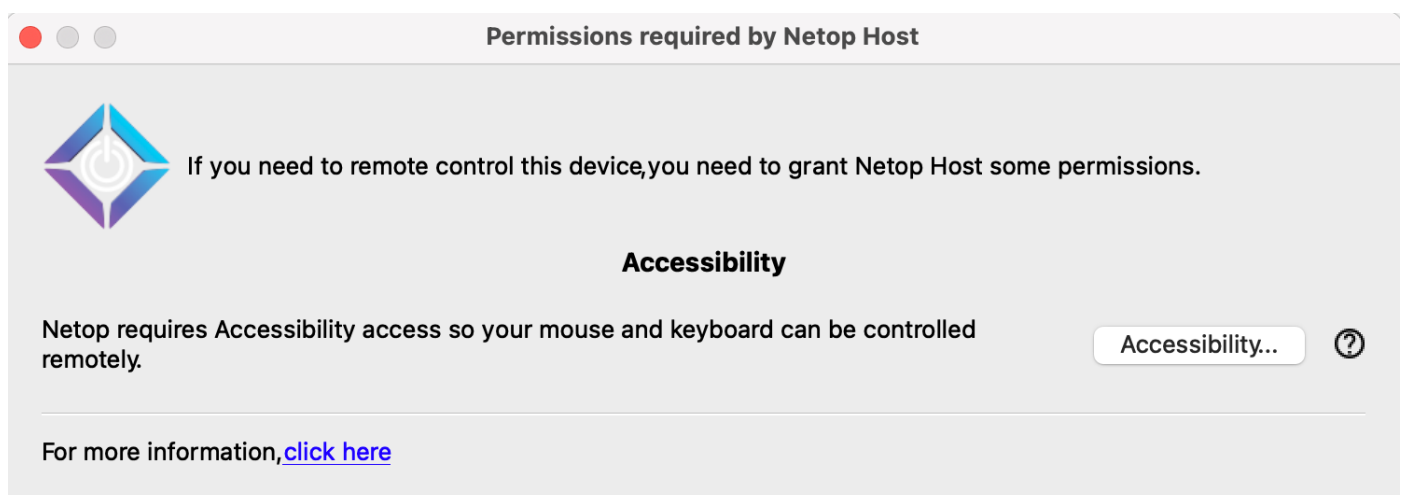
The **Host** includes the **Host** Program for macOS. The **Host** Program for macOS loads and initializes when the computer operating system starts.

To use the **Host** on macOS 10.14 and above, the **Host** requires the following permissions to be granted manually by the user:

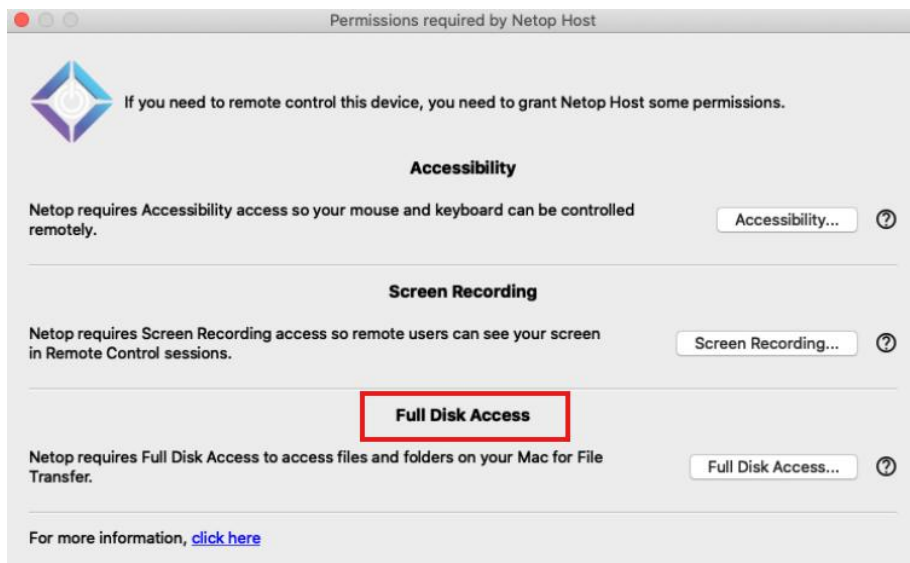
- **Accessibility**
- **Screen recording**

**NOTE:** The **Screen recording** permission applies to macOS 10.15.

- **Full Disk Access**



**NOTE:** The **Host** only prompts you for the unset permissions. You are prompted to grant these permissions manually after you successfully install the **Host**, start or restart the **Host**.



To grant the **Screen Recording** permission, proceed as follows:

1. From the **Apple** menu, select **System Preferences**.
2. Click on the **Security & Privacy** icon.
3. Click on the **Privacy** tab at the top of the **Security & Privacy** window.
4. From the **Security & Privacy** window, select **Screen Recording**.
5. Click the lock to make changes.
6. To enable the **Screen recording** permission for the **NetopHost**, check the **NetopHost** checkbox.

**NOTE:** The **NetopHost** application is added to the list only after the first attempt to connect from a **Guest** to the **Host**.

To grant the **Full Disk Access** permission, proceed as follows:

1. From the **Apple** menu, select **System Preferences**.
2. Click on the **Security & Privacy** icon.
3. Click on the **Privacy** tab at the top of the **Security & Privacy** window.
4. From the **Security & Privacy** window, select **Full Disk Access**.
5. Click the lock to make changes.
6. To add the **NetopHost**, click on the **+** sign.



7. Browse for the **NetopHost**.
8. Click on **Open**.

To grant the **Accessibility** permission, proceed as follows:

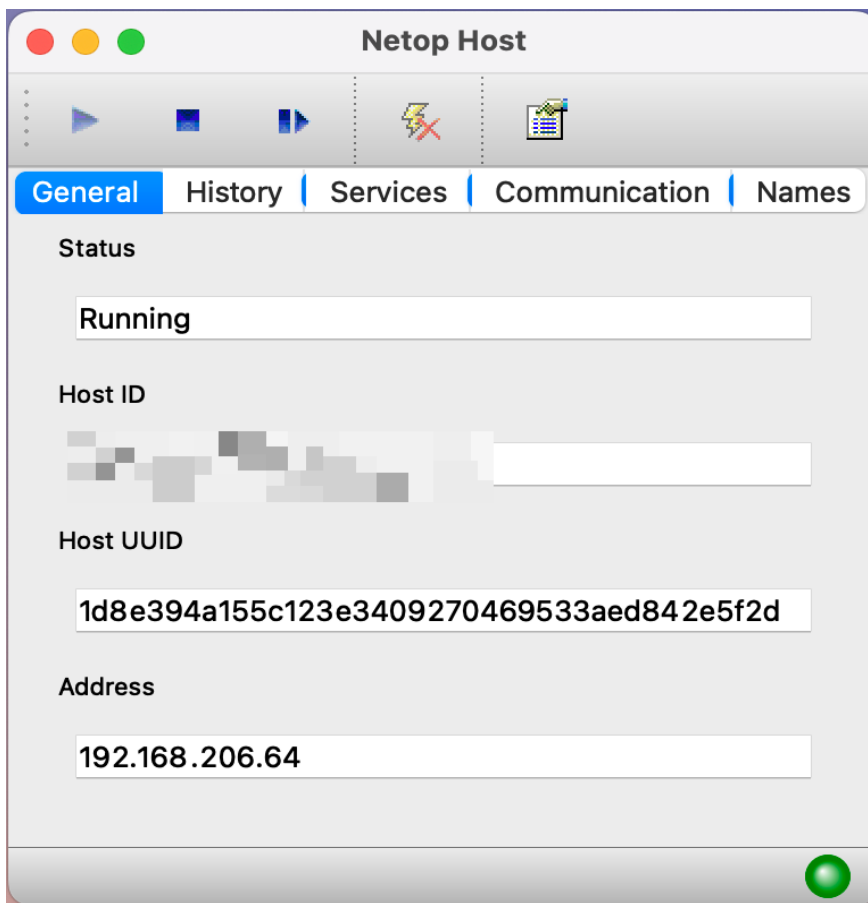
1. From the **Apple** menu, select **System Preferences**.
2. Click on the **Security & Privacy** icon.
3. Click on the **Privacy** tab at the top of the **Security & Privacy** window.
4. From the **Security & Privacy** window, select **Accessibility**.
5. Click the lock to make changes.
6. To enable the **Accessibility** permission for the **NetopHost**, check the **netophost** checkbox.

**NOTE:** You cannot add the **Accessibility** permission manually. If you remove the **Accessibility** permission for the "**netophost**", you cannot set it back again until you reinstall the **Netop Host**.

For more information on the macOS permission, refer to the following knowledge base [article](#).

The **Host** GUI for macOS does not start when the **Host** Program for macOS loads.

If the **Host** Program on macOS loaded, select Applications/NetopHost to start the **Host** GUI for macOS.



To unload the **Host** GUI for macOS to hide the **Host** on the macOS window, exit the **NetopHost** application.

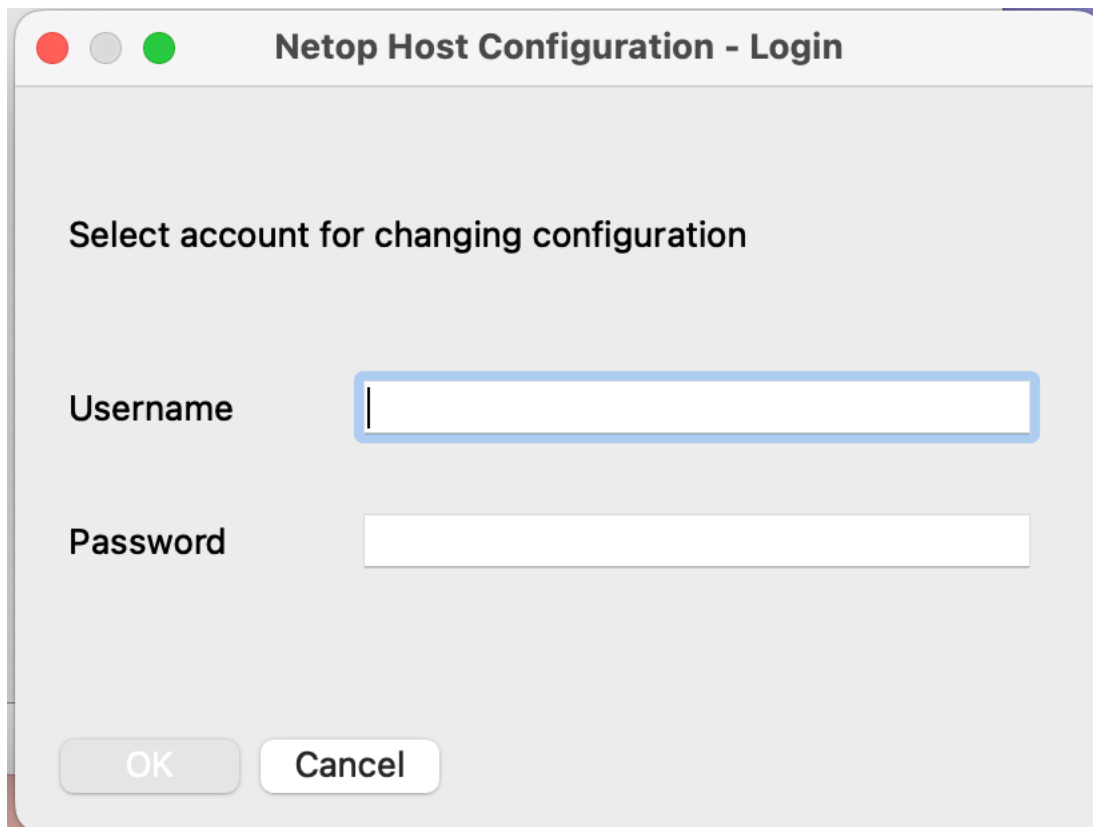
The **Host** for macOS window contains most of the **Host** for Windows window elements, but the **Host** for macOS is limited in functionality when compared to the Windows version and the setup is organized differently.

The **Host** for macOS enables a remote **Guest** to connect through the TCP/IP, TCP/IP (TCP), HTTP, WebConnect, WebConnect 3 and the Netop Portal communication protocols to:

- remote control the **Host**
- transfer files between the devices

- run a typed text chat session between the computer users

To change the setup options of the **Host**, click on the **Options** button from the toolbar or on the **Tools** menu.

A screenshot of a macOS-style dialog box titled "Netop Host Configuration - Login". The dialog has a light gray background and rounded corners. At the top, there are three colored window control buttons (red, gray, green) on the left. Below the title bar, the text "Select account for changing configuration" is centered. There are two input fields: "Username" and "Password". The "Username" field is currently selected, indicated by a blue border. At the bottom of the dialog, there are two buttons: "OK" and "Cancel".

Netop Host Configuration - Login

Select account for changing configuration

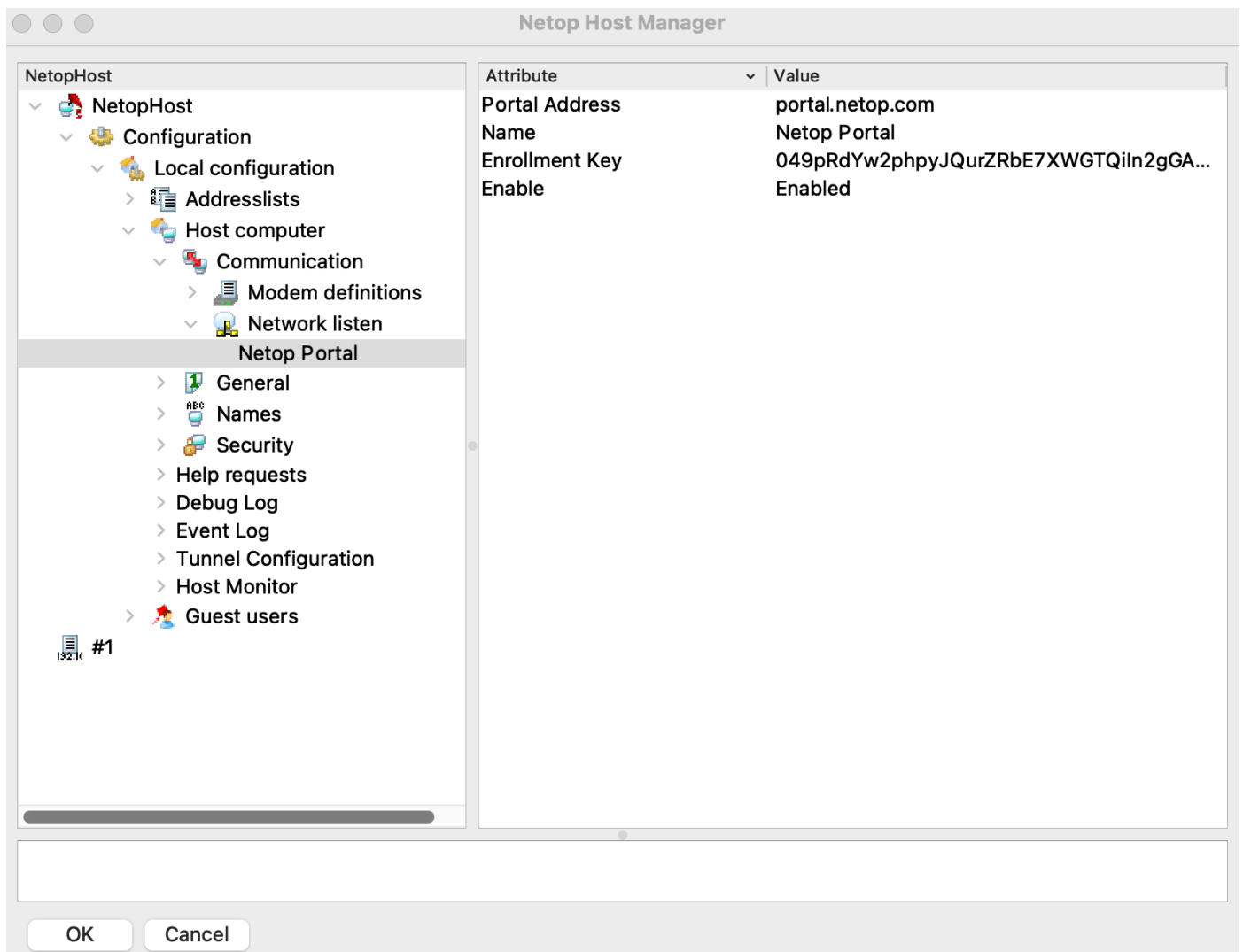
Username

Password

OK Cancel

Specify a valid macOS username. To change the setup options of the **Host**, make sure that the user has the privileges to edit the `/Library/Application/Support/Netop/host/host.xml` file.

Type the corresponding password and click on the **OK** button. The **Netop Host Manager** is displayed.



### 3.1.1.2.2 Linux

The **Host** includes the following programs:

- **Netop Host Daemon** (`netophostd`) - The **Netop Host Daemon** runs when the computer operating system starts. A user with system user privileges can start and stop the **Netop Host Daemon**.
- **Netop Host Program** (`netophost`) – The **Netop Host Program** loads and starts when the **Netop Host Daemon** loads. If started, the communication is initialized enabling a **Netop Guest** to connect. A user can typically control the **Netop Host** Program from the **Netop Host GUI**.
- **Netop Host GUI** (`netophostgui`) – The **Netop Host GUI** displays the **Netop Host** graphical user interface. It does not automatically load when the **Netop Host Program** loads. A user can load and unload the **Netop Host GUI**.

**NOTE:** Only a user with system privileges can make changes to the **Host** program options.

The **Host** uses the following communication protocols to connect to the **Guest**:

- Portal
- Internet (TCP)
- LAN (TCP)
- UDP
- HTTP
- WebConnect and WebConnect3

The **Host** can be installed on a Linux device via:

- [Software Installer](#)
- [Terminal](#)

Before you install the **Host**, make sure that your computer meets the following minimum technical requirements. For more information, refer to the following knowledge base [article](#).

To download the **Netop** application for the supported Linux distributions refer to the Netop [download](#) page.

- The download page includes separate installation or archive files for the **Guest** and **Host** depending on your Linux distribution.
- The archive file contains the following files:
  - o ca-certificates.crt
  - o eula.txt
  - o install.pl
  - o installpubkey
  - o netop.pub
  - o netop-\*.deb | netop-\*.rpm (based on the Linux distribution in use)

**install.pl** is a Perl script file that handles the installation process via the terminal.

To list all the parameters of the **install.pl** Perl script, use the following command:

```
install.pl --help
```

**install.pl** parameters table:

Function	Command
[--help]	Prints the help message and exits.
[--version]	Prints the version info and exits.
[--serial <serial>]	Installs <b>Netop Guest</b>   <b>Netop Host</b> with the <serial> number license key.
[--debug]	Turns debugging on.

[--license]	Prints the <b>Netop License</b> .
[--autoinstall]	Non-interactive installation assumes that you agree with the <b>Netop License</b> .

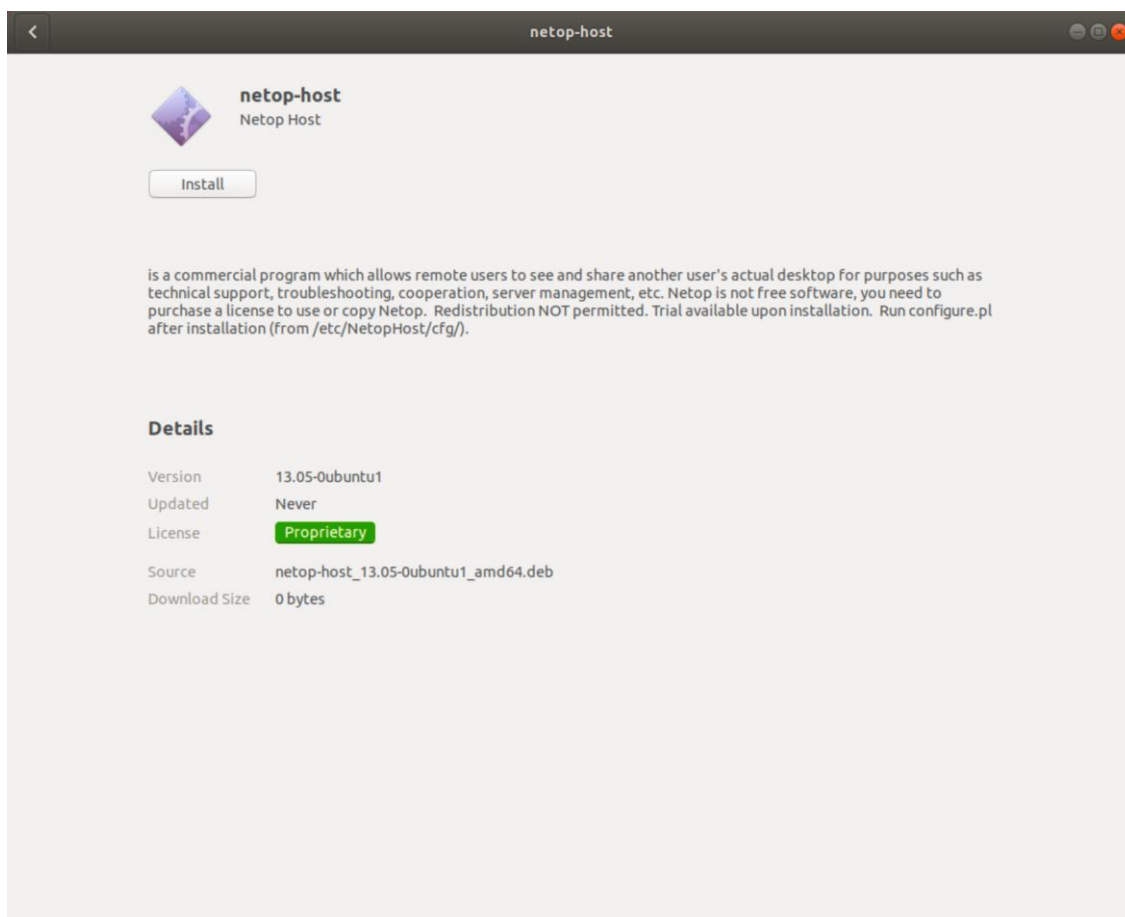
### Example:

For the non-interactive **Host** installations, use the following command:

#### 3.1.1.2.2.1 Install the Host via the Software Installer

To install the **Host** via the **Software Installer**, proceed as follows:

1. Go to the file path of the extracted **Host**.



2. Double click on the **netop-host\_\*.deb** | **rpm** installation file. The following window is displayed.
3. To install the **Host**, click on the **Install** button.
4. Specify the password for authentication.

### 3.1.1.2.2.2 Install the Host via the terminal

To install the **Host** via the terminal, proceed as follows:

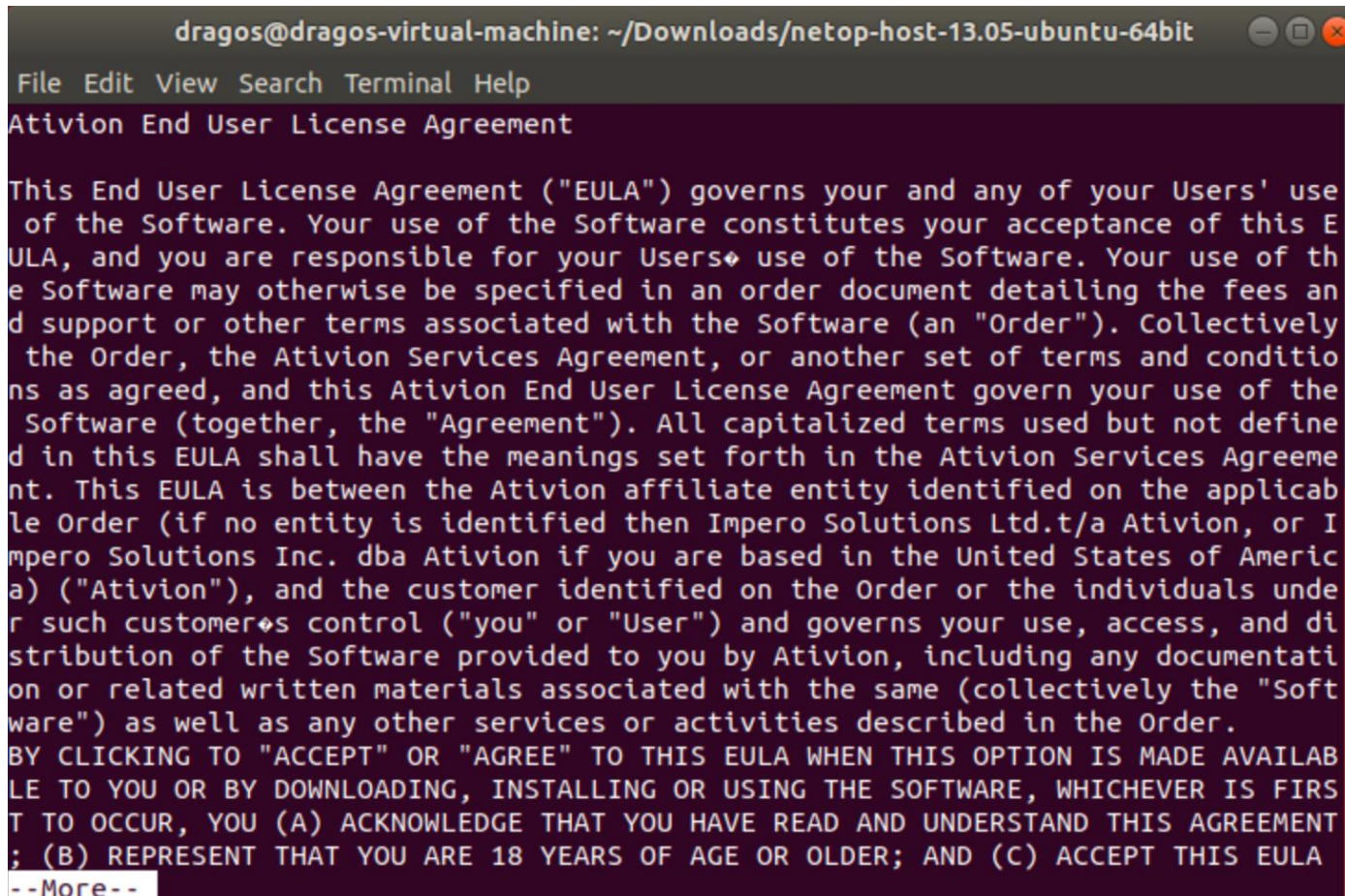
1. Go to the file path of the extracted **Host**.
2. Open up a terminal window.



3. Use the following Perl script to initiate the installation process:

```
sudo perl install.pl
```

4. As part of the installation process, it is necessary that you accept the **Acceptable Use Policy**.



```
dragos@dragos-virtual-machine: ~/Downloads/netop-host-13.05-ubuntu-64bit
File Edit View Search Terminal Help
Ativion End User License Agreement

This End User License Agreement ("EULA") governs your and any of your Users' use
of the Software. Your use of the Software constitutes your acceptance of this E
ULA, and you are responsible for your Users' use of the Software. Your use of th
e Software may otherwise be specified in an order document detailing the fees an
d support or other terms associated with the Software (an "Order"). Collectively
the Order, the Ativion Services Agreement, or another set of terms and conditio
ns as agreed, and this Ativion End User License Agreement govern your use of the
Software (together, the "Agreement"). All capitalized terms used but not define
d in this EULA shall have the meanings set forth in the Ativion Services Agreeme
nt. This EULA is between the Ativion affiliate entity identified on the applicab
le Order (if no entity is identified then Impero Solutions Ltd./a Ativion, or I
mpero Solutions Inc. dba Ativion if you are based in the United States of Americ
a) ("Ativion"), and the customer identified on the Order or the individuals unde
r such customer's control ("you" or "User") and governs your use, access, and di
stribution of the Software provided to you by Ativion, including any documentati
on or related written materials associated with the same (collectively the "Soft
ware") as well as any other services or activities described in the Order.
BY CLICKING TO "ACCEPT" OR "AGREE" TO THIS EULA WHEN THIS OPTION IS MADE AVAILAB
LE TO YOU OR BY DOWNLOADING, INSTALLING OR USING THE SOFTWARE, WHICHEVER IS FIRS
T TO OCCUR, YOU (A) ACKNOWLEDGE THAT YOU HAVE READ AND UNDERSTAND THIS AGREEMENT
; (B) REPRESENT THAT YOU ARE 18 YEARS OF AGE OR OLDER; AND (C) ACCEPT THIS EULA
--More--
```

5. Specify the type of license you want to use for the **Host**. The following options are available:
  - a. **Portal** – all communication happens using the **Portal** (an **Netop Portal** account is required)
    - i. Specify if you have a **Portal** account.

```

dragos@dragos-virtual-machine: ~/Downloads/netop-host-13.05-ubuntu-64bit
File Edit View Search Terminal Help
...
BY CLICKING TO "ACCEPT" OR "AGREE" TO THIS EULA WHEN THIS OPTION IS MADE AVAILAB
LE TO YOU OR BY DOWNLOADING, INSTALLING OR USING THE SOFTWARE, WHICHEVER IS FIRS
T TO OCCUR, YOU (A) ACKNOWLEDGE THAT YOU HAVE READ AND UNDERSTAND THIS AGREEMENT
; (B) REPRESENT THAT YOU ARE 18 YEARS OF AGE OR OLDER; AND (C) ACCEPT THIS EULA
Do you accept this license? [yes/No] >yes

[3] Which type of license do you want to use for Netop Host? [T]rial / [p]ortal
/ [c]ustom: p
Validating license ...
License key validated OK.
Your license has been saved.
[ ok ] Starting netophostd (via systemctl): netophostd.service.

Netop Host application has been installed and activated.
You can start the Netop Host user interface by typing 'netophostgui' as a regula
r user. Please note that this only starts the GUI, the Host is already running a
s a different process.
Thank you for using Netop Solutions Limited!

```

- ii. Specify the enrollment key for your **Portal** account.

```

Activities Terminal Lu 10:28
root@john-VirtualBox: ~/Downloads/wetransfer-ab5ac7/netop-host-12.81-ubuntu-64bit
File Edit View Search Terminal Help
...
to the Licensed Software. Netop Business Solutions may use this information, as
long as it is in a form that does not personally identify You, to improve its
products or to provide services or technologies to You.

10. Contact Information. Should you have any questions, complaints or claims wi
th respect to the Agreement, please contact us at Netop Business Solutions A/S,
Bregnerodvej 127, DK-3460 Birkerød, Denmark or +45 4590 25 25 or info@netop.co
m.

11. Vendor signing. For the Android version of Netop Mobile and Embedded it is
explicitly prohibited for end-users or any other to vendor sign or cause vendor
signing of this module and thereby enabling this module to reach necessary sys
tem resources needed for the viewing of the screen and injection of input to th
e devices, that it otherwise could not reach. Doing so immediately revokes the
license to use this module.

Do you accept this license? [yes/No/quit] >yes

[3] Which type of license do you want to use for Netop Host? [T]rial / [p]ortal
/ [c]ustom:
p
Validating license ...
License key validated OK.
Your license has been saved.
Do you have a Netop Portal account? [yes/No/quit] >y
Enrollment key : 

```

- b. **Trial** – a **15**-day fully-featured trial.
  - i. Specify if you have a **Portal** account.
  - ii. Specify the enrollment key for the **Portal** account.
- c. **Custom** – specify the required license after buying the product.
  - i. Specify the License key for the **Host**.

**NOTE:**

- You are prompted to specify a license key.
  - If you do not specify a license key, **Host** automatically installs itself in **Trial** mode.
- ii. Specify if you have an **Portal** account.
  - iii. Specify the enrollment key.

**NOTE:** The **Linux Host** version 12.79 and above allow you to connect to a UNIX device through the **Portal** and **Windows Guest**.

### 3.1.1.3 Windows XP & Vista

To install the **Host** on Windows XP & Vista, proceed as follows:

1. Go to the **Portal** under **Settings > Downloads** and click on the deployment package to retrieve the Enrollment key.

Package details

Name	12.80 dep
Status	● Active
Description	-
Valid from	2020-04-24
Valid to	-
Valid for	Unlimited devices
Enrollment key	
License Key	-

2. Download the **Host** online installer from the following [link](#).
3. Install the **Host** online installer.

**NOTE:** You can manually install it on the device you use or use a mass deployment tool. Refer to the following knowledge base [article](#) for more information on how to mass deploy the **Host**

4. Configure the **Host** to use the **Portal** communication profile in the Setup wizard with the default address and the above enrollment key. You can also add a new **Portal** communication profile from **Tools** > **Communication profiles** > **New**.

Communication Profile Edit

Communication Information

Communication Profile description:  
Portal Communication Profile

Communication Device:  
Netop Portal

Netop Portal

Address: portal.netop.com

Enrollment Key: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

Ok  
Cancel  
Help  
Test

### 3.1.2 Technician device

Technicians can use one of the following options to control a target device:

- [Connect through Guest](#)
- [Connect through browser](#) (Browser Based Support Console)



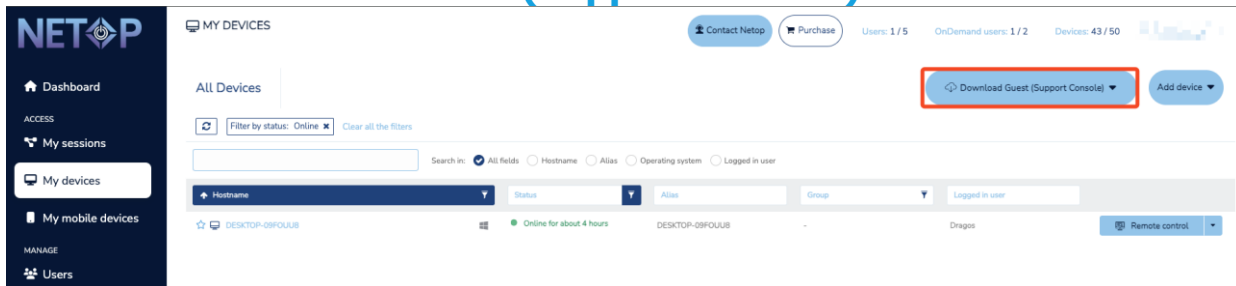
### 3.1.2.1 Connect through Guest

The **Guest (Support Console) application** is supported on the following platforms:

- Windows 7 & higher
- macOS
- Red Hat Enterprise 7.x / CentOS 7.x
- Ubuntu 16.04 / 18.04
- SUSE Enterprise 12.x

To download and install the **Guest (Support Console) application** on a Windows device, proceed as follows:

1. Go to the **My devices** tab.
2. Click on the **Download Guest (Support Console)** button.

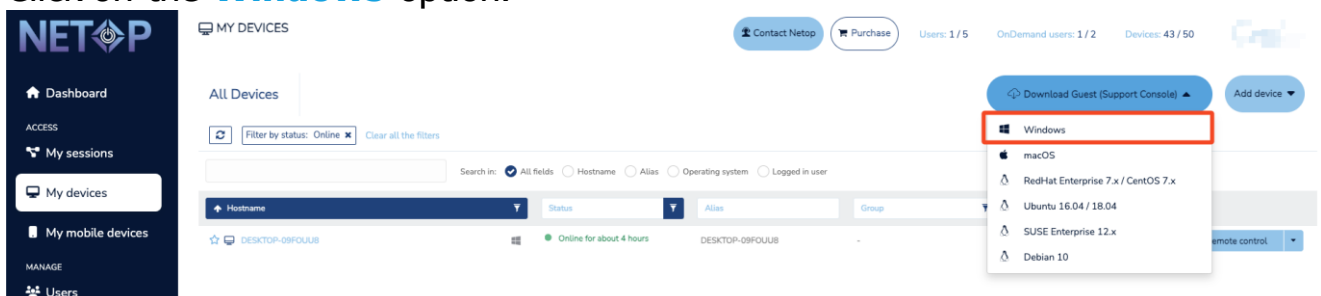


#### NOTES:

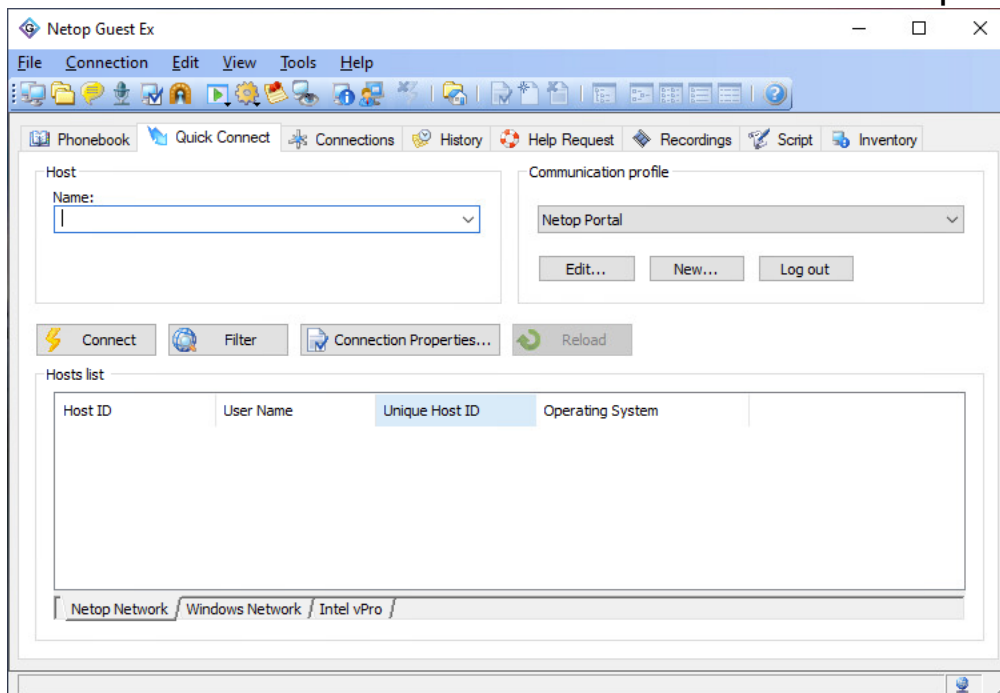
- Supported Windows versions: Windows 7 & higher
- Administrator permissions are required for the installation
- No license is required for the **Guest** (this is a **Portal** only installation, which means that the **Guest** only works with a **Portal** communication profile)

When the **Guest** is installed, any previous **Guest** installations are removed from the machine together with their corresponding settings

3. Click on the **Windows** option.



4. Click on the downloaded executable file.
5. Click on the **Finish** button to finish the installation process.



For more information on how to download and install the **Guest (Support Console)** application on a macOS or Linux device, click on one of the following links:

- [Linux Quick Install Guide](#)
- [macOS Quick Install Guide](#)

### 3.1.2.2 Connect through browser (Browser Based Support Console)

To connect to a **Host** device, click on the **Remote control** button near the online device. The **Remote control** button launches the default remote control action that it has been set to.

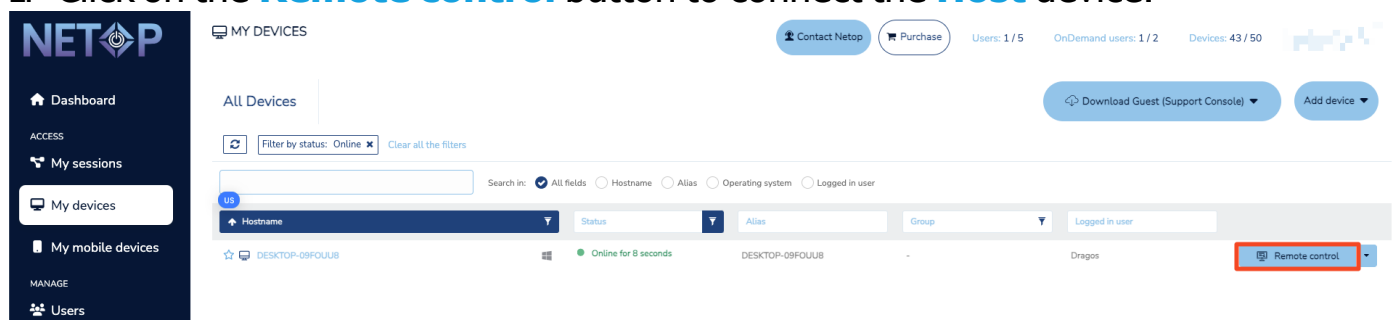
For more information on the **Browser Based Support Console**, refer to the [Browser Based Support Console User's Guide](#).

The default remote control action for the **Remote control** button is set to the **Control through browser** option.

For more information on how to set the default remote control action, refer to the [Set up the default remote control action](#) subchapter.

To connect to the **Host** device, proceed as follows:

1. Go to the **My devices** tab.
2. Click on the **Remote control** button to connect the **Host** device.



If the **Host** is configured to use **Portal** access rights, no other authentication is requested from the user and the remote control session starts.



Once logged in, the remote support session provides access permissions as defined by the role assigned in the **Portal**.

Keys not captured by the operating system, or the browser are added to the top menu.

For Windows these include:

- Windows key
- CTRL
- ALT
- SHIFT

For macOS these include:

- Command key
- Control
- Option
- Shift



Selecting one of the keys within the console, and then pressing any key on your keyboard, triggers the combination of those keys to be sent to the



target device. Once the keyboard key is released, the button in the browser menu is unclicked.

To use a key (e.g., **SHIFT**) multiple times, double-click on the button and the key stays engaged. To release the command, click on the button again.

Using the console, you can send a variety of Windows commands using the power button options.

These include:

- Logout
- Lock
- Restart
- Shut down
- CTRL + ALT + DEL

If the **Host** has multiple monitors, while in a remote control session, you can change the host monitor to be displayed on the screen. Click on the **View** button from the main menu and selecting the desired monitor.

Other options that are available include:

- Toolbar minimization
- Close session button

## 3.2 OnDemand Sessions

In many environments, end-user computers have no administrative or organizational relationship with the help desk center from which they request help.

Help desk centers face three major challenges to offer service to these end-user computers:

- connectivity problems through end-user firewalls
- software maintenance
- licensing issues

The **Portal** includes the **OnDemand Sessions** feature, which offers help desk centers remote control of Windows-based devices across the Internet without pre-installing software or configuring firewalls. Furthermore, licensing depends solely on the number of help desk employees or supporters – and not the number of end-users.

The **OnDemand Sessions** contains the **Browser Based Support Console**, a downloadable **Netop OnDemand** application, and the connectivity and role-based access provided by the **Portal**. Technicians can connect to the target **Host** device, by clicking on the **Start session** button from the **My sessions** tab.

**OnDemand Sessions** are well-suited to the vast and fast-growing market of Internet Service Providers, telephone companies, outsourced help desks, and call-centers.

The **Portal** allows a support technician to define **OnDemand Sessions** and to share the session details with someone else, to view or control their device. This can be done without installing anything on the remote device, by running a single-use and disposable **OnDemand** application on the device, when necessary.

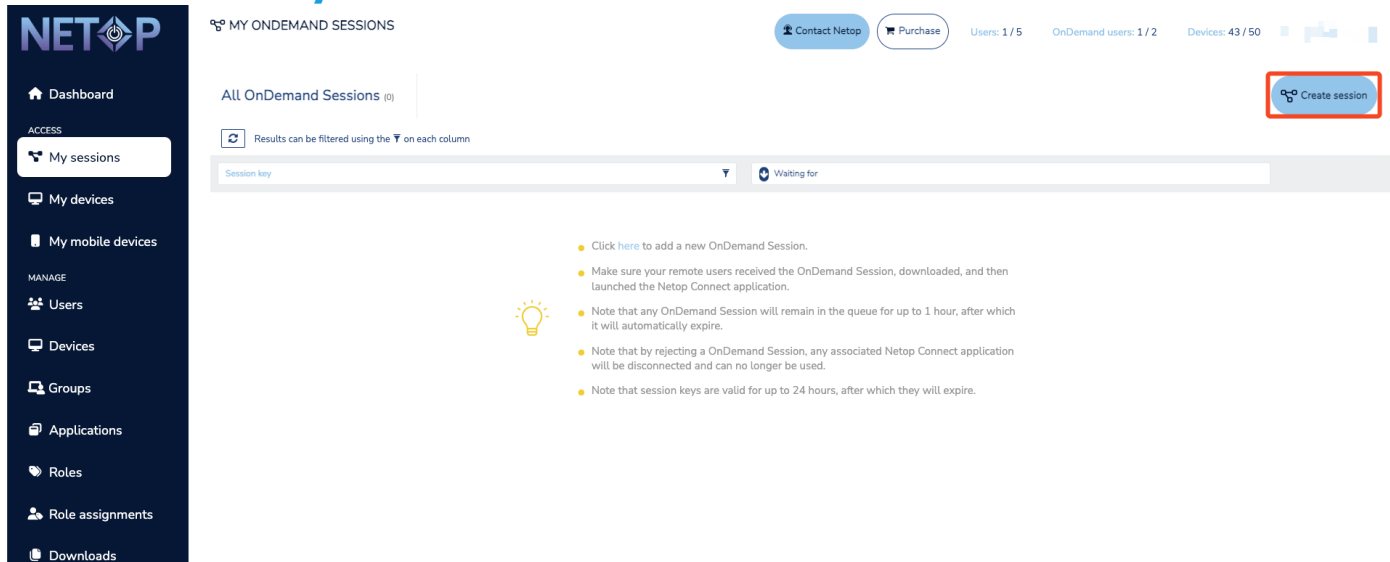
The **OnDemand Sessions** are valid only for one remote connection from the support technician to the device and are deleted automatically after the connection is closed.

**NOTE:** If you have an incompatible **OnDemand** client (i.e., you do not have the latest version of it) you are requested by the **Portal** to update it to the latest version.

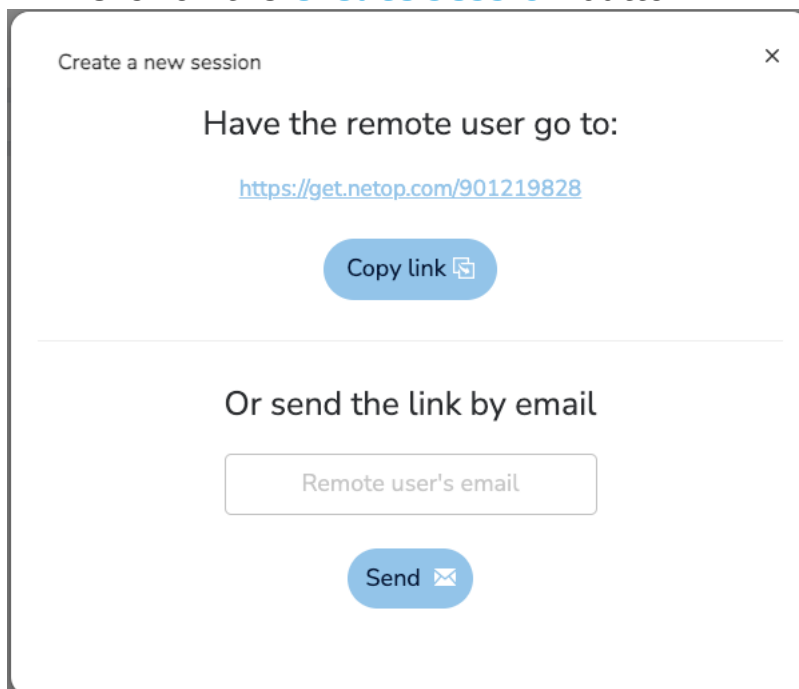
### 3.2.1 Browser Based Support Console – OnDemand Sessions

To create a new **OnDemand Session**, proceed as follows:

1. Access the **My sessions** tab from the menu on the left.

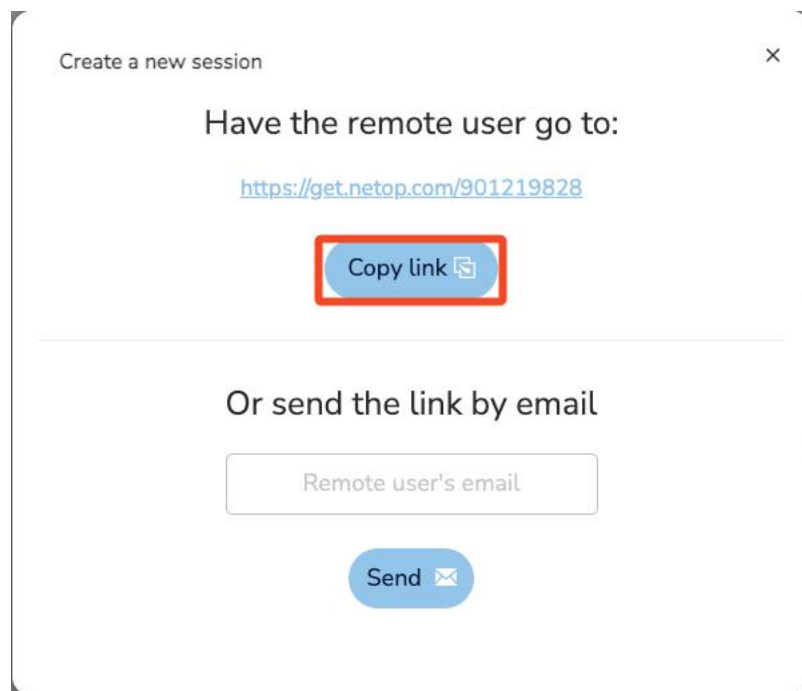


2. Click on the **Create session** button.

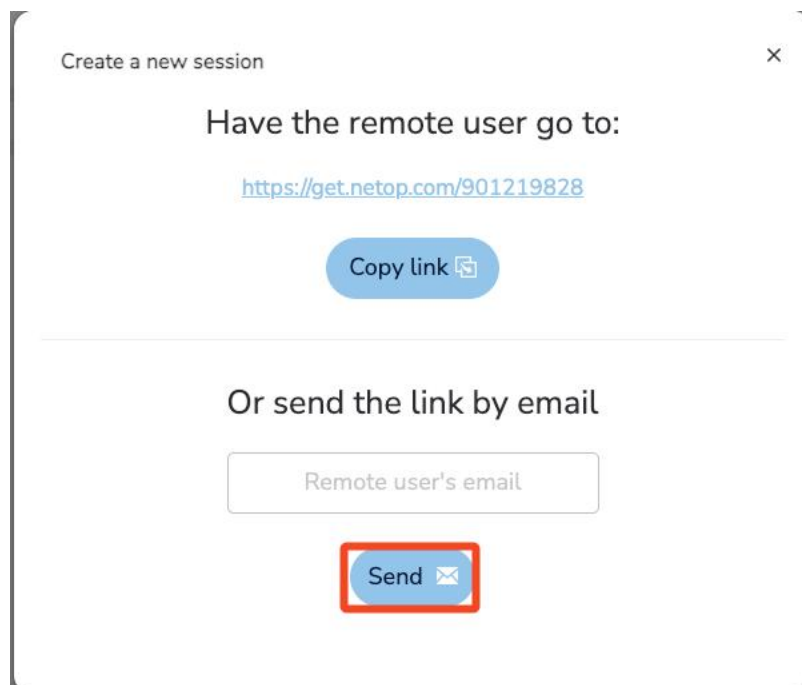


This automatically creates a one-time session key and provides you with several ways of sharing the session details with another user.

To copy the link to the clipboard, click on the **Copy link** button.



3. To send the link by email, specify the email of the user in the "*Remote user's email*" entry field and click on the **Send** button.



4. Once the remote user accesses the link received from the support technician, a custom download page is shown.



### ONDEMAND SESSION

Netop allows a support technician to remotely access and control a device.

Before a connection can be made, you need to download the Netop module on your device.



Click below to download and execute the Netop module on your device.

Please note that once the software is connected, this device will be reachable remotely by a support technician, so make sure you have received this link from a trustworthy source.

☒ I understand

---


Session key 901219828

[Download for macOS](#)  

Do you already have Netop Agent installed on your Mac?  
[Click here to open it](#)

---

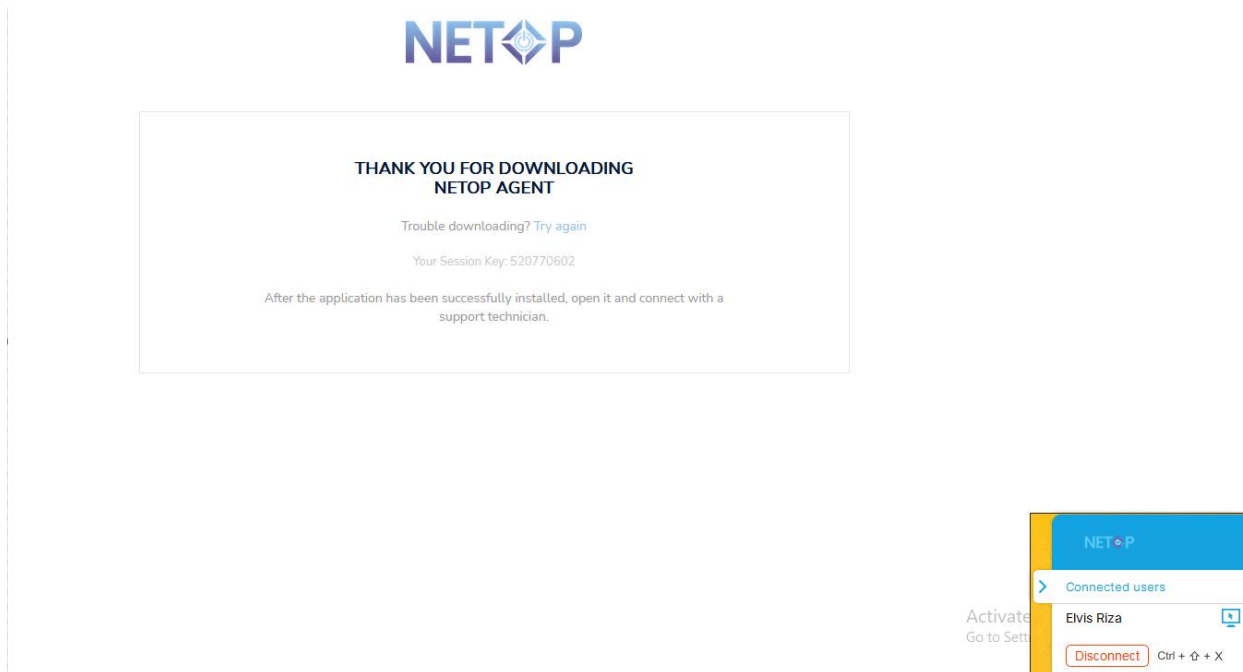
Looking for OnDemand for iPhone? Scan the QR below.



**NOTE:** The **Portal** detects the platform that you use to access the **OnDemand** session link and displays the corresponding download link.

The remote user first needs to acknowledge that the link was provided by a trustworthy source before being allowed to download the **OnDemand** application.

When you create an **OnDemand Session**, you receive a browser notification on the **Guest** device. Click on the notification to go to the **OnDemand** session queue.



To allow website notifications in the browser, proceed as follows:

- **For Chrome\***

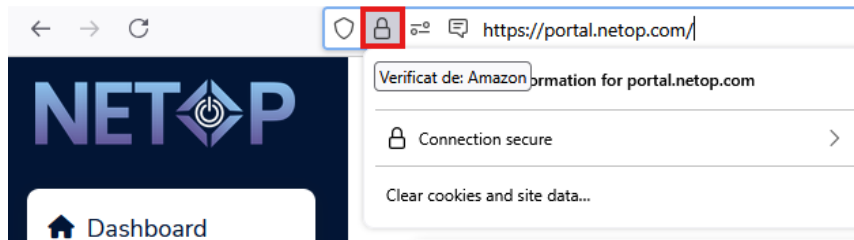
1. Open the **Chrome** internet browser.
2. In the address search bar, specify **portal.netop.com**.
3. Click on the "**View Site Information**" button (the lock icon in the search bar).
4. Select "**Allow**" from the "**Pop-ups and redirects**" drop-down menu.

---

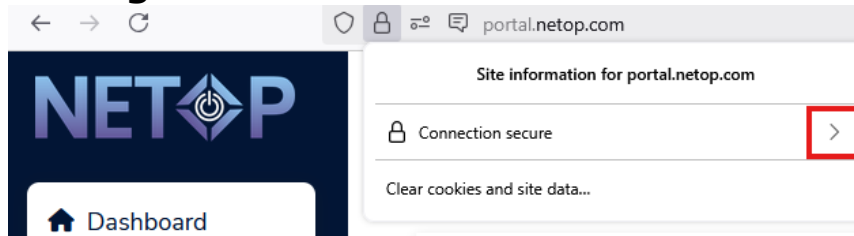
\* Latest version

- **For Firefox\***

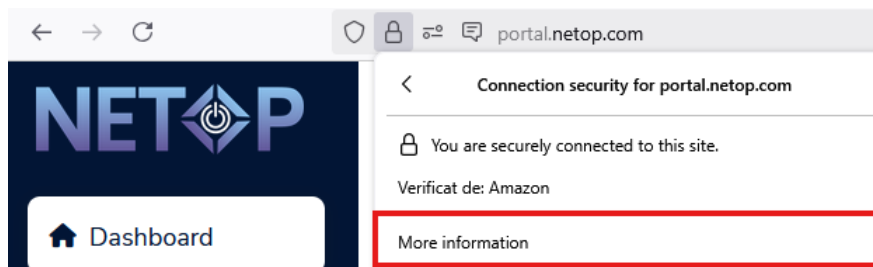
1. Open the **Firefox** internet browser.
2. In the address search bar, specify **portal.netop.com**.
3. To view the **Site information**, click on the **lock** icon in the address search bar.



4. Click on the **right arrow**.



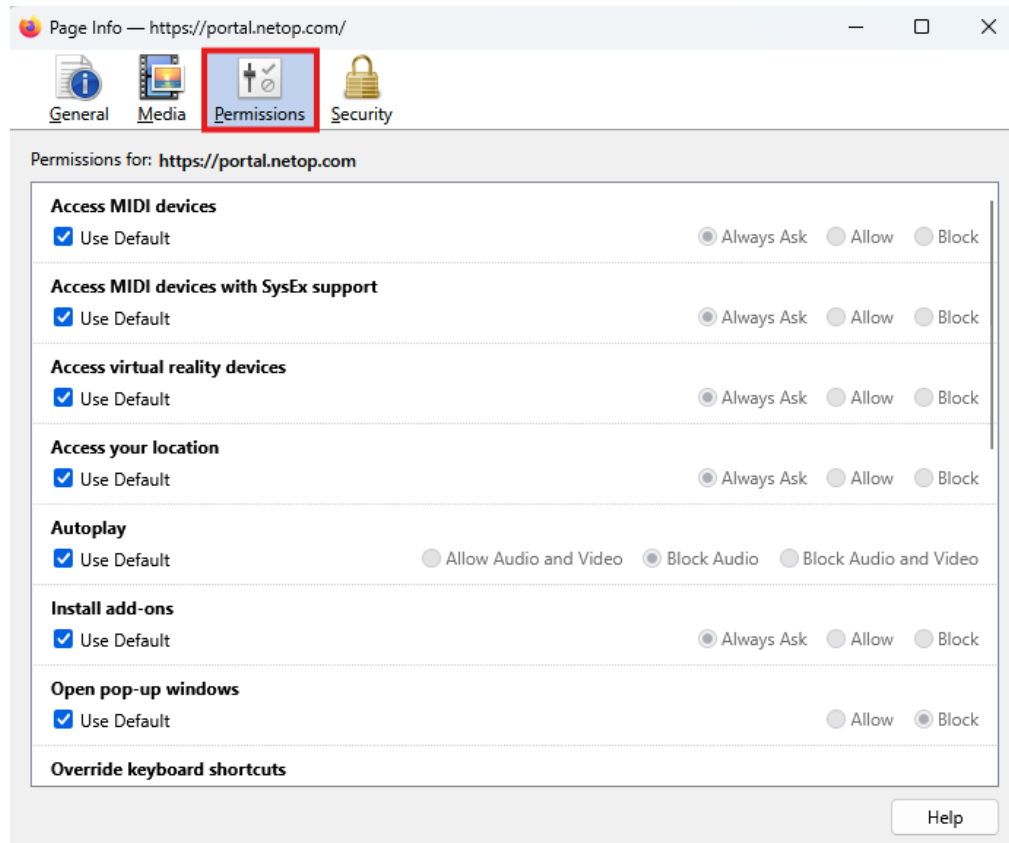
5. Click on the **More Information** button.



---

\* Latest version

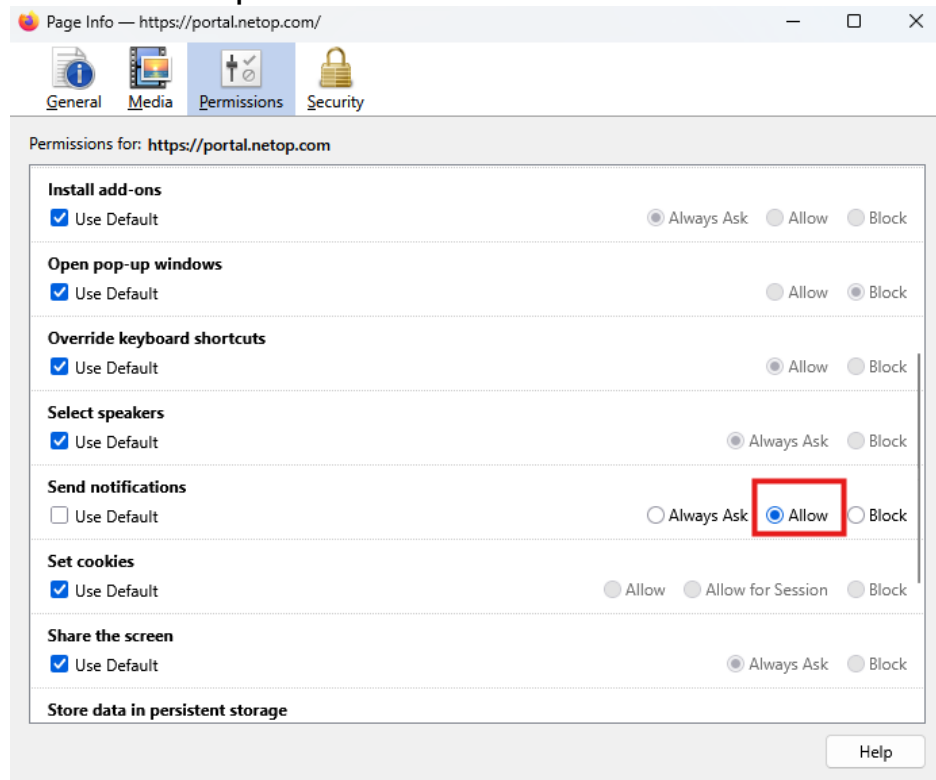
6. Click on the **Permissions** tab.



7. Uncheck the **“Use default”** check button for the **“Send Notifications”** permission.



## 8. Select the **"Allow"** option.



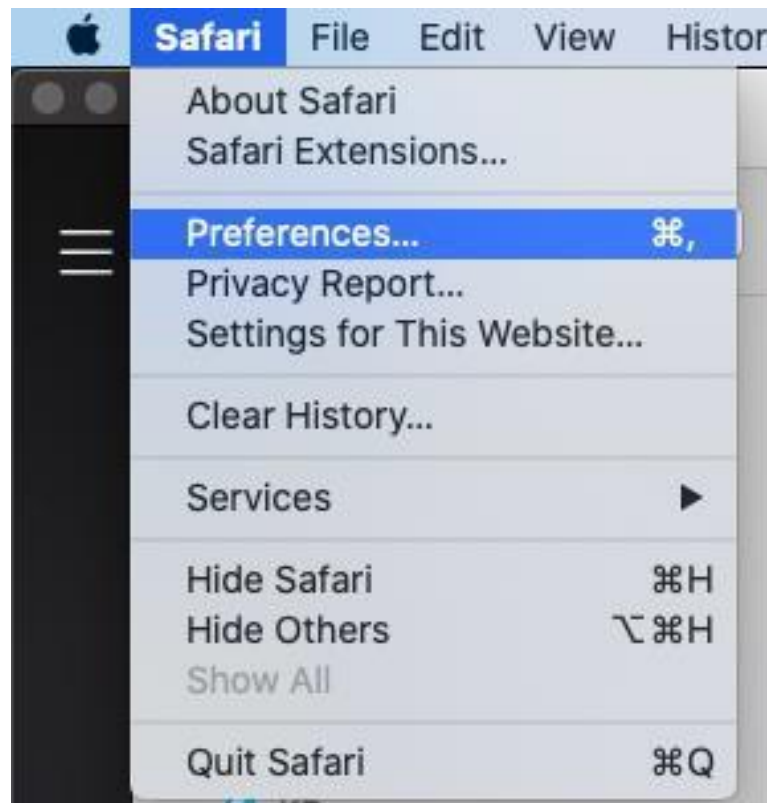
- **For Safari\***

1. Open the **Safari** internet browser.
2. In the address search bar, specify **portal.netop.com**.

---

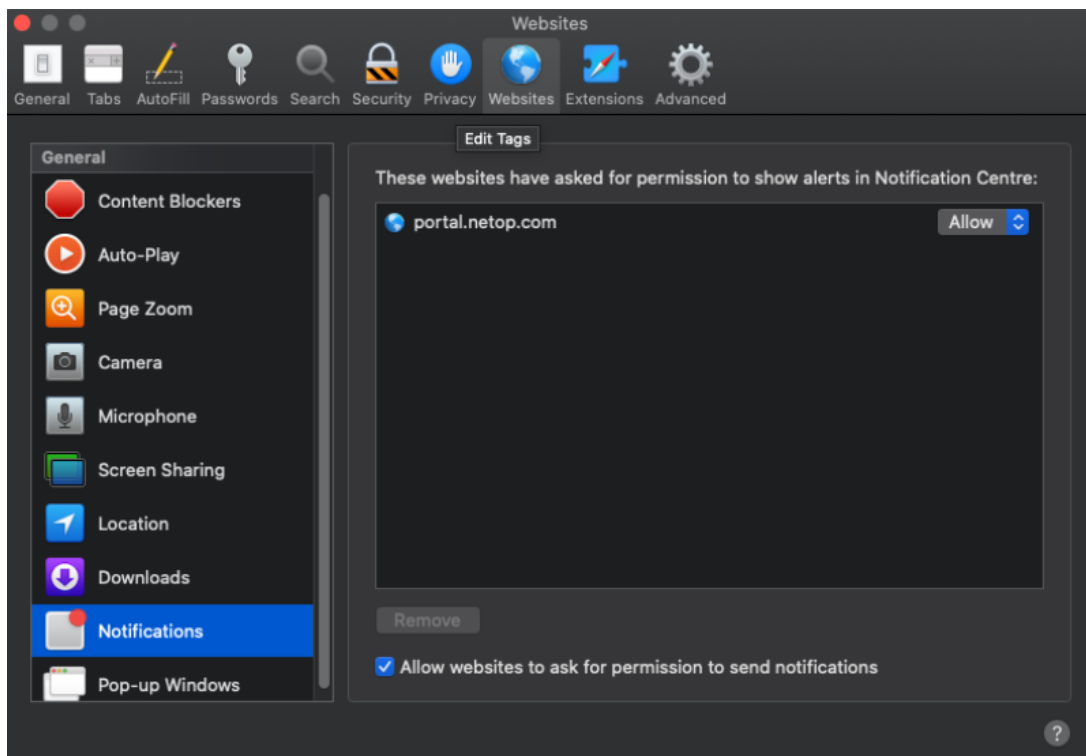
\* Latest version

3. In the **Safari** menu, go to **Preferences**.



4. In the **Preferences** window, click on the **Websites** icon and then on **Notifications**.

- Click on the dropdown button corresponding to the `portal.netop.com` and select **Allow**.



**NOTE:** To receive **OnDemand** browser notifications, make sure that notifications are allowed in the browser.

### 3.2.2 Start an OnDemand Session application on a Windows machine

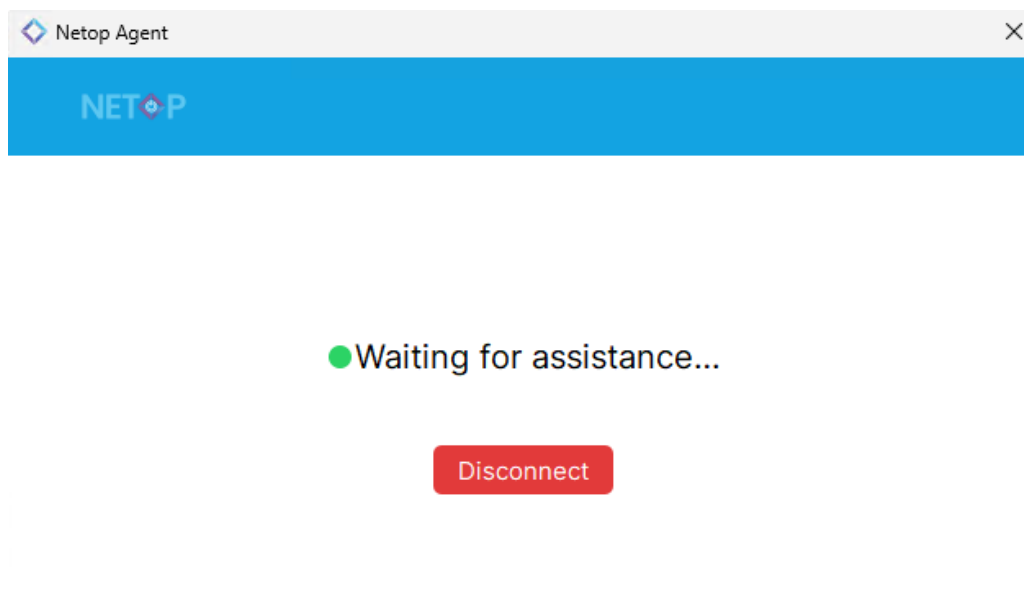
- Once the **OnDemand** application is executed, a **UAC** prompt might be displayed, asking the user to elevate the application.

If the elevation is granted, the support technician can fully control elevated applications (i.e., Task Manager) as well as **UAC** prompts, while required Firewall exceptions are automatically added to the system. If the elevation is not granted, the **OnDemand** application still runs and is not elevated.

The support technician can connect, and the elevated applications are not controllable with keyboard and mouse.

**NOTE:** While an elevated application is in the foreground and if the **OnDemand** application was not elevated, keyboard and mouse control are unavailable, until the user on the controlled machine switches to a non-elevated application.

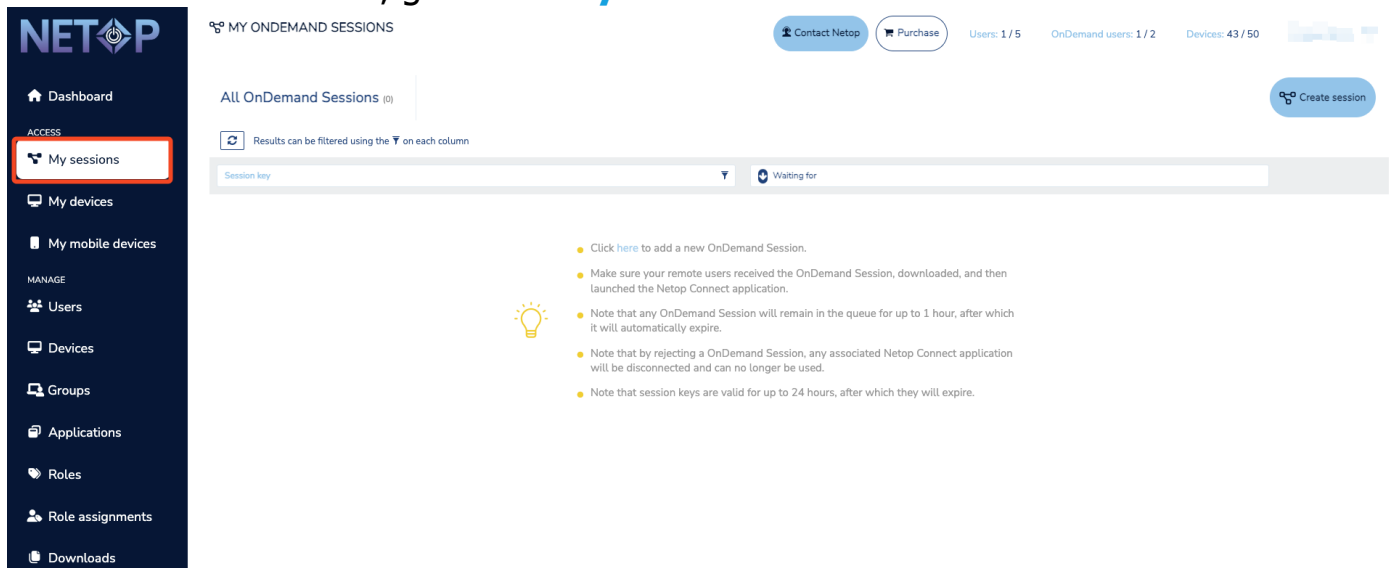
2. After the elevation is granted or denied, the **OnDemand** application starts and waits for a support technician to connect.



### 3.2.3 Initiate an OnDemand Session remote connection

To initiate an **OnDemand** session, proceed as follows:

1. Within the **Portal**, go to the **My sessions** tab.



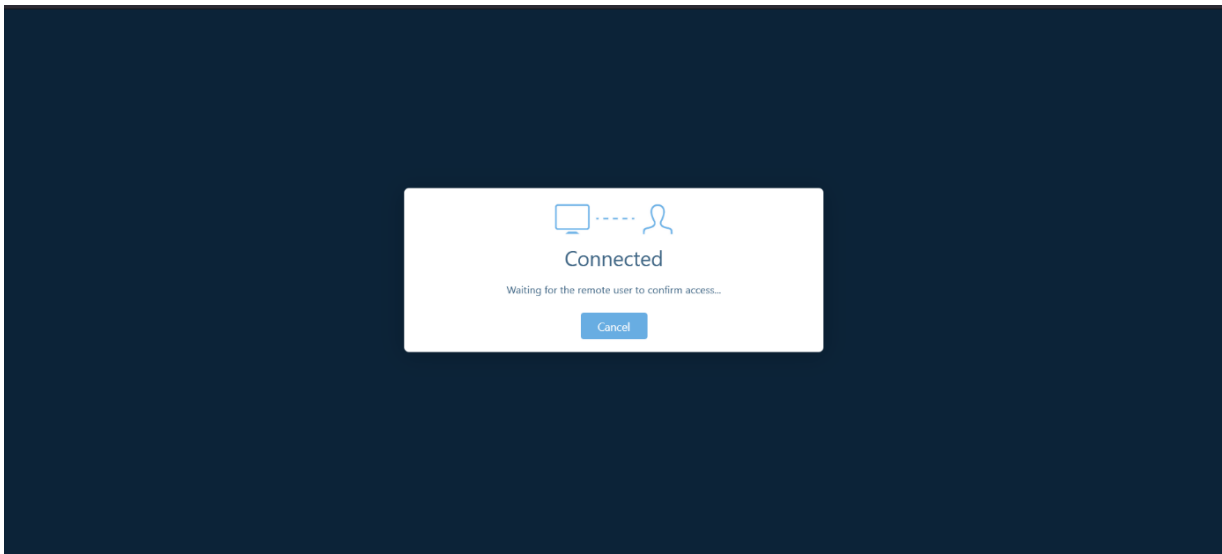
The displayed queue includes all the **OnDemand Sessions** started by remote users and the time since they are waiting for a connection. Only the running **OnDemand Sessions** can be seen in the queue.

**NOTE:** The **Session key** column includes icons for the permissions when connecting to that device, as granted by the role assignments for the current user.

Refer to the [Roles and Role assignments](#) sub-chapter for more information.

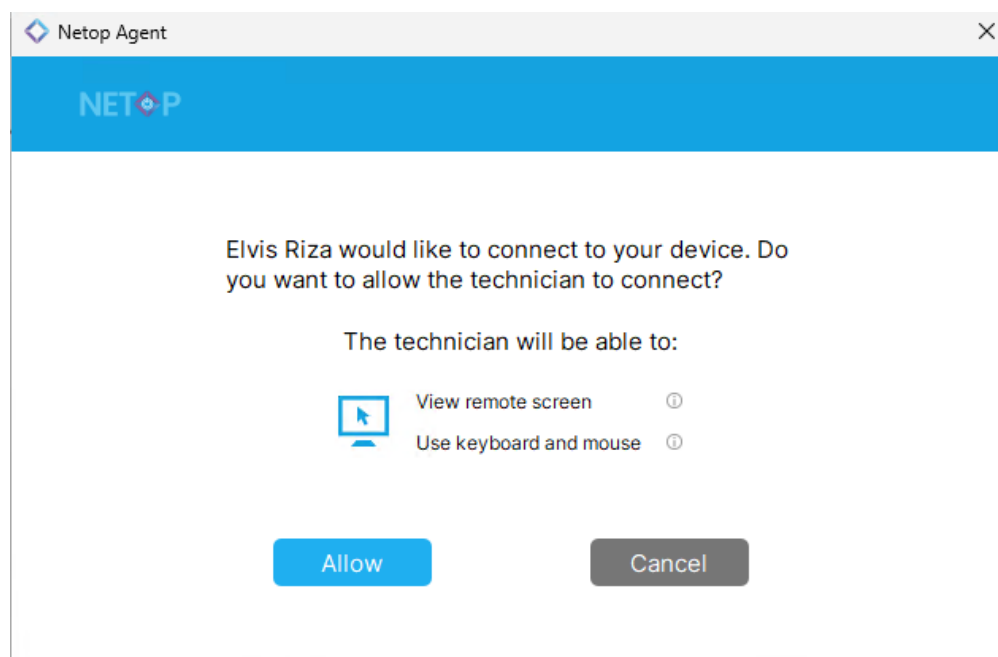
Only the running **OnDemand Session** can be seen in the queue. The **OnDemand Sessions** stay in the queue for **1h** before being automatically disconnected. An **OnDemand** session key is valid **24h** since it was created.

Click on the **Start session** button. The **Control through browser** page starts in a new tab.



**NOTE:** As an alternative to starting the session, the support technician can reject any session in the queue. This automatically disconnects the **OnDemand** application and disables the **OnDemand** session. A new **OnDemand** session is necessary to be created and sent to the remote user for a new remote session to be initiated.

2. The remote user needs to allow the support technician access to the device before the remote session starts.

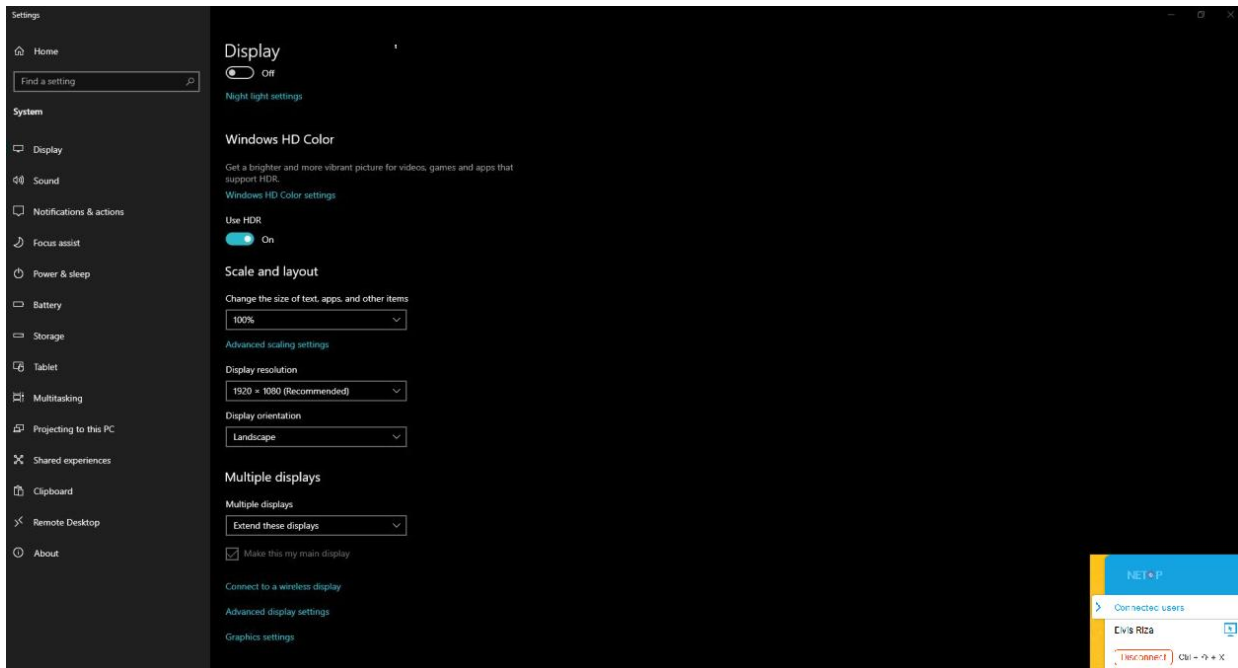


3. Once access is granted, the remote session starts.



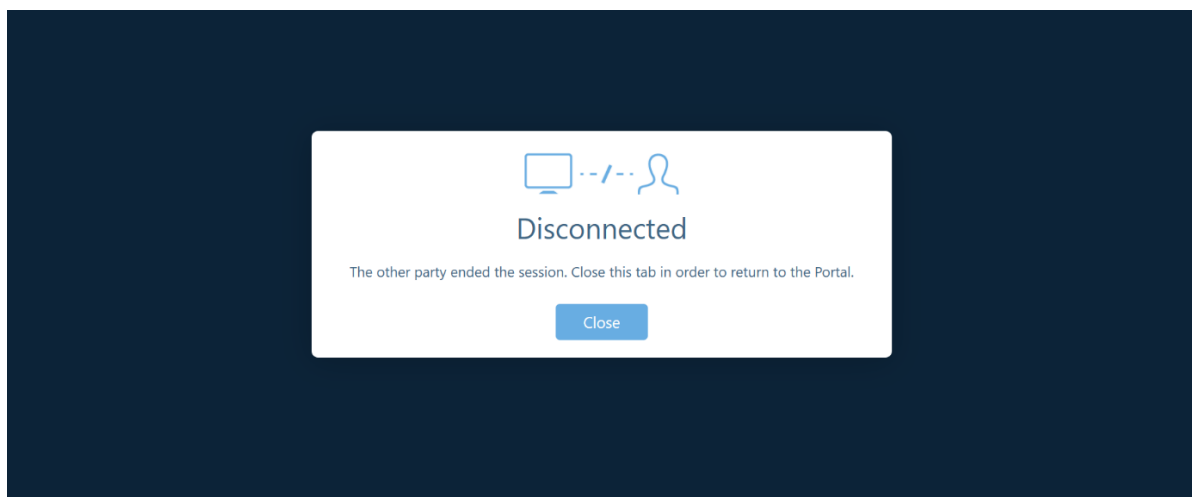
The **Browser Based Support Console** toolbar includes virtual key modifiers to use during the remote session. Each of the 4 key modifiers has 3 possible states: off, on, and always on (use it by double-clicking on the key modifier). These key modifiers help send various key combinations to the remote machine, whenever the physical keyboard cannot be used for this. The **View** menu allows the support technician to switch between **Fit To Screen** and **Actual Size** for the displayed image.

- The remote user sees a notification that the session has started, along with information about the support technician's name and the granted permissions. The remote user can close the session at any moment, by clicking on the **Disconnect session** button, or by using the keyboard hotkey (**CTRL + SHIFT + X**).



**NOTE:** Using the disconnect hotkey closes the session immediately, without confirmation. This is done to make sure the remote user has an unobstructed method of closing an ongoing session.

- Once the remote session is closed, the support technician is notified about it in the **Browser Based Support Console** page.





### 3.2.4 OnDemand Sessions Clipboard functionality

The **OnDemand Sessions** feature a simple text **Clipboard** functionality, which is achieved by synchronizing the clipboard between the **Agent** and the **Client** devices. The toolbar, right-click Copy/Paste, and the following key combinations are available for technicians to copy and paste the content:

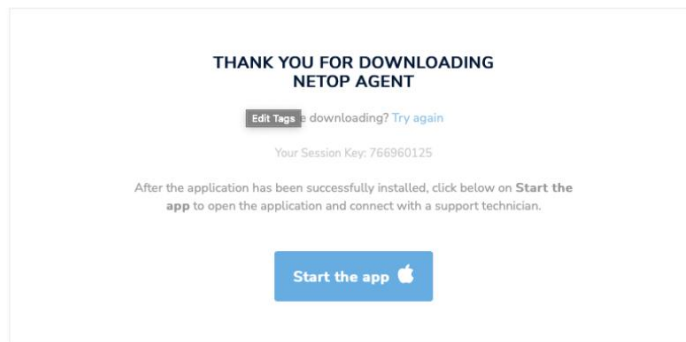
Client	Agent	Key combinations	Toolbar available
macOS	Windows	CTRL-V	no
		CTRL-V	yes
		CMD-V	no
		WIN-V	yes
		CMD-C	no
		WIN-C	yes
		CTRL-C	no
		CTRL-C	yes
		right click - Copy	no
		right click - Paste	no
Windows	macOS	CTRL-V	no
		CTRL-V	yes
		WIN-V	no
		CMD-V	yes
		WIN-C	no
		CMD-C	yes
		CTRL-C	no
		CTRL-C	yes
		right click - Copy	no
		right click - Paste	no

**NOTE:** The **Clipboard** functionality works between Windows and macOS **Agent** and **Client** devices.

The **Clipboard** functionality works on the following web browsers: Chrome, Firefox, and Safari.

**NOTE:** Due to the latest security and privacy implementations made by Apple, Safari does not allow to copy and paste content between the **Agent** and **Client** devices, without permission from the user.

To synchronize the clipboard between the **Client** and **Agent** devices, press on the following button:



### 3.2.5 Start an OnDemand Session application on a macOS machine

Prerequisite:

- The **OnDemand** application installed on your macOS device

To install the **OnDemand** application on your macOS device, proceed as follows:

1. To install the **OnDemand** application, click on the link you received from your technical support provider. The **Session** window is displayed.



#### ONDEMAND SESSION

Netop allows a support technician to remotely access and control a device.

Before a connection can be made, you need to download the Netop module on your device.



Click below to download and execute the Netop module on your device.

Please note that once the software is connected, this device will be reachable remotely by a support technician, so make sure you have received this link from a trustworthy source.

☒ I understand

---


Session key

[Download for macOS](#)  

Do you already have Netop Agent installed on your Mac?  
[Click here to open it](#)

---

Looking for OnDemand for iPhone? Scan the QR below.



2. Click on the **"I Understand"** button to allow the download.

3. Download the **Netop Agent.pkg** file.
4. Execute the **Netop Agent.pkg** file on your macOS device. The **OnDemand Installer** window is displayed.
5. Click on the **Continue** button to continue with the installation process.
6. Click on the **Continue** button to accept the **License Agreement**.
7. Click on the **Install** button to install the **OnDemand** application.

To use the **Netop Agent** on a macOS device, it is necessary that the following permissions are manually granted by the user.

These permissions require to be set only once.

- **Screen Recording** (applies for macOS 10.15 and above)
- **Accessibility** (applies for macOS 10.14 and above)

Without these permissions, the **Netop Agent Desktop** functionality can be restricted to:

- Viewing the desktop background, but no other applications
- Not being able to control the keyboard and mouse remotely

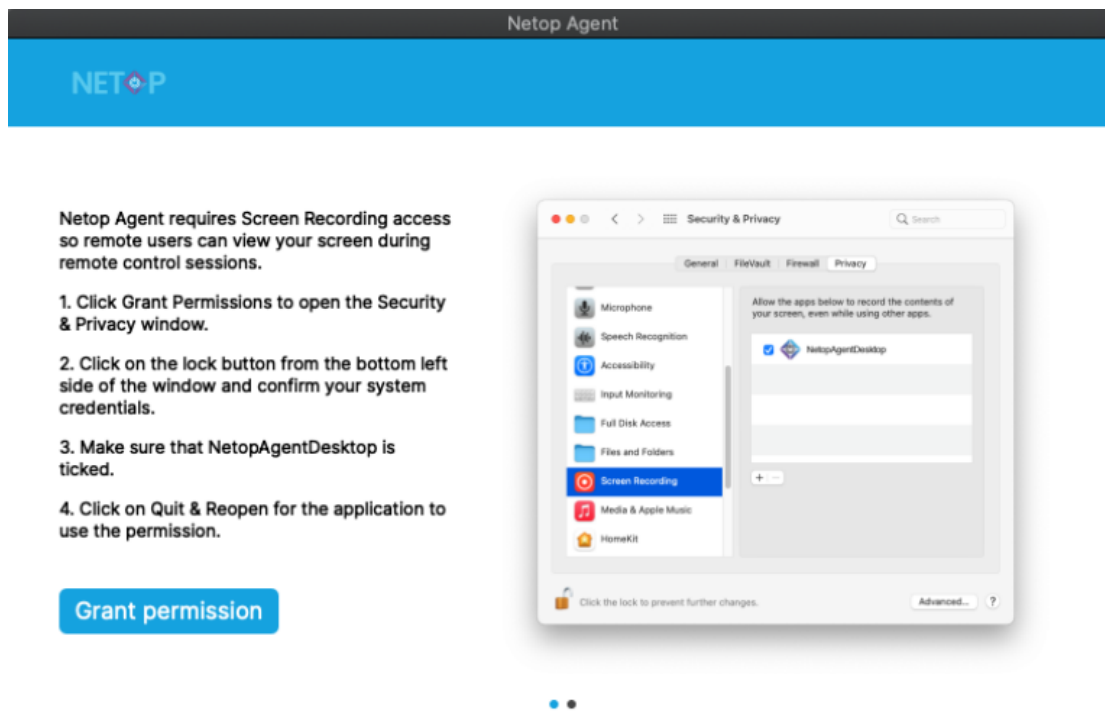
### 3.2.5.1 Screen Recording

**Netop Agent Desktop** requires **Screen Recording** access so remote users can view your screen during remote control sessions.

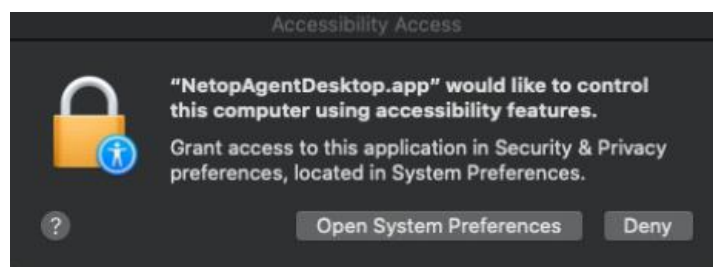
The first time you open the application on your device, you are prompted by the application to allow the **Screen Recording** permission.

To grant the permission, proceed as follows:

1. Click on the **Grant permission** button.

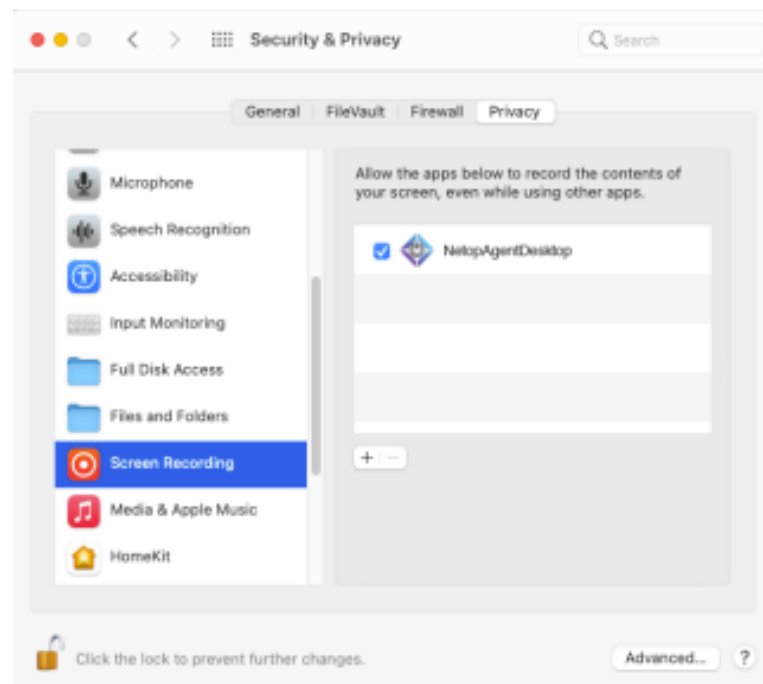


2. Open **System Preferences** when the **Screen Recording** dialog appears on the screen.

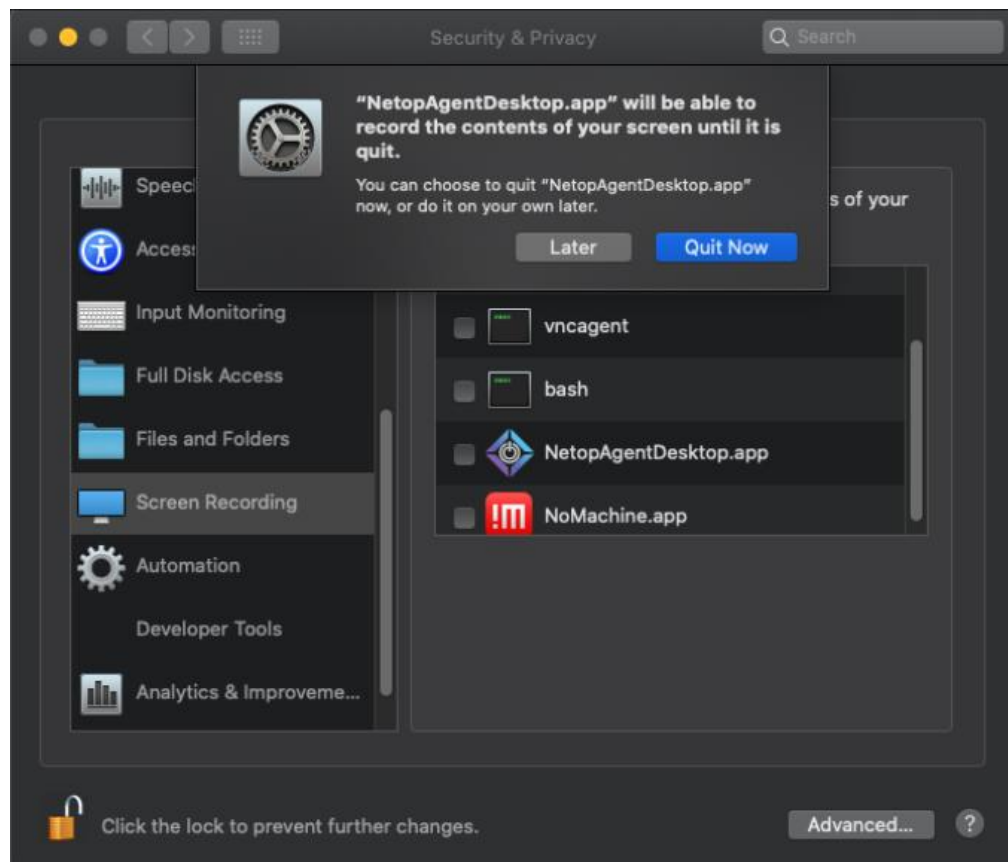


3. Click on the lock to make changes.

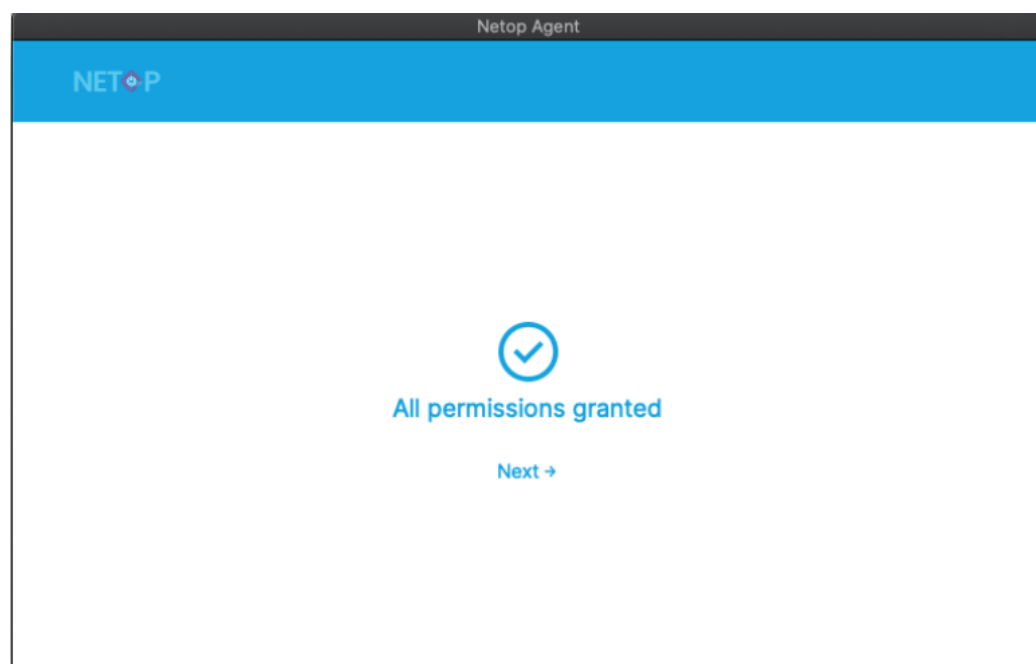
4. Select the **NetopAgentDesktop** checkbox to grant the **Screen Recording** permission.



5. **NetopAgentDesktop** requires to quit and reopen to use the permission. Click on the **Quit & Reopen** button to restart the application.



6. Click on **Next**.



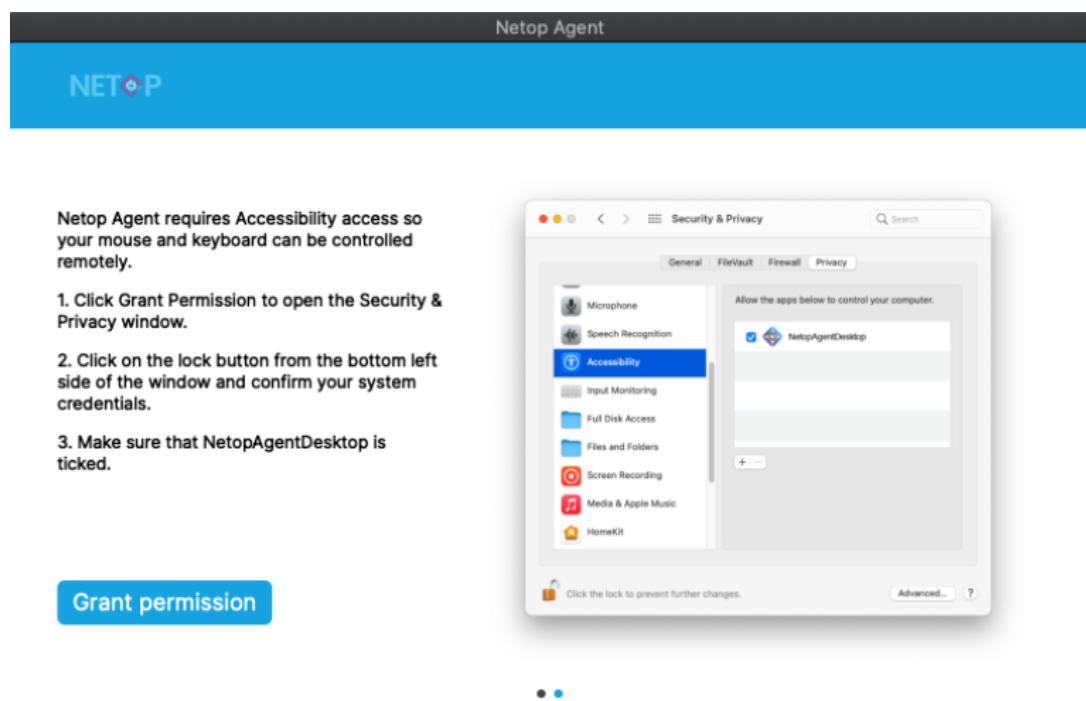
### 3.2.5.2 Accessibility

**Netop Agent Desktop** requires **Accessibility** access so your mouse and keyboard can be controlled remotely.

Once you granted the **Screen Recording** permission, the application prompts you to allow the **Accessibility** permission.

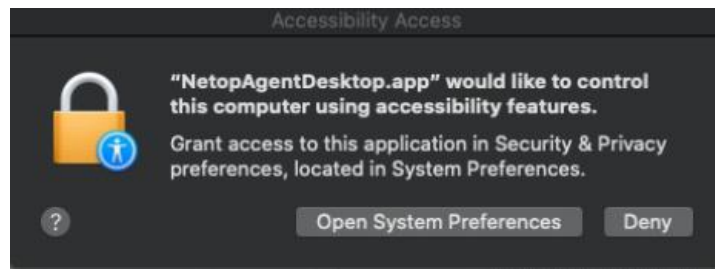
To grant the permission, proceed as follows:

1. Click on the **Grant permission** button.

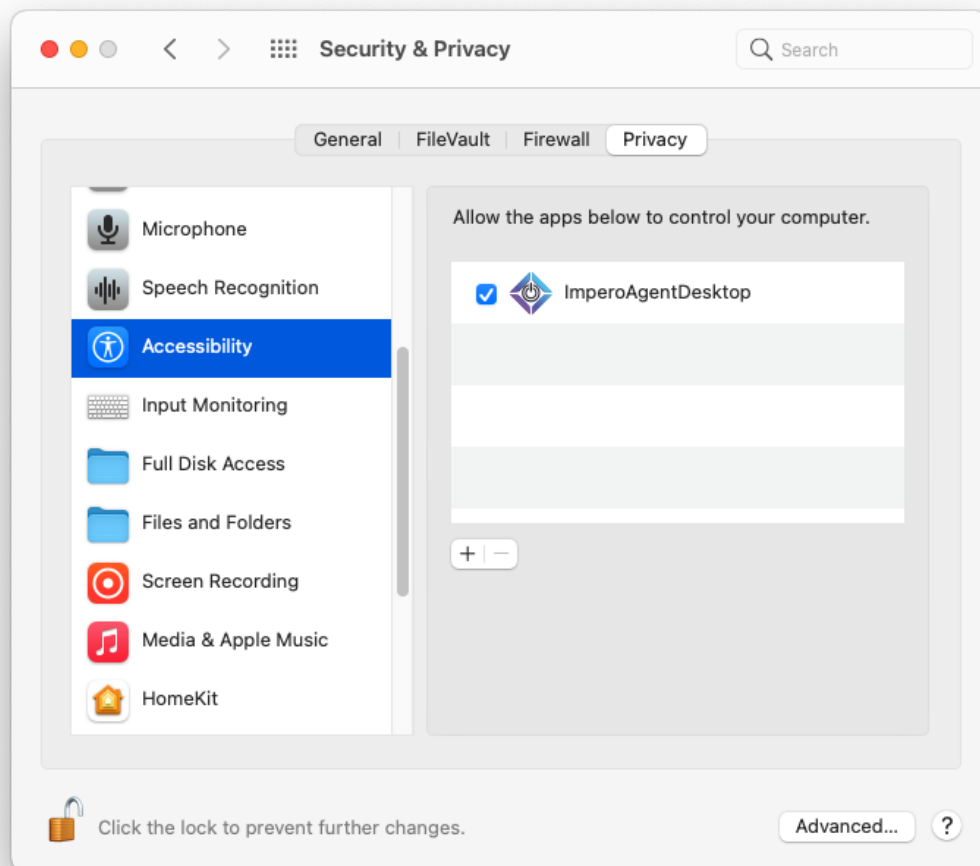




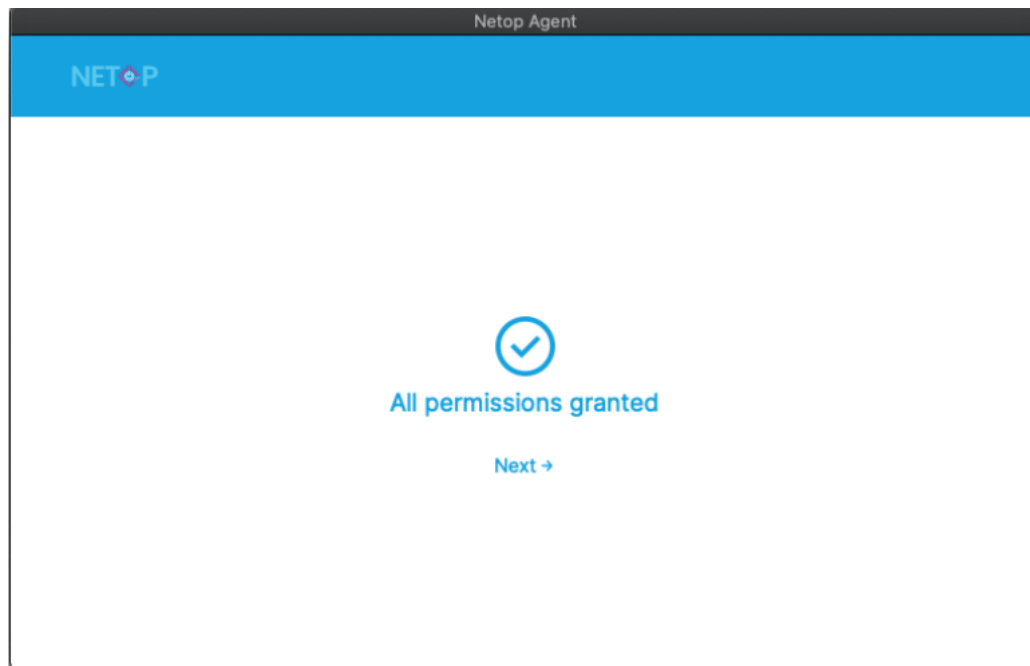
2. Open **System Preferences** when the **Accessibility** dialog appears on the screen.



3. Click on the lock to make changes.
4. Select the **NetopAgentDesktop** checkbox to grant the **Accessibility** permission.



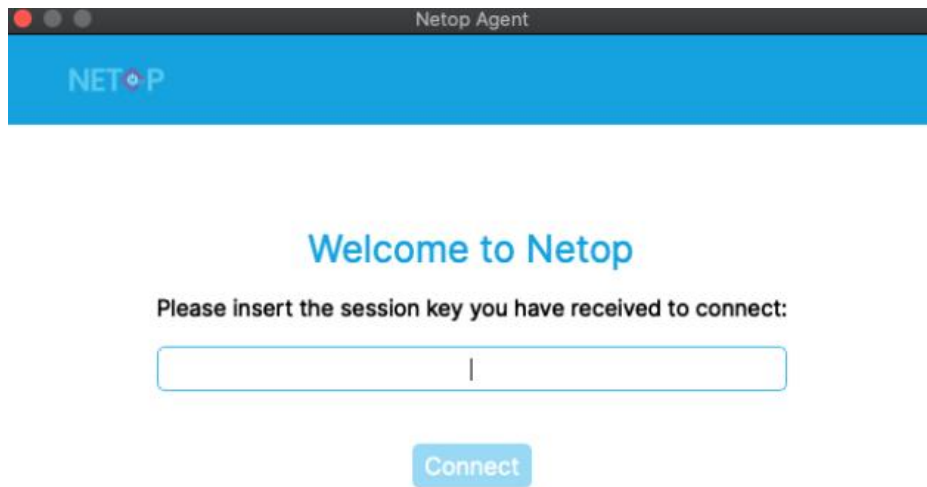
5. Click on **Next**.



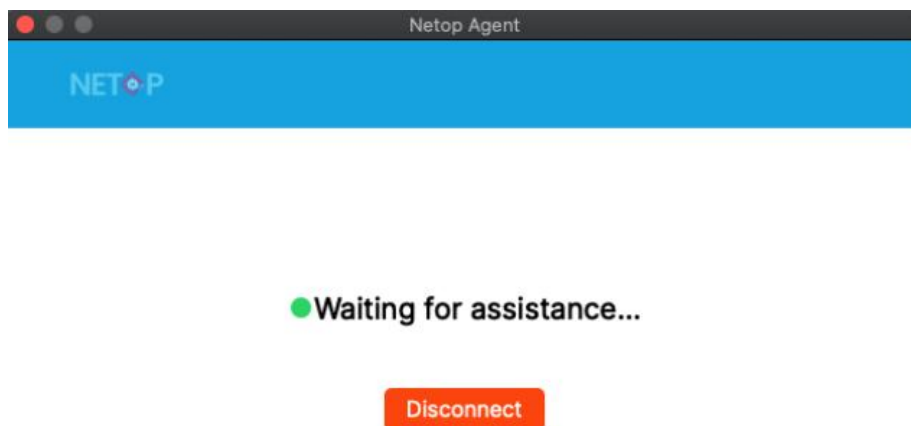
To start the **OnDemand** session, proceed as follows:

1. Open the **OnDemand** application.

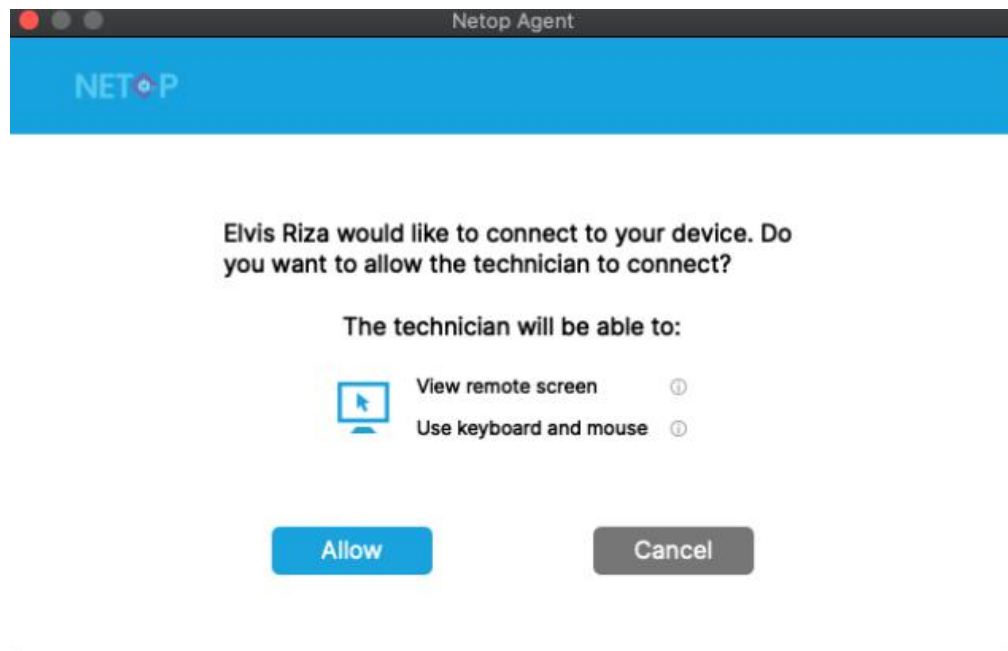
2. Specify the **session key** you received from your technical support provider.



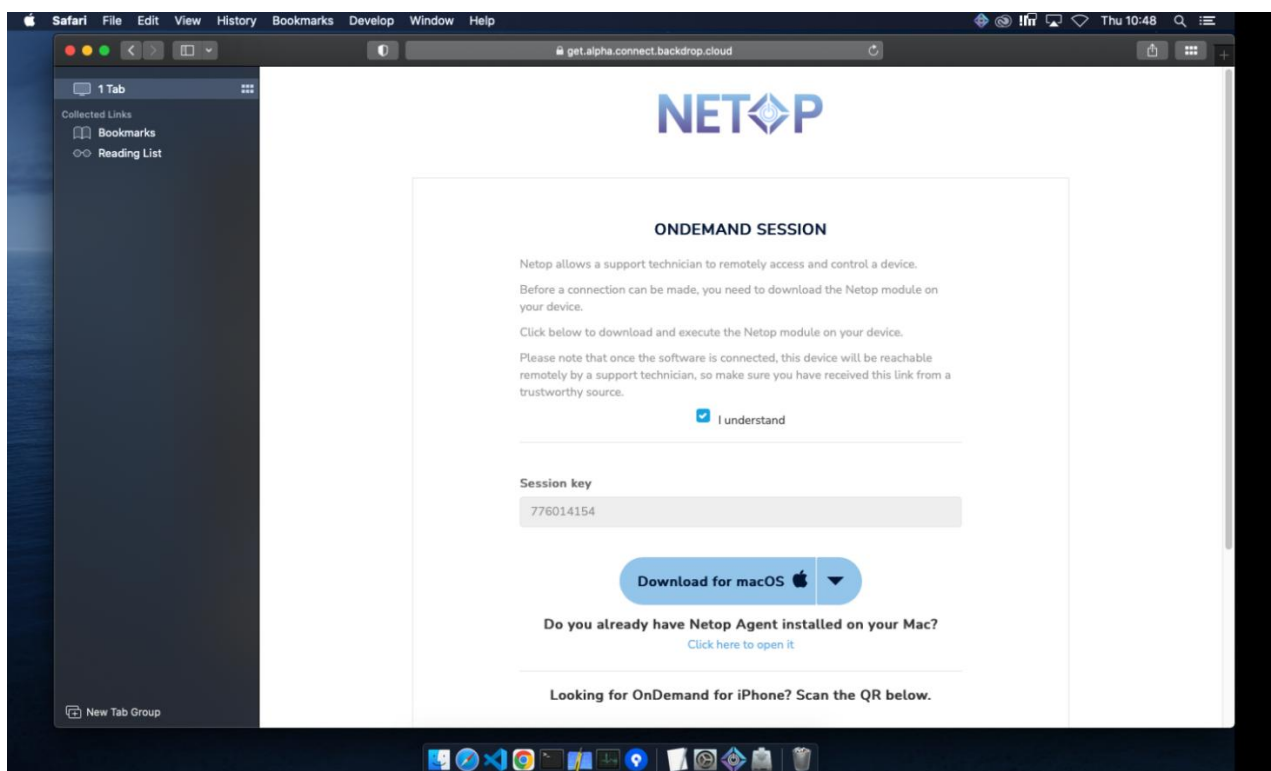
Wait for the technician to start the **OnDemand** session from the **Portal**.



- Once the technician starts the **OnDemand** session from the **Portal**, you are prompted to allow the technician permissions for **View remote screen** and **Use keyboard & mouse**.



- Click on the **Allow** button to start the **OnDemand** session.



### 3.2.6 Start an OnDemand Session application on an iOS device

With **OnDemand** for iOS you can view iOS devices screens and allow technicians to offer remote support.

Prerequisite:

- The **OnDemand** application installed on your iOS device

There are three ways to download the **OnDemand** application on your iOS device:

- From the AppStore
- From the link that you received from your technician
- By scanning the **QR** code from the download page

---

Looking for OnDemand for iPhone? Scan the QR below.



**NOTE:** If the **OnDemand** application is installed on your iOS device when you scan the **QR** code from the download page, the **OnDemand** app opens on your iOS device with the session key prefilled and ready for connection.

To start an **OnDemand** session, proceed as follows:

1. Open the **OnDemand** application on your iOS device.
2. Specify the **session key** that you received from your technician.

09:24 5G 59%

Initiate connection

**NETOP**

**Initiate connection**

Connect with a technician on the Netop Portal to troubleshoot your iOS device.

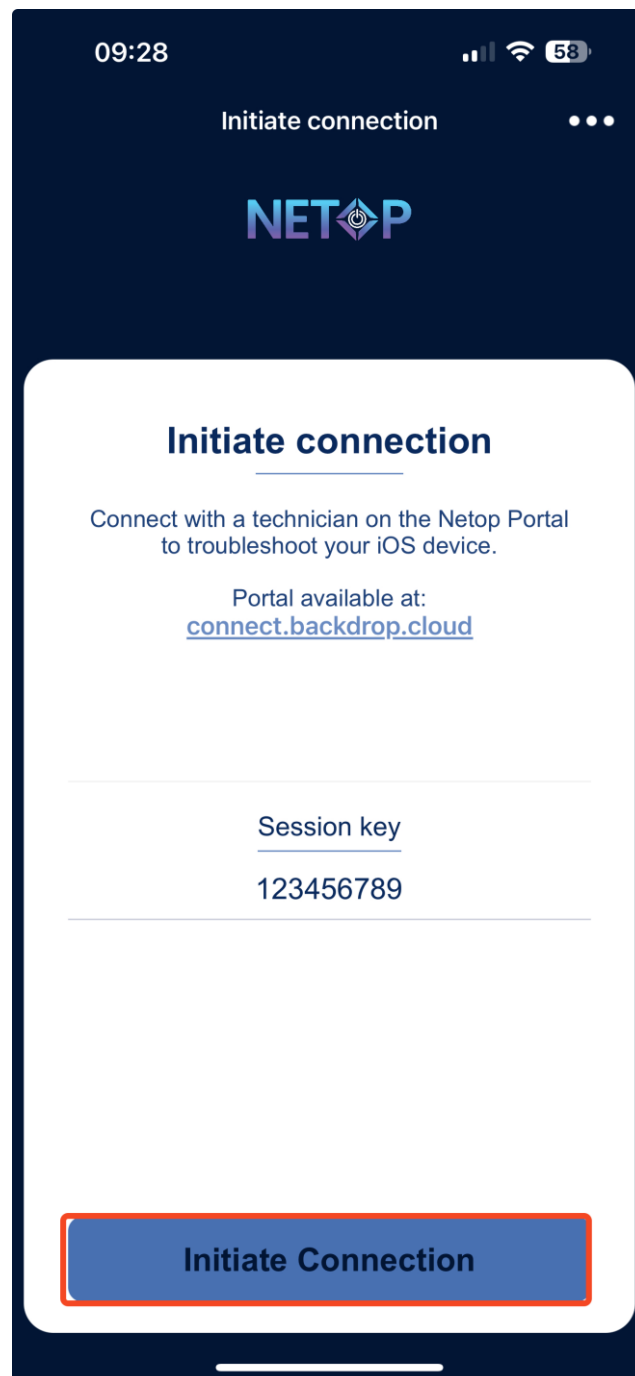
Portal available at:  
[connect.backdrop.cloud](https://connect.backdrop.cloud)

Session key

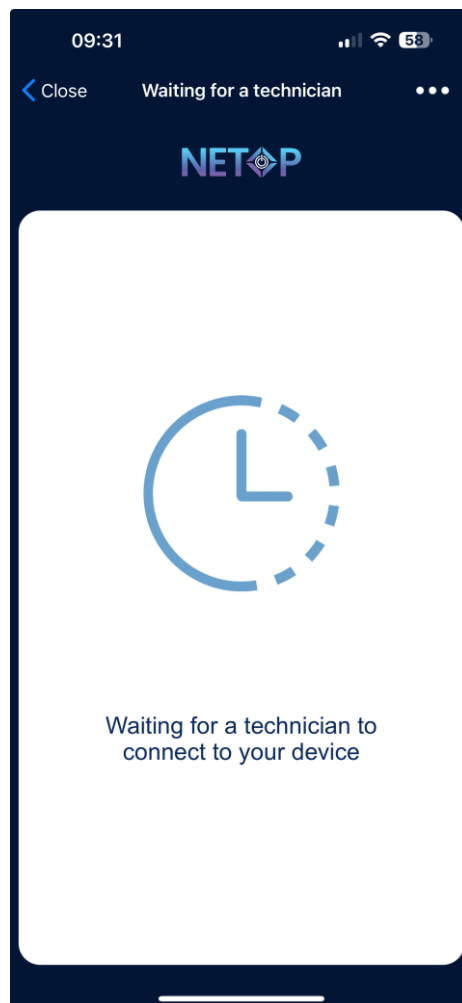
Type in the received session key

Initiate Connection

3. Click on the **Initiate Connection** button to initiate the **OnDemand** session.

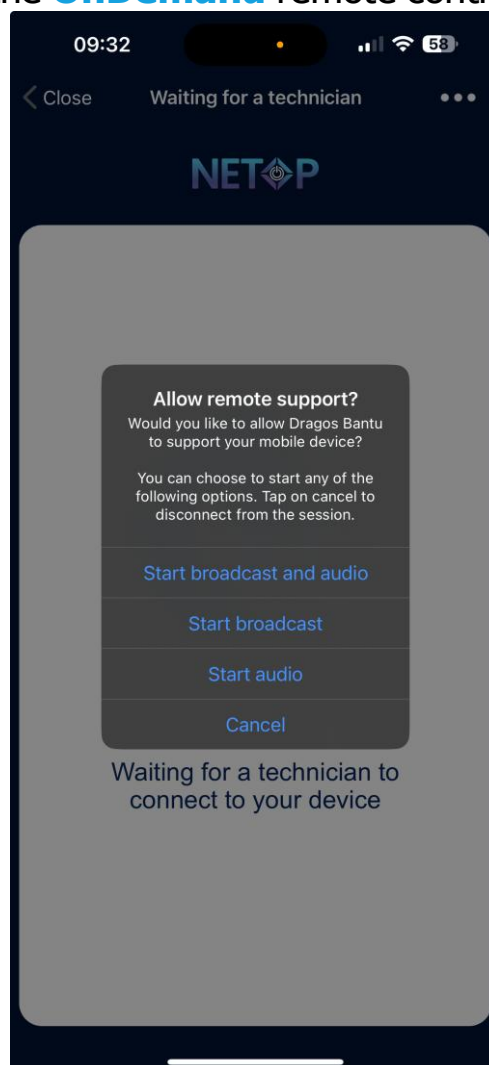


You connected successfully to the **OnDemand** session. Wait for the technician to start the **OnDemand** session from the **Portal**.

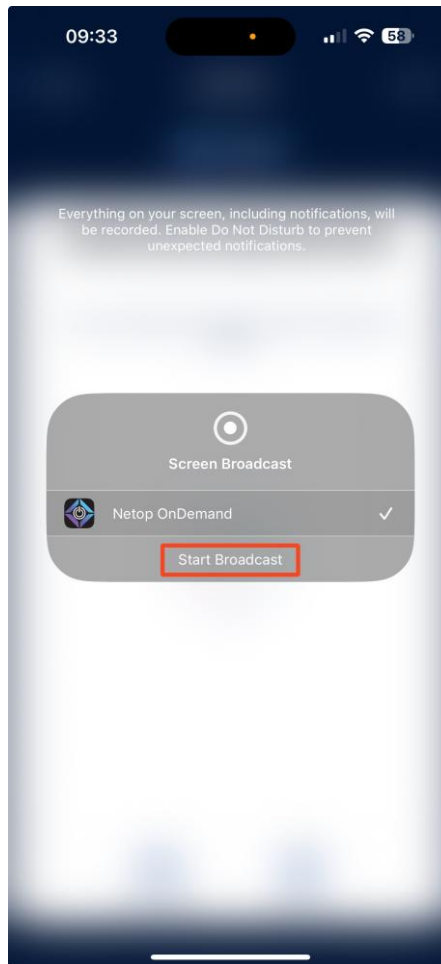




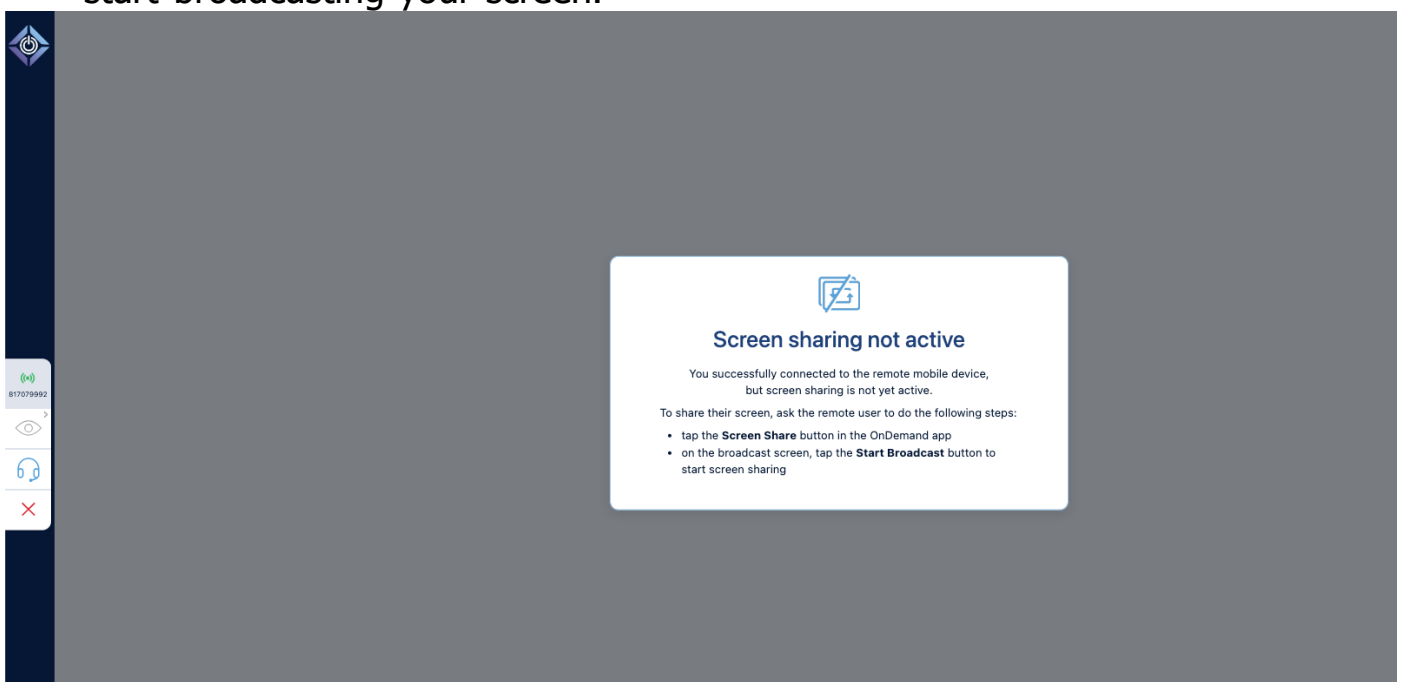
4. Select one of the following remote control options to allow the technician to connect to your iOS device:
- **Start broadcast and audio** – starts the **OnDemand session** with screen sharing and audio enabled
  - **Start broadcast** – starts with the **OnDemand session** only with the screen sharing enabled
  - **Start audio** – starts the **OnDemand session** only with the audio feature enabled
  - **Cancel** – cancels the **OnDemand** remote control session



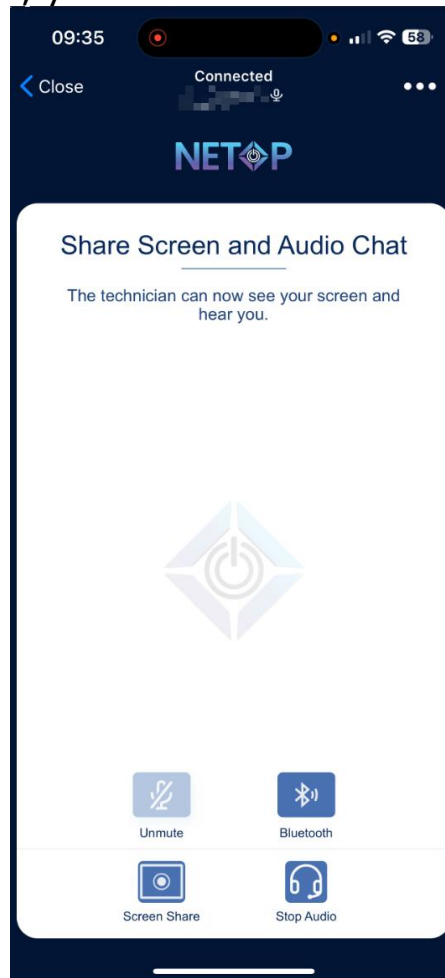
- Click on the **Start Broadcast** button to start broadcasting your screen.  
The broadcast screen is displayed.



The following window is displayed on the technicians' monitor until you start broadcasting your screen.



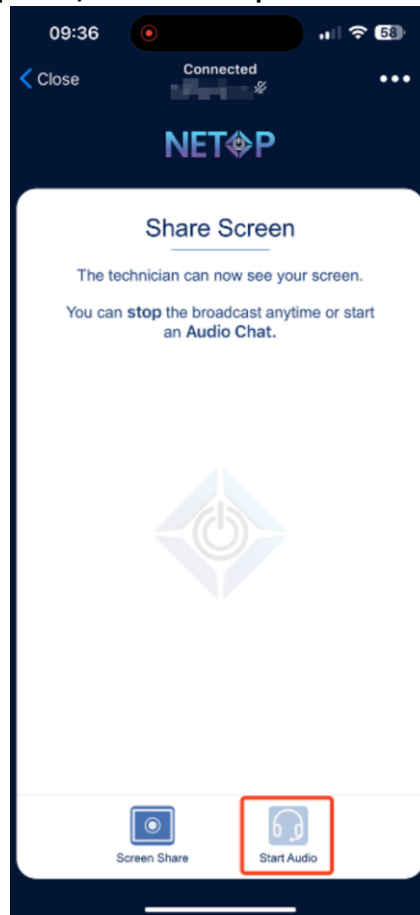
If you close this window, you are redirected to the following page:



6. You successfully started the **OnDemand** session.

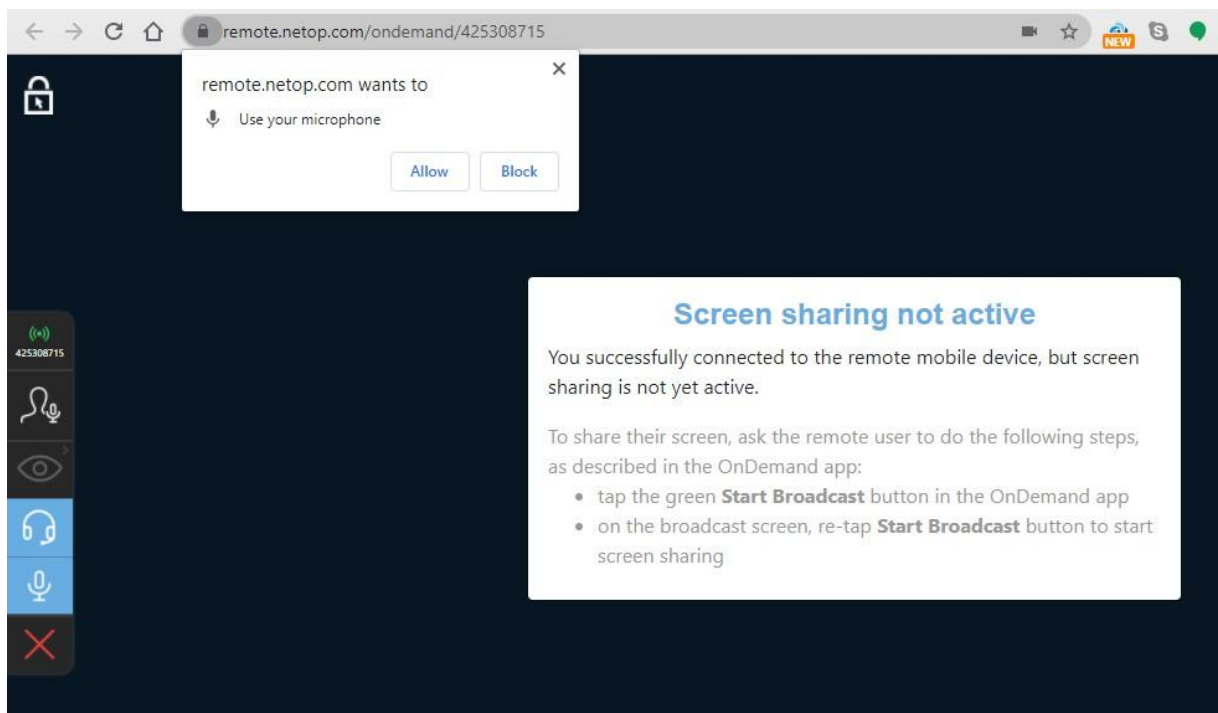
**NOTE:** **OnDemand** for iOS offers a view-only mode of the iOS device screen.

To make an audio chat request, click or tap on the **Start Audio** button.

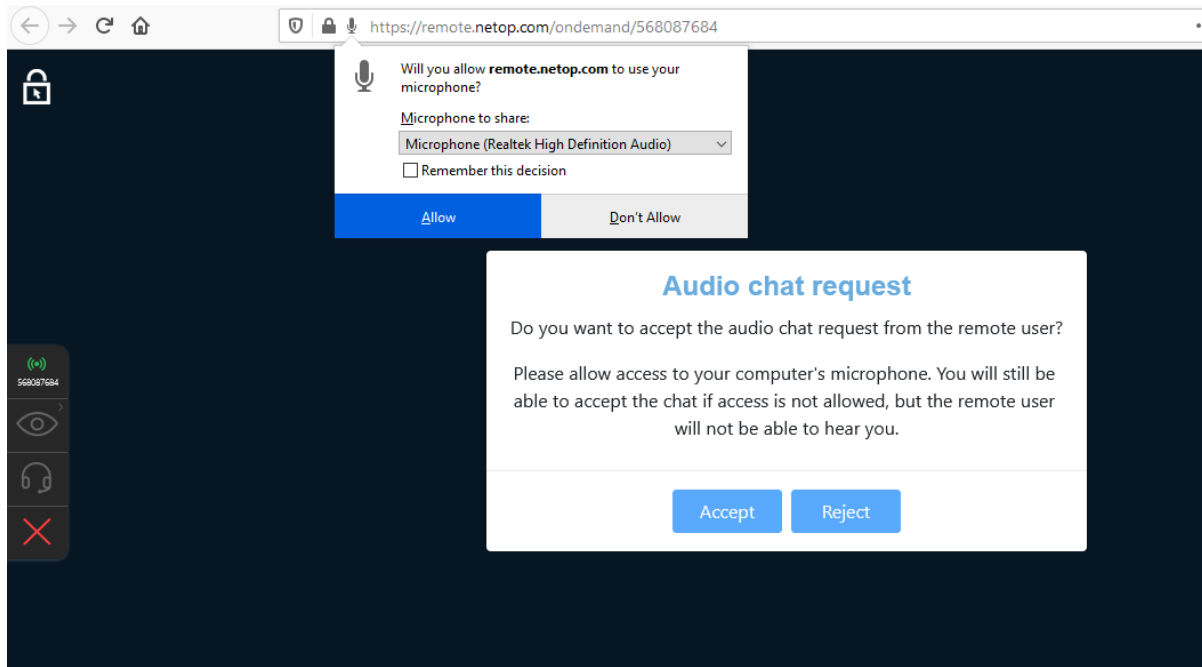


On the first use of the **Audio Chat** feature, you need to allow in the browser for the microphone to be used. A popup is displayed in the browser that requests the Technician to Allow or Deny the use of the microphone. To allow the microphone use, click on the **Allow** button in the popup.

## • For Chrome



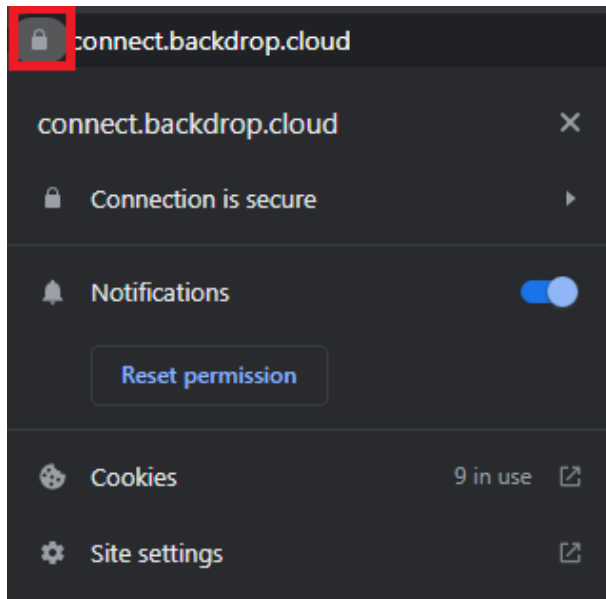
## • For Firefox



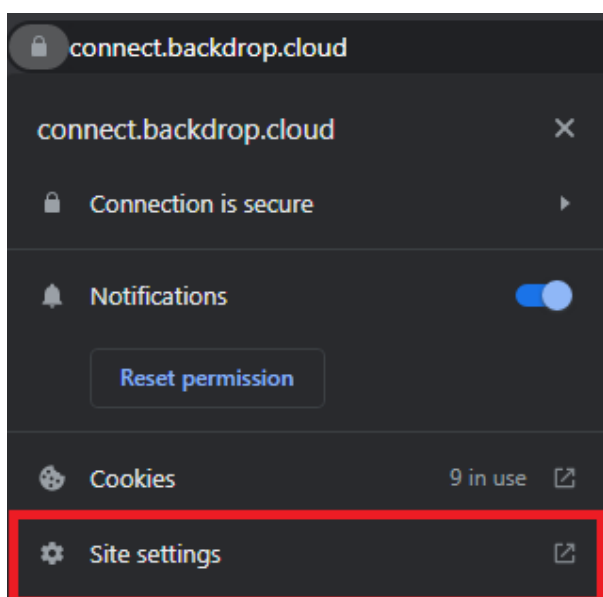
To allow the microphone to be used in the browser, proceed as follows:

- **For Chrome**

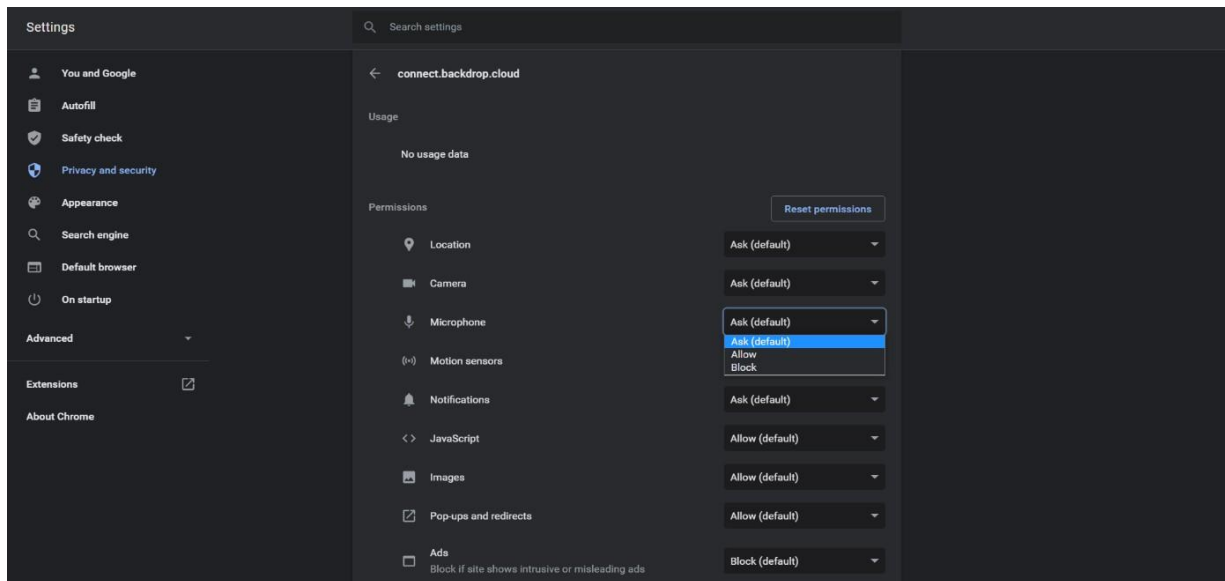
1. Open the **Chrome** internet browser.
2. In the search address bar, type in `portal.netop.com`.
3. Click on the "**View Site Information**" button (the lock icon in the search bar).



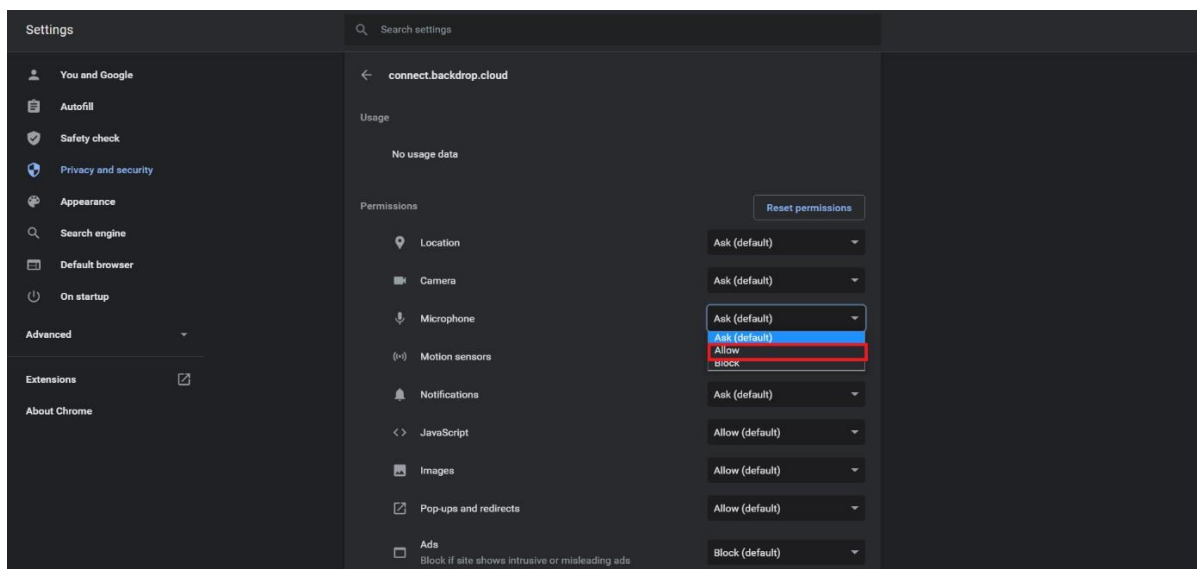
4. Click on **Site settings**.



5. Click on the dropdown button corresponding to **Microphone**.

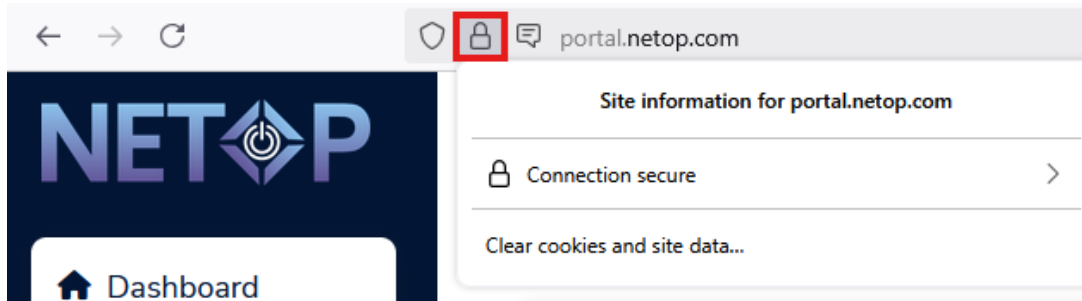


6. To enable the Microphone use, select the **Allow** option.

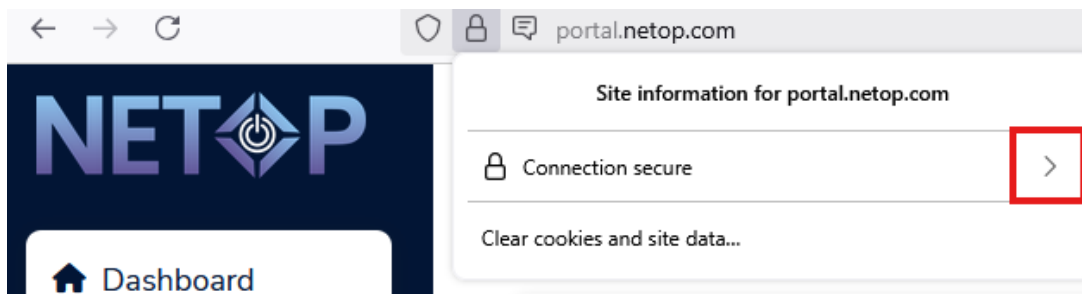


- **For Firefox**

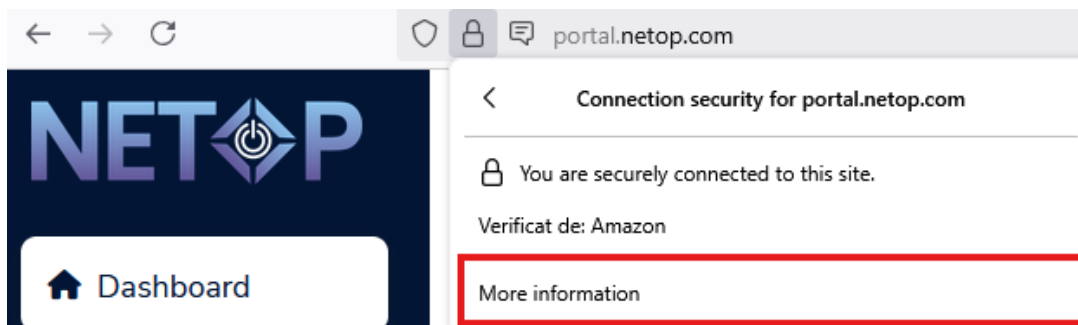
1. Open the **Firefox** internet browser.
2. In the search address bar, type in **portal.netop.com**.
3. Click on the **lock** icon.



4. Click on the **arrow** button.

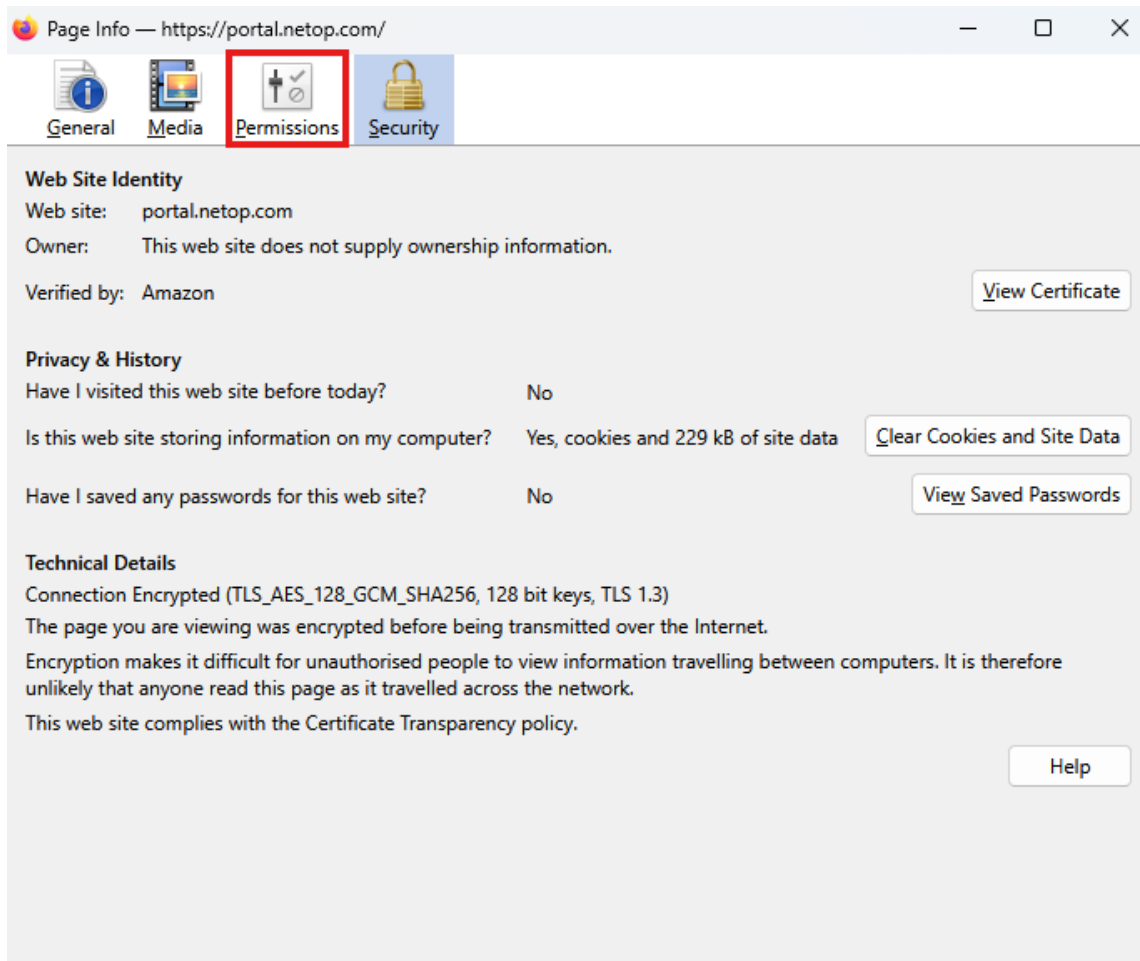


5. Click on the **More information** button.

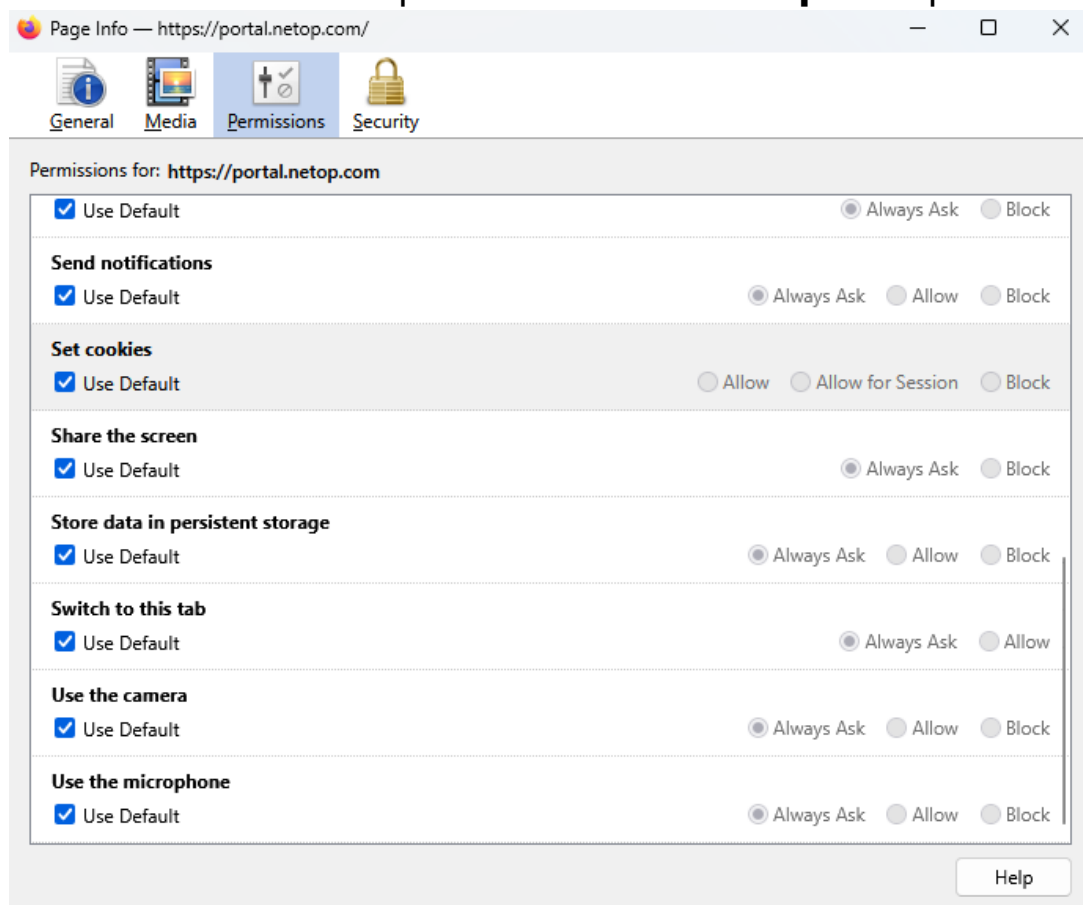




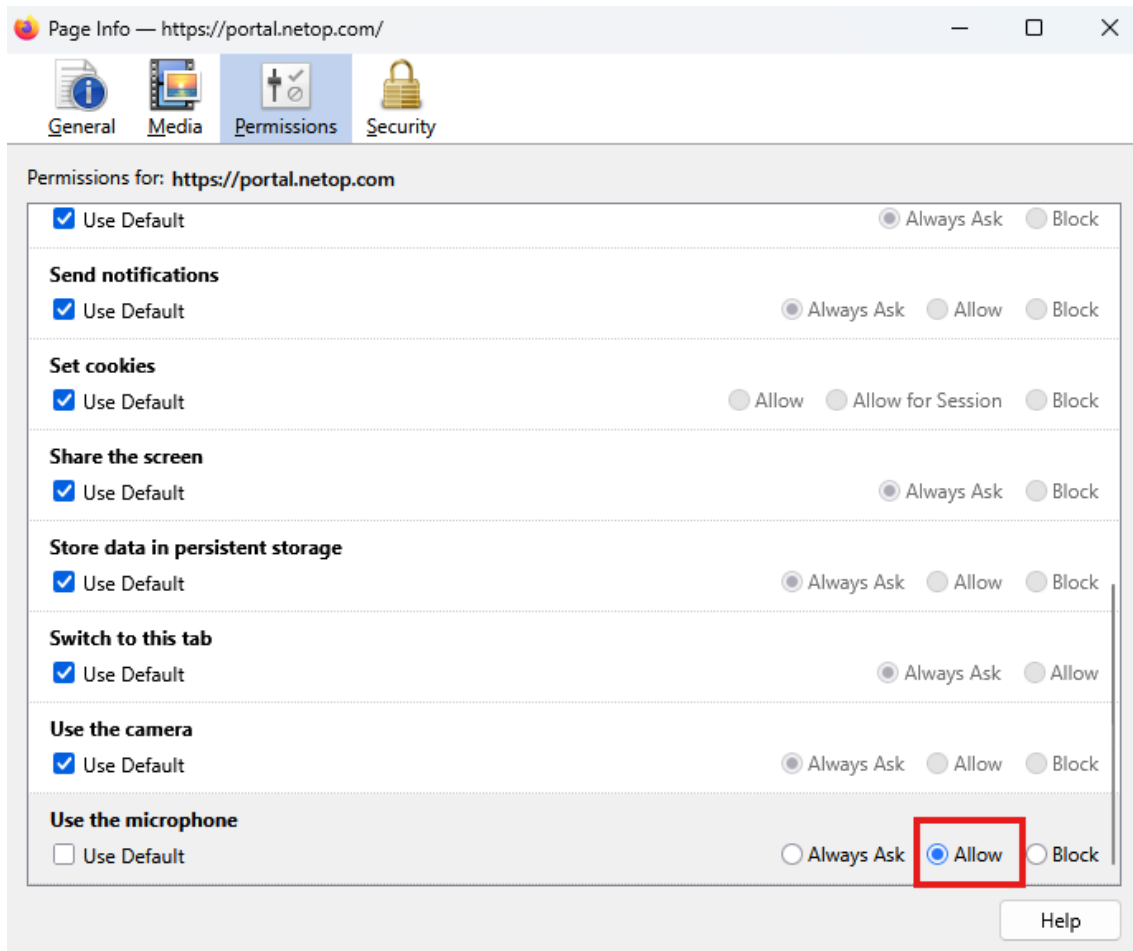
## 6. Click on the **Permissions** icon.



## 7. Uncheck the "Use default" option for the **Use Microphone** permission.



8. To enable the **Use the Microphone** permission, select the **Allow** option.



- **For Safari**

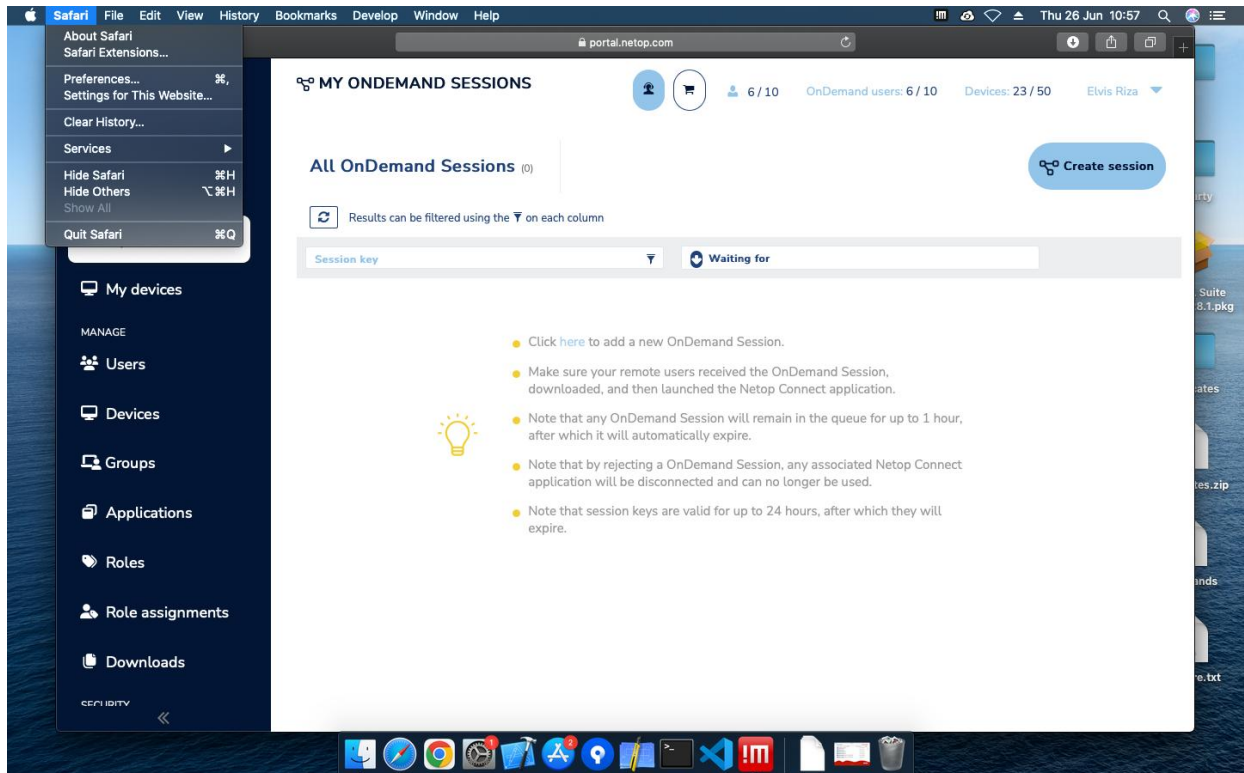
When a user initiates the audio chat feature, the **Safari** browser displays a pop-up notification that requires you to allow or deny **Microphone** use. Click on the **Allow** button, to use the Microphone.



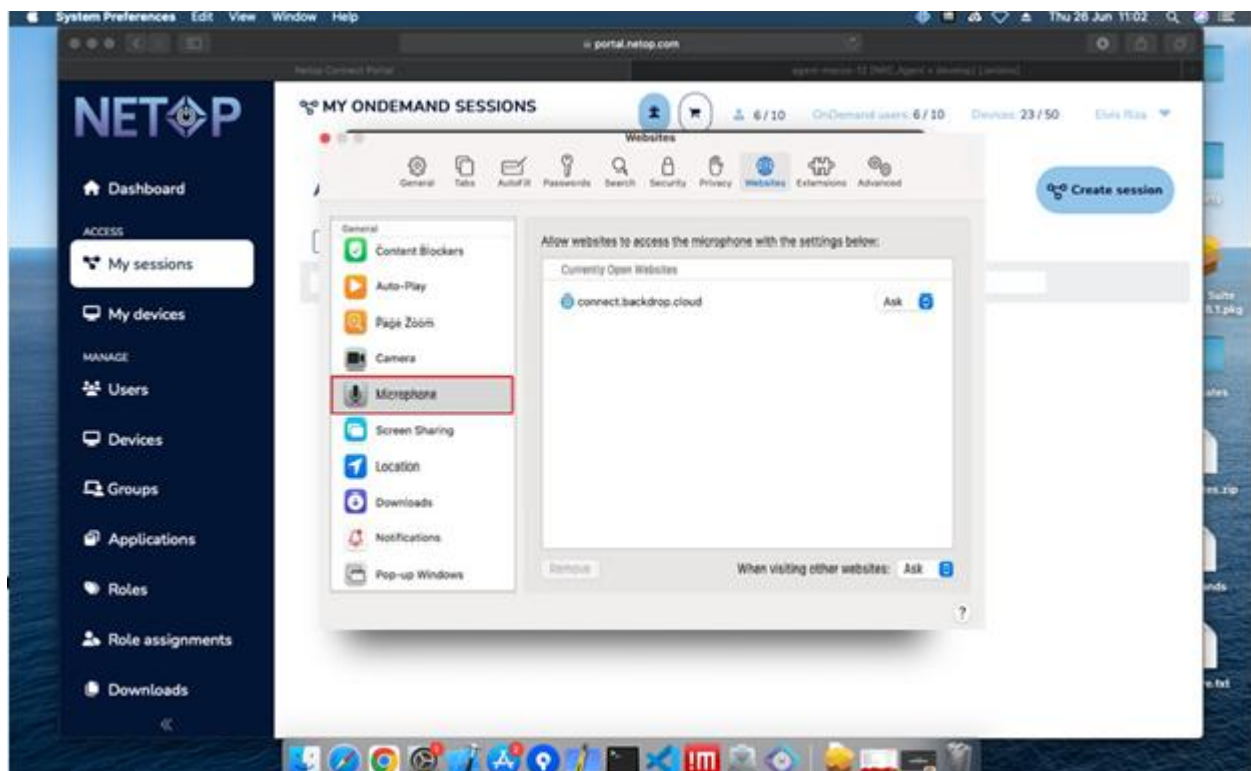
Alternatively, to manually allow the use of the **Microphone**, proceed as follows:

1. Open the **Safari** Internet browser.
2. In the address bar, specify **portal.netop.com**.
3. Click on **Safari**.

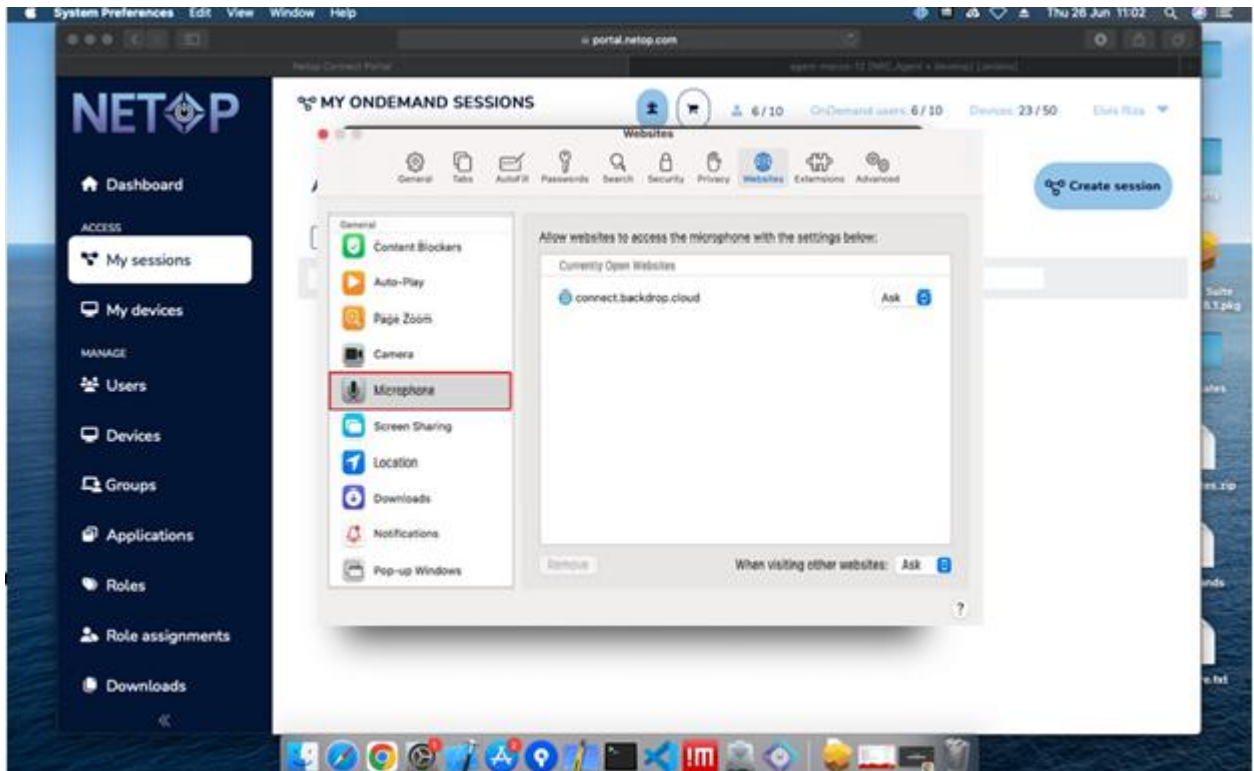
#### 4. Go to **Preferences**.



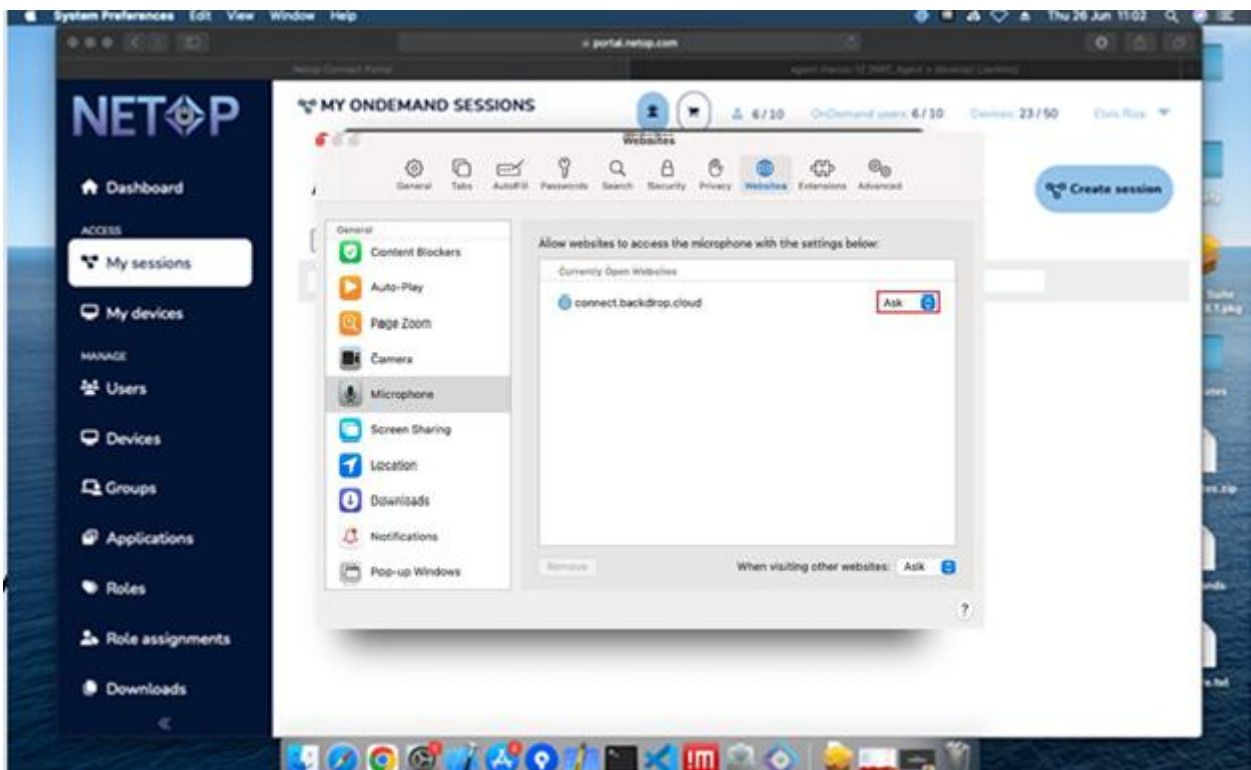
#### 5. Click on the **Websites** icon.



6. Click on **Microphone**.



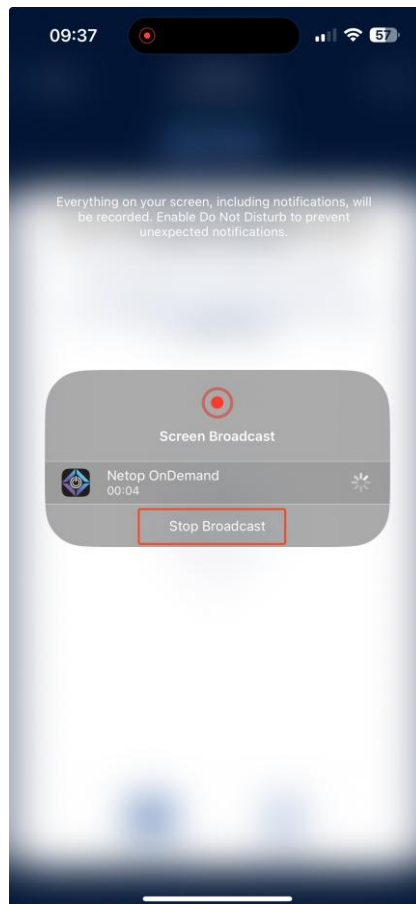
7. Click on the dropdown button near the **portal.netop.com** address.



8. Select **Allow**.

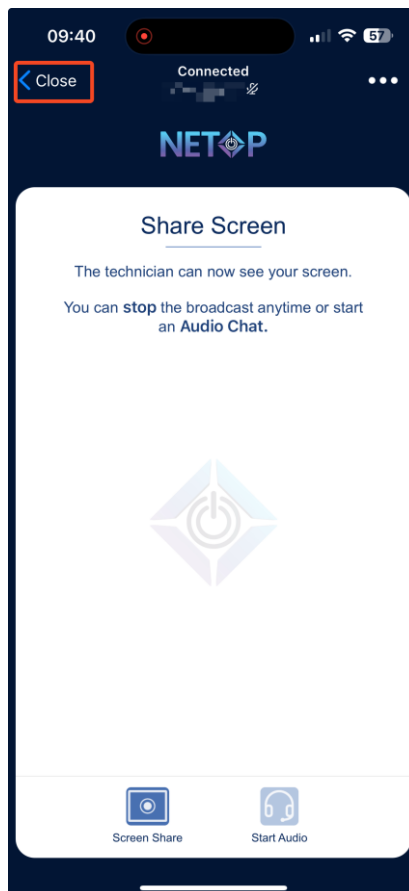
To stop the **OnDemand** session, proceed as follows:

1. Click on the **Stop Broadcast** button to stop broadcasting your screen.

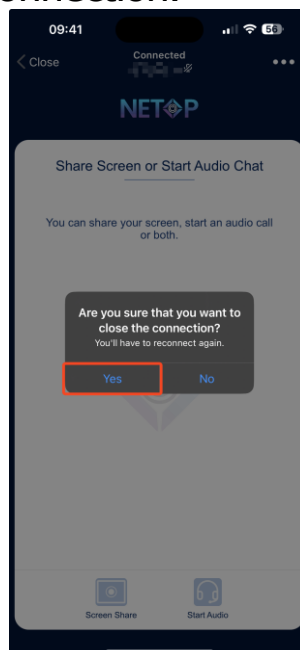


**NOTE:** The **OnDemand** session is still available. To start broadcasting your screen again, click on the **Start Broadcast** button.

2. Click on the **Close** button to disconnect from the **Portal**. You receive a prompt to confirm to disconnect from the **OnDemand** session.

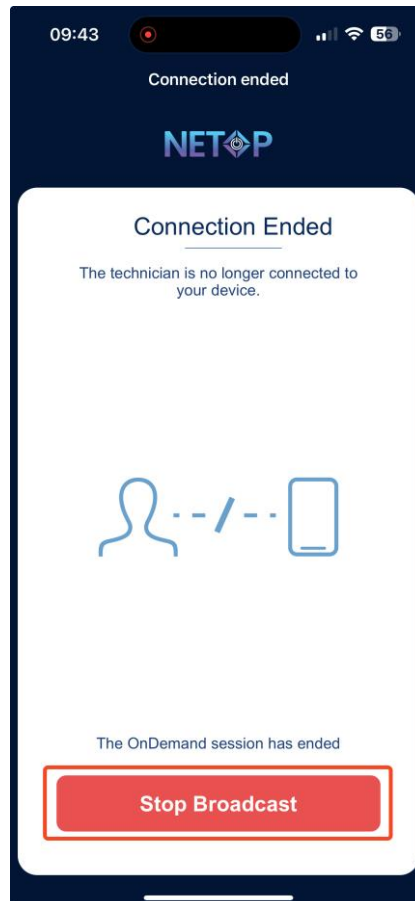


3. Click on **Yes** to close the connection.





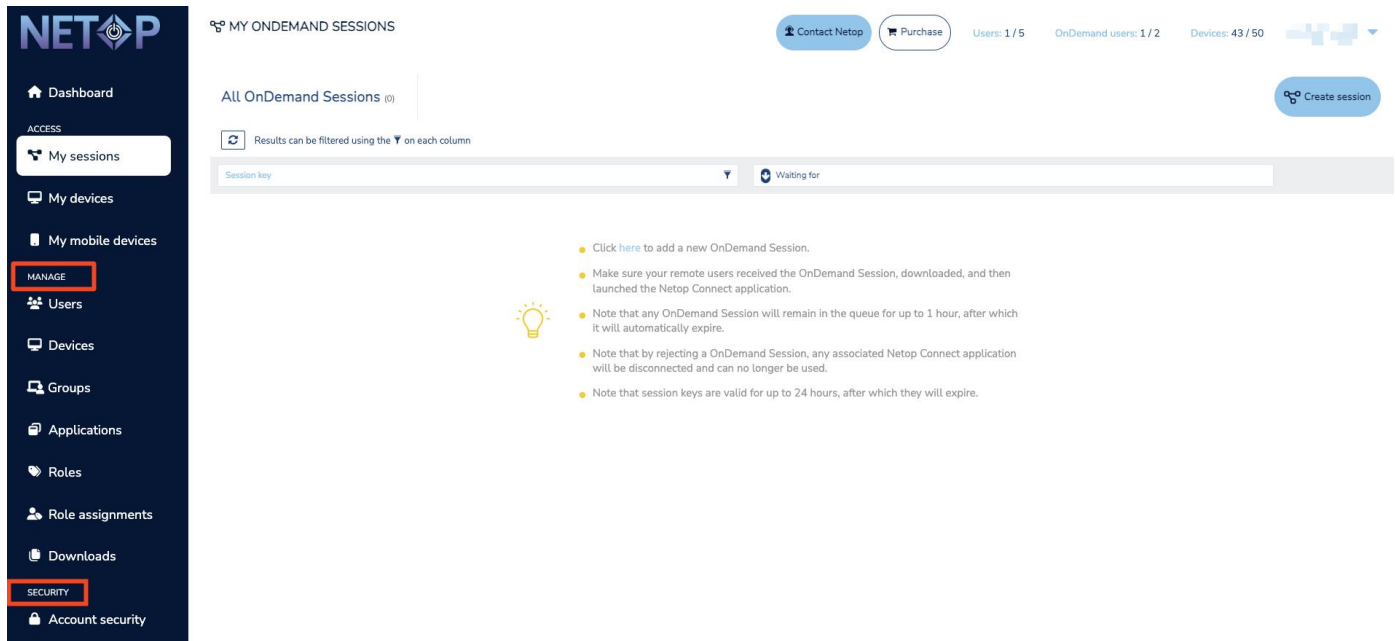
- Click on the **Stop Broadcast** button to close the **OnDemand** client.



## 4 How to manage your account

The **Portal** provides a central place for managing users, devices, security settings, role-based access, audit logs and a variety of options.

If the logged-in user has a **Group Manager** role or higher, a Manage and Security areas in the sidebar menu are available.



This provides access to the management area. The homepage for the management area is the **Dashboard** with various information including devices and users, account information, activity information, and recent updates.

The expiration date from the **Account info** section turns **red** when the account subscription is about to expire.

**Account Owners** are notified as follows:

- For regular accounts you are notified when there are **15** days or less until the subscription expires
- For trial accounts you are notified when there are **7** days or less until the subscription expires

The screenshot displays the Netop Portal dashboard with the following sections:

- Devices & Users:**
  - Devices:** Total devices: 44, Online devices: 1, Pending devices: 1, Device groups: 1.
  - Users:** Total users: 1, Online users: 1, User groups: 1.
- Activity:**
  - Active users: 1 (the same as the week before)
  - Remote sessions: 5 (5 more than the week before)
  - Enrolled devices: 7 (7 more than the week before)
- Account info:**
  - Company: Dragos Bantu Account
  - Expiration date: 2026-12-31
  - Account owner: Dragos Bantu (dragosbantu@gmail.com)
  - Timezone: UTC
- Documentation:**
  - Netop Connect Portal Quick Start Guide
  - Netop Connect Portal User's Guide
  - Browser-based Support Console User's Guide
  - Mass deploy Portal components
- Recent updates:**
  - NEW** April 24th, 2025
    - All Impero Connect branded applications will now appear as Netop across the product interface, installer packages, documentation, and support materials. The Impero Connect Portal (https://connect.backdrop.cloud) will become Netop Portal (https://portal.netop.com)
    - Mass Activation & Deactivation for Intel vPro Devices in the Netop Portal. Managing large fleets just got easier. You can now mass activate or deactivate Intel vPRO devices in a single action — saving time and boosting operational efficiency.
    - Enhanced vPro Details View. We've improved the Settings & Hardware Info in the Netop Portal section by adding richer, more detailed information
    - Login Token Security Enhancement.
    - Account Naming Restrictions.
    - Improved Account Selection UI.
    - Security Improvement: enhancements to how system files are handled on the Host machine to further protect user information.
    - Read more [here](#).

**NOTE:** The user's access varies within the management area based on the user's role. Upon login to the **Portal**, Account Owners, Account Administrators, and Group Managers are redirected to the **Dashboard** page, while Regular Users are redirected to the **My devices** page.

## 4.1 Manage Users

The **Portal** allows you to centrally manage users within your organization. This can be done by one or several users with administrative privileges.

The **Portal** interface provides easy access for managing the users.

There are four user types:

- **User** - view assigned devices and manage your profile
- **Group manager** – all the permissions of the User, plus the ability to manage users and devices, view roles and role assignments, view and generate log reports

- **Account administrator** – manage users, devices, groups, roles and role assignments, authentication methods, plus the ability to view account details and manage deployment packages
- **Account owner** – all the permissions of the Account Administrator plus the ability to manage the Account configuration

To view information about the users who have access to the **Portal**, on the menu bar click on the **Users** tab. The list of users is displayed.

Refer to the [Portal user privileges](#) knowledge base article for the detailed list of access privileges.

### 4.1.1 Create a new user

As a **Group manager** or higher, you have access to invite users to your portal organization account via email.

To create a new user, proceed as follows:

1. Go to the **Users** tab.
2. Click on the **Invite users** button.

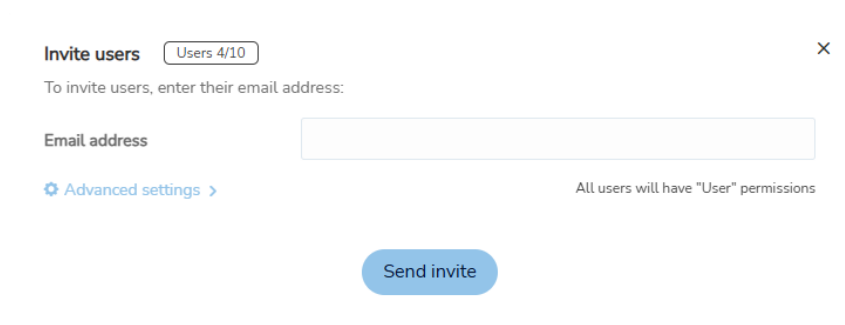
The screenshot shows the Netop Portal interface. On the left, a dark sidebar contains a menu with 'Dashboard' and 'ACCESS' sections. Under 'MANAGE', the 'Users' option is highlighted. The main area is titled 'USERS' and shows 'All Users (1)'. A table lists user details. In the top right of the table area, an 'Invite users' button is circled in red.

Name	Status	Type	Group	Authentication method	Modified	
[Avatar]	Online for 1 second	Account Owner	-	INTERNAL	2025-04-29 05:28:16	<input type="checkbox"/>

At the bottom right of the table, there are controls: 'Show Rows' set to 10, 'Go to page' set to 1, and '1 - 1 of 1'.

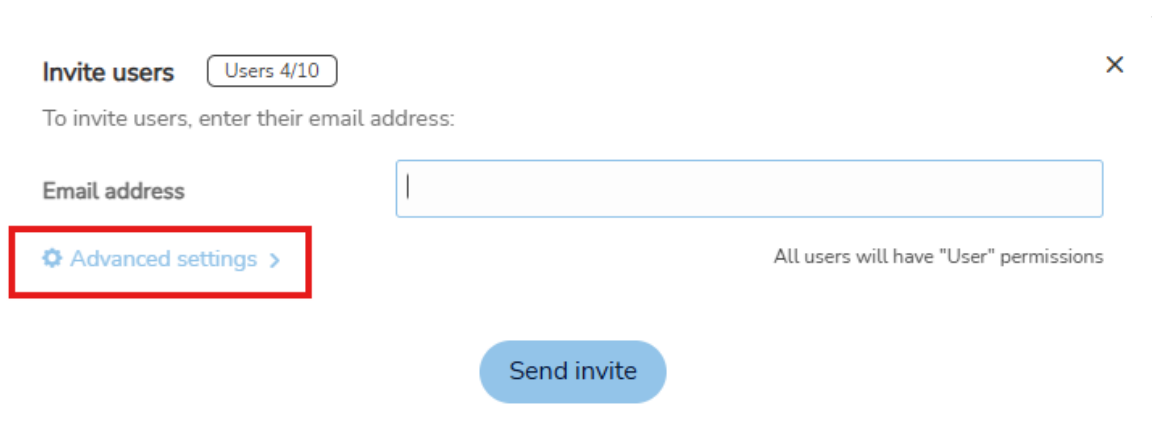
The **Invite users** form is displayed.

3. Specify the email addresses of the users you want to invite to the **Portal** account in the **Email addresses** entry field. You can specify it manually or by copy and pasting a list of emails.



The screenshot shows the 'Invite users' form. At the top, it says 'Invite users' with a 'Users 4/10' indicator and a close button. Below this, it says 'To invite users, enter their email address:'. There is a text input field labeled 'Email address'. Below the input field, there is a link for 'Advanced settings' and a note that 'All users will have "User" permissions'. At the bottom, there is a 'Send invite' button. A red rectangle highlights the 'Email address' input field.

4. Click on the **Advanced settings** drop-down button to specify additional information about the invited users. Note that the **Advanced settings** apply to all invited users.



The screenshot shows the 'Invite users' form. At the top, it says 'Invite users' with a 'Users 4/10' indicator and a close button. Below this, it says 'To invite users, enter their email address:'. There is a text input field labeled 'Email address'. Below the input field, there is a link for 'Advanced settings' and a note that 'All users will have "User" permissions'. At the bottom, there is a 'Send invite' button. A red rectangle highlights the 'Advanced settings' link.

5. Select a **User type** for the invited users from the **User type** drop-down field.

**NOTE:** By default, all users are assigned the “**User**” type.

Invite users

Users 4/10

×

To invite users, enter their email address:

Email address

⚙️ Advanced settings ▾

All users will have "User" permissions

User type

User ▾

[Read more on user types here](#)

Group (Optional)

Default remote control action

Control through browser ▾

☒ Enabled *(This user is enabled)*

☒ OnDemand Sessions *(OnDemand Sessions are enabled for this user)*

☐ Multi-Factor Authentication *(Email MFA disabled)*

Send invite

6. Optionally, you can select a group for the invited users from the **Group** drop-down button.

Invite users

Users 4/10

×

To invite users, enter their email address:

Email address

⚙️ Advanced settings ▼

All users will have "User" permissions

User type

User ▼

Read more on user types [here](#)

Group (Optional)

Default remote control action

☐ NetRom

☒ Enabled (This user is enabled)

☒ OnDemand Sessions (OnDemand Sessions are enabled for this user)

☐ Multi-Factor Authentication (Email MFA disabled)

Send invite

7. Select a default remote control action from the **Default remote control action** drop-down field. By default, this option is the default setting on the account.

Invite users

Users 4/10

×

To invite users, enter their email address:

Email address

⚙️ Advanced settings ▾

All users will have "User" permissions

User type

User ▾

Read more on user types [here](#)

Group (Optional)

▾

Default remote control action

Control through browser ▾

Control through Guest

Control through browser

☒ Enabled *(This user is enabled)*

☒ OnDemand Sessions *(OnDemand Sessions enabled)*

☐ Multi-Factor Authentication *(Email MFA disabled)*

Send invite



8. Enable or disable **OnDemand Sessions** for the invited users by clicking on the toggle button. By default, this option is enabled.

Invite users

Users 4/10

×

To invite users, enter their email address:

Email address

⚙️ Advanced settings ▼

All users will have "User" permissions

User type

User ▼

Read more on user types [here](#)

Group (Optional)

▼

Default remote control action

Control through browser ▼

☒ Enabled (This user is enabled)

☒ **OnDemand Sessions** (OnDemand Sessions are enabled for this user)

☐ Multi-Factor Authentication (Email MFA disabled)

Send invite

9. Enable or disable **Multi-Factor Authentication** by clicking on the toggle button. By default, this option is disabled.

Invite users

Users 4/10

×

To invite users, enter their email address:

Email address

⚙️ Advanced settings ▾

All users will have "User" permissions

User type

User ▾

Read more on user types [here](#)

Group (Optional)

▾

Default remote control action

Control through browser ▾

☒ Enabled (This user is enabled)

☒ OnDemand Sessions (OnDemand Sessions are enabled for this user)

☐ Multi-Factor Authentication (Email MFA disabled)

Send invite

10. To send the invitation, click on the **Send invite** button.

Invite users

Users 4/10

×

To invite users, enter their email address:

Email address

⚙️ Advanced settings ▾

All users will have "User" permissions

User type

User ▾

Read more on user types [here](#)

Group (Optional)

Default remote control action

Control through browser ▾

☒ Enabled (This user is enabled)

☒ OnDemand Sessions (OnDemand Sessions are enabled for this user)

☐ Multi-Factor Authentication (Email MFA disabled)

Send invite

To resend the invitation email to users, simply select the invited users that you want to resend the invitation email to and then click on the **Resend invite** button.

USERS

Contact Netop

Purchase

Users: 5 / 10

OnDemand users: 5 / 10

Devices: 7 / 50

Monica Nicolae ▾

The user has been invited. In case they don't see the email in their inbox, please advise them to also check the spam folder.

Attach to group

Edit

Remove

Check permissions

Resend invite

Invite users

Results can be filtered using the ▾ on each column

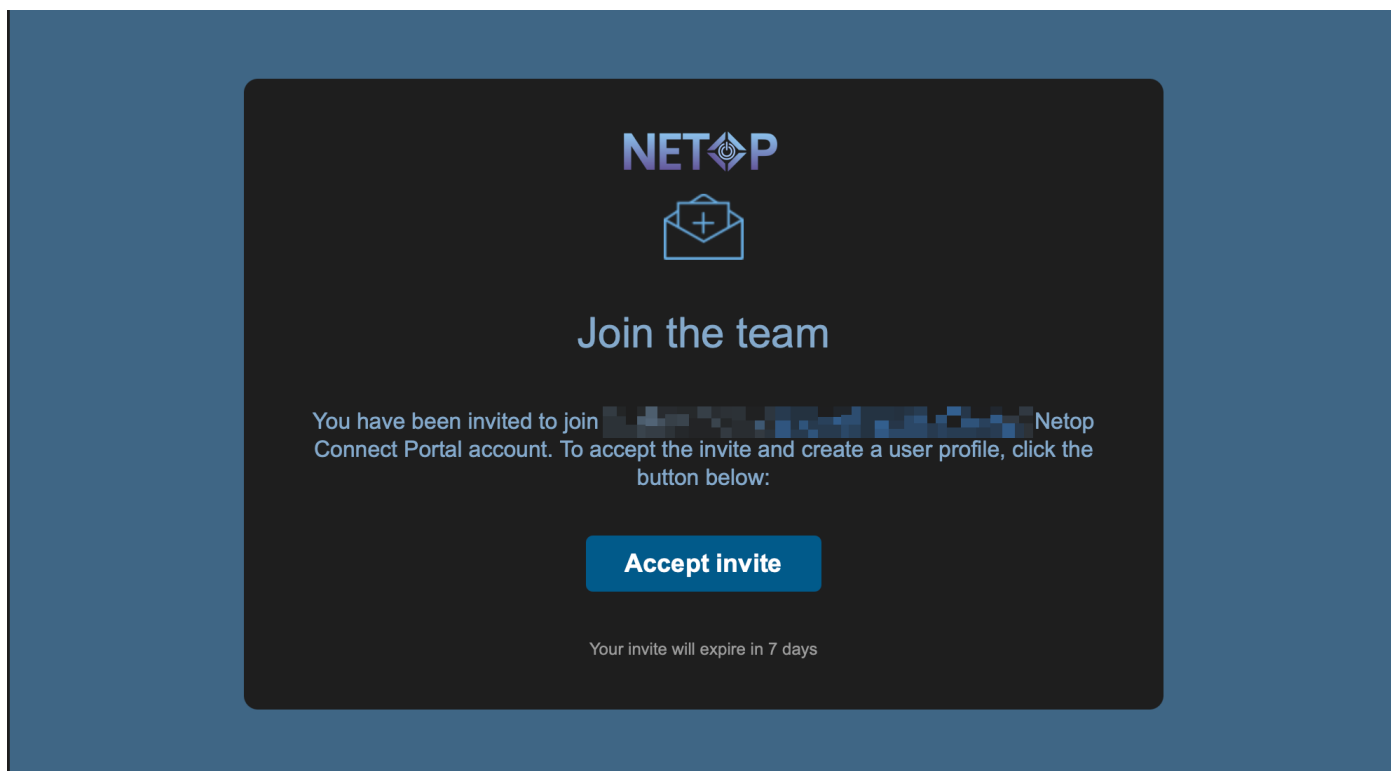
Name ▾	Status ▾	Type ▾	Group ▾	Authentication method ▾	Modified ▾	
Elvis Riza (eliza@etvion.com)	Online for about 1 hour	Account Owner	-	INTERNAL	2025-06-05 11:29:23	<input type="checkbox"/>
Monica Nicolae (mnicolae@etvion.com)	Last seen online: 2 days ago	Account Administrator	-	INTERNAL	2025-05-16 10:54:04	<input type="checkbox"/>
Monica Nicolae (mnicolae@netop.com)	Online for about 52 minutes	Account Administrator	-	INTERNAL	2025-06-04 13:26:37	<input type="checkbox"/>
NetRum Software (netop@netrum.ro)	Last seen online: 1 day ago	Account Administrator	-	INTERNAL	2025-05-22 08:53:53	<input type="checkbox"/>
user@gmail.com	Invite pending	User	-	INTERNAL	2025-06-05 12:25:31	<input checked="" type="checkbox"/>

Show Rows 10 ▾

Go to page 1 1 - 5 of 5 < >

**NOTE:** The invitation email can be resent for a maximum of **5** times and is valid for **7** days.

Invited users receive the invitation into the account via the specified email addresses:



After the users accept the invitation by clicking on the **Accept invite** button, they are automatically redirected to the **Set up your account** landing page.

A screenshot of the 'Set up your user account' page. The NETOP logo is at the top. On the left, there is an envelope icon and text: 'You have been invited by Dragos Bantu to join Netop Remote Control. Please provide the necessary details to create a user profile'. On the right, there are input fields for 'First name', 'Last name', 'Password', and 'Confirm password'. Each field has an information icon. Below the password field is a 'password strength' indicator. At the bottom right is a blue button labeled 'Save & login'.

To finish setting up the user account, click on the **Save & login** button.

Set up your user account

You have been invited by Dragos Bantu to join Netop Remote Control  
Please provide the necessary details to create a user profile

First name  
John

Last name  
Doe

Password  
password strength - weak

Confirm password

Save & login

### 4.1.2 LDAP users - automatically added into the Portal at first login

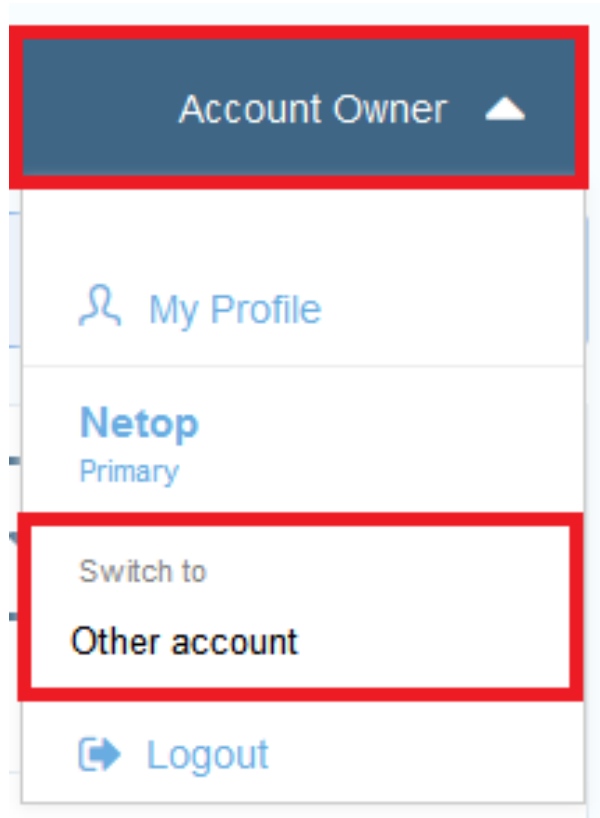
This only applies if you are using [LDAP authentication](#). On the first login using the **LDAP** credentials (**username:** `domain identifier\LDAP username`, **password:** the domain password), the user is added to the **Portal**. The user type is **User** (more information on the user types [here](#)).

**NOTE:** The user is not attached to a group by default, but if there is a role assignment in the **Portal** which allows all the users to access all the devices (User: **everyone**, Devices: **everything**), the **LDAP** user has access to all devices. Refer to the [LDAP](#) user groups sub-chapter to attach the User to a Group on login.

### 4.1.3 Multiple accounts

Users can belong to multiple **Portal** accounts when invited via email by an **Account Owner**, **Account Administrator**, or **Group Manager** to a secondary **Portal** account.

Users that belong to multiple **Portal** accounts can switch between them. They do so by clicking on the **User Profile** button and selecting the secondary account that they want to switch to.



By default, the primary account is the account that the user was first invited to. User settings are not transferred from the primary to any other secondary accounts. As such users can have different permissions, roles, or other settings on other secondary accounts without them interfering with each other.

Users can set an account alias for the primary and secondary accounts.

To set an account alias, proceed as follows:

1. Click on the **User Profile** button.

**DASHBOARD**

Contact Netop Purchase Users: 5 / 10 OnDemand users: 5 / 10 Devices: 7 / 50 Monica Nicolae

**Devices & Users**

**Devices**

Total devices:	7
Online devices:	2
Pending devices:	0
Device groups:	0

**Users**

Total users:	5
Online users:	2
User groups:	1

**Activity**

Active users:	2	the same as the week before
Remote sessions:	3	23 less than the week before
Enrolled devices:	5	the same as the week before

View more logs

2. Click on the **My Profile** button.

**NETOP**

USERS

Contact Netop Purchase Users: 1 / 5 OnDemand users: 1 / 2 Devices: 43 / 50

User has been removed.

All Users (1)

Results can be filtered using the ▼ on each column

Name	Status	Type	Group	Authentication method	Modified	
[User Name]	Online for 1 second	Account Owner	-	INTERNAL	2025-04-29 05:28:16	

Show Rows 10 Go to page 1 1 - 1 of 1

3. Click on the **Set account alias** button.

**PROFILE**

Contact Netop Purchase Users: 24 / 50 OnDemand users: 9 / 25 Devices: 61 / 70 Monica Nicolae

Monica Nicolae (mnicolae@netop.com)

Edit Change password Set account alias

**Personal info**

Username	mnicolae@netop.com
First name	Monica
Last name	Nicolae
Email	mnicolae@netop.com
Default remote control action	Control through browser

**Account Membership**

Account	NetRom (Primary account)
Alias	NetRom
Type	Account Administrator
Multi-Factor Authentication	None
OnDemand Sessions	Enabled
Account	NETOP

4.

5. Specify an alias for the accounts in the **Alias** text input field.



SET ACCOUNT ALIAS

Account

NetRom

Alias

NetRom

Account

NETOP

Alias

NETOP

You are currently logged into this account

Save

6. To save your changes, click on the **Save** button.

SET ACCOUNT ALIAS

Account

NetRom

Alias

NetRom

Account

NETOP

Alias

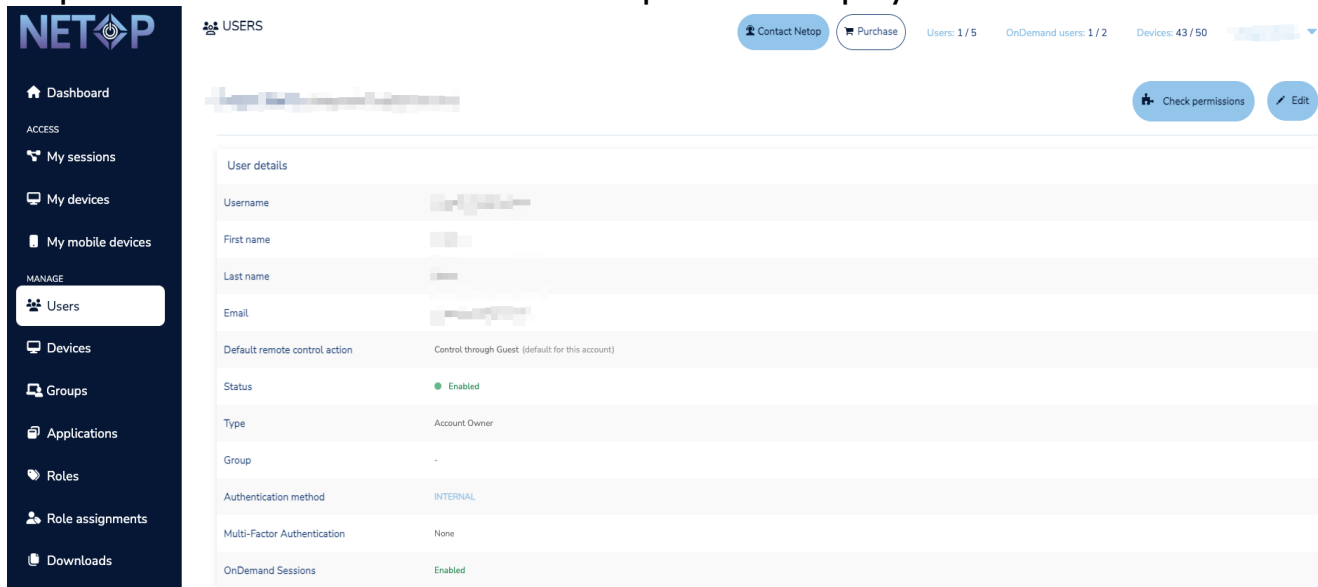
NETOP

You are currently logged into this account

Save

## 4.1.4 View User Info

To view user information, in the **Users** list click on the desired username. Specific information from the user's profile is displayed.



Field	Description
Username	A unique identifier used to log in.
Status	Indicates whether the user is Online / Offline or if they cannot log in to the <b>Portal</b> ( <b>Inactive</b> ), as well as the period of time of the user while being Online/Offline. <ul style="list-style-type: none"> <li><b>Online</b> = User is logged in the <b>Portal</b></li> <li><b>Offline</b> = User is not logged in the <b>Portal</b></li> <li><b>Inactive</b> = User is disabled and cannot log in the <b>Portal</b>.</li> </ul>
First Name	User's first name.
Last Name	User's last name.
Email	The email address to which the user receives notifications from the <b>Portal</b> and the multi-factor authentication code if enabled.
Group	The group the user belongs to.
Authentication method	Internal (username or password) or the name of the authentication method defined under <b>Account</b> > <b>Authentication</b> .
Multi-factor authentication	Indicates if multi-factor authentication is enabled for the user or not.
Type	Indicates the type of the account: <b>Account Owner</b> ,

Field	Description
	<b>Account Administrator</b> , <b>Group manager</b> or <b>User</b> .
Default remote control action	Sets up the default remote control action for the user.
Created	The date and time when the user account was created.
Created by	The first and last name of the user who created the user account.
Modified	The date and time when the user account was last modified.
Modified by	The first and last name of the user who last modified the user account.

#### 4.1.5 Edit the user

To edit an existing user, in the **Users** area click on the username of the user you want to modify and in the upper right corner of the page click on the **Edit** button. The **Edit User** window is displayed.

Depending on the authentication method of the user, edit user is as follows:

For Internal authentication, you can modify the following:

- Basic profile information (such as **First Name**, **Last Name**, and **Email**)
- Access permissions (toggle on or off the **Active** button and select the user type to give specific access permissions within the **Portal**)
- Select the groups the user belongs to and whether the user authenticates using **multi-factor authentication** or not
- Set up the default remote control action

## EDIT USER



First name


Last name

Email

Username  


Password  

Confirm password  

User type  

Read more on user types [here](#)

Group (Optional)  

Default remote control action  

☒ Enabled *(This user is enabled)*

☒ OnDemand Sessions *(OnDemand Sessions are enabled for this user)*

☐ Multi-Factor Authentication *(Email MFA disabled)*

Save

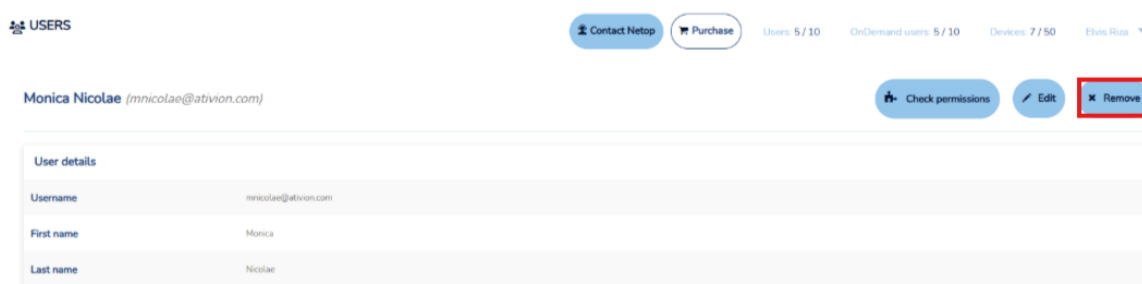
**NOTES:**

- If you toggle off the **Active** button, it disables the users so they can no longer log in to the **Portal**. Disabling does **NOT** remove the user from your Portal organization account.
- You are not allowed to edit the username.
- You are not allowed to edit a user whose role is higher than the user you are logged in as.
- You are not allowed to change the role of an Account Owner from here. Use the account configuration area instead.
- For **ADFS / Azure AD based authentication**. You can modify the role (toggle on or off the **Active** button and select the user type to give specific access permissions within the **Portal**), select the groups the user belongs to and whether the user authenticates using multi-factor authentication or not, or set up the default remote control action.

Once you have finished updating user information and access permissions, click on the **Save** button to save the user updates.

#### 4.1.6 Remove user

To remove an existing user, in the **Users** area, click on the username of the user you want to remove and in the upper right corner of the page, click on the **Remove** button.



**NOTE:** Only an **Account Owner**, **Account Administrator** or **Group Manager** can remove users. The logged-in user can only remove users with roles below their role.

You can also remove an existing user, from the **Users** area by selecting the desired user and above the content area click on the **Remove** button.

A confirmation dialog is displayed. To remove the selected user, click on **Yes**.

**NOTE:** For users that belong to multiple accounts, when removing them from their main **Portal** account, they are automatically removed from their secondary accounts as well.

### 4.1.7 Remove multiple users






To remove multiple users at once, in the **Users** area, select the users you want to remove and above the content area, click on the **Remove** button. A confirmation dialog is displayed. To remove the selected users, click on **Yes**.

**USERS**

[Contact Netop](#) [Purchase](#) Users: 5 / 10 OnDemand users: 5 / 10 Devices: 7 / 50 Elvis Riza

[Attach to group](#) [Remove](#) [Invite users](#)

Results can be filtered using the ▼ on each column

Name	Status	Type	Group	Authentication method	Modified	
 Elvis Riza (elvisr@elvis.com)	Online for about 5 minutes	Account Owner	-	INTERNAL	2025-06-05 11:29:23	<input type="checkbox"/>
 Monica Nicolae (monica@elvis.com)	Last seen online: 2 days ago	Account Administrator	-	INTERNAL	2025-05-16 10:54:04	<input type="checkbox"/>
 Monica Nicolae (monica@netop.com)	Online for about 1 hour	Account Administrator	-	INTERNAL	2025-06-04 13:26:37	<input checked="" type="checkbox"/>
 NetRun Software (netop@netrun.ro)	Last seen online: 1 day ago	Account Administrator	-	INTERNAL	2025-05-22 08:53:53	<input checked="" type="checkbox"/>
 user@gmail.com	Invite pending	User	-	INTERNAL	2025-06-05 12:25:31	<input type="checkbox"/>

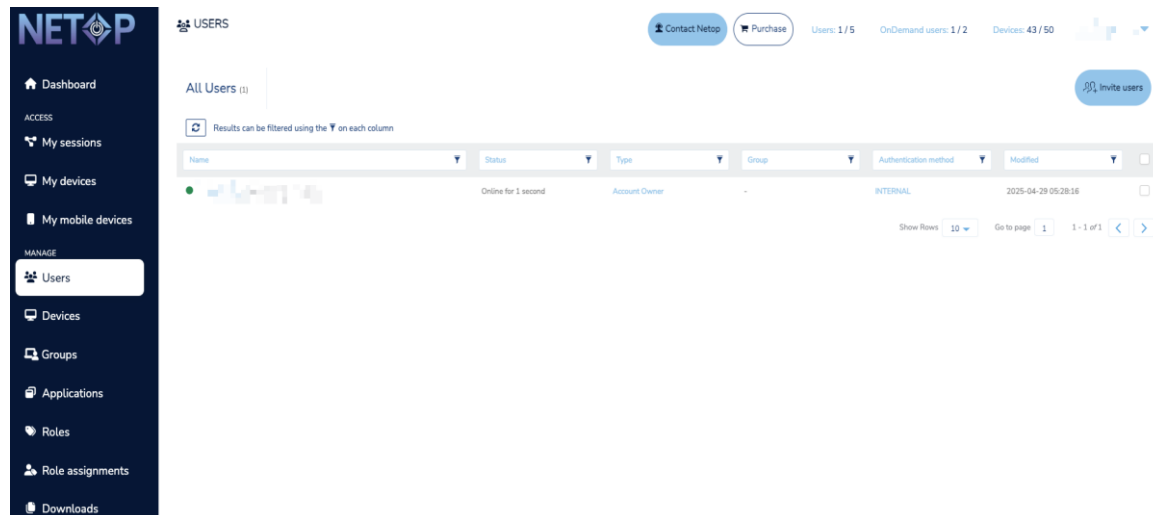
**NOTE:** If you remove an **LDAP**, **ADFS** or **Azure AD** user it does not mean that the user is not able to log in again. On the next login, the user is created again. To disable the user, edit the user and set the status to inactive.

## 4.1.8 Set up the default remote control action

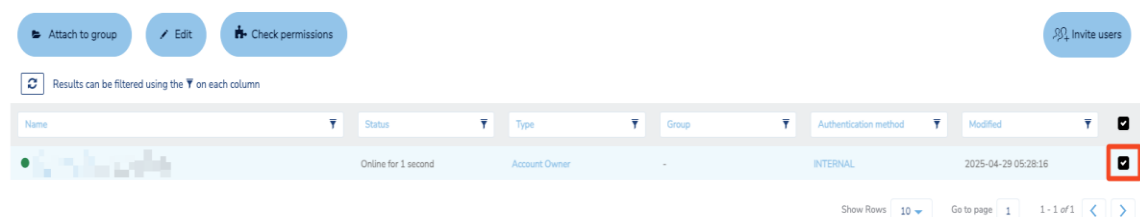
In the **Portal** you can set up the default remote control action for each user or for all the users that belong to the account.

To set up the default remote control action for a user, proceed as follows:

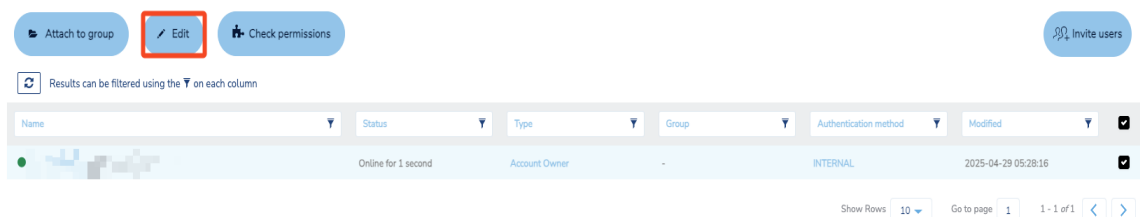
1. Go to the **Users** tab.



2. Select the user you want to edit.



3. Click on the **Edit** button.





- Click on the **Default remote control action** drop-down menu.

EDIT USER

X

First name

Andrei

Last name

Cucos

Email

ancu@netop.com

Username

ancu@netop.com

i

User type

Account Administrator

▼

Read more on user types [here](#)

Group (Optional)

ioana new group X upgrade X

▼

Default remote control action

Control through browser (default for this account) ▼

Control through Guest

Control through browser (default for this account)

Enabled (This user is)

OnDemand Session

Multi-Factor Authentication (Email MFA enabled)

Save

- Select the default remote control action.

6. Click on the **Save** button to save your changes.

EDIT USER

X

First name

Andrei

Last name

Cucos

Email

ancu@netop.com

Username

ancu@netop.com

i

User type

Account Administrator

▼

Read more on user types [here](#)

Group (Optional)

ioana new group X

upgrade X

▼

Default remote control action

Control through browser (default for this account)

▼

Enabled (This user is enabled)

OnDemand Sessions (OnDemand Sessions are enabled for this user)

Multi-Factor Authentication (Email MFA enabled)

Save

**NOTE:** An **Account Owner** can set up the default remote control action for all the users in the account. For more information refer to [Account Configuration](#).

## 4.2 Manage Groups

The **Portal** allows you to group users and devices. Using these groups, role-based access can be applied:

- Create a local user group and attach users to the group
- Add an **LDAP** group (**LDAP** authentication method required)
- Add **Azure AD** user groups from the **Azure Portal** (**Azure AD** authentication method required)

- Create a device group and attach devices to the group
- Add role assignment to define permissions for a user group when connecting to a device group.

For more information refer to the [Add role assignment](#) sub-chapter.

## 4.2.1 Create a new group

To create a user group, proceed as follows:

1. From the **Manage > Groups** tab, click on the corresponding **Add group** button to create a device group, an LDAP user group, Azure AD user group, or a local user group.
2. Provide the group name and group description and select whether the group is **Active** or not.
3. Click on the **Save** button. The group is successfully created.

## 4.2.2 Attach users to user groups

To attach users to a user group, proceed as follows:

1. Go to the **Users** tab, select the desired user(s).
2. Above the content area, click on the **Attach to group** button. A window is displayed.

**USERS**

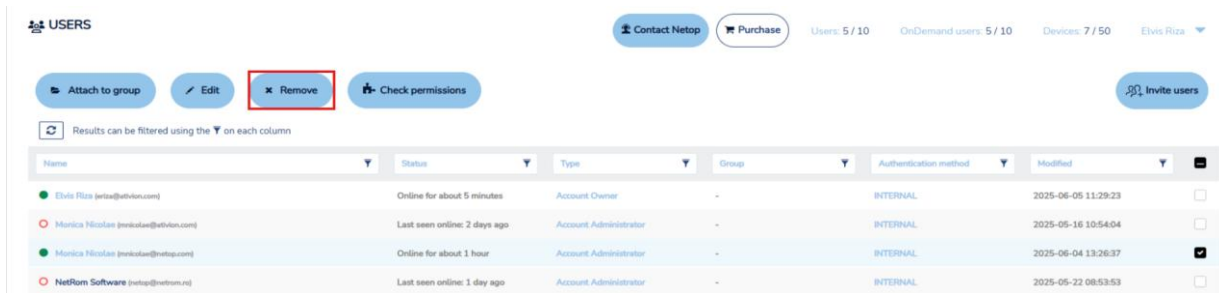
Buttons: **Attach to group** (highlighted), **Edit**, **Remove**, **Check permissions**, **Invite users**

Results can be filtered using the ▼ on each column

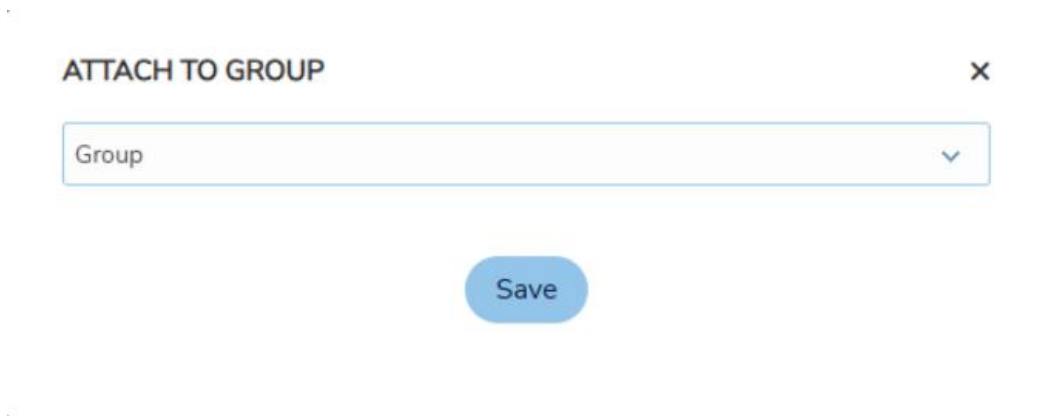
Name	Status	Type	Group	Authentication method	Modified	
Elvis Riza (elvis@elvis.com)	Online for about 5 minutes	Account Owner	-	INTERNAL	2025-06-05 11:29:23	<input type="checkbox"/>
Monica Nicolae (monica@netop.com)	Last seen online: 2 days ago	Account Administrator	-	INTERNAL	2025-05-16 10:54:04	<input type="checkbox"/>
Monica Nicolae (monica@netop.com)	Online for about 1 hour	Account Administrator	-	INTERNAL	2025-06-04 13:26:37	<input checked="" type="checkbox"/>
NetRom Software (netrom@netrom.com)	Last seen online: 1 day ago	Account Administrator	-	INTERNAL	2025-05-22 08:53:53	<input type="checkbox"/>
user@gmail.com	Invite pending	User	-	INTERNAL	2025-06-05 12:25:31	<input type="checkbox"/>

Page controls: Show Rows 10, Go to page 1, 1 - 5 of 5

3. Select the group to which the user(s) belongs.



- Click on the **Save** button. The selected user(s) belong(s) now to this user group as well.



**NOTE:** A user can be attached to multiple groups.

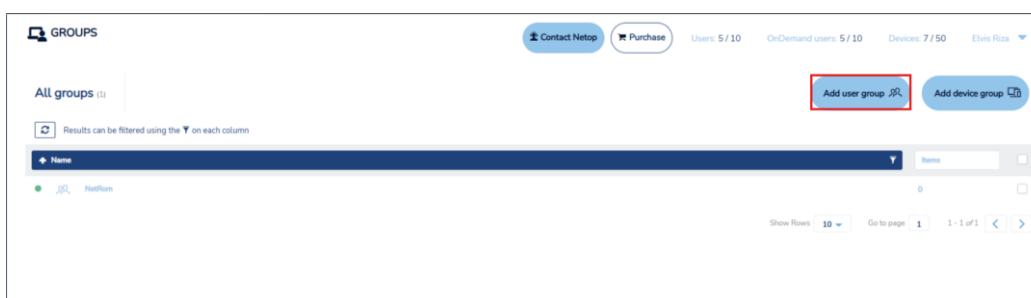
### 4.2.3 Add Azure AD user groups

Prerequisites:

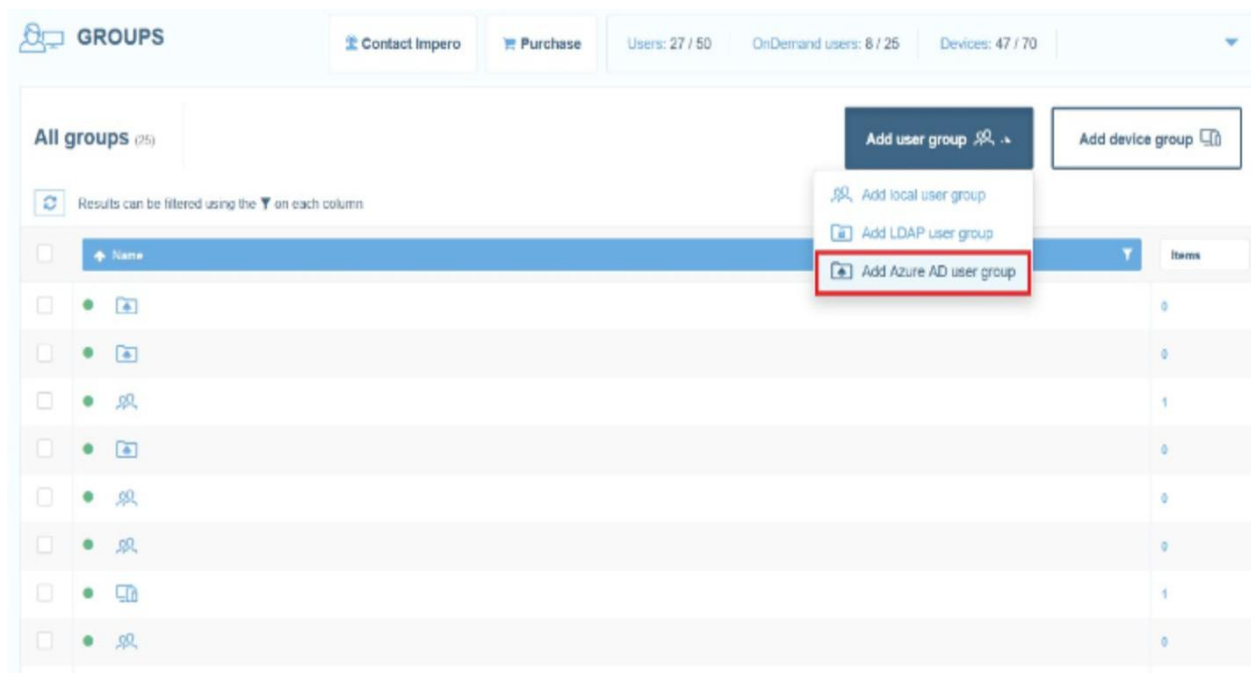
- The **Azure AD authentication method** is correctly set up and enabled. Refer to subchapter [Enabling ADFS/Azure AD authentication](#), for information on how to set up the **Azure AD authentication method**.

To add **Azure AD** user groups to the **Portal**, proceed as follows:

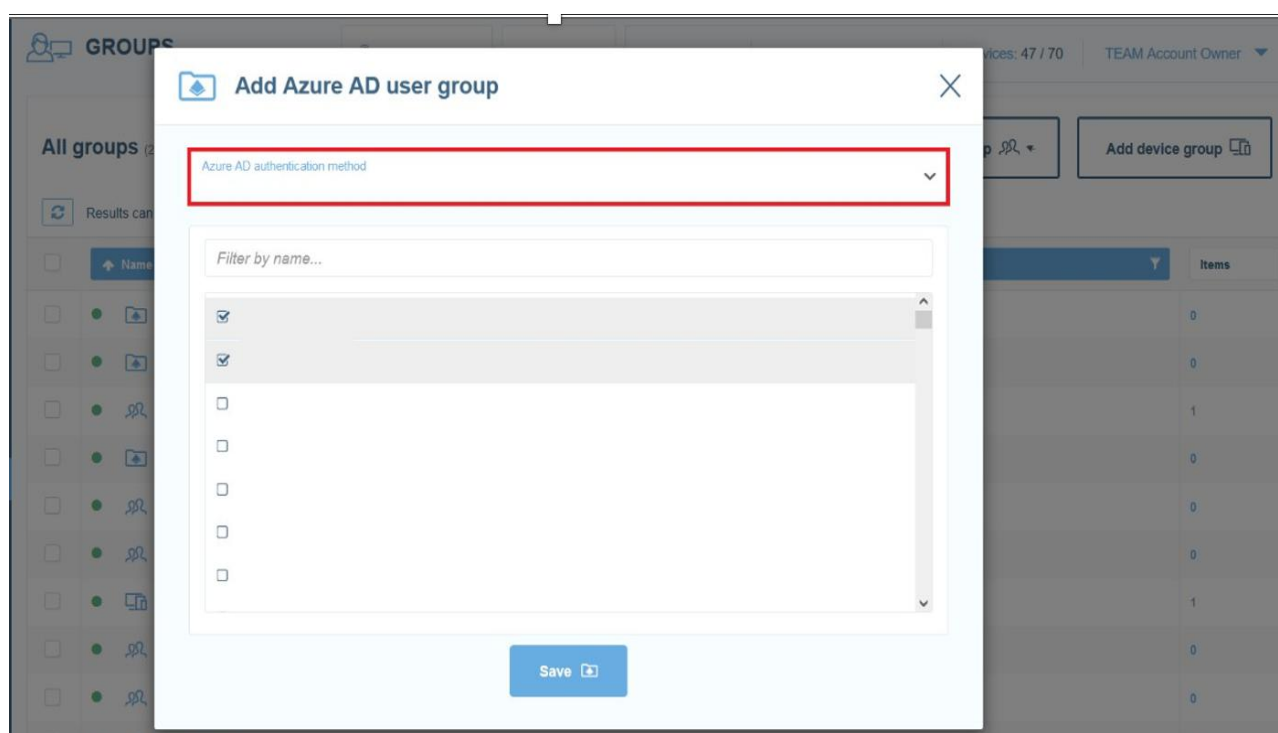
- From the **Manage > Groups** tab, click on the **Add user group** button.



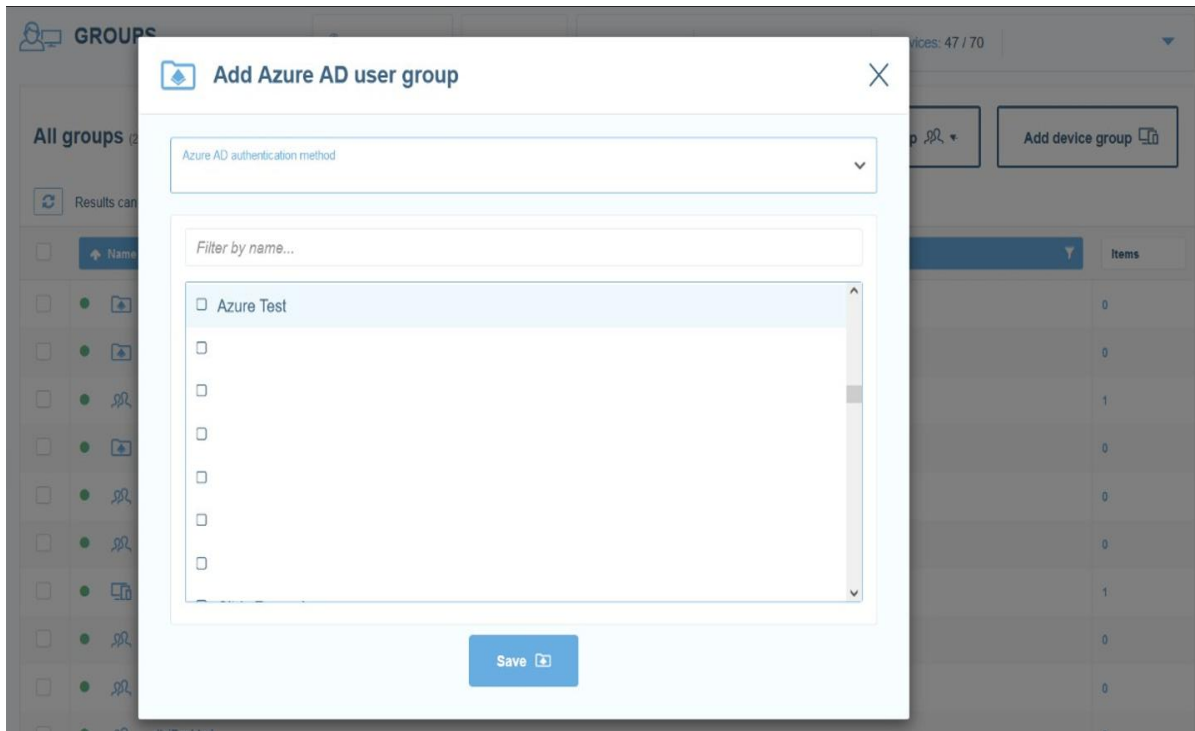
2. Select the **Add Azure AD user group** option from the dropdown field.  
The **Add Azure AD user group** page is displayed.



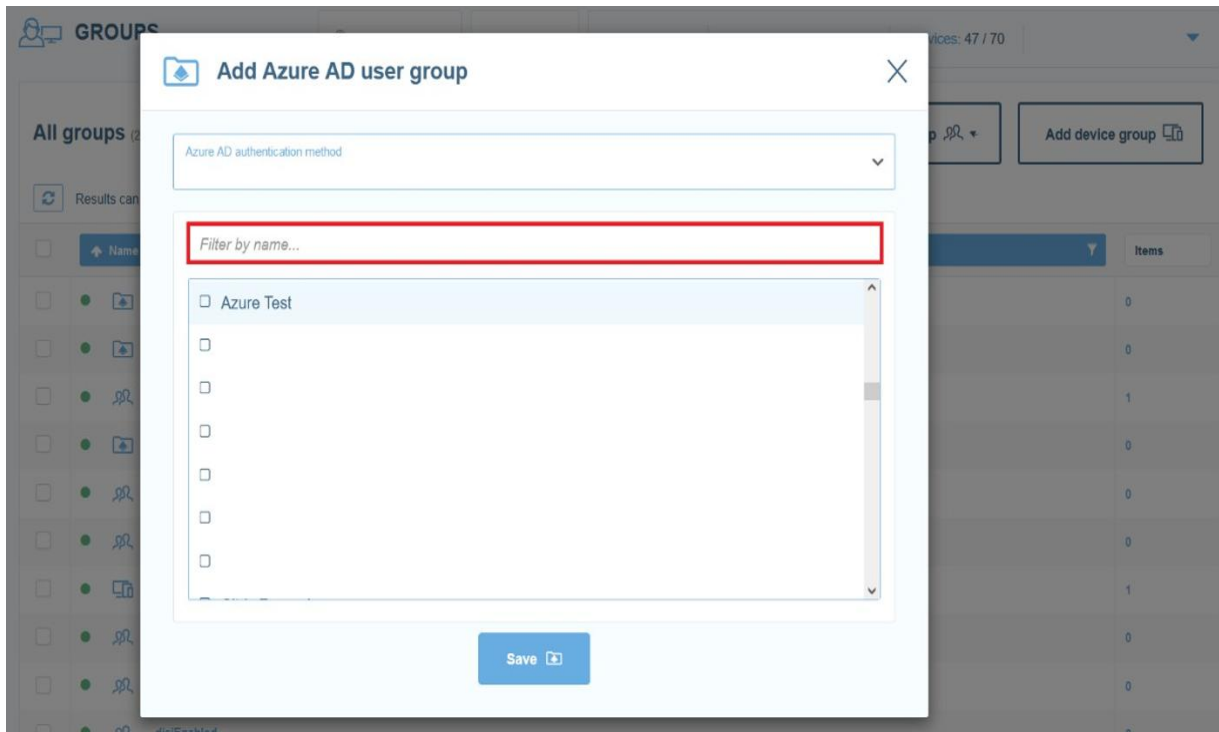
3. Select the **Azure AD authentication method** from the dropdown button.



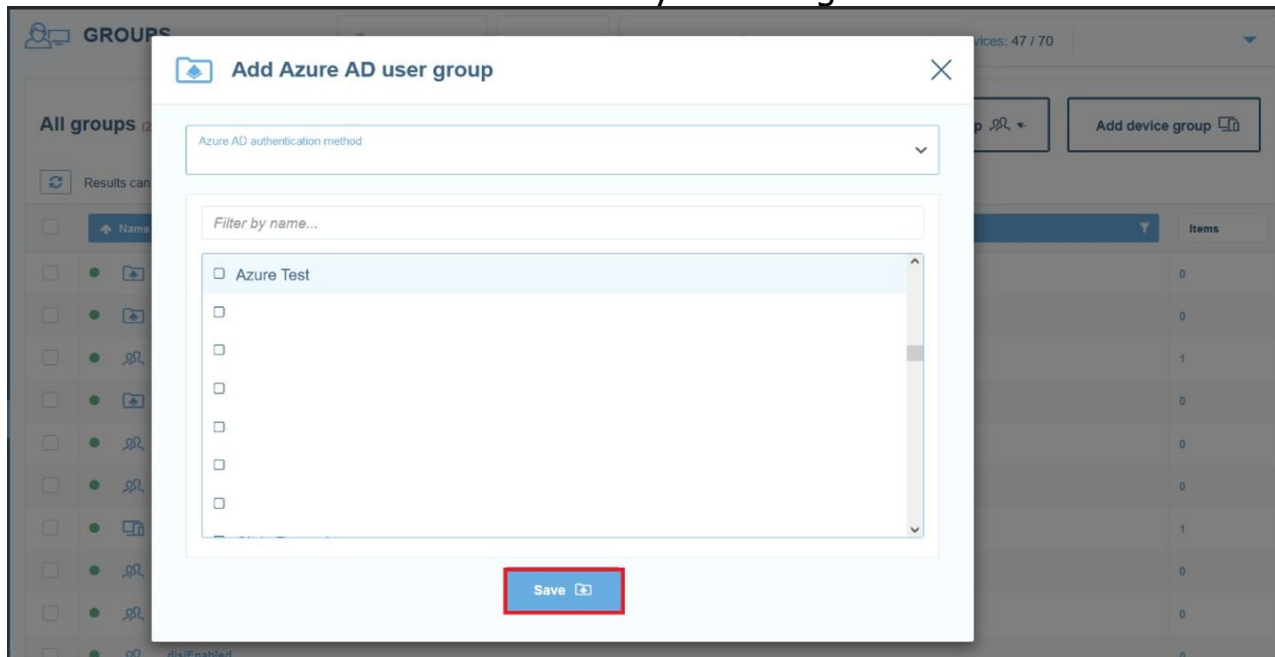
4. Select the user groups you want to add. Previously added groups are marked in gray.



Use the „*Filter by name entry*” field to quickly find the Azure AD user group that you want.



5. Click on the **Save** button to save your changes.



On every user login, the group membership is verified. If the user belongs to any of the **Azure AD** user groups that were added to the **Portal**, the group membership is also updated in the **Portal**.

#### 4.2.4 LDAP user groups

To keep the same group membership in the **Portal** as you have in your **LDAP** directory, add (import) the corresponding **LDAP** groups.

Every time a new employee comes and needs to be added to one of the groups, or an employee leaves the company or changes groups, the user can be managed (added/removed/disabled) directly in the company's **LDAP** directory (instead of having to manage the user in both the **LDAP** and the **Portal**).

To achieve this, proceed as follows:

1. Add the **LDAP** authentication.
2. Add **LDAP** user groups.

By adding an **LDAP** user group, a special group is created in the **Portal** with the same name as in the **LDAP** directory.

This special type of group works as follows:

- No users can be manually attached to the group
- The only way the users are associated with the group is to add them in the **LDAP** directory and on the next login of the user, that is automatically synced with the **Portal**
- The only things that can be edited/changed in the group are the status (active/inactive) and the description

To add an **LDAP** group in the **Portal**, proceed as follows:

1. Go to **Manage > Groups** tab.
2. In the upper-right corner of the page click on the **Add user group** button.
3. Select the **Add LDAP user group** option from the drop-down field. The **Add LDAP user group** page is displayed.
4. From the drop-down select the **LDAP** authentication method from which groups are imported. The drop-down lists all the **LDAP** authentication methods you added from the **Account > Authentication** tab. For information on how to add an **LDAP** authentication method, refer to the [Enable LDAP authentication](#) sub-chapter.
5. Select the user groups to import. The groups that were imported in the **Portal** are marked in gray.
6. To import the selected group in the **Portal**, click on the **Save** button. The users are not synchronized at this stage.



**NOTE:** You can attach an **LDAP** user to the **Portal** groups. A user cannot be attached to an **LDAP** group.

On every use login, the group membership is verified. If the user belongs to any of the **LDAP** groups added to the **Portal**, the group membership is also updated in the **Portal**. The name and email are synchronized on the user login.

Name	Status	Type	Group	Authentication method	Modified
[Empty table body]					

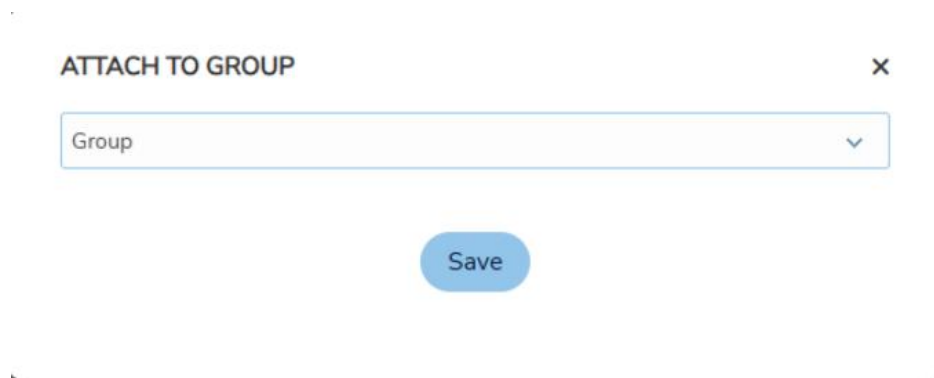
  

User details	
Username	johndoe
First name	John
Last name	Doe
Email	
Default remote control action	Control through browser (default for this account)
Status	Enabled
Type	User
Group	-
Authentication method	ldap auth (NU STERGE)
Multi-Factor Authentication	None
OnDemand Sessions	Disabled

## 4.2.5 Attach devices to device groups

To attach devices to a device group, proceed as follows:

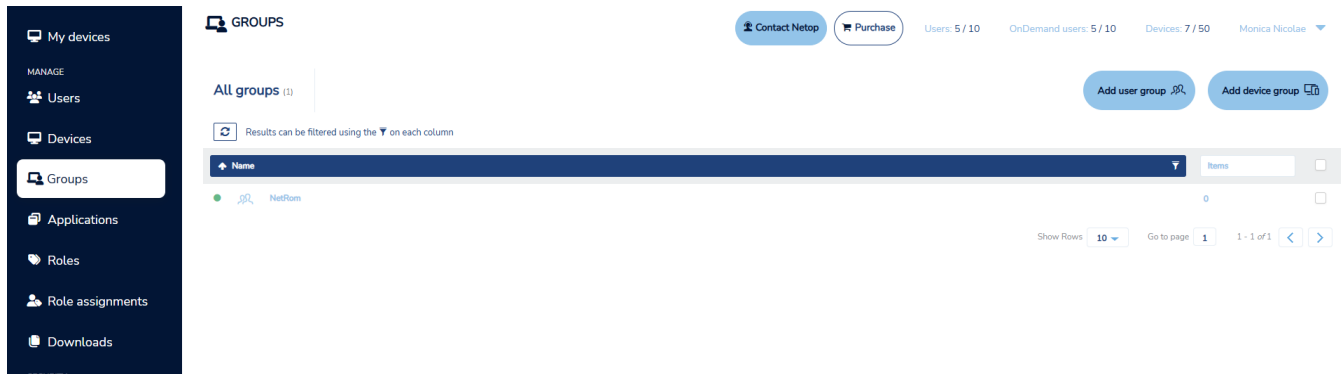
1. Go to the **Devices** tab, select the desired device(s).
2. Above the content area, click on the **Attach to group** button. The **Attach to Group** window is displayed.
3. Select the group to which the device(s) belongs.
4. Click on the **Save** button. The selected device(s) belong now to this device group as well.



**NOTE:** You can attach a device to groups by editing the device and specifying the corresponding device groups.

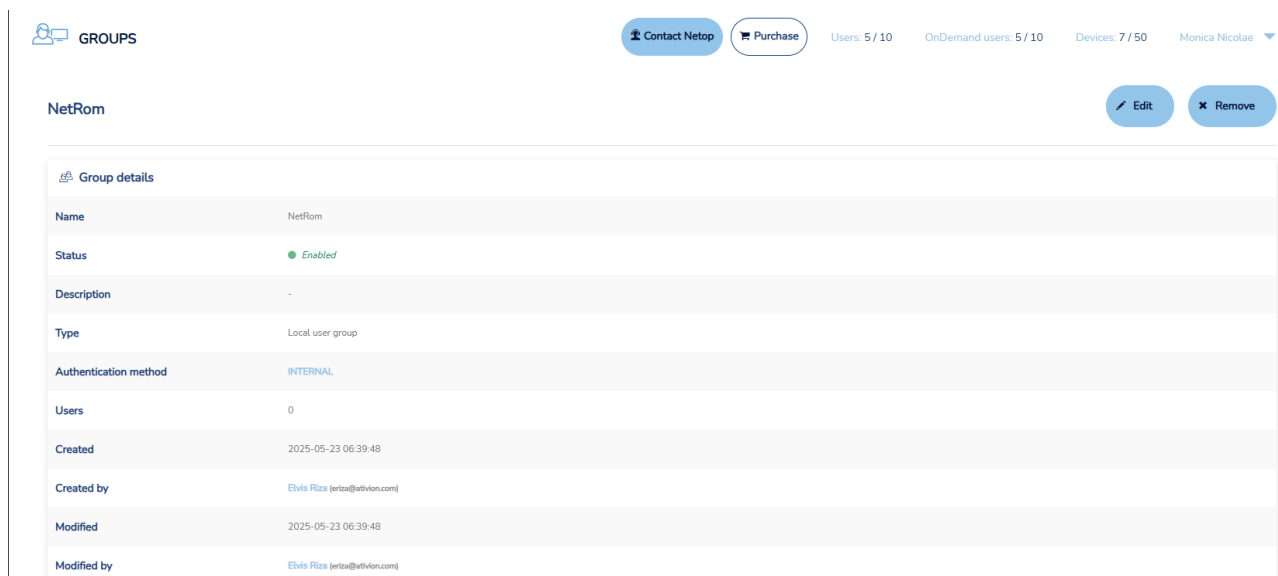
## 4.2.6 View group details

To view the details of a user group, go to the **Groups** tab and click on the desired group in the **Name** column. The group details are displayed.



From the user group details page, you can:

- View the users/devices who belong to the group
- **Edit group** details, such as the group name, group status and description (**LDAP** group allow editing of status and description only)
- Remove the group



## 4.2.7 Edit Groups

To edit group details, go to the **Manage** > **Groups** tab, and click on the specific **Group**.

Above the content area click on the **Edit** button. The **Edit Group** window is displayed.

EDIT USER GROUP

Group name

☒ Active

Users (Optional)

Description (Optional)

Save

Change the group details, such as the group name, group status or description and click on the **Save** button.

**NOTE:** For **LDAP** groups you can only change the description and the status. If you toggle off the **Active** button, it disables the group so that role assignments no longer apply. Disabling does **NOT** remove the group.

## 4.2.8 Remove groups

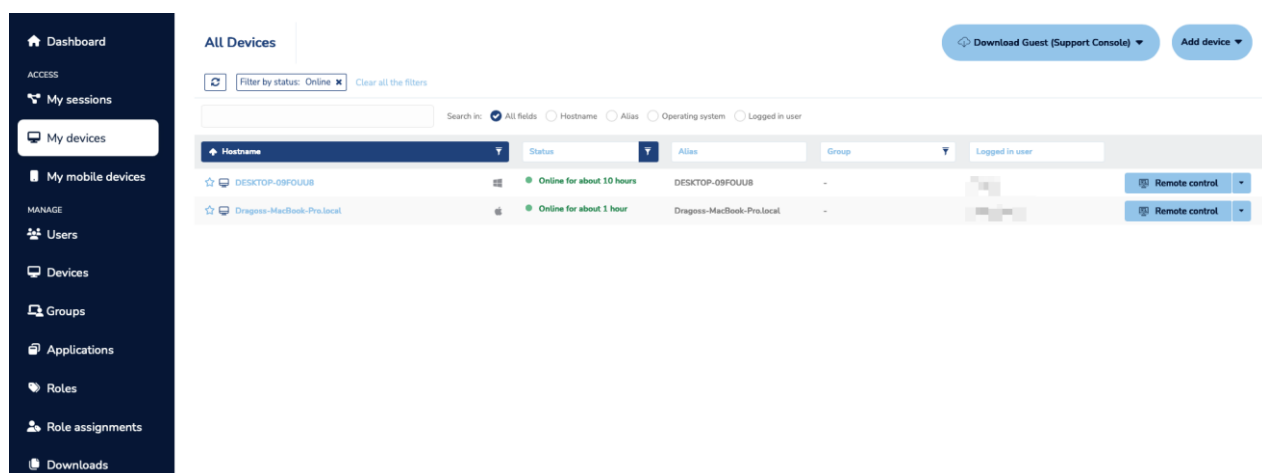
To remove a group, proceed as follows:

1. Go to the specific group in the **Manage** > **Groups** tab.
2. Above the content area, click on the **Remove** button. A confirmation window is displayed.
3. Click on **Yes**.

**NOTE:** By removing the group, the users/devices which are members of that specific group are not removed.

## 4.3 Manage Devices

Once a device is configured with the **Portal** profile and is online, it is automatically displayed in the **Portal** interface, **Devices** section and **My devices** tab.



To easily manage your devices, the **My devices** tab contains information such as the hostname, the online availability of the device, device alias, group of belonging, and the user.

In the **Manage > Devices** tab you can select the columns you want to view.

To modify the column view, proceed as follows:

1. Go to the **Manage > Devices** tab.
2. From the top-right corner of the screen, click on the **Choose columns** button.

3. Select the columns you want to view or hide. The changes that you make have an immediate effect.

### 4.3.1 Edit devices

To edit a device, proceed as follows:

1. Go to the **Manage > Devices** tab.
2. Select the specific device.
3. Click on the **Edit** button.

You can also edit the device by selecting the device and click on the **Edit** button on the top-right menu.

Setting	Description
Alias	An internal name that could help supporters and administrators to identify faster the device.
Group	The Device group(s) that the device is attached to. A device can be attached to any number of device groups.
Description	An extended description for the device.

EDIT DEVICE

×

Change the details for the device below

Alias

localhost.localdomain

Group

▼

Description (Optional)

Save

### 4.3.2 Remove devices

To remove devices, go to the **Devices** area, select the devices you want to remove and above the content area click on the **Remove** button. A confirmation dialog is displayed. To remove the selected devices from the **Portal**, click on **Yes**. This is useful for devices that are not online anymore (e.g., devices that are not used any longer or that do not have a **Host** installed). For the devices that have a **Host** installed on them and are connected to the **Portal**, they are re-enrolled on the next **Host** restart (they show up again in the device list).

Refer to the [Revoke deployment packages](#) sub-chapter for more information on how to disable devices associated with a deployment package.

**NOTE:** Make sure that you have an Account Administrator user type or higher to remove a device.

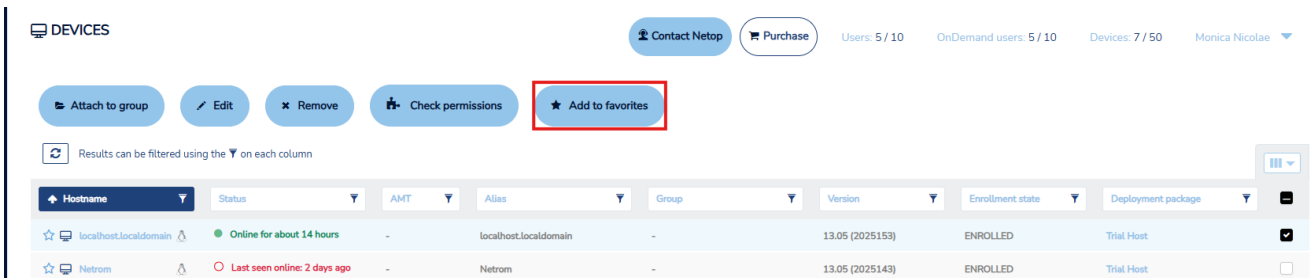
### 4.3.3 Favorite Devices

With the **Portal**, you can add devices to favorites. Favorite devices are displayed first in the list in the **Devices** tab.

**NOTE:** This feature is only available when using the new **Connection Manager**. The **Connection Manager** serves as a meeting hub for **Guests** and **Hosts** and is responsible for managing the connections between modules.

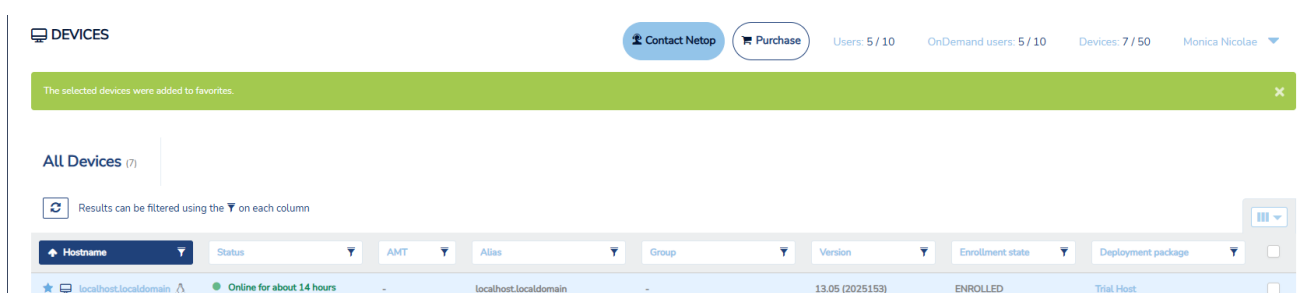
To add a device to favorite, proceed as follows:

1. Go to the **Devices** tab.
2. Select the device you want to add to favorite.
3. Click on the **"Add to favorites"** button, which is found in the top-right of the screen.

4. The screenshot shows the 'DEVICES' tab in the Netop Portal. At the top, there are buttons for 'Attach to group', 'Edit', 'Remove', 'Check permissions', and 'Add to favorites' (which is highlighted with a red box). Below these buttons is a table with columns: Hostname, Status, AMT, Alias, Group, Version, Enrollment state, and Deployment package. The table contains two rows: 'localhost.localdomain' (Online for about 14 hours) and 'Netrom' (Last seen online: 2 days ago). Both are marked as 'ENROLLED' and 'Trial Host'. A blue star icon is visible next to the 'localhost.localdomain' entry.

Alternatively, through the **Portal** you can add a device or multiple devices to favorite as follows:

- Click on the blue star near the device **Hostname** in the **Devices** tab; favorite devices display a filled blue star near the device **Hostname**
- Select the device or multiple devices with the check button in the **Devices** tab and click on the **"Add to favorites"** button

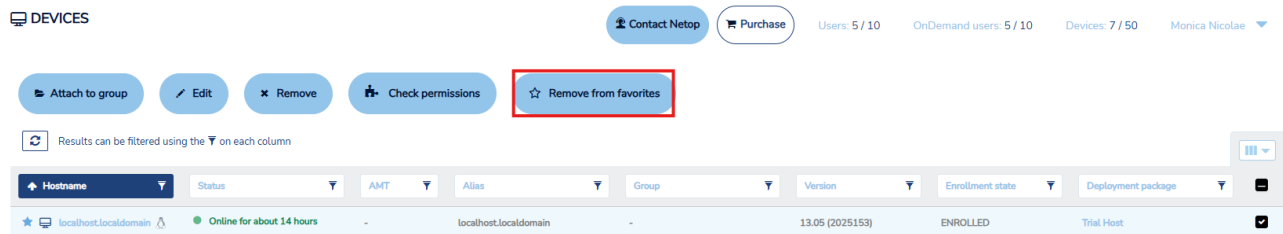
The screenshot shows the 'DEVICES' tab in the Netop Portal. At the top, there are buttons for 'Contact Netop' and 'Purchase'. Below these buttons is a green banner with the text 'The selected devices were added to favorites.' Below the banner is a table with columns: Hostname, Status, AMT, Alias, Group, Version, Enrollment state, and Deployment package. The table contains two rows: 'localhost.localdomain' (Online for about 14 hours) and 'Netrom' (Last seen online: 2 days ago). Both are marked as 'ENROLLED' and 'Trial Host'. A blue star icon is visible next to the 'localhost.localdomain' entry.



To remove a device from favorite, proceed as follows:

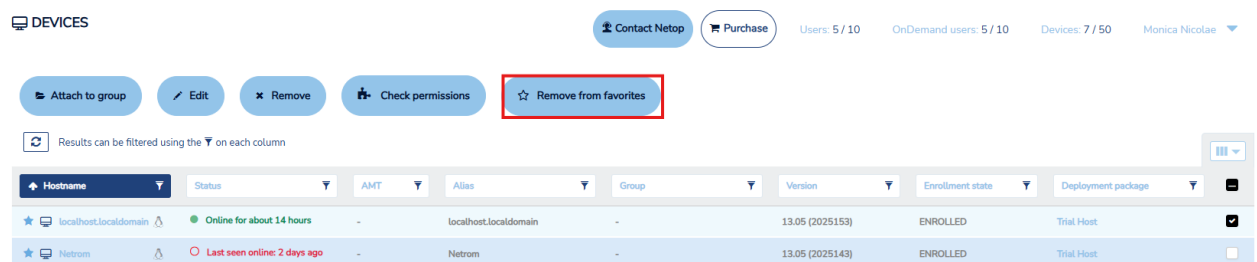
1. Go to the **Devices** tab.

2. Select the device you want to remove from favorite.
3. Click on the **Remove from favorites** button, which is found in the top-right of the screen.



Alternatively, through the **Portal** you can remove a device or multiple devices from favorite as follows:

- Click on the blue star near the device **Hostname** in the **Devices** tab; removed devices display an empty blue star near the device **Hostname**
- Select the device or multiple devices with the check button in the **Devices** tab and click on the **Remove from favorites** button



## 4.3.4 My Mobile Devices

To add mobile devices to the **Portal**, open the email received from **Netop** with your **myCloud** account information. Activate your account by using the link received in the email and set up a password.

In the Chrome Internet browser, add the **WiseMo Guest for myCloud** extension from the Chrome Web Store [link](#).

To add a **Host** on your mobile device, proceed as follows:

1. Download the **WiseMo Host** App from the App/Play Store on your mobile device. Depending on the manufacturer of your mobile device, it might be necessary for you to install an extra add-on to allow remote desktop features on your mobile device.
2. Open the **WiseMo Host** app.
3. Grant permissions when asked by the **WiseMo Host** app.
4. Specify your **myCloud** credentials.
5. Restart the **Host**.

To access your mobile device(s) from the **Portal**, proceed as follows:

1. Log in the **Portal**.
2. Access the **My mobile devices** tab.
3. There are two ways that you can control your mobile device. Click on the **Remote control** dropdown button and you can select between:
  - Control through Chrome app (default action)
  - Control through WiseMo Guest

If you directly click on the **Remote control** button, the **Portal** starts the remote control session via the Chrome app, which is the default action.

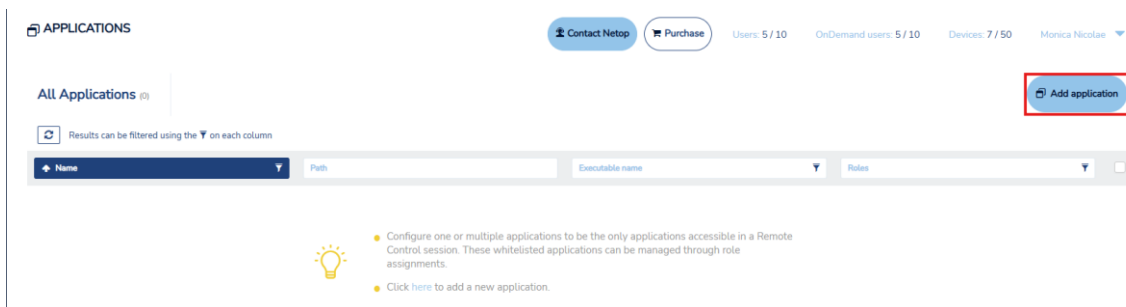
**NOTE:** Refer to the [supported versions](#) article in the **Knowledge Base** for more information about the supported mobile devices in the **Portal**.

### 4.3.5 Applications

With whitelisted applications, account administrators can restrict remote control sessions to a single application (or list of applications) on the **Host** device. This includes viewing the screen and using a keyboard and mouse for those applications.

To add an application, proceed as follows:

1. Click on the **Add application** button.



2. Fill in the required information.

3. Click on **Save**.

ADD APPLICATION

Name

☒

Enabled (This application is enabled)

Path - for instance: C:\Program Files\My Application (Optional)

Executable name - for instance: notepad.exe

Description (Optional)

Save

Setting	Description
Name	A name for the application
Path	The path for the application, including system environment variables (e.g., %windir%\system32)
Executable name	Executable name (e.g., notepad.exe)


Setting	Description
Description	Description of the application

**NOTE:** The role assignment automatically becomes disabled if the applications set as part of whitelisted applications are disabled.

## 4.4 Roles and Role assignments

Roles are a set of permissions that can be applied to a group of users through **Role Assignments**.

A role assignment is comprised of a role, a group of users, and a group of devices. Create user groups (including **LDAP** and **Azure AD** user groups) and device groups before adding new role assignments.

Add role assignment  ×

Name

☒ **Active** *(This role assignment is active)*

Role

User group

Device group

Description (Optional)

Save

These are used for defining the permissions for the users in the **Portal** and remote accessing a device.

**NOTE:** The devices listed in the **Portal** under the **My devices** tab are only the devices that the user is allowed to connect to (at least one Role assignment needs to exist containing a User group with that User and a

Device group with that Device). For a user to be allowed to create (and use) **OnDemand Sessions** under the **My sessions** tab, create the role assignments for that group with an **OnDemand** - role type.

#### 4.4.1 View Predefined Roles

The page provides a listing of the available roles, their type, name, and a short description.

Multiple role types have been implemented, each representing a specific set of permissions:

- The **Device** role type includes a set of permissions related to remote control sessions. By clicking on the name of a specific role from the roles page, the user is provided information about the role and the full list of associated permissions.

**NOTE:** When creating a **Device** role type, make sure to select the corresponding client type for your **Guest** device.

- The **OnDemand** role type includes a set of permissions related to the **OnDemand Sessions**. The permissions include keyboard and mouse access and to view the remote screen.
- The **Confirm access** role type provides increased security through the addition of a confirmation dialog on the **Host** side.
- The **Whitelisted applications** role type provides the capability to restrict remote control sessions to a single application.

**NOTE:** **Account Administrators**, **Owners** and **Group Managers** can view the **Roles**.

Predefined Roles	Description
Administrator	Provides full access to the remote device when using the <b>Control through browser</b> option or an installed <b>Guest</b> .
Web Support	Provides full access to the <b>Control through browser</b> option. Access from an installed <b>Guest</b> is not allowed.
Full Access	Provides full access to the remote device when using

Predefined Roles	Description
(OnDemand Sessions)	the <b>OnDemand</b> Session. This role does not apply to regular <b>Guests</b> and <b>Hosts</b> .
Confirm Access Required	Requires that the local user at a remote device to confirm a session before it starts; except for when the computer is locked, or no one is logged in.

## 4.4.2 How to add a role

To add a role, proceed as follows:

1. Go to the **Roles** tab.
2. Click on the **Add** button.
3. Specify a name for the role.
4. Select the role type from the drop-down list.
5. Enable or disable the role.
6. To save the changes made, click on the **Save** button.

## 4.4.3 How to edit a role

To edit a role, proceed as follows:

1. Go to the **Roles** tab.
2. Select a role to edit.
3. To edit the role, click on the **Edit** button.
4. In the **Edit role** dialog box, you can:

- Edit the **Role** Name.
- Edit the **Type** from the drop-down list.
- Edit the description.
- Enable or disable the role.
- Edit additional **Role type** options

5. To save the changes made, click on the **Save** button.

EDIT ROLE

The permissions will change following the role saving.

Name: Test Role

Type: Device

Description (Optional):

☒ Enabled (This role is enabled)

Remote session ☒ ▼

Tunnel ☐ ▼

Client type ☐ ▼

Save

#### 4.4.4 How to copy a role

To copy a role, proceed as follows:

1. Go to the **Roles** tab.
2. Select a role to copy.
3. Click on the **Copy role** button. The **Add role** dialog box is displayed.
4. Edit the name of the role you want to copy.
5. Edit the description of the role you want to copy.
6. Enable or disable the role.
7. Edit additional **Role type** options.



8. To save the changes made, click on the **Save** button.

ADD ROLE

×

Name

Copy of Test Role role

Type

Device

▼

Description (Optional)

☒

Enabled (This role is enabled)

Remote session

☒ ▼

Tunnel

☐ ▼

Client type

☐ ▼

Save

#### 4.4.5 How to remove a role

To remove a role, proceed as follows:

1. Go to the **Roles** tab.
2. Select the role you want to remove.
3. Click on the **Remove** button. The **Remove Role** dialog box for confirmation is displayed.
4. To remove the role, click on **Yes**.

REMOVE ROLE

×

Are you sure you want to remove the role?

The following 6 role assignments will be disabled:

test only, Ioana's CAVE RA, admin, cfacrgi, fa2, ad5

Yes

Cancel

**NOTE:** If the user deletes a role which is part of an active role assignment, the role assignment becomes disabled and the user receives a warning about this.

#### 4.4.6 Add role assignment

To add a role assignment, proceed as follows:

1. Go to the **Role assignments** tab and click on the **Add role assignment** button.
2. Provide the role name and make sure that the assignment is enabled.
3. From the appropriate drop-down lists, select the role, user group, and device group. Role assignments can be applied to multiple user and device groups.

**Add role assignment** X

Name

☒ Active (This role assignment is active)

Role

User group

Device group

Description (Optional)

☐ Everyone

☐ adsads

☐ cfacrgi

☐ disiUsersGroup

☐ driv

Save

**Add role assignment** X

Name

☒ Active (This role assignment is active)

Role

User group

Device group

Description (Optional)

☐ Everything

☐ aaa

☐ cfacrgi

☐ custom sandu ciorba mocks

Save

4. To save your changes, click on the **Save** button.

Add role assignment
✕

Name

☒ **Active** *(This role assignment is active)*

Role

User group

Device group

Description (Optional)

Save

**NOTE:** For a role assignment to govern the permissions of a remote user, make sure that the **Host's Guest Access Security** settings are configured to use **Portal** access rights. Refer to the [Netop User's Guide](#) for more information on the **Guest Access Security** settings within the **Host**. For the **OnDemand** – type roles, device groups cannot be selected, as these role assignments do not apply to regular devices.

#### 4.4.7 Edit role assignment


To edit a role assignment, proceed as follows:

1. Go to the **Role assignments** section, select the role assignment you want to edit.
2. Above the content area click on the **Edit** button. The **Edit Role Assignment** window is displayed.
3. Make the desired changes.

4. To save your changes, click on the **Save** button.

**Edit role assignment** ×

Make sure that users from the selected **User group** who are used on the Host do not have Multi factor enabled. ×

 This role assignment is scheduled starting from April 2, 2021, every day, full time (Europe/Bucharest time).

Name

ad5

☒ **Active** *(This role assignment is active)*

Role

Add Devices ▼

User group

Everyone × ▼

Device group

Everything × ▼

Description (Optional)

Save

**NOTE:** Disabling the role assignment does not remove it from the **Portal**.

### 4.4.8 Create a schedule for a role assignment

A schedule can be created for a role assignment. In the scheduler you can specify the following information:

- Schedule interval
- Recurrence

**SCHEDULE FOR ADMIN** Close x

**Schedule interval**

Start date

Start time End time ☐ All day Timezone **Europe Bucharest (GMT+03:00)**

**Recurrence**

Recurrence **No recurrence**

End date **No end date**

**Save**

**NOTE:** This feature is only available when using the new **Connection Manager**. The **Connection Manager** serves as a meeting hub for **Guests** and **Hosts** and is responsible for managing the connections between modules.

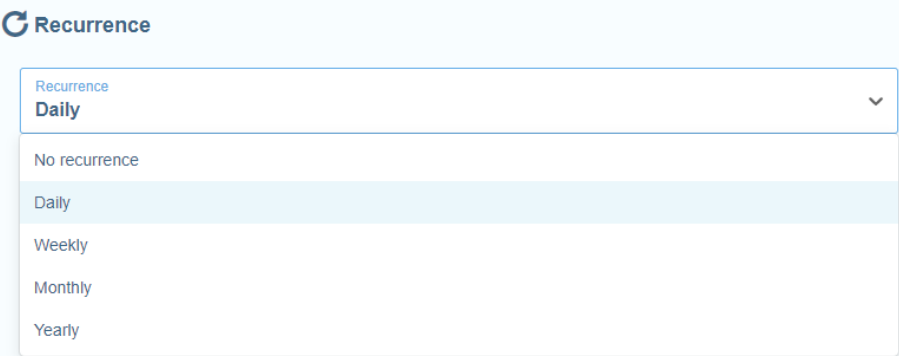
In the **Schedule interval** you can specify the following information:

- **Start date** – you specify the day that the role assignment starts
- **Start time** – you specify the time when the role assignment starts
- **End time** – you specify the time when the role assignment becomes inactive
- **All day** – you use this option to specify that the role assignment is valid throughout the day; when you use this option, the **Start date** and the **Start time** fields become inactive
- **Timezone** – you specify the **Timezone** for the role assignment

In the **Recurrence** area, you specify the recurrence for the role assignment.

The following options are available:

- no recurrence
- daily
- weekly
- monthly
- yearly



The screenshot shows a 'Recurrence' dropdown menu. The menu is open, displaying the following options: 'No recurrence', 'Daily' (which is highlighted with a blue background), 'Weekly', 'Monthly', and 'Yearly'. The dropdown is set against a light blue background.

Recurrence	Description
No recurrence	Select this option to apply the schedule indefinitely.
Daily	<p>You use this when you want the schedule to recur on specific days or every X number of days.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• Only weekdays</li> <li>• Only weekends</li> <li>• Custom</li> </ul>
Weekly	<p>Possible values:</p> <ul style="list-style-type: none"> <li>• Every X week on</li> <li>• Monday</li> <li>• Tuesday</li> <li>• Wednesday</li> <li>• Thursday</li> </ul>

	<ul style="list-style-type: none"> <li>• Friday</li> <li>• Saturday</li> <li>• Sunday</li> </ul>
Monthly	Possible values: <ul style="list-style-type: none"> <li>• Every X month on</li> <li>• Day of the month</li> <li>• Last day of the month</li> </ul>
Yearly	Possible values: <ul style="list-style-type: none"> <li>• Every X year on</li> <li>• Month of the year</li> <li>• Day of the month</li> </ul>

The **Schedule** status can be:


- Active

Status

 Active, due to schedule

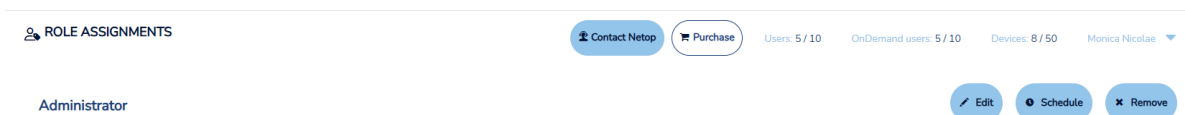
- Inactive

Status

 Not active, due to schedule

To create a schedule for a role assignment, proceed as follows:

1. In the **Portal** page, click on the **Role assignments** tab.
2. In the **Role assignments** tab, click on the **Role assignment** you want to assign a schedule to.
3. To add a schedule to the **Role assignment**, click on the **Schedule** button.



The **Schedule** window for the **Role assignment** is displayed.

The screenshot shows the 'Schedule' window for a 'Role assignment'. It includes the following fields:

- Start date:** A text input field with a calendar icon.
- Start time:** A dropdown menu.
- End time:** A dropdown menu.
- All day:** A checkbox.
- Timezone:** A dropdown menu showing 'Europe Bucharest (GMT+03:00)'.
- Recurrence:** A section header with a circular arrow icon, followed by a dropdown menu showing 'No recurrence'.
- End date:** A dropdown menu showing 'No end date'.

4. Specify the schedule interval:

4.1. Specify the Start date.

4.2. Specify the Start time.

4.3. Specify the End time.

**NOTE:** If you click on the **Save** button and you do not specify a Start date, Start time, and End time, the Schedule applies starting on the present day, for All day, full time.

5. Specify the recurrence for the schedule:

5.1. Specify the recurrence.

5.2. Specify the End date for the recurrence.

**NOTE:** If you do not specify a recurrence for the schedule, the schedule applies until you manually remove it, or you add an end date to the recurrence.

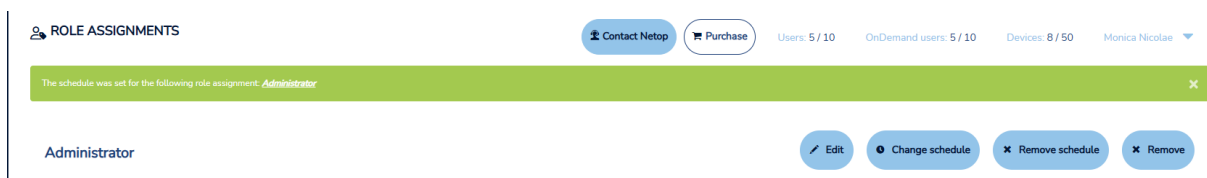


6. To save your changes, click on the **Save** button.

**NOTE:** You can assign a schedule to multiple role assignments.

To edit a schedule for a role assignment, proceed as follows:

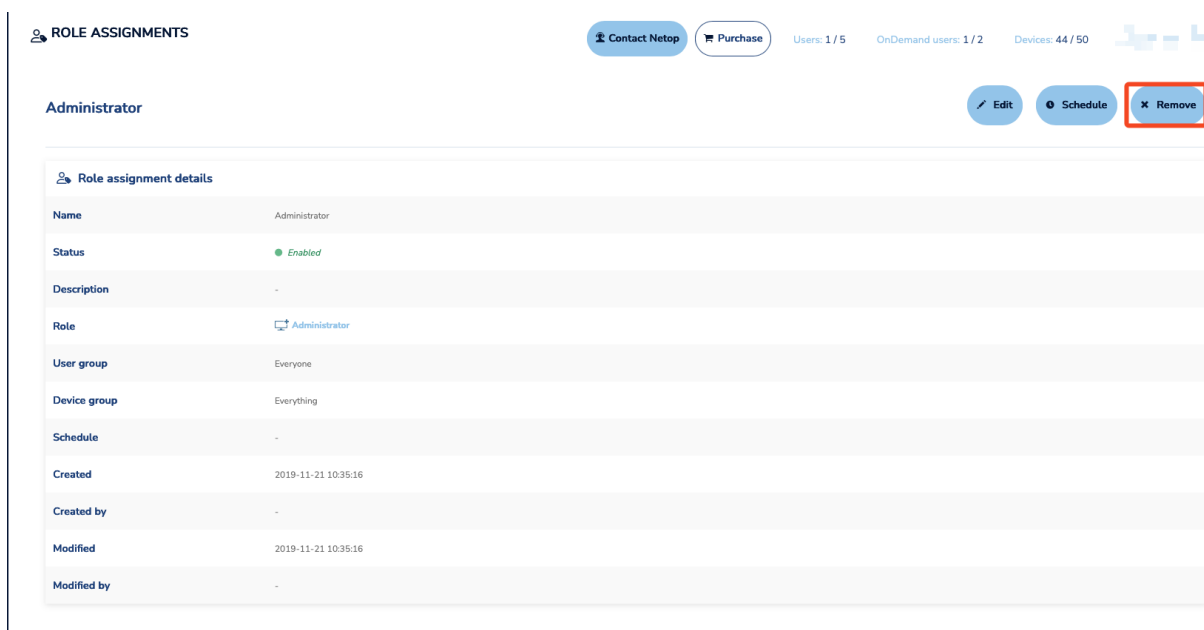
1. In the **Portal** page, click on the **Role assignments** tab.
2. In the **Role assignments** tab, click on the Role assignment you want to assign a schedule to.
3. To edit a schedule of the Role assignment, click on the **Change Schedule** button.



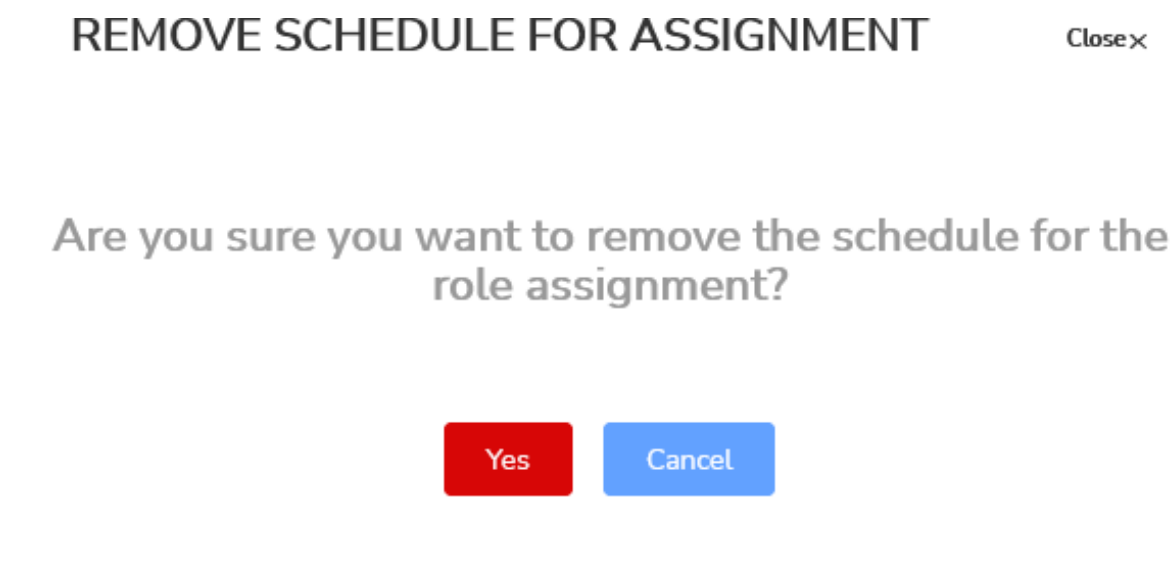
4. Make the changes you want.
5. To save your changes, click on the **Save** button.

To remove a schedule from a role assignment, proceed as follows:

1. In the **Portal** page, click on the **Role assignments** tab.
2. In the **Role assignments** tab, click on the **Role assignment** you want to remove the schedule.
3. To remove the schedule of the Role assignment, click on the **Remove Schedule** button.



The **Remove Schedule for Assignment** warning is displayed.



4. Click on **Yes** to confirm.

**NOTE:**

- You can remove a schedule from multiple role assignments.
- A schedule is removed if you delete the role assignment(s).

#### 4.4.9 Remove role assignments

To remove role assignments, go to the **Role assignments** tab, select the items you want to remove and above the content area click on the **Remove** button. A confirmation dialogue is displayed. To remove the selected role assignments, click on **Yes**.

#### 4.4.10 Confirm Access role

Starting with **Netop** version 12.67 for Windows **Hosts** and 12.70 for Linux and macOS **Hosts**, the **Confirm access** functionality was added, and starting with version 12.82 for Windows **Hosts** the **Confirm access via email** feature was introduced. The **Confirm access** feature provides improved security by adding a confirmation dialog on the end-user side (**Host** side).

The **Confirm access via email** feature is configured along with a user group. Once **Confirm access via email** is triggered, all the users in that group receive an email requesting them to provide access to the **Host**. The email contains a confirm access link, the name of the user requesting access, and the name of the **Host**. Once the link in the email is clicked on, you are redirected to the **Portal** where you can allow or deny access to the device for the user that requested it.

**CONFIRM ACCESS** [Close]

You are seeing this page because your user belongs to a role which has confirm access via email enabled.

Whenever a user assigned to that role tries to access a device, a confirm access request such as this will be issued and you will be asked to allow or deny access for that user.

Do you want to confirm access for the following connection?

Connection attempt details	
User firstname lastname	John Doe
Username	
Host name	DESKTOP
Connection attempt	2021-09-16 16:17:43

The access granted through the confirm access email is audited.

#### 4.4.10.1 How to add a Confirm Access role

To create a **Confirm Access** role, proceed as follows:

1. Go to the **Roles** tab.
2. Click on the **Add role** button.
3. Specify a name for the role.
4. From the **Type** drop-down list, select the **Confirm access** type.
5. Enable or disable the role.
6. You can use either the **Confirm access** or **Confirm access via email** option or both for the **Confirm access** role. To use the options, select the **Enable confirm access**, respectively **Enable confirm access via email**

checkboxes. If you use **Confirm access via email** you must add a user group or multiple groups that receive an email when a user requests access to a device.

ADD ROLE
×

Please note that the **Confirm Access via Email** functionality works only on Hosts v12.82 or later. For older Hosts, the connection to them will be denied if Confirm Access via Email is enabled in any of their role assignments.

Please note that the locked computer/logged in user constraints are only supported on Windows Hosts. For other Hosts, the confirm access mechanism will always be triggered if enabled in any of their role assignments.

Name

Type

Description (Optional)

☒ Enabled (This role is enabled)

Confirm access	<input checked="" type="checkbox"/> ▼
Confirm access via email	<input checked="" type="checkbox"/> ▼

User groups

Save

7. To save the changes made, click on the **Save** button.

**NOTE:** If both the **Confirm access** and **Confirm access via email** features are enabled, whichever type of confirmation happens first, the user is granted access to the **Host**.

#### 4.4.10.2 How to add a Confirm access role assignment

To add the **Confirm access** role to a role assignment, proceed as follows:

1. Go to the **Role assignments** tab.
2. Click on the **Add role assignments** button.
3. Specify a name for the role assignment.
4. Activate the role assignment.
5. From the **Role** drop-down list, select the **Confirm access** role.

6. Assign the role to a **User group**.

**NOTE:** When the **Confirm access via email** option is enabled, you allow or deny access to a device for users that belong to this User group.

7. Assign the role to a **Device group**.

**NOTE:** When the **Confirm access via email** option is enabled, you allow or deny access to devices that belong to this Device group.

8. To save the changes made, click on the **Save** button.

Add role assignment
×

Name

☒ **Active** *(This role assignment is active)*

Role
 ⓘ

User group
 ×

Device group
 ×

Description (Optional)

Save

**NOTE:**

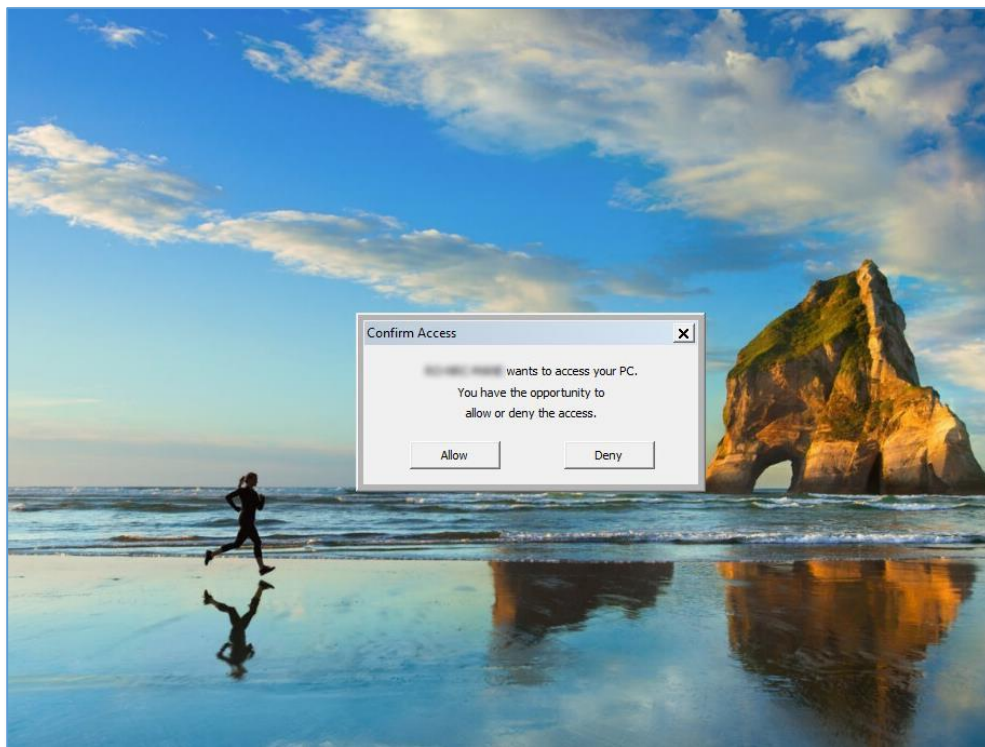
- The **Confirm Access** functionality works only on **Hosts** and **Guests** v12.67 or later. For older **Guests** and **Hosts**, the connection between them is denied if the **Confirm Access** feature is enabled in any of their role assignments.
- The **Confirm Access via email** functionality works only on **Guests** and **Hosts** version 12.82 or later. For older **Guests** and **Hosts**, the connection between them is denied if the **Confirm Access via email** feature is enabled in any of their role assignments.

Once the **Confirm access** is defined, on the next remote session between the **Guest** and **Host**, a confirm access prompt is displayed to the end-user on the **Host** side.

There are two extra exceptions when the **Confirm access** and the **Confirm access via email** can be set to be overruled even though it is enabled.

#### **For Confirm Access:**

- **Except when computer is locked** - if the computer is in the locked screen.
- **Except when no user is logged in** - if no user is logged into the system.



#### **For Confirm access via email:**

- **Only when computer is locked**
- **Only when no user is logged in**

When confirmed, the remote session is initiated. If denied, the confirm session is not initiated.

**NOTE:** The exceptions for **Confirm Access** and **Confirm access via email** do not apply to the macOS and Linux Hosts.

#### 4.4.11 Whitelisted applications role

Starting with **Netop** version 12.74 for Windows **Hosts**, the capability of whitelisting applications is available. With whitelisted applications, users can restrict remote control sessions to a single application (or list of applications) on the **Host** device. This includes viewing the screen and using the keyboard and mouse for those applications.

##### 4.4.11.1 How to add a Whitelisted applications role

To create a whitelisted applications role, proceed as follows:

1. Go to the **Roles** tab.
2. Click on the **Add role** button.
3. Specify a name for the role.
4. From the **Type** drop-down list, select the **Whitelisted applications** type.
5. Enable or disable the role.
6. Edit additional **Whitelisted applications** options.
7. Select the application(s) to be whitelisted.



8. To save the changes, click on the **Save** button.

**ADD ROLE** ×

Name

Type

Description (Optional)

☒ Enabled (This role is enabled)

**Whitelisted applications** ☒ ^

Enable whitelisted applications ☒

Except when computer is locked ☒

Except when no user is logged in ☒

Whitelisted applications



**Save**

#### 4.4.11.2 How to add a Whitelisted applications role to a role assignment


To add a whitelisted applications role to a role assignment, proceed as follows:

1. Go to the **Role assignments** tab.
2. Click on the **Add role assignment** button.
3. Specify a name for the role assignment.
4. Activate or deactivate the role assignment.
5. From the **Role** drop-down list, select the whitelisted application's role.
6. Select the **User group**.
7. Select the **Device group**.

8. To save the changes made, click on the **Save** button.

**Add role assignment**  

**Name**

 **Active** *(This role assignment is active)*

**Role**

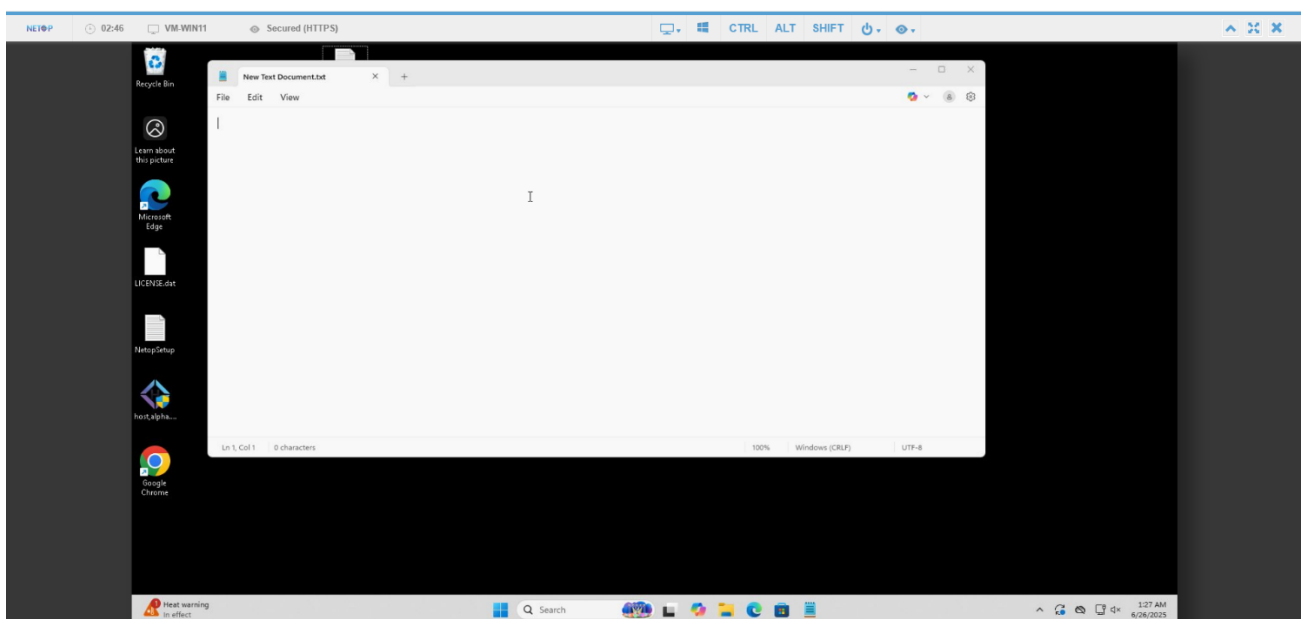
**User group**

**Device group**

**Description** (Optional)

**Save**

Once the whitelisted applications are enabled, on the next remote session between the **Guest** and **Host**, only these apps are visible to the user.



There are two extra exceptions when the whitelisted application can be set to be overruled even though it is enabled:

- **Except when computer is locked** - if the computer is in the locked screen.
- **Except when no user is logged in** - if no user is logged into the system.

In either of these exceptions, the whitelisting applications are not enabled throughout the session.

**NOTE:** The role assignment automatically becomes disabled if all the applications that are set as part of the whitelisted applications become disabled.

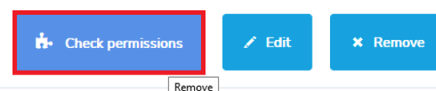
For more information on whitelisted applications, refer to the following knowledge base [article](#).

#### 4.4.12 Check permissions

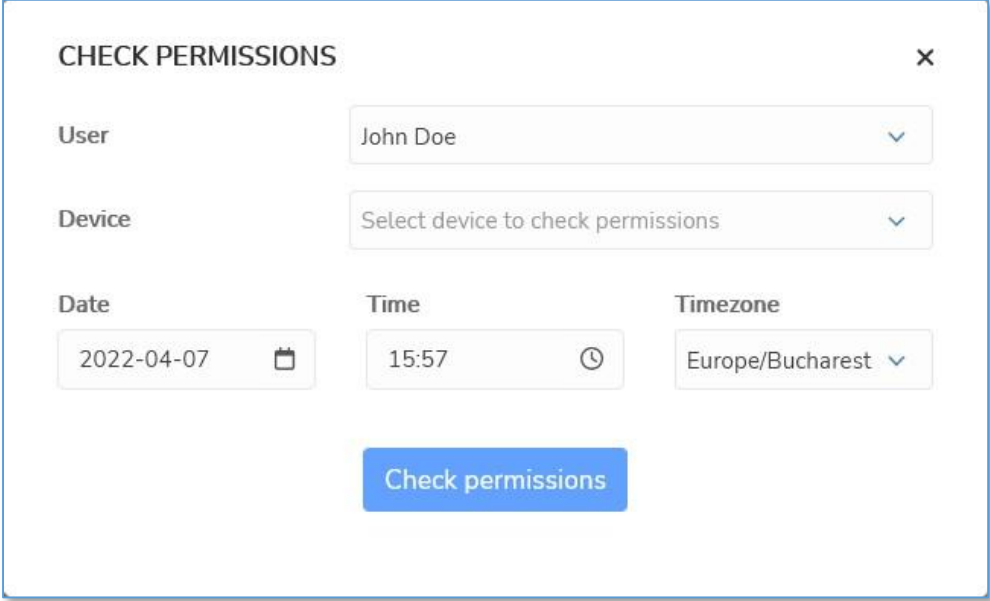
To verify the permissions of a user on a certain device, use **Check permissions**.

1. Click on the **Check permissions** button. It is available in different areas of the **Portal** (Role assignments, Device view, User view).

John Doe




## 2. Select the User and the Device.


A dialog box titled "CHECK PERMISSIONS" with a close button (X) in the top right corner. It contains three main sections: "User" with a dropdown menu showing "John Doe"; "Device" with a dropdown menu showing "Select device to check permissions"; and a row of three fields: "Date" with a date picker showing "2022-04-07", "Time" with a time picker showing "15:57", and "Timezone" with a dropdown menu showing "Europe/Bucharest". At the bottom center is a blue button labeled "Check permissions".

**CHECK PERMISSIONS** ×

User  ▼

Device  ▼

Date  

Time  

Timezone  ▼

**Check permissions**

3. Since permissions can change in time due to existing schedules applied on the Role Assignments, you can specify a date to check for the permissions.
4. Specify the time for the permissions.
5. Specify the **Timezone** for the permissions.

6. To view the granted permissions, click on the **Check permissions** button. This provides an overview of the exact permissions of the User on the Device, plus an overview of the Role assignments that involve both the User groups and the Device.

Granted permissions for user  
time)
on device
valid at 2022-04-07, 15:57 (Europe/Bucharest)

Remote control

User details

Username

Device details

Hostname

Permissions

Remote session

View remote screen

Use keyboard and mouse

Lock keyboard and mouse

Blank the screen

Transfer clipboard

Execute command

Yes

Yes

Yes

Yes

Yes

Yes

## 4.5 Downloads - using Deployment Packages

The deployment package represents a way of enrolling the devices into the **Portal**. The deployment package describes among other things the interval in which the **Host** can be installed, for how many installations or what device group belongs to on enrollment.

Prerequisites for deployment packages:

- Windows **Host** running version 12.65 or later
- Linux & macOS **Host** version 12.75 or later

For versions earlier than the above, refer to the [Role assignments](#) sub-chapter on how to enroll them.

The **Manage > Downloads** tab allows the management of deployment packages.

**NOTE:** Account administrators or higher can manage deployment packages.

### 4.5.1 Create a deployment package

To create a deployment package, click on the **Add deployment package** button in the upper-right corner of the Deployment Packages page. The **Add deployment package** window is displayed.

Specify the deployment package details.

Setting	Description
Name	The name of the deployment package.
Description	Optional description of the deployment package.
Valid from	The <b>Host</b> can be installed using this <b>Enrollment key</b> only when starting with this date (the time is UTC based).
Valid to	The <b>Host</b> can be installed using this <b>Enrollment key</b> only before this date (the time is UTC based). If no date is

Setting	Description
	selected, the enrollment key has no expiration date.
Number of devices	The number of devices, which can be enrolled using this <b>Enrollment key</b> .
Package status	Indicates whether the <b>Enrollment key</b> can be used or not. If disabled, new device enrollments do not work. Already enrolled devices continue to work.
License key	This is the license key that is applied to the <b>Host</b> . If empty, the <b>Host</b> is set to <b>Trial mode</b> . If the <b>Trial mode</b> expired, the <b>Host</b> converts to a <b>Portal only</b> mode, which allows only the <b>Portal</b> communication profile (only works with a <b>Portal</b> account).
Move to device group	The group to which the device automatically belongs to on enrollment.
Enrollment state	Specify if an administrator is required to review the status of the device ( <b>Pending</b> ) or not ( <b>Enrolled</b> ) before the device is enrolled. Check <a href="#">Pending state</a> for how to enroll pending devices.

Once you've specified all the necessary details, click on the **Save** button. The deployment package is created. Upon creation, a unique **Enrollment key** and **Online installers** are generated.

The screenshot displays the Netop Portal interface. On the left is a dark sidebar with the 'NETOP' logo and a navigation menu including Dashboard, ACCESS (My sessions, My devices, My mobile devices), MANAGE (Users, Devices, Groups, Applications, Roles, Role assignments), Downloads (highlighted), SECURITY (Account security, Authentication), and a footer with Netop logo and contact information.

The main content area is titled 'DOWNLOADS' and shows a 'new test' package. At the top right of this section are buttons for 'Contact Netop', 'Purchase', and status indicators: 'Users: 1 / 5', 'OnDemand users: 1 / 2', and 'Devices: 44 / 50'. Below these are 'Edit', 'Upload', and 'Revoke' buttons.

The 'new test' package details are shown in a card format:

- Download installers:** A section with links for 'Download online installer' (preconfigured with account information), 'Download offline installer (.msi file. Additional info on mass deployment here)', and 'To download the offline installer for Windows XP/Vista, click here'. A 'System requirements' link is also present.
- macOS:** A dropdown menu currently showing 'macOS'.
- Linux:** A dropdown menu currently showing 'Linux'.
- Send installer to another user:** A section with 'Copy link' and 'Send link' options.
- Package details:** A table showing:
 

Name	new test
Status	Active
Description	-

To view the enrollment key, from the Deployment packages list, click on the name of the deployment package.

## 4.5.2 Download and install the Host using default configuration

When a deployment package is created, an online installer is also generated. The online installer uses a default configuration for setting up the latest version of the Windows **Host**. When installing the **Host** using an online installer, an available internet connection is necessary as the files are retrieved from online. You can find offline installers for all the supported platforms in the **Deployment Package** details page.

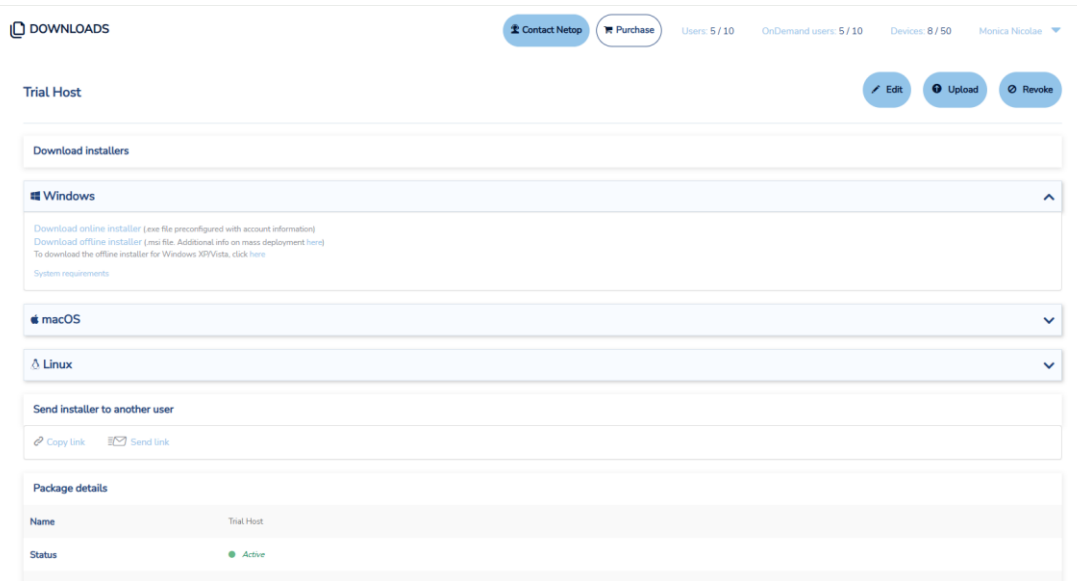
### 4.5.2.1 Download and install the Host using an Online installer (.exe file)

To download and install the **Host** using the online installer, proceed as follows:

1. Go to the **Downloads** tab.
2. Click on the deployment package that you want to install. The **Deployment package details** page is displayed.



- Download the **Online installer** available in the **Download installers** section.



**NOTE:** Do not change the name of the online installer. Otherwise, the deployment package installation is unsuccessful.

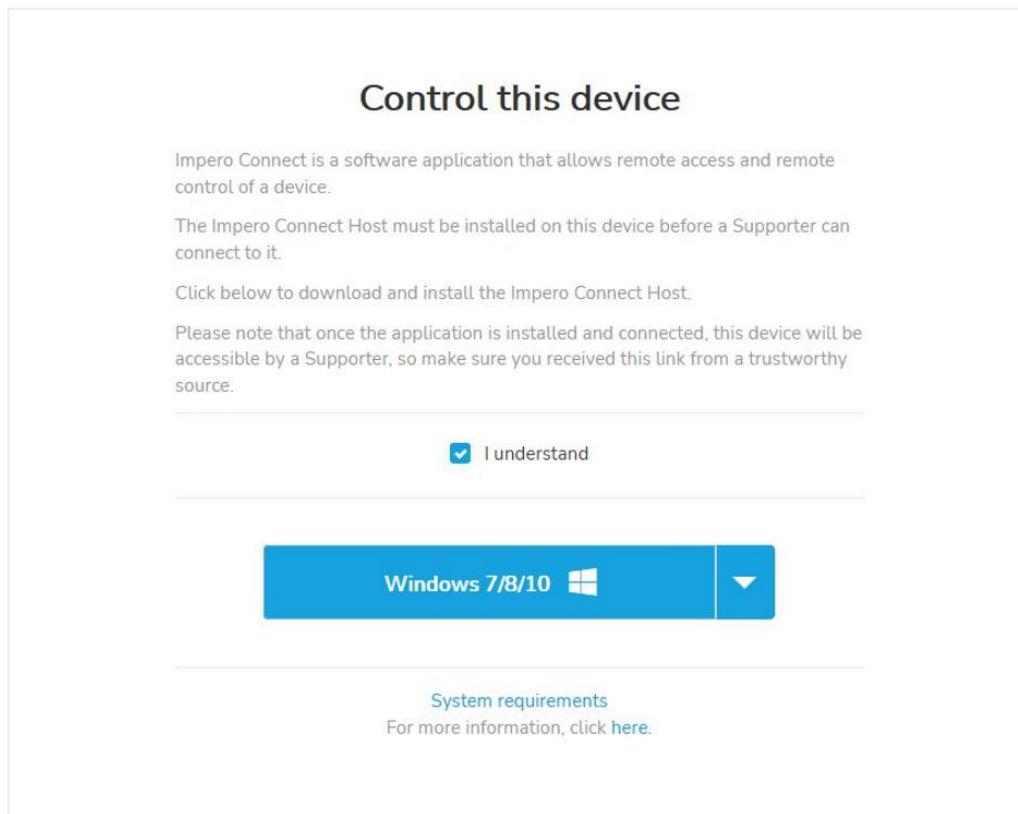
- To install the deployment package, double-click on the downloaded installer (admin rights are necessary on the device).
- Read and accept the **Netop License Agreement**.
- Click on the **Next** button.

The **Host** is installed and automatically configured to connect to the associated **Portal** account. Further configurations are no longer necessary.

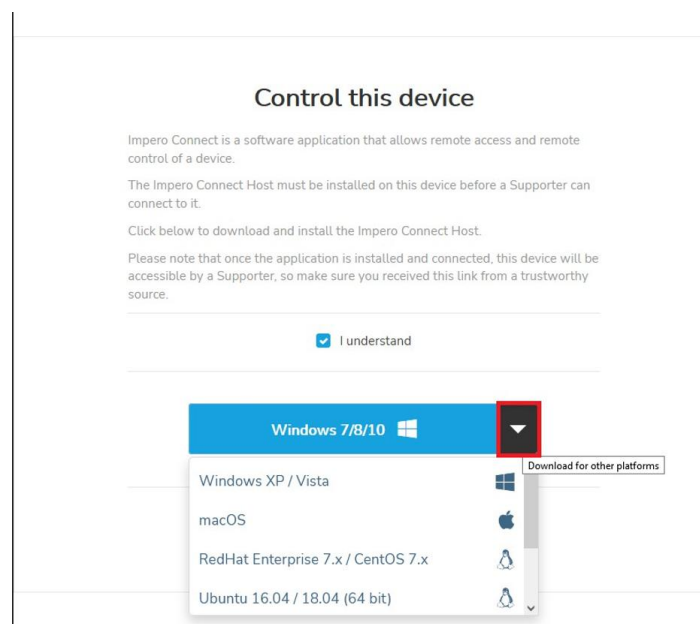
#### 4.5.2.2 Share the Online installer link

- If you would like to share a unique link with the online installer, click on the **Copy link** button to copy it into the clipboard or click on the **Send link** button to open your email client with the link.

- On the target device, the user can open the link. By clicking on **I understand**, the user can download and install the **Host**.



- Users can download the **Host** for a different OS platform, by clicking on the dropdown button near the **Download** button and click on the respective OS button.



4. Install the online installer as described above.

### 4.5.3 Download and install online installer using a custom Host configuration (Windows)

If you want to use a custom **Host** configuration, create the configuration file (**.MST** file). Refer to the [Pack'n'Deploy User's Guide](#) for information on how to create custom **Host** configuration files using **Netop**.

Once you created the custom **Host** configuration file, go to the deployment package details page and click on the **Upload** button. Upload the **.MSI** and the **.MST** files.

UPLOAD CUSTOM HOST

The online installer uses default files and configuration for setting up the Host. If you want to use a custom configuration, upload the files below.  
 More info on how to create the files is available [here](#).  
 On next installation using the online installer, the custom files will be used.  
 Note: If you want to revert to the default files, you will need to create a new deployment package.

Upload new MSI file

(Uploaded on: 2020-04-24 18:11:10)

Upload new MST file

After uploading an **.MSI** or an **.MST** file, the date and time when the file was uploaded are displayed under the corresponding upload buttons. This allows you to easily identify if the deployment package contains a custom **Host** configuration or if the default online installer is used for deployment.

On the next installation using the online installer, the custom files are used.

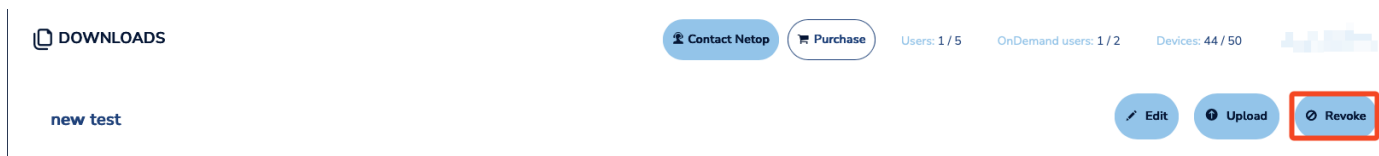
**NOTE:** To revert to the default files, create a new deployment package.

## 4.5.4 Mass deploy the Host (Windows)

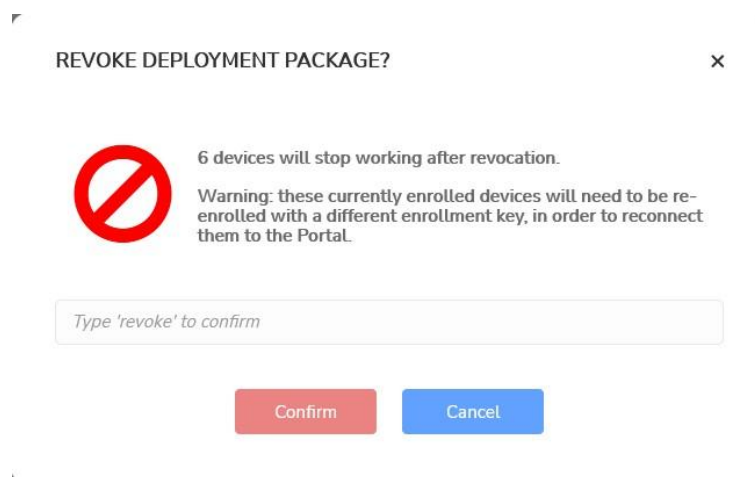
For instructions on how to mass deploy the **Host** on Windows, refer to the [Mass deploy Portal components](#) knowledge base article.

## 4.5.5 Revoke deployment packages

You revoke the deployment packages by clicking on the **Revoke** button in the upper-left corner of the **Deployment package details** page.



The **Revoke Deployment Package** warning prompt is displayed.



Specify "**revoke**" in the "**Type 'revoke' to confirm**" entry field to confirm.

Revoking deployment packages means that:

- You are no longer able to install devices using that enrollment package.
- Devices enrolled using the deployment package, can no longer connect to the **Portal**; another enrollment key is necessary.
- Revoked devices are still displayed in the device list with a state name **Revoked**.

The revoked deployment package is marked with a red sign: 

To re-enroll these devices into the **Portal**, create another deployment package and configure the **Host** on the devices to use the new enrollment key.

## 4.5.6 Remove deployment packages

You can remove deployment packages by clicking on the **Remove** button in the upper-left corner of the Deployment package details page.

Edit

Revoke

Remove

Add deployment package

Results can be filtered using the ▼ on each column

Name	Enrollment state	Valid from	Valid to	Devices	
new test	Enrolled	2024-11-20	-	10	Online installer <input type="checkbox"/>
new test 2	Pending	2024-11-20	-	0	Online installer <input checked="" type="checkbox"/>
Trial Host	Enrolled	2019-11-21	-	34	Online installer <input type="checkbox"/>

Show Rows 10
Go to page 1
1 - 3 of 3

**NOTE:** You can only remove deployment packages that have no devices associated or which are revoked.

## 4.5.7 Pending state

For devices in the **Pending** state, go to the **Manage > Devices** tab. Identify the **Pending** device and enroll it by clicking on the **Enroll** button.

DESKTOP-3TGGLT7	Enroll	Add to favorites	Check permissions	Edit	Remove
-----------------	--------	------------------	-------------------	------	--------

## 5 Security

This section provides various options for overall account security.

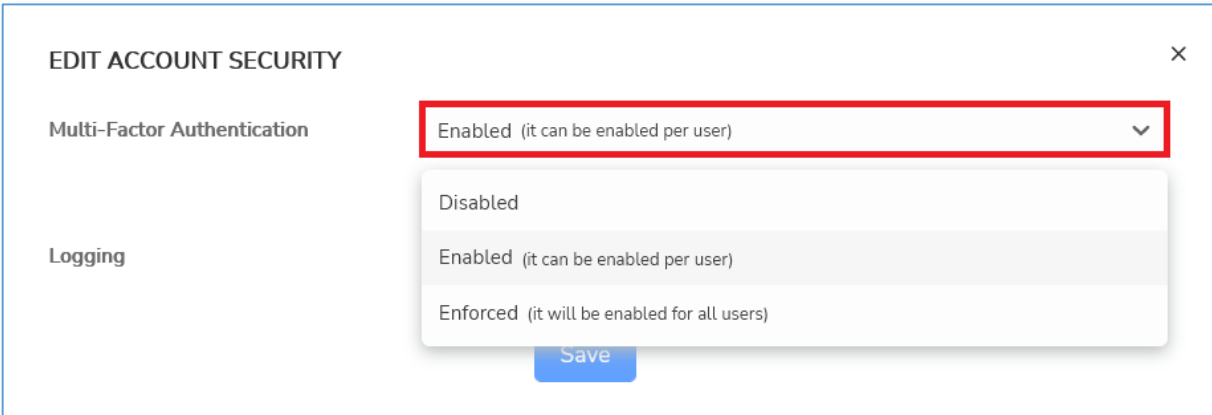
### 5.1 Enable Multi-Factor authentication

The authentication can be configured to use two factors: the first authentication factor is the username and password (something the user knows), the second factor is a passcode received by email (something the user has).

To manage the account security, administrator rights or higher are necessary. You have the option to enable MFA per user or to enforce the option to all users. When the **Enforced** option is selected, users cannot modify the Multi-Factor authentication settings for themselves or other users.

To enable or enforce the multi-factor authentication, proceed as follows:

1. Go to **Security** > **Account security** area and click on the **Edit** button.
2. Click on the **Multi-factor authentication** dropdown field.
3. Select **Enabled** or **Enforced**.
4. Click on the **Save** button.



The screenshot shows a dialog box titled "EDIT ACCOUNT SECURITY" with a close button (X) in the top right corner. Inside the dialog, there are two sections: "Multi-Factor Authentication" and "Logging". The "Multi-Factor Authentication" section has a dropdown menu that is currently open, showing three options: "Disabled", "Enabled (it can be enabled per user)" (which is highlighted with a red border), and "Enforced (it will be enabled for all users)". Below the dropdown menu is a blue "Save" button.

Once email-based multi-factor authentication is enabled for your account, you can enable the use of multi-factor authentication on individual users.

When editing users, you can now enable multi-factor authentication as well.

Go to the **Manage > Users** tab, select the desired user and in the upper-left corner of the page, click on the **Edit** button.

**EDIT USER** [X]

First name: John

Last name: Doe

Email: [Empty field]

Username: [Disabled field]

User type: Account Administrator [Dropdown arrow]

[Read more on user types here](#)

Group (Optional): [Dropdown arrow]

Default remote control action: Control through browser [Dropdown arrow]

☒ Enabled (This user is enabled)

☒ OnDemand Sessions (OnDemand Sessions are enabled for this user)

☐ Multi-Factor Authentication (Email MFA disabled)

**Save**

Enable **multi-factor authentication** and click on the **Save** button.

#### NOTE:

- User credentials are used to configure the communication profile on both **Guest** and **Host**. For security reasons, we strongly recommend creating dedicated users assigned to enroll devices in the **Portal**.
- If you enable multi-factor authentication for a user, make sure that those user credentials are not used in the definition of the **Guest** or **Host** communication profile (**Portal** communication device). If credentials from a user with multi-factor authentication enabled are used, the **Guest** or the **Host** are not able to make a connection to the **Portal**.
- Starting with Netop version 12.65 (on Windows 7 and later) and **Netop** version 12.75 (Linux & macOS) enrollment keys are

used for the **Portal** communication profile. Therefore, the above note does not apply anymore.

## 5.2 Authentication

The **Portal** provides the following authentication methods:

- Internal (username & password saved in the **Portal** database)
- **ADFS** (Active Directory Federation Services)/**Azure AD**
- **LDAP** (Lightweight Directory Access Protocol)

### 5.2.1 LDAP authentication

With the integration to the Lightweight Directory Access Protocol (**LDAP**), the **Portal** provides another way of integration into the company's central user directory. This enables administrators to manage the users and users' permissions from only one place – the company's user directory. The integration with **LDAP** is done in such a manner that no passwords are stored in the **Portal** – the credentials are checked on every login.

**NOTE:** Only account administrators or higher can manage **Authentication**.

#### 5.2.1.1 Enabling LDAP authentication

To enable **LDAP** authentication, proceed as follows:

1. Go to the **Security > Authentication** tab.
2. In the upper-left corner of the page click on the **Add LDAP** button. The **Add LDAP authentication method** page is displayed.



3. Enable **LDAP** authentication.
4. Specify the information for setting up the **LDAP** connection.



5. To save the authentication settings, click on the **Save LDAP authentication method** button.

Group schema settings

Additional Group DN (Optional)	<input type="text"/>
Group Search Filter - for instance: (objectClass=group)	<input type="text"/>
Group Browse Filter - for instance: (!(objectClass=group)) (objectClass=organizationalUnit)	<input type="text"/>
Group Attribute - for instance: group	<input type="text"/>
Group members Attribute - for instance: member	<input type="text"/>

More information on how to securely integrate with LDAP is available [here](#)

**Save LDAP authentication method** **Cancel**

Once you enable the **LDAP** authentication, you can [import LDAP groups](#) in the [create role assignments](#) for each of the groups to associate with the corresponding role.

**NOTE:** When logging in using **LDAP** credentials, make sure to log in using the domain `identifier\username`. There can be multiple **LDAP** authentication methods added.

## 5.2.2 ADFS/Azure AD authentication

### 5.2.2.1 Enabling ADFS/Azure AD authentication

To enable **ADFS/Azure AD** authentication, proceed as follows:

1. Go to the **Security > Authentication** tab.
2. In the upper-left corner of the page, click on the **Add ADFS/Azure AD** button. The **Add authentication method** page is displayed.



3. Fill in the information required for the **ADFS/Azure AD** authentication method (for more information, refer to the following [knowledge base article](#)).
4. To test the configuration, click on the **Test configuration** button.

5. To add the **ADFS/Azure AD** authentication method, click on the **Save** button.

**EDIT ADFS / AZURE AD**

More information on how to integrate with ADFS and Azure AD is available [here](#).

**Name**: ADFS TEST

**Enabled** (This authentication method is enabled)

**Authentication type**: ADFS  
The authentication type will be automatically filled in once you upload the FederationMetadata.xml file.

**Domain identifier**: test1  
This will be used when logging in (domain identifier/username)

**IdP**:  
Identity Provider's (IdP) URL

**Group (Optional)**:  
The user will become a member of this group on first login.

**ADFS / Azure AD FederationMetadata.xml file**:  
Browse

**Certificate valid from**: 2020-01-10T10:03:11.000Z

**Certificate valid to**: 2021-01-09T10:03:11.000Z

**Application ID (Optional)**:  
Fill in the Application ID and Client secret to use Azure AD groups.

**Client secret (Optional)**:

Test configuration

**Save**

**NOTE:** When logging in using **ADFS/Azure AD** credentials, verify that you log in using the domain **identifier\username**. There can be multiple **ADFS/Azure AD** authentication methods added.

For more information about the **ADFS/Azure AD** feature and integration with the **Portal**, refer to the following knowledge base [article](#).

## 5.3 Enable logging

The **Portal** offers thorough audit logs (audit trails).

The audit logs contain the following security-relevant data:

- The date
- Time and activity of each user including sign-in events
- User creation and removal
- Role assignments
- Account configuration
- Remote control sessions
- File transfers and others

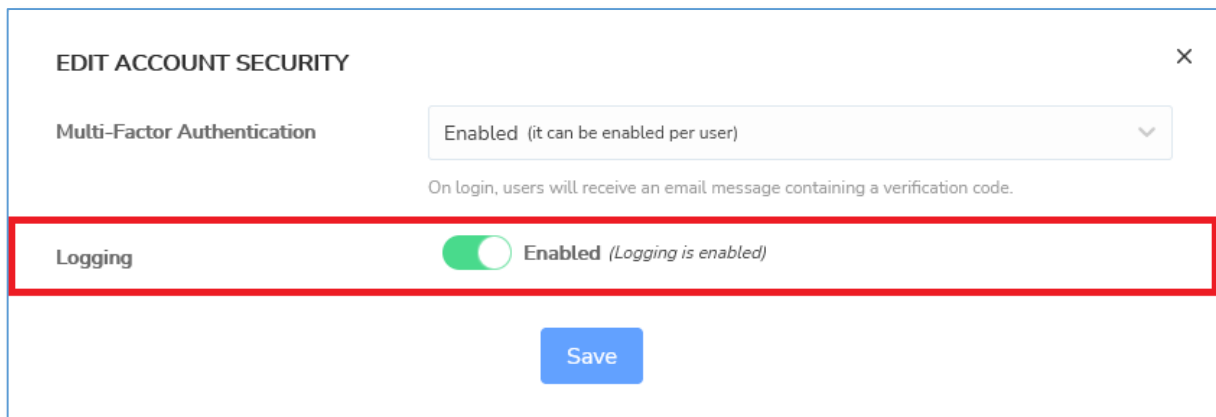
**NOTE:** The audit log data is stored for a period of six months. This means that the data that exceeds the fixed period is automatically removed. This is done in a chronological order – older data is removed and the more recent is maintained.

Audit logs help you monitor data for any potential security breaches or internal misuses of information. Moreover, the audit logs available in the **Portal** provide an insight into how various parties are using the **Portal**.

**NOTE:** Audit logs containing information regarding connections between a **Guest** or **Control through browser** option and a **Host** are sent only by Windows **Hosts** version 12.67 or later.

### 5.3.1 Enabling audit logging

Audit logging is enabled by default within the **Portal**. If for any reason it is disabled for your account, go to the **Security > Account security** tab, click on the **Edit** button and enable it. To manage audit logging, administrator or higher rights are required.



EDIT ACCOUNT SECURITY

Multi-Factor Authentication: Enabled (it can be enabled per user)

On login, users will receive an email message containing a verification code.

Logging: ☒ Enabled (Logging is enabled)

Save

### 5.3.2 Retrieve Audit Logs

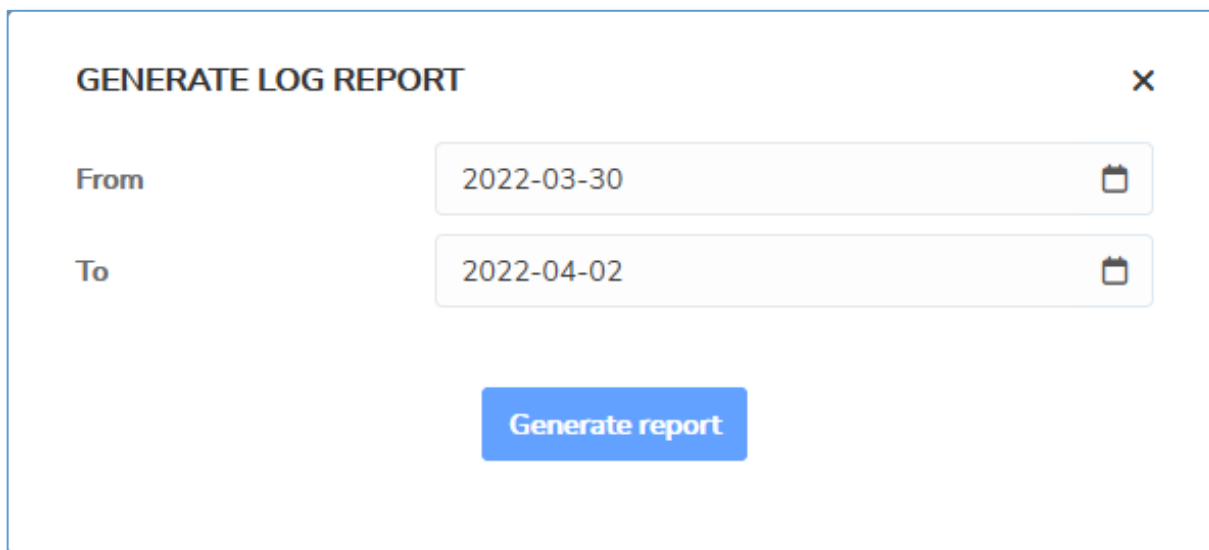
The audit logs provide valuable information about the users' activity in the **Portal**.

**NOTE:** Account managers or higher can view and generate log reports. Account administrator or higher is required to delete a log report.


To retrieve the audit logs, go to the **Security > Logs** tab and click on the **Generate report** button.




Select the date interval:



**GENERATE LOG REPORT** ×

From 2022-03-30 

To 2022-04-02 

**Generate report**

Click on the **Generate report** button. A new report is created as a \*.csv file containing all events logged within the selected date interval and it is displayed as a new log entry in the **Logs** page.

Once you generate a log report, from the **Status** column, click on the corresponding **Download** link. On download, choose to save the report on the disk.

To make the report readable, open a blank workbook in Microsoft Excel and import the \*.csv file by connecting to it (from the **Data** tab and from the **Get and Transform Data** toolbar, click on **From Text/CSV**). Make sure that you use the comma (,) as a column delimiter and the apostrophe (') as the text qualifier.

For more information on understanding the report, refer to the following knowledge base [article](#).

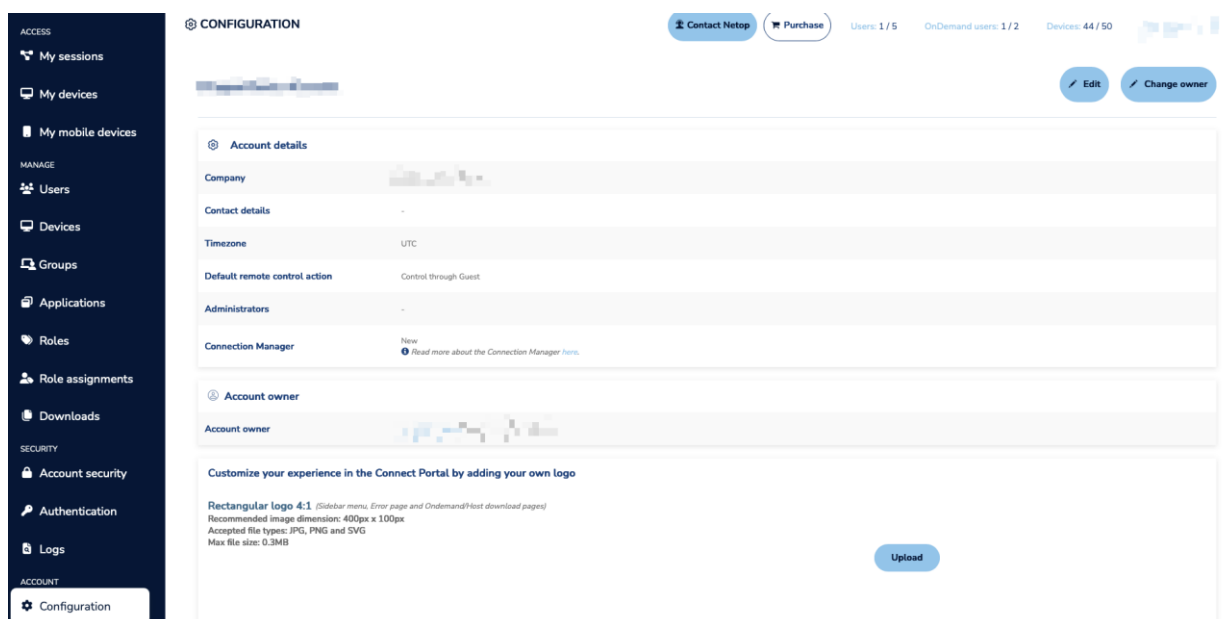
## 6 Account Configuration

The **Account > Configuration** tab allows the configuration of the Account details and the Account owner as well as modify the **Portal** logo. Only an **Account Owner** user type can manage and modify the account configuration.

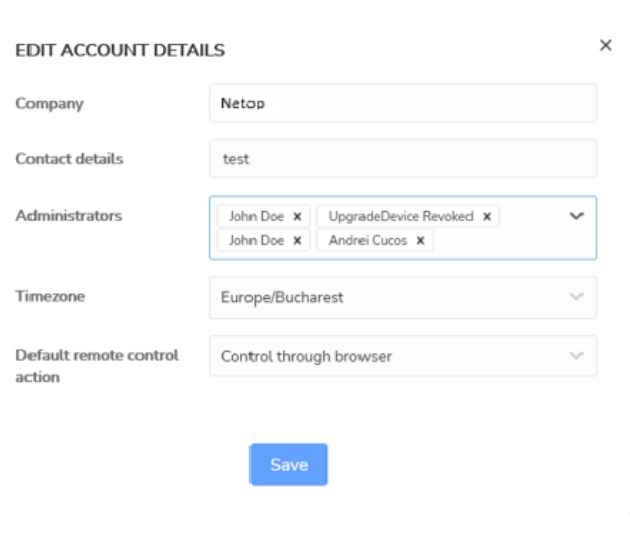
### 6.1 Account details

The account details contain information on the actual **Portal** account such as:

- The company name
- The contact details
- The account administrators
- The Timezone
- The default remote control action
- The Connection Manager



To edit them, click on the **Edit** button.



EDIT ACCOUNT DETAILS

Company: Netop

Contact details: test

Administrators: John Doe x UpgradeDevice Revoked x John Doe x Andrei Cucos x

Timezone: Europe/Bucharest

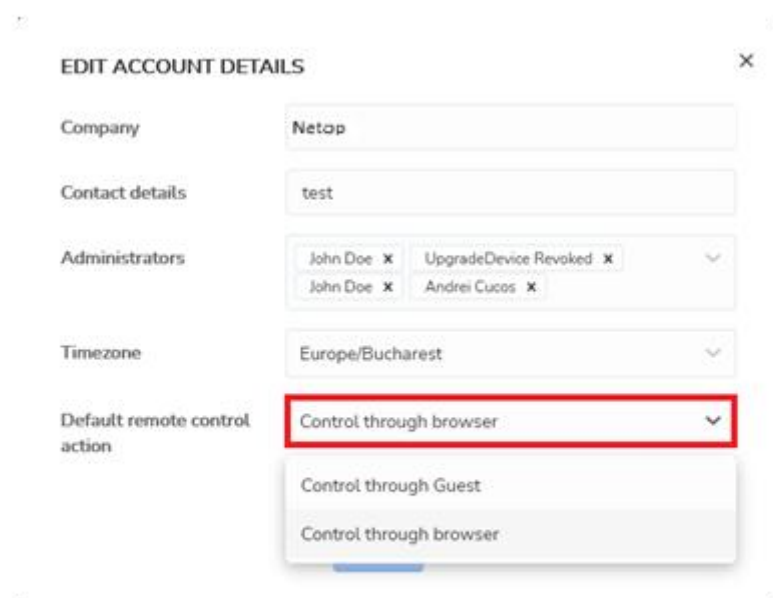
Default remote control action: Control through browser

Save

To save your changes, click on the **Save** button.

To set up the default remote control action for all the users, proceed as follows:

1. Click on the **Default remote control action** drop-down menu.



EDIT ACCOUNT DETAILS

Company: Netop

Contact details: test

Administrators: John Doe x UpgradeDevice Revoked x John Doe x Andrei Cucos x

Timezone: Europe/Bucharest

Default remote control action: Control through browser

Control through Guest

Control through browser

2. Select the default remote control action according to your needs.

3. Click on the **Save** button to save your changes.

#### EDIT ACCOUNT DETAILS

Company	Netop
Contact details	test
Administrators	<div>John Doe ✕ UpgradeDevice Revoked ✕</div> <div>John Doe ✕ Andrei Cucos ✕</div>
Timezone	Europe/Bucharest
Default remote control action	Control through Guest

Save

## 6.2 Change the account owner

To change the **Account Owner**, proceed as follows:

1. Login to the **Portal** with an **Account Owner**.
2. Go to the **Account > Configuration** tab.
3. Click on the **Change owner** button in the top-right of the screen.

The screenshot displays the 'CONFIGURATION' page in the Netop Portal. The left sidebar contains navigation links under 'ACCESS', 'MANAGE', 'SECURITY', and 'ACCOUNT'. The 'ACCOUNT' section is active, showing 'Configuration'. The main content area is titled 'CONFIGURATION' and includes a header with 'Contact Netop', 'Purchase', and user statistics. Below the header, there are two main sections: 'Account details' and 'Account owner'. The 'Account details' section shows fields for Company, Contact details, Timezone, Default remote control action, Administrators, and Connection Manager. The 'Account owner' section shows the current account owner and a section for adding a custom logo. In the top-right corner of the 'Account owner' section, the 'Change owner' button is highlighted with a red box.



4. Select a user to become the new Account owner and click on the **Save** button.

**CHANGE ACCOUNT OWNER** ×

**ARE YOU SURE YOU WANT TO CHANGE THE ACCOUNT OWNER?**

Once you hit save, you will not be an Account owner any longer.  
You will be immediately demoted to an Account administrator. You will also be required to re-login.

Select Account Owner

**Save**

## 6.3 Change Portal logo

As the Account Owner you can modify the logo of the Connect Portal. This can be achieved by going to the Configuration tab.

Customize your experience in the Connect Portal by adding your own logo

**Rectangular logo 4:1** *(Sidebar menu, Error page and Ondemand/Host download pages)*  
Recommended image dimension: 400px x 100px  
Accepted file types: JPG, PNG and SVG  
Max file size: 0.3MB

**Upload**

**Square logo 1:1** *(Collapsed Sidebar menu and Ondemand client)*  
Recommended image dimension: 256px x 256px  
Accepted file types: JPG, PNG and SVG  
Max file size: 0.3MB

**Upload**

Click on the **Upload** button to upload your custom logo.

## 7 How to contact the Netop support team

The **Portal** allows users to directly contact a Netop representative in order to receive help as fast as possible.

To contact the **Netop** support team, proceed as follows:

1. Click on the **Contact Netop** button at the top of the page.

The screenshot shows the Netop Portal Dashboard. At the top right, there is a navigation bar with a 'Contact Netop' button highlighted by a red box. Other buttons include 'Purchase'. Below the navigation bar, the dashboard is divided into several sections: 'Devices & Users' (showing device and user statistics), 'Account info' (showing company, expiration date, and owner), 'Documentation' (with links to guides), 'Activity' (showing user activity), and 'Recent updates' (showing system updates).

2. This will open the **Support Portal** where you can **Submit a request**.

The screenshot shows the Netop Knowledge Base Support Portal. At the top right, there is a 'Submit a request' button highlighted by a red box. Below the header, there is a large banner image of a city skyline at night. In the center of the banner is a search bar with the text 'Search'. Below the banner, there are two main sections: 'Netop Support' (Resources for Netop troubleshooting and support) and 'Documentation & Downloads' (Netop manuals, guides, and downloads).

### Promoted articles

[Whitelisting Applications for Netop Portal](#)

[Download Netop for Windows, Linux and Mac](#)

[Netop Manuals & Guides](#)