NETOP PORTAL - PERMISSIONS

NETOP®
RemoteControl
Secure Remote Management and Support

Version 1.2

NETOP
RemoteControl

Contents

1 Description

The Netop Portal governs role-based access for Users connecting to Devices (Hosts).

Role-based access is managed with the help of Role assignments. A Role assignment contains the following:

- Role (set of permissions)
- User group
- Device group

Based on the Role assignments, the following will happen:

- A group of users is given access to a certain group of devices
- On every connection from the User group to the Device group, the **Role** (permissions) will be applied
- The device is visible under the **My devices** area in the Portal (The devices are visible under **My devices** only if there is an active **Role assignment** that include both the **Device group** containing the device and the **User group** containing the logged in user with a **Role** different than **Add devices**).

Pre-requisites: The Hosts needs to be configured to use the **Netop Portal access rights** (this is set by default when using the Online installer).

2 How to set up

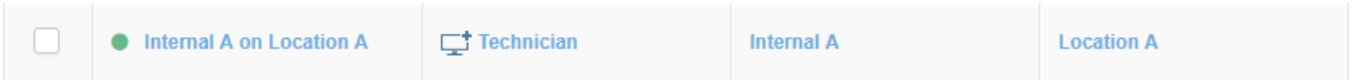
2.1 Check initial setup

When the account is created, there is a default Role assignment that provides **Everyone** (all users in the account) access to **Everything** (all devices) with a Role different than Add devices.

Although this makes it easier for the initial setup of devices and users, **it is not recommended** to have a generic role assignment like this, but rather a more targeted one clearly specifying the users, devices and permissions. So please make sure you edit this one or remove it and create new ones as seen below.

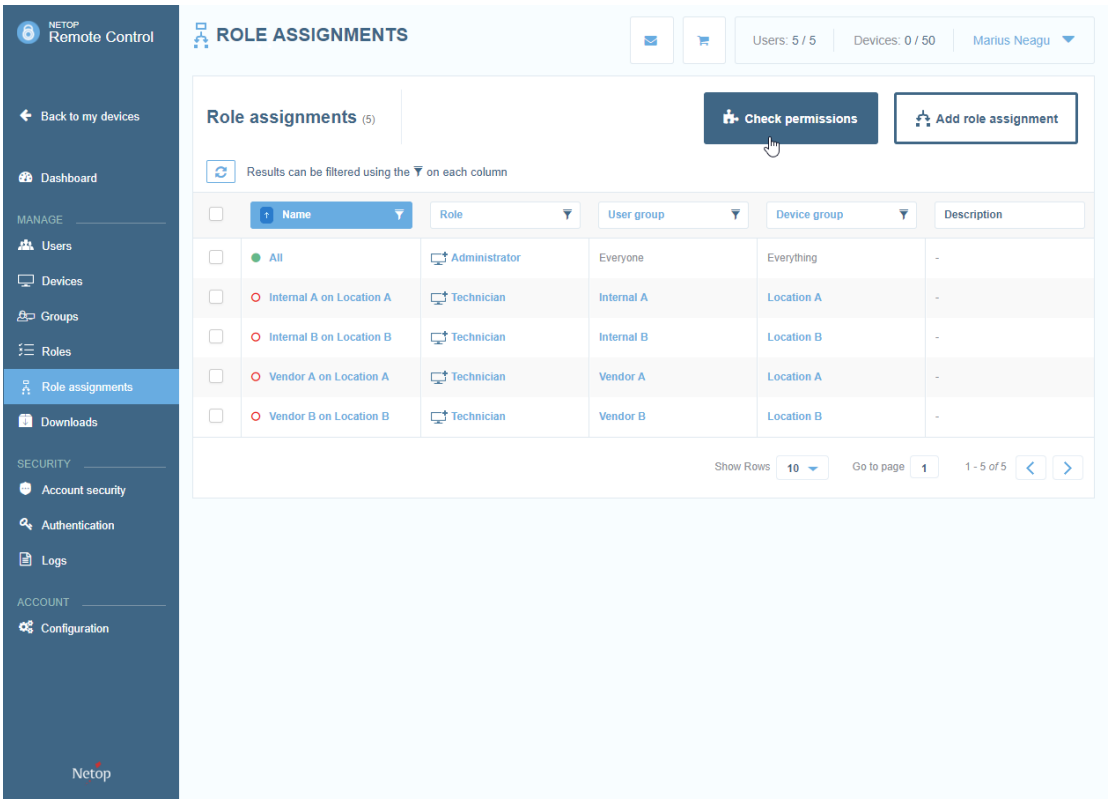
2.2 Create role assignments

Create a role assignment for each specific **User group** that needs to reach a **Device group**, with the desired Role. A full list of available roles and their description can be found in the Roles section of the Portal. More information on managing Role assignments is available in the Netop Remote Control Portal User's Guide.



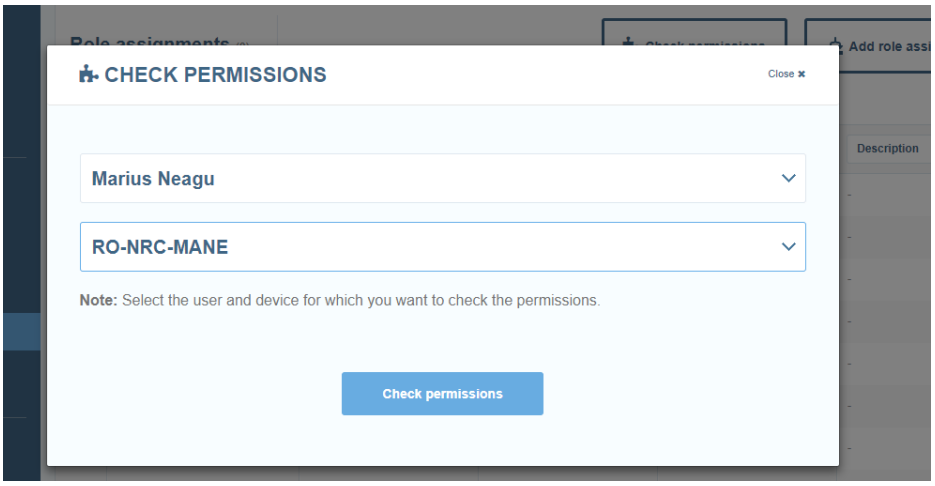
2.3 Verify effective permissions

Click the Check permissions button

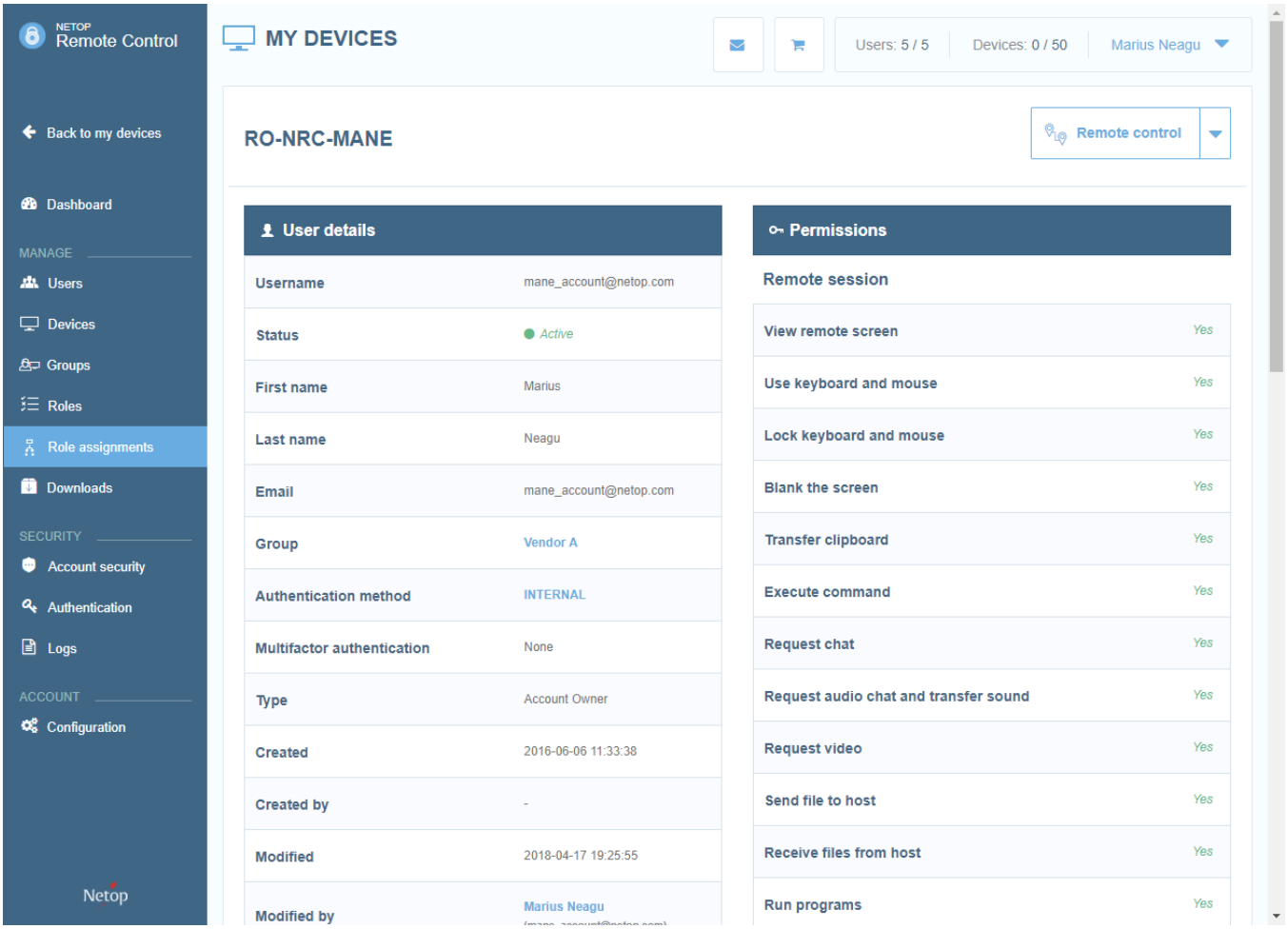


2.3.1 Positive scenario

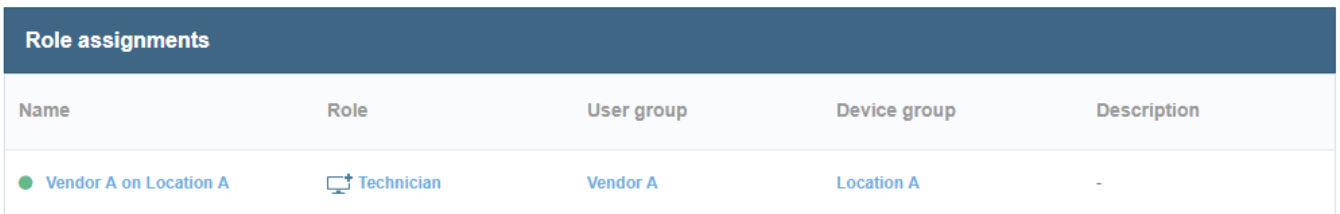
- Choose the user that you want to verify and choose a device that the **user should have access to** and click **Check permissions.**



- The Permissions in the Permissions column should indicate the sum of all permissions from all **Roles** that were used in the **Role assignment(s)**.



- The Role assignments that are contributing to these effective permissions are displayed at the bottom (these include **User groups** containing the **User** and **Device groups** containing the **Device**).



Note: This list will also display the disabled Role assignments. They do not however influence the list of effective permissions.

2.3.2 Negative scenario

- Same steps as in the positive scenario, except that you should choose the same user that you want to verify and a device that the **user should NOT have access to** and click **Check permissions.**
- The result should show that the user does not have any permission and that there is no active Role assignment.

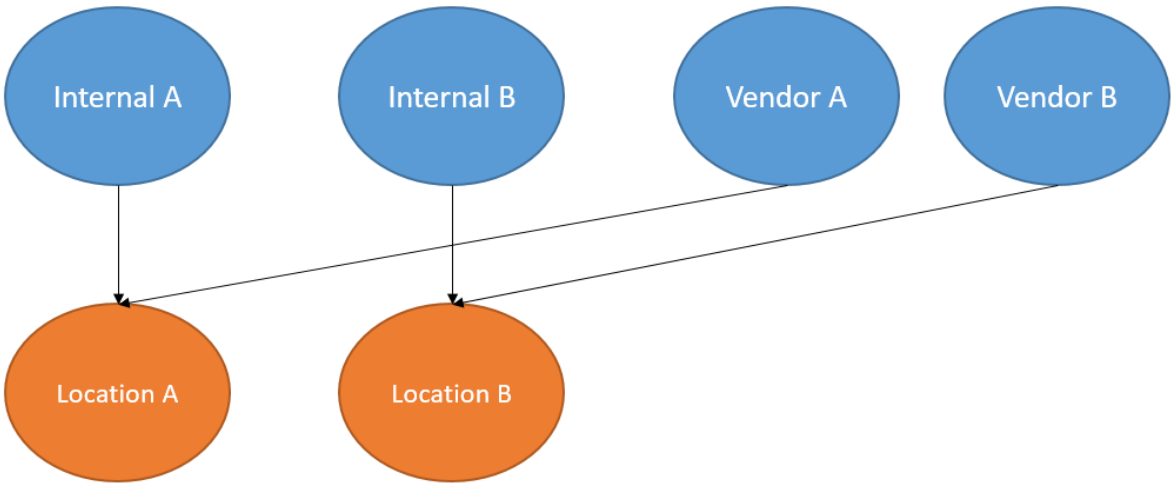
3 Sample scenario

3.1 Description

- There are two branches for a company (2 groups of Devices – **Location A** and **Location B**)
- On every branch, a local team (**Internal A** or **Internal B**) needs to have access to the Devices from the corresponding branch.
- External vendors (**Vendor A** and **Vendor B**) need to have access to the branches.
- The type of access for both internal users and external vendors users should be that of **Technician** (remote control, inventory and chat)

The above translates into:

- **Internal users from Branch A** should have **Technician** access to **Devices from Branch A**
- **Internal users from Branch B** should have **Technician** access to **Devices from Branch B**
- **Vendor A** should have **Technician** access to **Devices from Branch A**
- **Vendor B** should have **Technician** access to **Devices from Branch B**

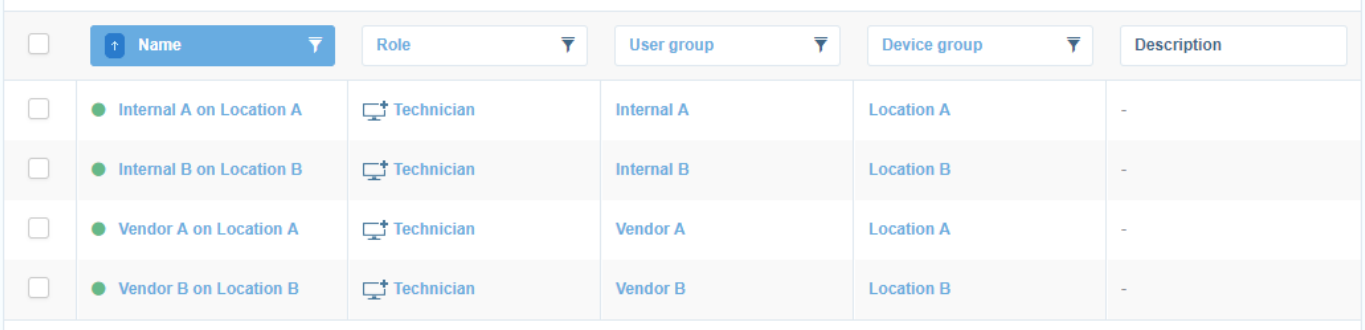


3.2 Set up steps

1. Create the corresponding user and device groups:

- User groups: **Internal A**, **Internal B**, **Vendor A** and **Vendor B**
- Device groups: **Location A** and **Location B**

2. Create the users and associate them to the corresponding group
3. Create a deployment package for each of the two device groups. The difference between the two devices will be the **On enrollment** > **Move to device group** (this will place the device in the specific device group – **Location A** or **Location B**).
4. Install the Hosts in the corresponding location (On device enrollment into the Portal, it will create the device and will associate it with the corresponding device group into the Portal).
5. Create the Role assignments



Name	Role	User group	Device group	Description
Internal A on Location A	Technician	Internal A	Location A	-
Internal B on Location B	Technician	Internal B	Location B	-
Vendor A on Location A	Technician	Vendor A	Location A	-
Vendor B on Location B	Technician	Vendor B	Location B	-

6. Make sure that everything is fine by **Checking permissions**:
    a. Checking that a user from **Internal A** has the correct permissions to **Location A** devices.
    b. Checking that a user from **Internal A** does not have any permissions on **Location B** devices.
    c. ...