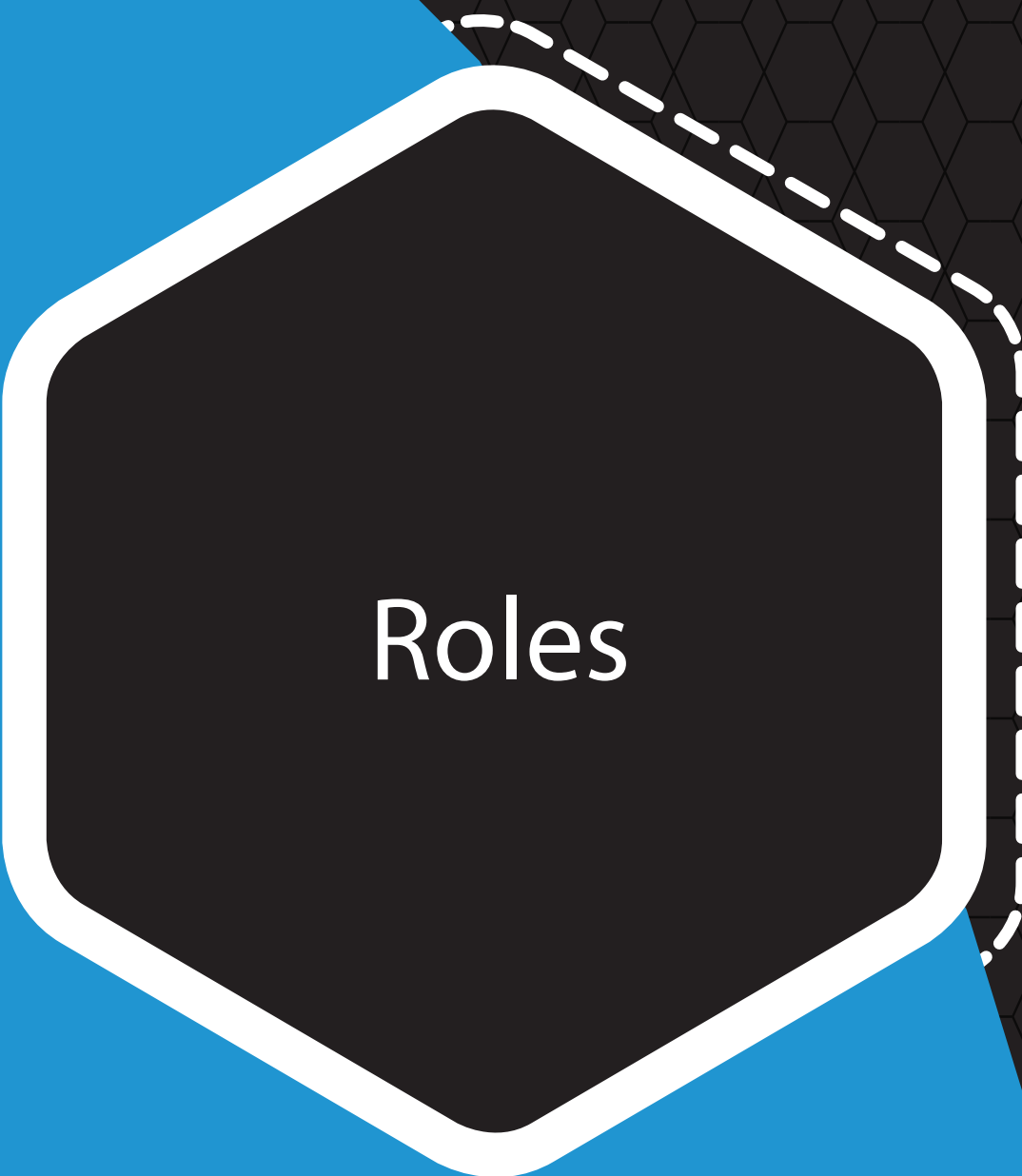


A large, dark blue hexagon with a thick white border, centered on the page. A dashed white line follows the top and right edges of the hexagon. The word 'Roles' is written in white in the center of the hexagon.

Roles

Technical doc

Roles define the specific actions and permissions users can perform in 247connect. By assigning roles, you can control access to features and functions, ensuring each user has the right level of responsibility and authority.

Each role combines a set of permissions tailored to tasks, such as managing account settings, device groups and users or controlling what features are available during managed device and on-demand sessions.

Available roles

When you first create your 247connect account, a Global Administrator role is created automatically. This role has full permissions and can't be edited or deleted. We recommend using it only for the initial set-up of 247connect, then creating your own administrator roles.

247connect provides the following pre-defined roles:

Global Administrator

This role has full access to all actions and settings.

Note: To allow the Global Administrator to access on-demand support sessions, you must assign an On-demand licence to them.

On-demand User

Grants permissions to perform actions required for on-demand support sessions.

Managed User

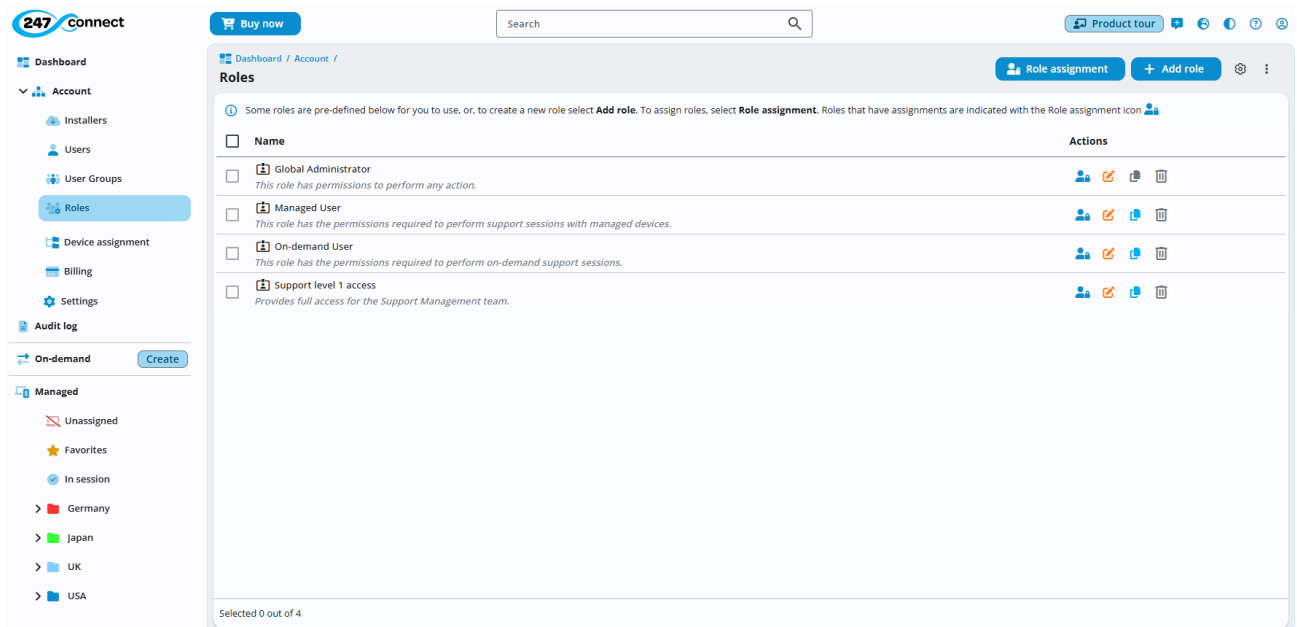
Grants permissions to perform actions required for support sessions on managed devices.

Notes:

- There must always be one user that has the Global Administrator role assigned to them.
- You can't delete a user if they are the only one assigned the Global Administrator role.
- If there is only one user with a Global Administrator role, you can't remove the role from them.

View roles

1. In the 247connect Web Portal, go to **Account** > **Roles** in the side menu.
2. The display area shows a list of roles.



To find a specific role, click in the search bar and enter your search term. A list of matching roles appears as you type. Select the required role. Click **Close**  to end the search.

Notes:

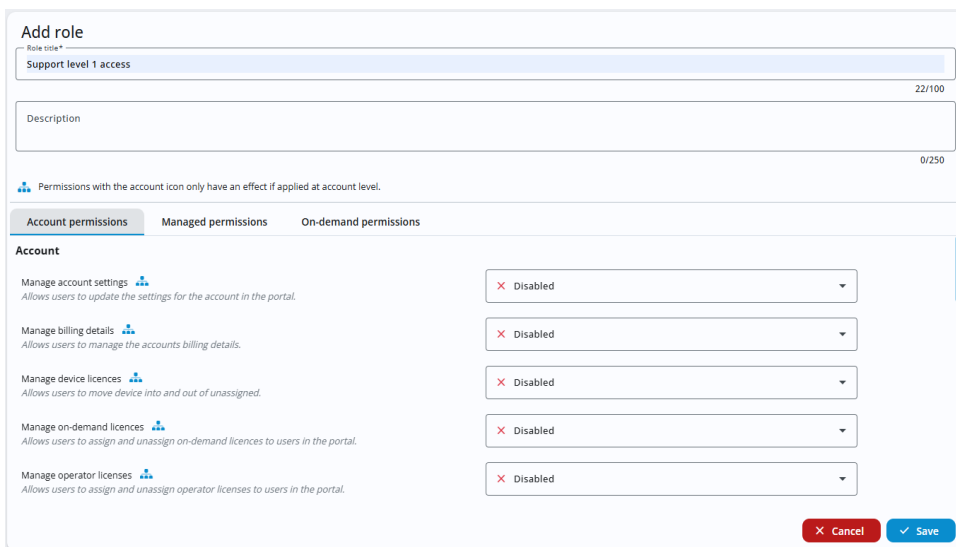
- You can easily see which roles are assigned to users, as they are indicated by the **Role assignment**  icon.
- Changes to role permissions take effect when assigned users log out and log back in. Updates may take up to five minutes to apply.

Create a role

In addition to the Global Administrator role (which can't be edited or deleted), 247connect includes two pre-defined roles. You can create your own custom, define their permissions or clone an existing role.

Create a role

1. In the 247connect Web Portal, go to **Account > Roles** in the side menu.
2. Click **Add role**.



3. Enter a role name.
4. (Optional) Add a description of the role's purpose or permissions.
5. Set the role permissions. By default, no permissions are selected.

Note: Account-level and on-demand permissions must be assigned at the account level to take effect. These are identified by the **Account**  icon.

6. Click **Save**.

Clone a role

To save time when creating new roles, you can clone an existing one. This is useful when the new role needs similar permissions to an existing role.

Note: You can't clone the Global Administrator role.

1. In the 247connect Web Portal, go to **Account** > **Roles** in the side menu.
2. Select the **Clone**  icon next to the role you want to copy.
3. In the Confirmation dialog, you can enter a new name for the role. Click **Clone**.
4. The new role appears in the list.
5. Click the **Edit**  icon to adjust its permissions.

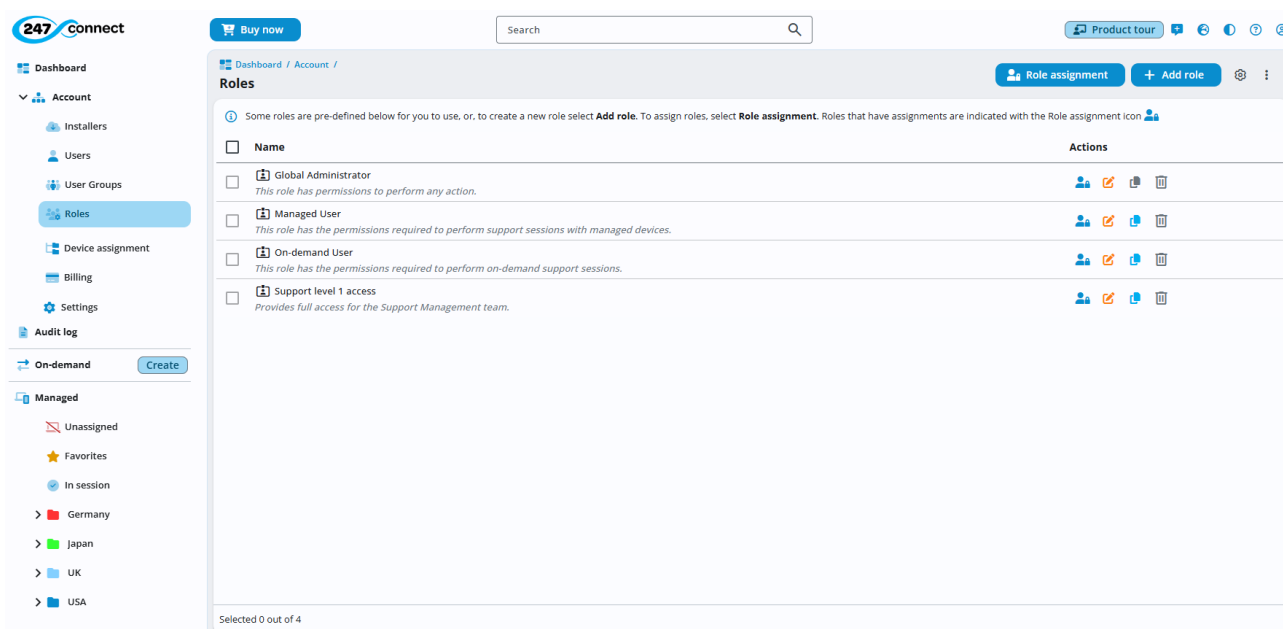
Manage roles

If you have the required permissions, you can edit and delete roles as needed.

Note: You can't edit or delete the Global Administrator role.

Edit a role

1. In the 247connect Web Portal, go to **Account** > **Roles** in the side menu.
2. The display area shows a list of roles.



3. Click the **Edit**  icon next to the role.
4. Make the required changes to the role.
5. Click **Save**.

Delete roles

You can delete roles individually or in bulk.

Note: You can't delete a role while it's still assigned to users. To delete the role, first reassign or remove affected users. Click the **Role assignment**  icon to remove users.

1. In the 247connect Web Portal, go to **Account** > **Roles** in the side menu.
2. Click the **Delete**  icon next to the role.

Or

To delete multiple roles, select the checkboxes next to each role. To select all roles available for deletion, click the checkbox at the top of the column. Click the **Delete**  icon in the top right.

3. A confirmation message appears. Click **Yes**.

Permissions

Each permission controls specific actions users can perform within 247connect. By default, all permissions are set to **Disabled** when you create a new role. To enable a permission, select **Enabled** from the drop-down list.

Notes:

- When you clone a role, the new role inherits its permissions from the original role.
- Permissions with the **Account**  icon only have an effect when applied at account level.
- Changes to role permissions take effect when assigned users log out and log back in. Updates may take up to five minutes to apply.

Account permissions

Account

Account

Manage account settings

Allows users to update the settings for the account in the portal.

✗ Disabled

Manage billing details

Allows users to manage the accounts billing details.

✗ Disabled

Manage device licences

Allows users to move device into and out of unassigned.

✗ Disabled

Manage on-demand licences

Allows users to assign and unassign on-demand licences to users in the portal.

✗ Disabled

Manage account settings: Enables users to modify the 247connect account settings.

Manage billing details: Lets users manage billing information.

Manage device licences: Enables users to move managed devices into and out of the Unassigned device group.

Manage on-demand licences: Lets users assign and unassign On-demand licences.

Audit log

Audit log

View audit log

Allows users to view the audit log entries in the portal.

✗ Disabled

View audit log: Grants access to view the audit log entries for 247connect.

Device groups

Device groups

Delete device groups

Allows users to delete device groups in the portal.

✖ Disabled

Manage device group settings

Allows users to update the settings associated with a device group in the portal.

✖ Disabled

Manage device groups

Allows users to create and edit device groups in the portal.

✖ Disabled

Delete device groups: Lets users remove existing device groups.

Manage device group settings: Enables users to configure the device group settings.

Manage device groups: Enables users to create and edit device groups.

Roles

Roles

Delete roles

Allows users to delete roles in the portal.

✖ Disabled

Manage role assignments

Allows users to assign and unassign roles for users at both the account and device group levels.

✖ Disabled

Manage roles

Allows users to create and edit roles in the portal.

✖ Disabled

Delete roles: Enables users to remove roles that are no longer needed.

Manage role assignments: Allows users to assign and unassign roles for users at both the account and device group level.

Manage roles: Enables users to create and edit roles.

User groups

User Groups

Delete user groups

Allows users to delete user groups in the portal.

✖ Disabled

Manage user groups

Allows users to create and edit user groups in the portal.

✖ Disabled

Delete user groups: Enables users to remove user groups that are no longer needed.

Manage user groups: Enables users to create and edit user groups.

Users

Users

Delete users

Allows users to delete users from the portal.

✗ Disabled

Edit users

Allows users to edit the details of users in the portal.

✗ Disabled

Invite users

Allows users to invite new users via email address.

✗ Disabled

Manage user 2FA

Allows users to manage the 2FA of other users in the portal.

✗ Disabled

Delete users: Grants the ability to remove users from the Web Portal.

Edit users: Allows users to edit the details of users.

Invite users: Enables users to invite new users to join 247connect.

Manage user 2FA: Enables users to manage the two-factor authentication (2FA) for other users in the Web Portal.

Note: Users can only disable other users' 2FA.

Managed permissions

Managed devices

Managed devices

Access clipboard for devices

Allows user to have access to the clipboard feature of managed devices in the device groups they are assigned to.

✗ Disabled

Access installers

Allows users to access the installers for managed devices in the portal.

✗ Disabled

Blank screen for devices

Allows user to blank the screen of managed devices in the device groups they are assigned to.

✗ Disabled

Chat with devices

Allows users to chat with managed devices in the device groups they are assigned to.

✗ Disabled

Delete devices

Allows users to delete a managed device from the portal.

✗ Disabled

Edit devices

Allows users to modify editable details of a managed device, e.g. Display Name.

✗ Disabled

File transfer to devices

Allows users to file transfer to managed devices in the device groups they are assigned to.

✗ Disabled

Message devices

Allows users to message managed devices in the device groups they are assigned to.

✗ Disabled

Move devices

Allows users to move a managed device between device groups in the portal.

✗ Disabled

Remote control devices

Allows users to remote control managed devices in the device groups they are assigned to.

✗ Disabled

Screenshot devices

Allows user to take a screenshot of managed devices in the device groups they are assigned to.

✗ Disabled

Send Ctrl+Alt+Del to devices

Allows user to send Ctrl+Alt+Del to managed devices.

✗ Disabled

Use PowerShell for devices

Allows users to use PowerShell for managed devices.

✗ Disabled

Use registry editor for devices

Allows users to use the registry editor for managed devices.

✗ Disabled

Use task manager for devices

Allows users to use the task manager for managed devices.

✗ Disabled

Note: These permissions apply only to the managed devices within the device groups assigned to the user.

Access clipboard for devices: Lets users access the clipboard of managed devices.

Access installers: Grants access to the installers for managed devices in the Web Portal.

Blank screen for devices: Enables users to blank the screen on managed devices during a session.

Chat with devices: Permits users to chat with managed devices.

Delete devices: Enables users to remove a managed device from the Web Portal.

Edit devices: Grants permission to modify the editable details of a managed devices, for example, the display name.

File transfer to devices: Allows users to transfer files directly to managed devices.

Message devices: Lets users send messages directly to managed devices.

Move devices: Enables users to move managed devices between device groups.

Remote control devices: Allows users to remote control managed devices.

Screenshot devices: Enables users to take a screenshot of managed devices.

Send Ctrl+Alt+Del to devices: Lets users send Ctrl+Alt+Del to managed devices.

Use PowerShell for devices: Enables users to run PowerShell commands on managed devices.

Use Registry Editor for devices: Allows users to access and edit the registry on managed devices.

Use Task Manager for devices: Enables users to monitor and manage system activity on managed devices.

On-demand permissions

On-demand devices

On-demand devices Access clipboard for devices  <i>Allows user to have access to the clipboard feature of on-demand devices.</i>	× Disabled ▼
Chat with devices  <i>Allows users to chat with on-demand devices.</i>	× Disabled ▼
Elevate sessions  <i>Allows users to elevate their session with an on-demand device.</i>	× Disabled ▼
File transfer to devices  <i>Allows users to file transfer to on-demand devices.</i>	× Disabled ▼
Message devices  <i>Allows users to message on-demand devices.</i>	× Disabled ▼
Remote Control Devices  <i>Allows users to remote control on-demand devices.</i>	× Disabled ▼
Screenshot devices  <i>Allows user to take a screenshot of on-demand devices.</i>	× Disabled ▼
Send Ctrl+Alt+Del to devices  <i>Allows user to send Ctrl+Alt+Del to on-demand devices. Requires Elevate sessions permission.</i>	× Disabled ▼
Use PowerShell for devices  <i>Allows users to use PowerShell for on-demand devices.</i>	× Disabled ▼
Use registry editor for devices  <i>Allows users to use the registry editor for on-demand devices.</i>	× Disabled ▼
Use task manager for devices  <i>Allows users to use the Task Manager for on-demand devices.</i>	× Disabled ▼

Access clipboard for devices: Lets users access the clipboard of the on-demand device.

Chat with devices: Permits users to chat with on-demand devices.

Elevate sessions: Lets users elevate their session with an on-demand device.

File transfer to devices: Allows users to transfer files directly to on-demand devices.

Message devices: Lets users send messages directly to on-demand devices.

Remote control devices: Enables users to remote control on-demand devices.

Screenshot devices: Lets users take a screenshot of on-demand devices.

Send Ctrl+Alt+Del to devices: Lets users send Ctrl+Alt+Del to on-demand devices. Requires the Elevate sessions permission.

Use PowerShell for devices: Enables users to run PowerShell commands on devices in on-demand sessions.

Use Registry Editor for devices: Allows users to access and edit the registry on devices in on-demand sessions.

Use Task Manager for devices: Enables users to monitor and manage system activity on devices in on-demand sessions.

Role assignment

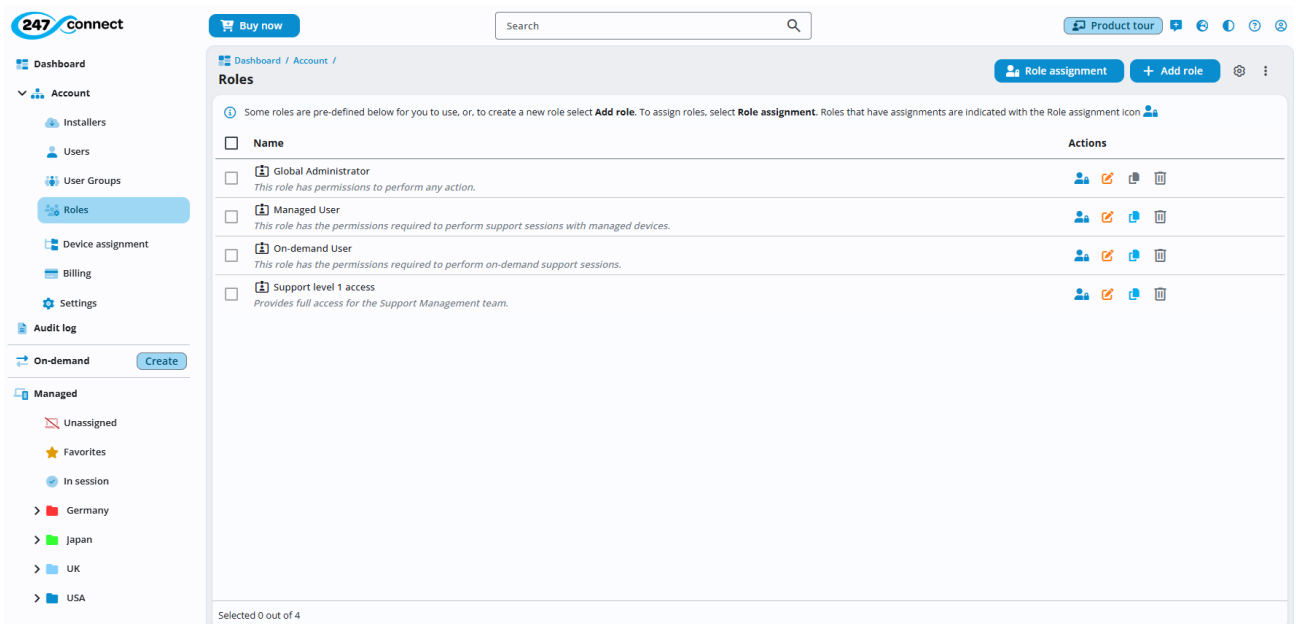
After creating roles with the necessary permissions, you must assign them to your users or user groups. Role assignment in 247connect determines which users can access specific features, managed devices and sessions. You can assign one or more roles to one or more users or groups and choose to apply these roles at account level or to specific device groups.

Notes:

- Assigning a role at device group level applies those permissions only to the selected group and its sub-groups. Roles assigned to users at account level give users permissions to the entire organisation and take precedence over roles assigned at device group level.
- Changes to role permissions take effect when assigned users log out and log back in. Updates may take up to five minutes to apply.
- You can easily see which roles have users assigned to them, as they are indicated by the **Role assignment** [person and padlock] .

Assign roles

1. In the 247connect Web Portal, go to **Account > Roles** in the side menu.



2. Click **Role assignment**.
3. Select the role(s) you want to assign.

Dashboard / Account / Roles /

Role assignment

1 Select role — 2 Select user groups — 3 Select users — 4 Select device group

1 Select the role(s) you wish to assign.

Global Administrator	☐
Managed User	☒
On-demand User	☐
Support level 1 access	☐

Total 4 items.

✕ Cancel → Next

- Click **Next**.
- To assign the role(s) to a group, select the user group(s).

Dashboard / Account / Roles /

Role assignment

1 Select role — 2 Select user groups — 3 Select users — 4 Select device group

1 Select the user group(s) you want to assign the selected role(s) to.

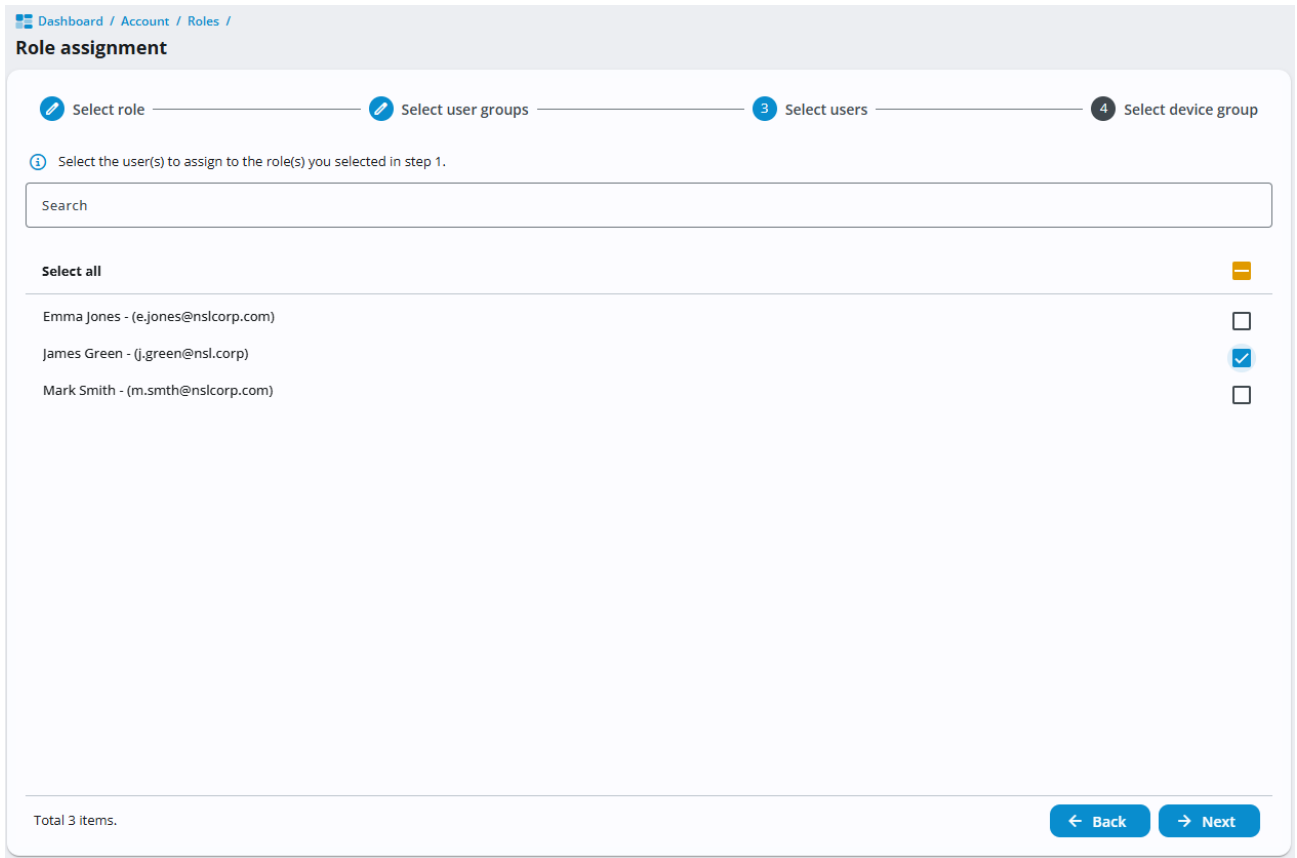
Select all ☐

IT Administrators	☐
Team Leaders	☐
Tech Support level 1 access	☐
Tech Support level 2 access	☐
UK Support team	☒
US Support team	☐

Total 6 items.

← Back → Next

6. Click **Next**.
7. To assign the role(s) to individual, select the user(s) from the list.



Dashboard / Account / Roles /

Role assignment

1 Select role — 2 Select user groups — 3 Select users — 4 Select device group

③ Select the user(s) to assign to the role(s) you selected in step 1.

Search

Select all

Emma Jones - (e.jones@nslcorp.com)	☐
James Green - (j.green@nsl.corp)	☒
Mark Smith - (m.smth@nslcorp.com)	☐

Total 3 items.

← Back → Next

8. Click **Next**.
9. Select the level at which you want to apply the assignment:
 - **Account/On-demand:** Applies the assignment across the whole account, including on-demand and device groups.
 - **Device groups:** Applies the assignment only to the selected device group, including sub-groups.

Dashboard / Account / Roles /

Role assignment

Select role — Select user groups — Select users — **4 Select device group**

Select the device group(s) you want to assign the selected role(s) and user(s) to. Choosing the Account option will apply the assignment everywhere. Assigning to a parent device group will automatically include child groups.

Search

- Account / On-demand
 - Germany
 - Munich
 - Japan
 - North office
 - UK
 - Cambridge office
 - Oxford office
 - USA
 - East coast
 - West coast

Total 1 items.

[← Back](#)
[✓ Create](#)

10. Click **Create**.

View and remove role assignments

You can view where each role is assigned and, if you have the required permissions, remove those assignments.

Note: Removing a role always removes it from the assigned device group.

By role

See which users, user groups and device groups are assigned to a role.

- Go to **Account > Roles** in the side menu.
- Click the **Role assignment** [person and padlock] icon  next to the role.
- The Web Portal displays a list of users, user groups and device groups assigned to the role.
- To remove a user or user group, click the **Delete**  icon next to it.
- Click **Yes** to confirm the removal.

By user

View the roles assigned to a user and the device group where those roles apply.

1. Go to **Account > Users** in the side menu.
2. Click the required user.
3. Select the User role assignments tab.
4. The Web Portal displays the roles assigned to the user and the device groups where those roles apply.
5. To remove the role assignment, click the **Delete**  icon next to the role.
6. Click **Yes** to confirm the removal.

By user group

View the roles assigned to a user group and the device group where those roles apply.

1. Go to **Account > User Groups**.
2. Click the required group.
3. Select the Role assignments tab.
4. The Web Portal displays the roles assigned to the group and the device groups where those roles apply.
5. To remove the role assignment, click the **Delete**  icon next to the role.
6. Click **Yes** to confirm the removal.

By device group

See the roles, users and user groups assigned to a device group.

1. Go to **Managed** in the side menu.
2. Click the required device group.
3. Select the Group role assignments tab.
4. The Web Portal displays the role assignments for the device group.
5. To remove a role assignment from the device group, click the **Delete**  icon next to it.
6. Click **Yes** to confirm the removal.

Notes:

- To delete multiple users or roles at once, select the checkboxes next to each item and click the **Delete**  icon in the top right.
- To add users, user groups and device groups to a role, click **Role assignment** and follow the steps in **Assign roles**.