How to create a new role with custom permissions and assign it to users

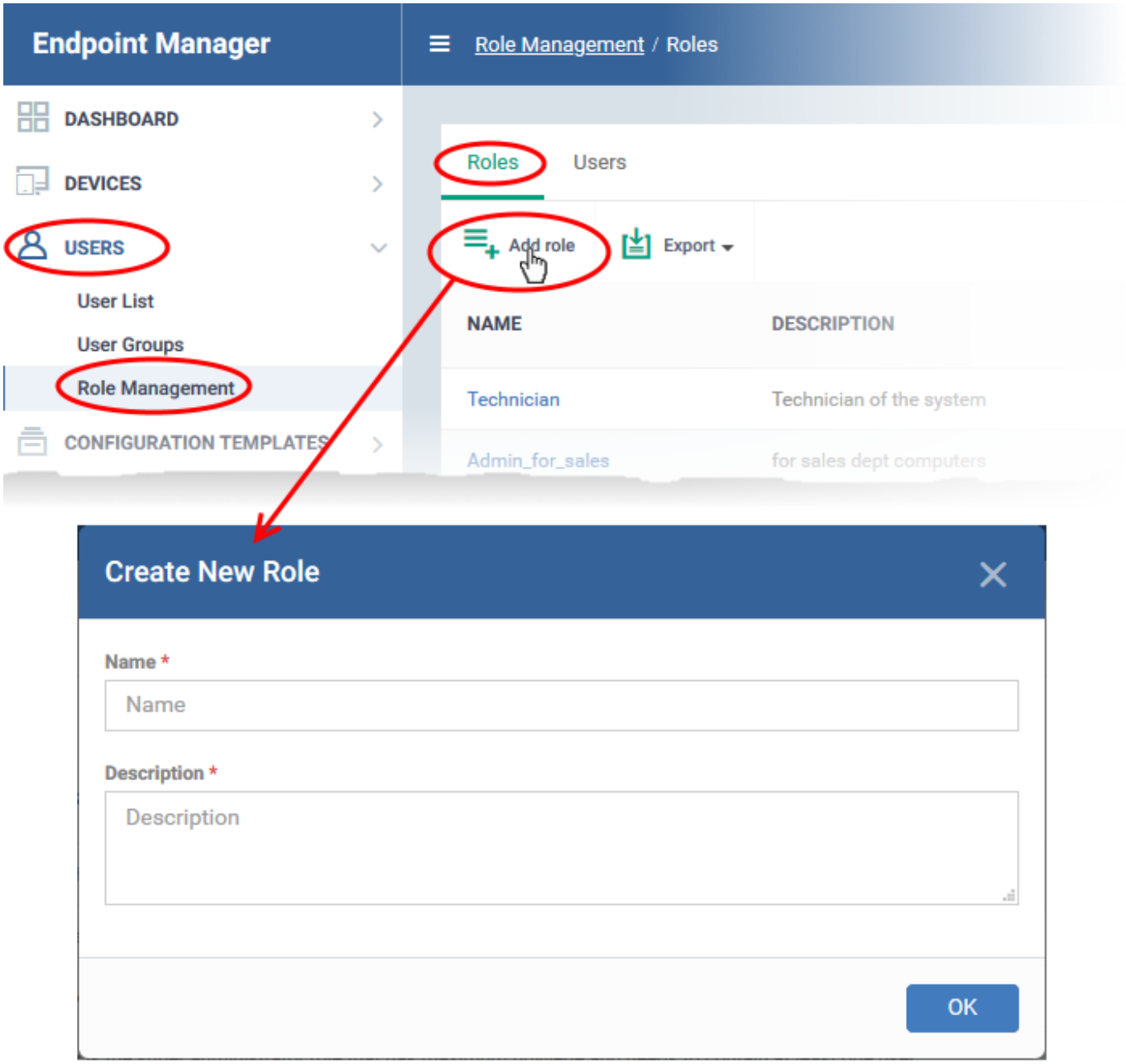
Click 'Users' > 'Role Management'

- User privileges depend on the roles assigned to them. Admins can create custom roles with different access privileges and assign them to users as required. A single user can be assigned to any number of roles.
- You can restrict a role to specific companies and groups. Staff can only manage the devices of companies/groups allowed by their role.
- A user assigned with multiple roles, then user can take access scope settings from the multiple roles.
- Endpoint Manager ships with four roles, 'Account Admin', 'Administrators', 'Technician' and 'Users'.
    - The 'Account Admin' role can be viewed but not edited. The permissions in the other three roles can be modified.
- You can also create roles with read-only privileges. These allow staff to view certain interfaces but not make changes.

Use the links below to jump to the task you need help with:

Add a new role

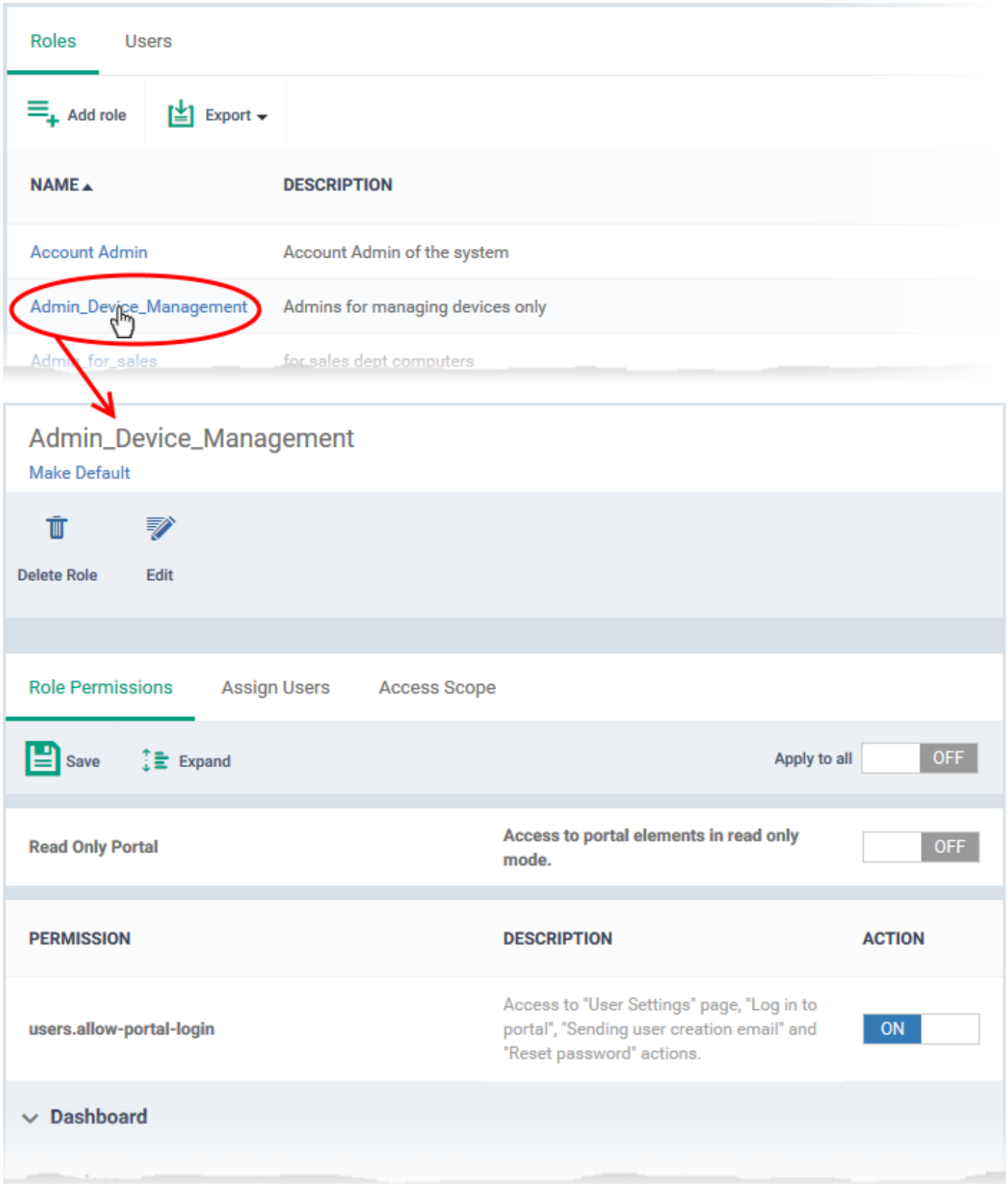
- Log into Xcitium
- Click ‘Applications’ > ‘Endpoint Manager’
- Click 'Users' > 'Role Management'
- Click 'Add Role'



- Create a name and description for the role then click ‘Ok’.

The new role is added to the list in the 'Roles' screen.

- Click on the new role to edit its permissions, assign users, and specify which entities the role is allowed to manage.

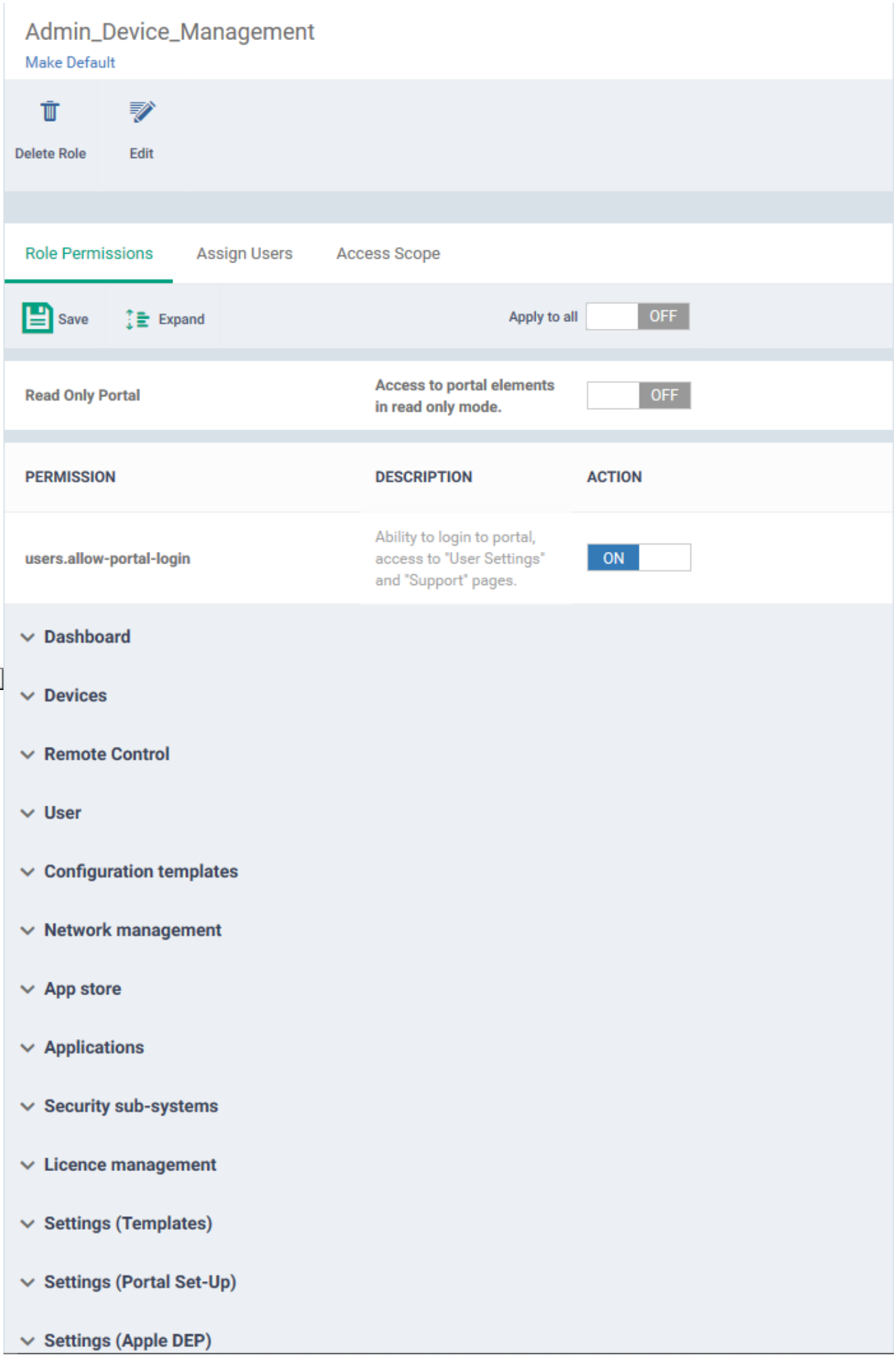


The edit screen has three tabs:

- Role Permissions - Define access rights and privileges for the role
- Assign Users - Select users who should have the role.
- Access Scope - Select which companies and groups can be accessed by role members.

Select access rights and privileges for the role

- Click the 'Role Permissions' tab if it is not open


Admin_Device_Management
Make Default
Delete Role
Edit
Role Permissions
Assign Users
Access Scope
Save
Expand
Apply to all
OFF
Read Only Portal
Access to portal elements in read only mode.
OFF
PERMISSION
DESCRIPTION
ACTION
users.allow-portal-login
Ability to login to portal, access to "User Settings" and "Support" pages.
ON
Dashboard
Devices
Remote Control
User
Configuration templates
Network management
App store
Applications
Security sub-systems
Licence management
Settings (Templates)
Settings (Portal Set-Up)
Settings (Apple DEP)

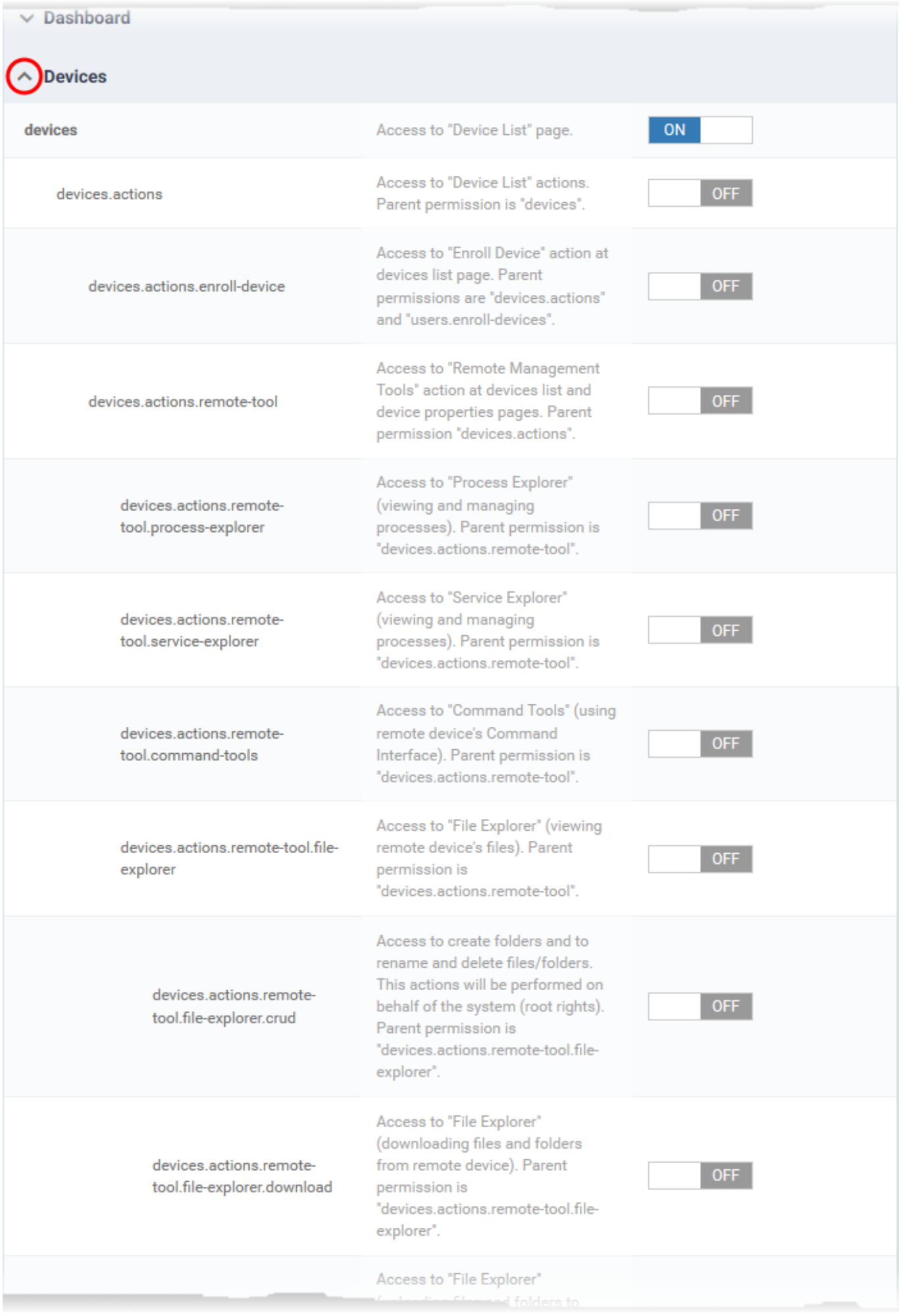
- **Read Only Portal** – Role-members can view areas to which you assign them permission, but cannot make changes.
    - The read-only switch applies to every permission you enable in the list below.
- **Users.allow-portal-login** - Role-members can login to Endpoint Manager (EM). EM sends an account activation mail to users assigned to the role. The user can login to EM and manage as per the permissions you assign below.

Each item in the list lets you choose permissions for a specific area.

- Click the down arrow next to a module name to view its permissions

  OR

- Click 'Expand' at the top to view all permissions

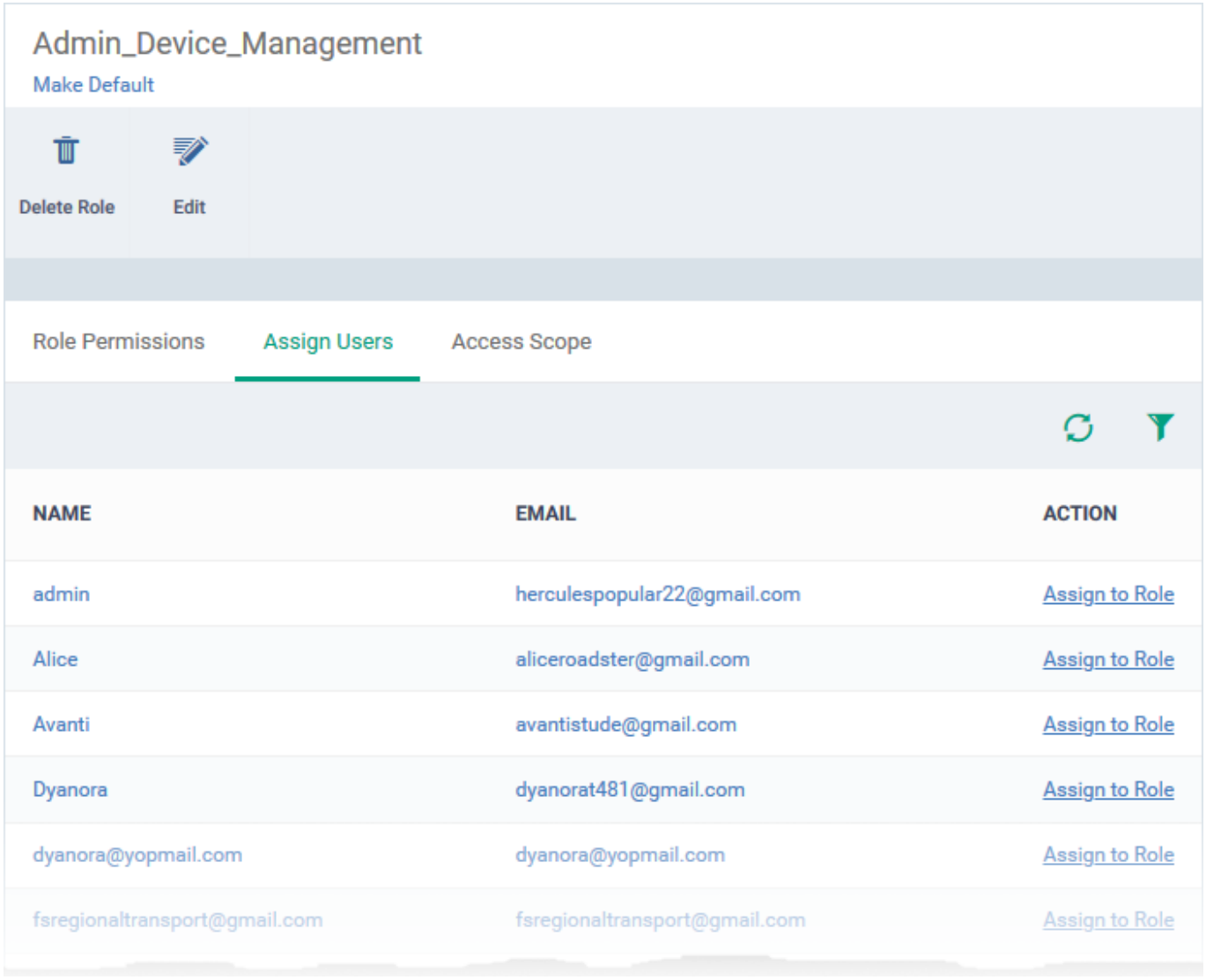

Dashboard
Devices
devices
Access to "Device List" page.
ON
devices.actions
Access to "Device List" actions. Parent permission is "devices".
OFF
devices.actions.enroll-device
Access to "Enroll Device" action at devices list page. Parent permissions are "devices.actions" and "users.enroll-devices".
OFF
devices.actions.remote-tool
Access to "Remote Management Tools" action at devices list and device properties pages. Parent permission "devices.actions".
OFF
devices.actions.remote-tool.process-explorer
Access to "Process Explorer" (viewing and managing processes). Parent permission is "devices.actions.remote-tool".
OFF
devices.actions.remote-tool.service-explorer
Access to "Service Explorer" (viewing and managing processes). Parent permission is "devices.actions.remote-tool".
OFF
devices.actions.remote-tool.command-tools
Access to "Command Tools" (using remote device's Command Interface). Parent permission is "devices.actions.remote-tool".
OFF
devices.actions.remote-tool.file-explorer
Access to "File Explorer" (viewing remote device's files). Parent permission is "devices.actions.remote-tool".
OFF
devices.actions.remote-tool.file-explorer.crud
Access to create folders and to rename and delete files/folders. This actions will be performed on behalf of the system (root rights). Parent permission is "devices.actions.remote-tool.file-explorer".
OFF
devices.actions.remote-tool.file-explorer.download
Access to "File Explorer" (downloading files and folders from remote device). Parent permission is "devices.actions.remote-tool.file-explorer".
OFF
Access to "File Explorer"

- Use the switches on the right to enable or disable specific permissions
- Use the 'Apply to all' switch to enable or disable all permissions
- Click 'Save' for your settings to take effect

Assign the new role to selected users

- Click the 'Assign Users' tab.

This opens a list of all enrolled users:



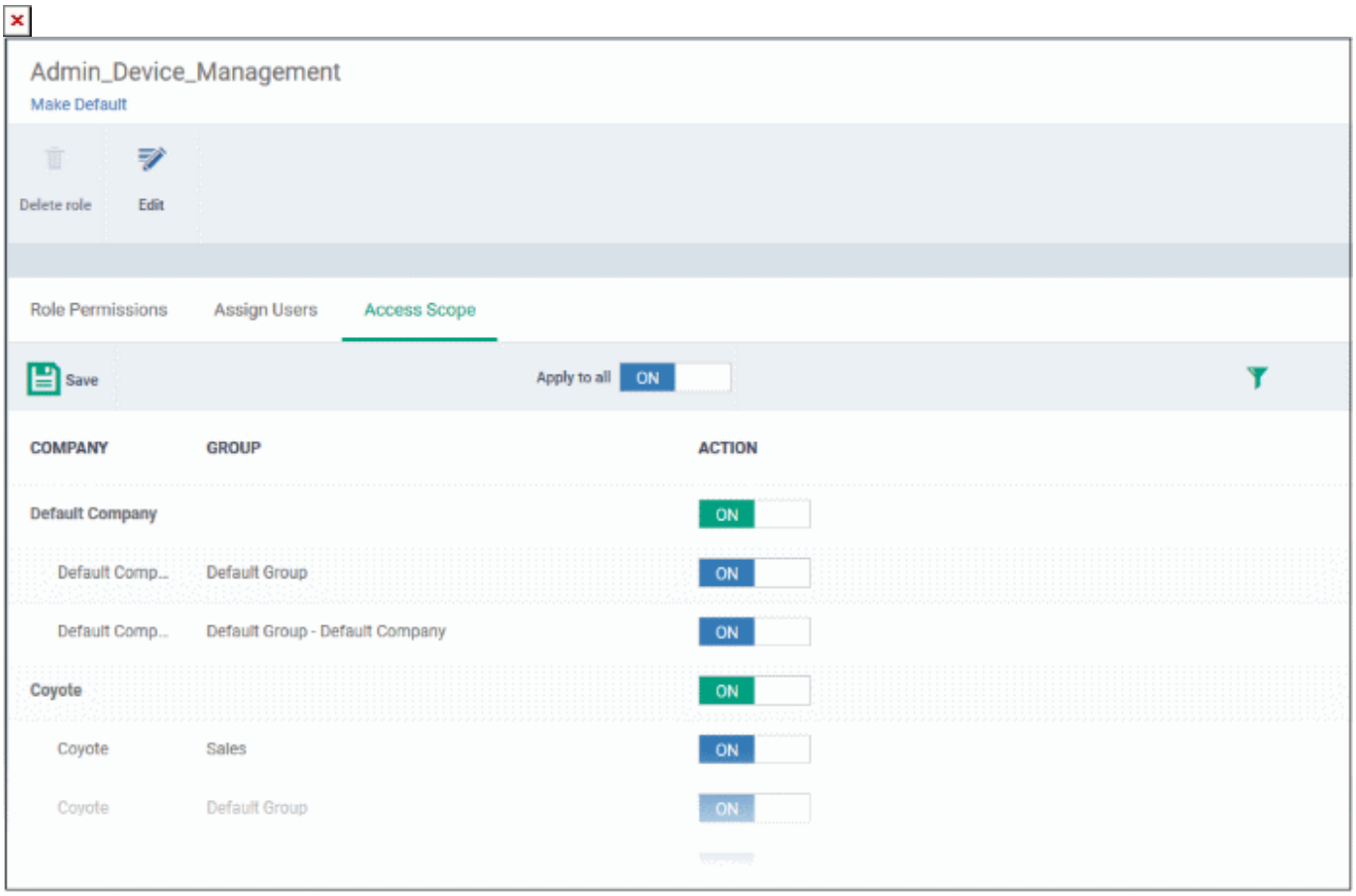
- **Assign to Role** – Click to place the user in a particular role.

Tip: You can search for specific users by clicking the funnel icon at the top-right.

Select which companies and device groups can be accessed by the role

- Click the 'Access Scope' tab.

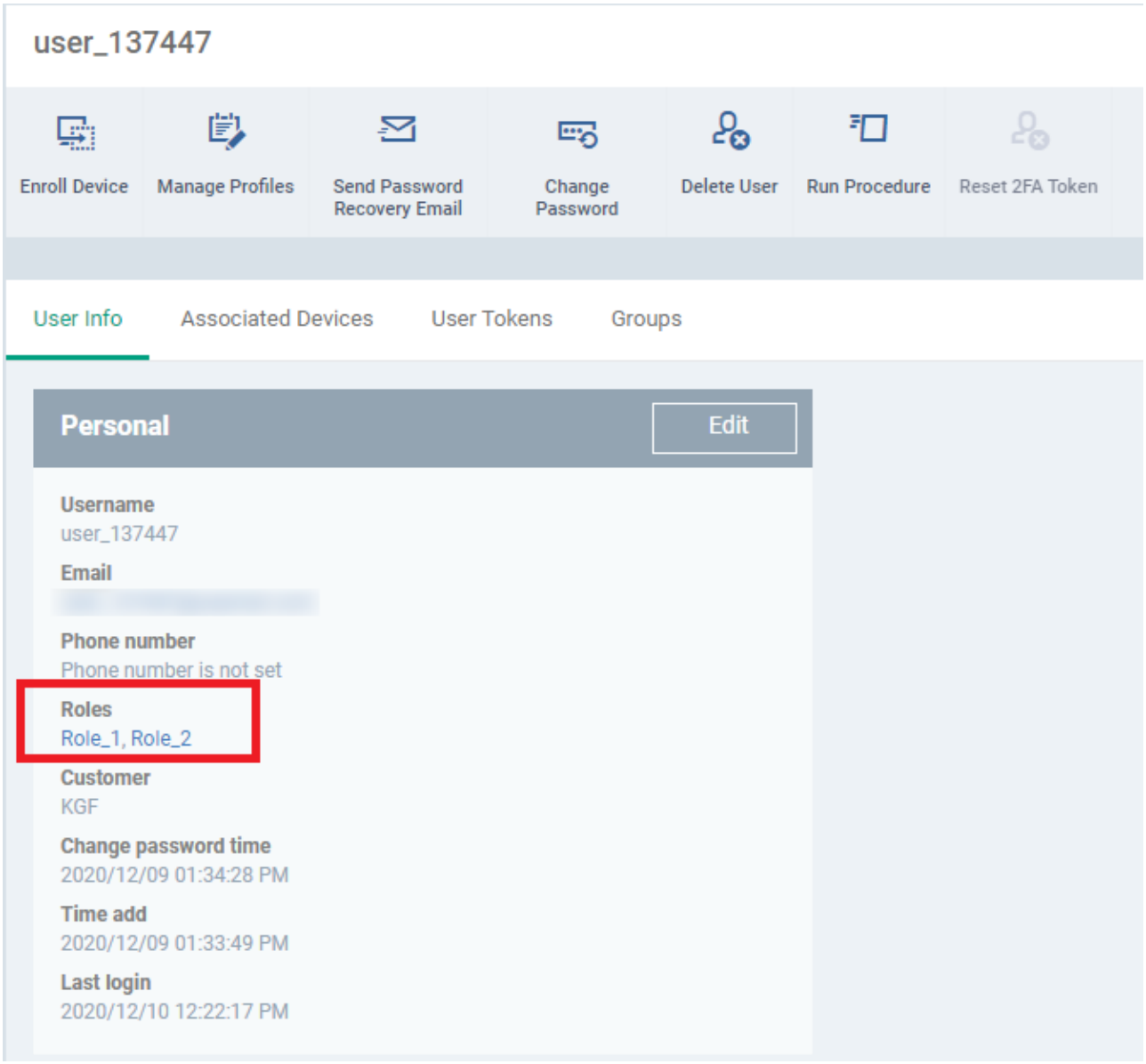
This opens a list of all companies added to the Endpoint Manager. Device groups in each company are listed below the company name.



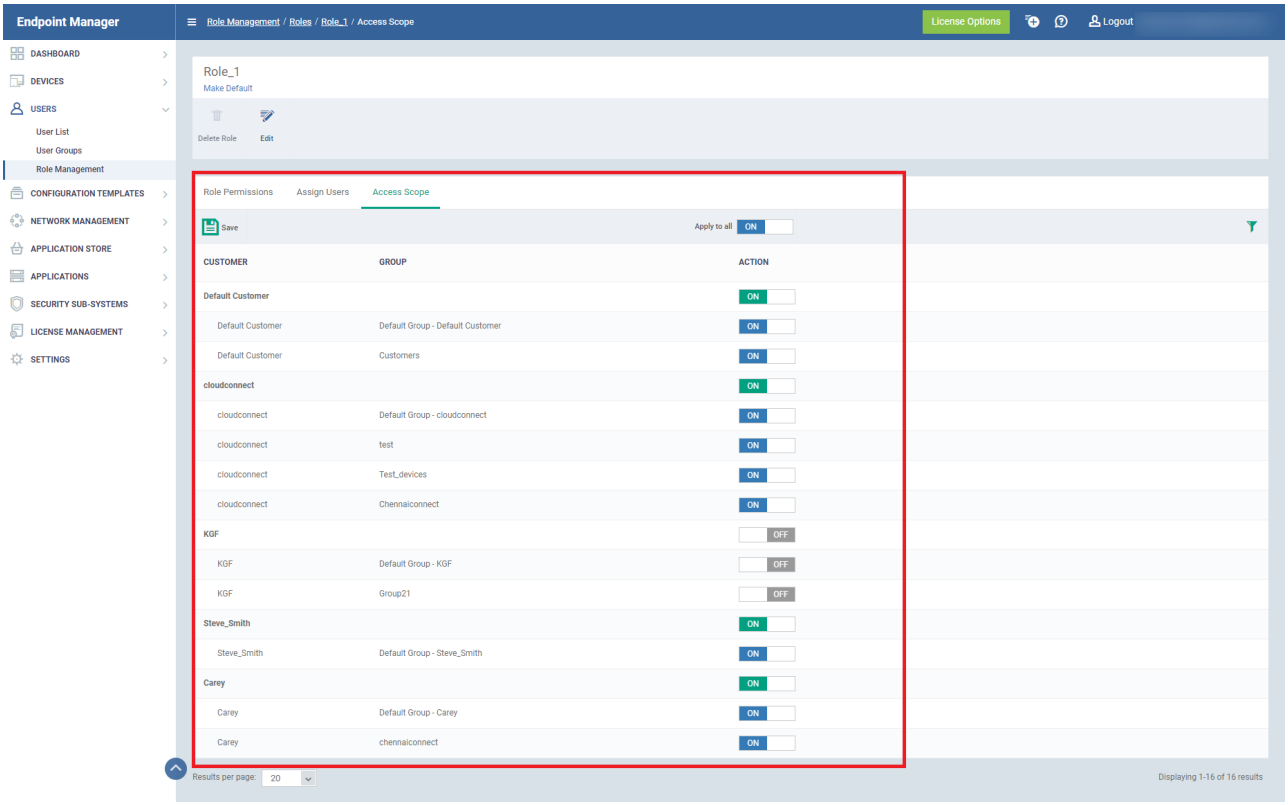
Configure the access scope of the role as follows:

- Use the green 'master' switch next to a company name to enable / disable the ability to manage groups under the company.
- Use the switch next to a device group to control access to a specific group.
- **Apply to All** - Enable or disable access to all companies and groups on the page.
- Click 'Save' for your settings to take effect.
- Click 'Make Default' if you want this to be the role that is initially assigned to new users.
- If the user is assigned with more than one role. The user can take access scope settings from the assigned multiple roles. So, that they able to manage the whole devices according to access scope settings of multiple roles.

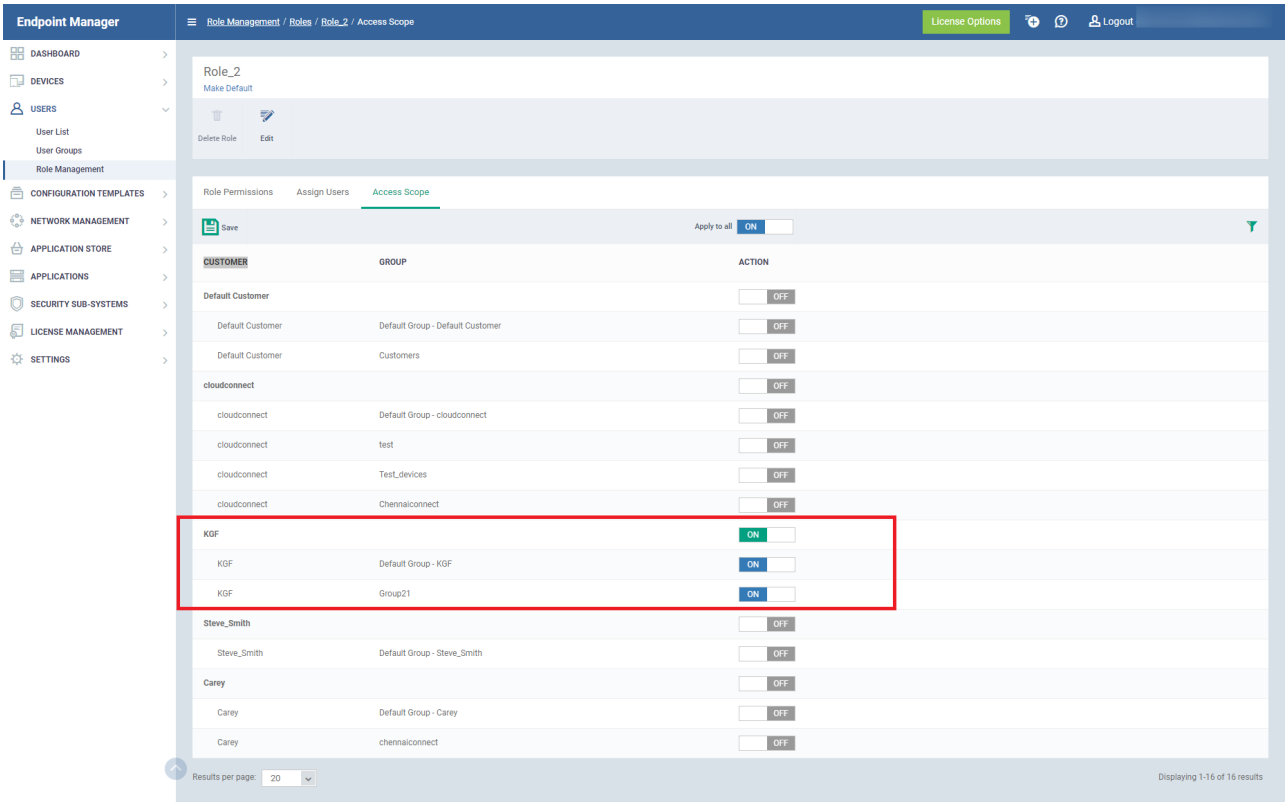
  For Example: Role_1, Role_2 are the roles assigned to the same user.



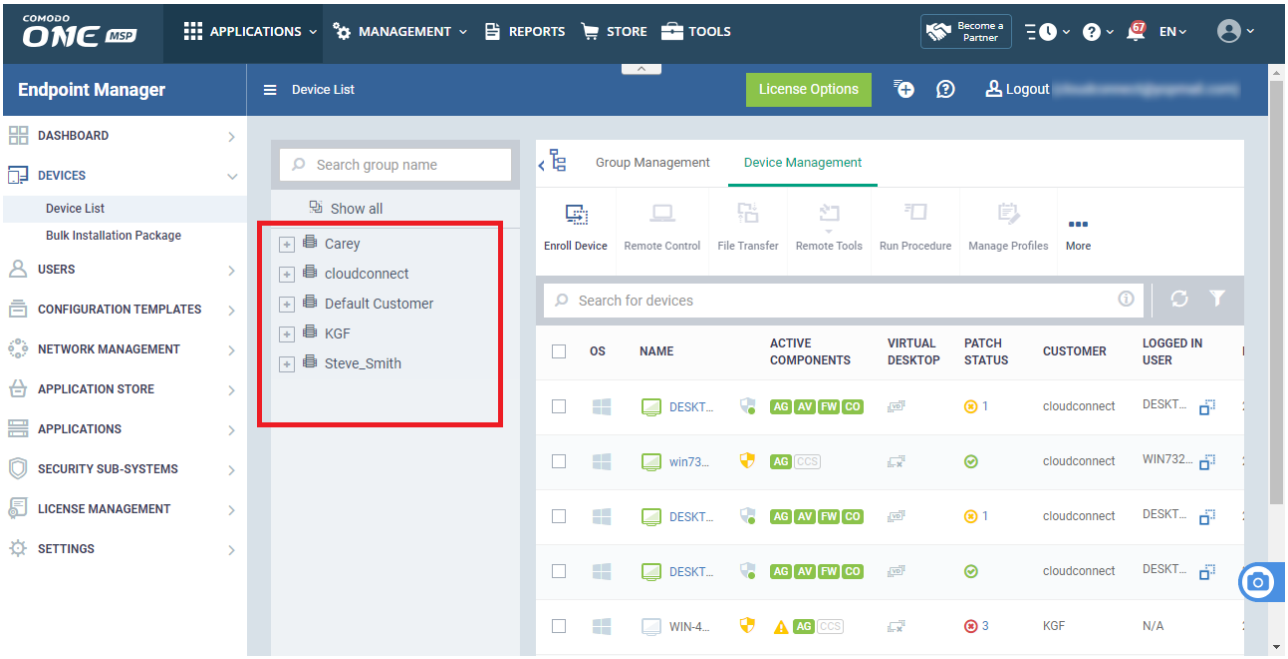
In Role_1, KGF customer is turned off in access scope



In Role_2, KGF customer is only turned on in the access scope.



Now the user has the access to the customers of both roles.


APPLICATIONS
MANAGEMENT
REPORTS
STORE
TOOLS
Become a Partner
EN
Endpoint Manager
Device List
License Options
Logout
DASHBOARD
DEVICES
Device List
Bulk Installation Package
USERS
CONFIGURATION TEMPLATES
NETWORK MANAGEMENT
APPLICATION STORE
APPLICATIONS
SECURITY SUB-SYSTEMS
LICENSE MANAGEMENT
SETTINGS
Search group name
Show all
Carey
cloudconnect
Default Customer
KGF
Steve_Smith
Group Management
Device Management
Enroll Device
Remote Control
File Transfer
Remote Tools
Run Procedure
Manage Profiles
More
Search for devices
OS
NAME
ACTIVE COMPONENTS
VIRTUAL DESKTOP
PATCH STATUS
CUSTOMER
LOGGED IN USER
cloudconnect
KGF
N/A