# Managed devices

Technical doc

Managed devices are those with a permanently installed Managed Agent, enabling continuous monitoring, support and remote management. These devices are always accessible for remote control actions, ensuring reliable connectivity and streamlined maintenance for users.

**Note:** Users must have the Control component installed (Windows, iOS or macOS) to connect to and interact with managed devices.

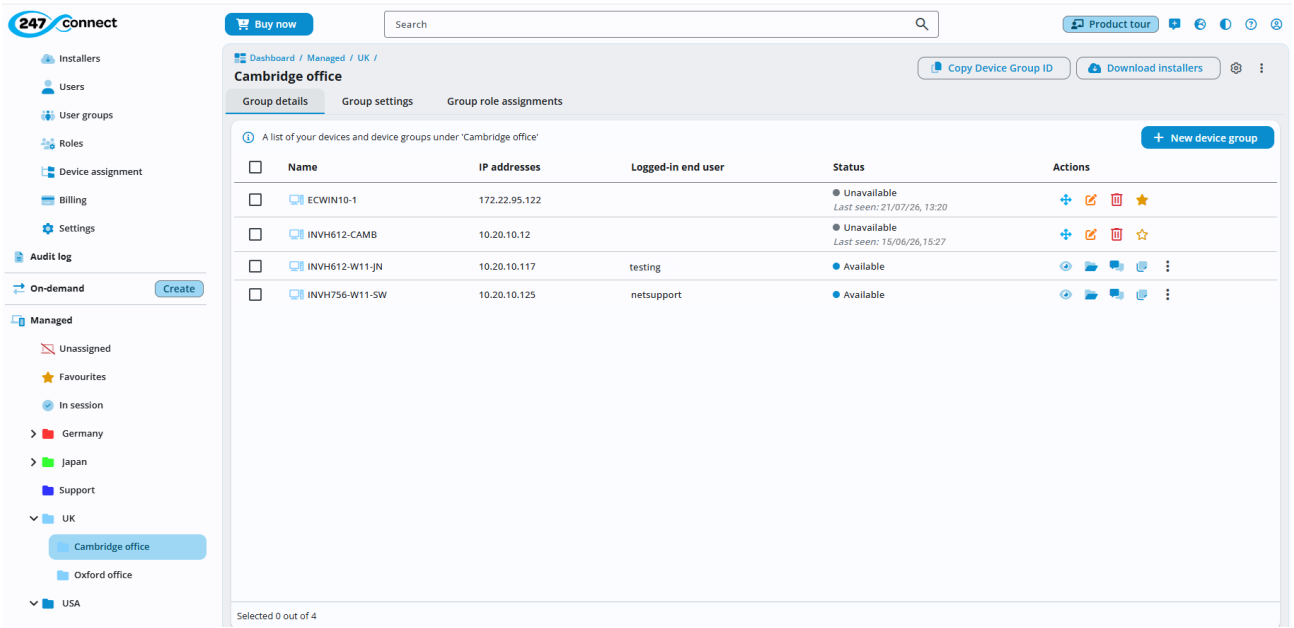
## View managed devices

1. Go to **Managed** in the side menu.

   **Note:** By default, when you install a Managed Agent on a device, it appears in the Unassigned device group. You can't connect to or interact with managed devices in this group. To enable remote access, move it to a device group. Devices moved out of the Unassigned group cannot return to it for 90 days. You can use device assignment rules to move devices into a selected device group automatically.

2. Select a device group to display its devices.

   **Note:** You can search for managed devices by entering your search term in the search bar. Matching devices appear as you type and you can interact with a device using the remote feature icons. Click **Close** ✕ to end the search.




You can sort the table by clicking a column header. Click again to change the sort direction. An arrow icon next to the column header indicates the current sort direction.

You can customise the table by selecting which columns to show and adjusting their order. Click the settings icon at the top of the display area. In the Manage columns pane, remove a column by clicking the close icon or drag and drop column names to reorder them, then click **Save**.

**Note:** Locked columns (indicated with a padlock icon) can't be removed. To reinstate a removed column, select it from the **Add new column** drop-down list. To restore the default column layout, click **Reset**.

You can export the table to a PDF or .CSV file. Click the three dots icon at the top right of the display area, then select **Export to PDF** or **Export to CSV**. The file is saved in your Downloads folder.

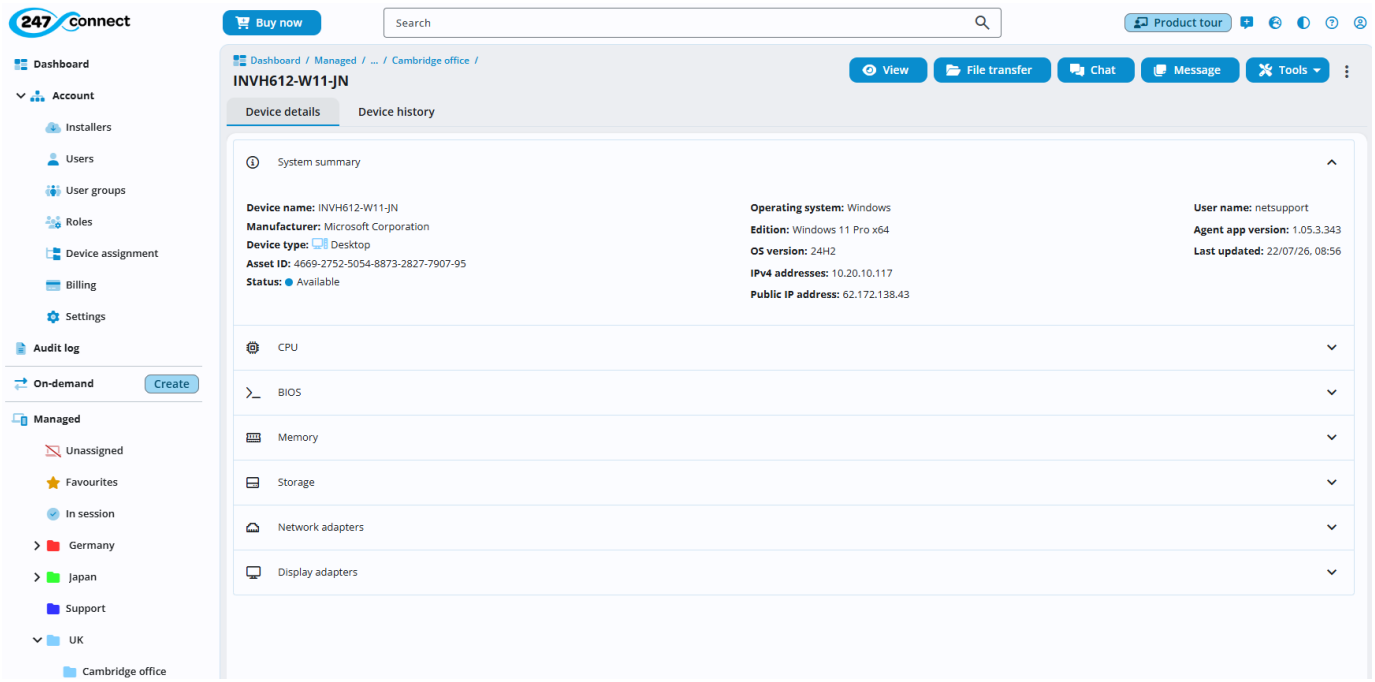
3. The following information is shown for each device:
    - The name of the device.
    - The current IP address of the device.
    - The logged-in end user.
    - The current status: Unavailable, Available or In session.

    The icons in the Actions column change depending on the device's availability status:

    - If a device is Unavailable, the column displays icons that let you manage the device, such as move, edit, delete and add to favourites.
    - If a device is Available, the column shows icons for performing remote control tasks, such as View, File transfer, Chat and Message. To access the device management options for an available device, click the three dots icon .

## View device details

When you select a managed device, you can view detailed information about its hardware and device history.




- **Device details:** Shows system and hardware information, current status and the Agent version.
- **Device history:** Lists past activity and the user who performed each action. Click **Filter** to customise the view. Select your filter criteria, then click **Apply**.
- From the toolbar, you can launch remote control functions, including View, File transfer, Chat, Message, or open the **Tools** menu to access additional features.

## Edit a managed device

You can update the name of a managed device.

1. Locate the required managed device.
2. If the device is unavailable, in the Actions column, click the **Edit** icon.

   Or

   If the device is available, in the Actions column, click the three dots icon and choose **Edit**.
3. Update the device name.
4. Click **Update**.

## Delete managed devices

You can delete managed devices individually or in bulk.

1. Locate the required managed device.
2. If the device is unavailable, in the Actions column, click the **Delete** icon.

   Or

   If the device is available, in the Actions column, click the three dots icon and choose **Delete**.
3. To delete multiple devices, select the checkboxes next to each device. To select all devices, click the checkbox at the top of the column. Click the **Delete** icon in the top right.
4. Click **Yes** to confirm the deletion.

## Move managed devices

You can move your managed devices between device groups to better organise and manage your devices.

**Note:** Devices moved from the Unassigned device group can't return for 90 days.

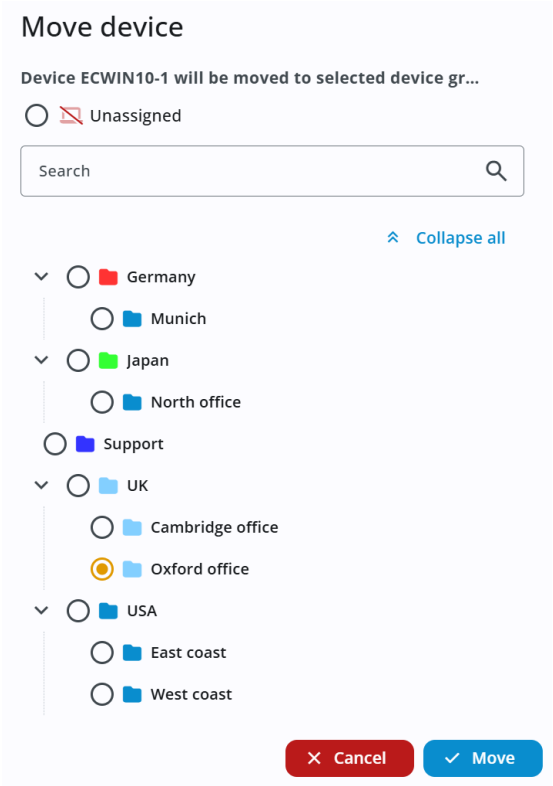
1. Locate the required managed device.
2. If the device is unavailable, in the Actions column, click the **Move** icon.

   Or

   If the device is available, in the Actions column, click the three dots menu and choose **Move**.

   Or

   To move multiple devices, select the checkboxes next to each device. To select all devices, click the checkbox at the top of the column. Click the **Move** icon in the top right.




3. Select the new device group (use the search bar to find the group, if needed).

   **Note:** If you move a device to the Unassigned group, its licence is removed. You can't interact with an unlicensed device, meaning no remote access or management actions are possible. To restore access, move it back to a valid device group to reassign a licence.

4. Click **Move**.

**Note:** Permissions for the new group apply immediately.

## Mark as Favourites

You can mark commonly accessed devices as Favourites.

1. Locate the required managed device.
2. If the device is unavailable, in the Actions column, click the **Favourites** icon.

   Or

   If the device is available, in the Actions column, click the three dots icon and choose **Favourite**.

3. The device now appears in the **Favourites** folder in the side menu. Click the **Favourites** icon again to remove it.

# Device groups

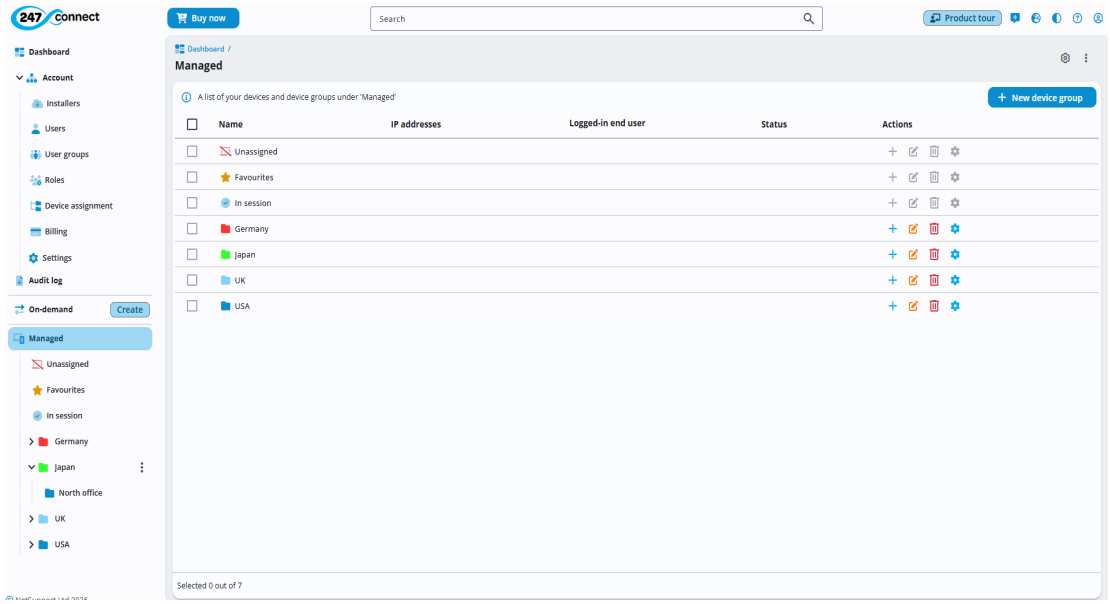
Device groups enable you to organise your managed devices and control access to them, ensuring only authorised users can interact with these devices. Without a device group, managed devices remain unlicensed and inaccessible.

**Notes:**

- Some settings can be applied to device groups. Users must have the appropriate permissions to use a feature if it is enabled. If the feature is disabled at the group level, it is unavailable to all users - regardless of their permissions.
- To assign Windows managed devices directly to a device group during installation, go to **Account** > **Settings** and turn on the **Enable installer device group assignment** option.

## View device groups

1. Go to **Managed** in the side menu.
2. A list of all your device groups appears.




You can sort the table by clicking a column header. Click again to change the sort direction. An arrow icon next to the column header indicates the current sort direction.

You can customise the table by selecting which columns to show and adjusting their order. Click the settings icon at the top of the display area. In the Manage columns pane, remove

a column by clicking the close icon or drag and drop column names to reorder them, then click **Save**.

> **Note:** Locked columns (indicated with a padlock icon) can't be removed. To reinstate a removed column, select it from the **Add new column** drop-down list. To restore the default column layout, click **Reset**.

You can export the table to a PDF or .CSV file. Click the three dots icon at the top right of the display area, then select **Export to PDF** or **Export to CSV**. The file is saved in your Downloads folder.

- **Unassigned:** Lists devices that do not have an assigned licence. To update the device counter, hover over **Unassigned** and click **Refresh**. The latest number of unassigned devices is displayed.

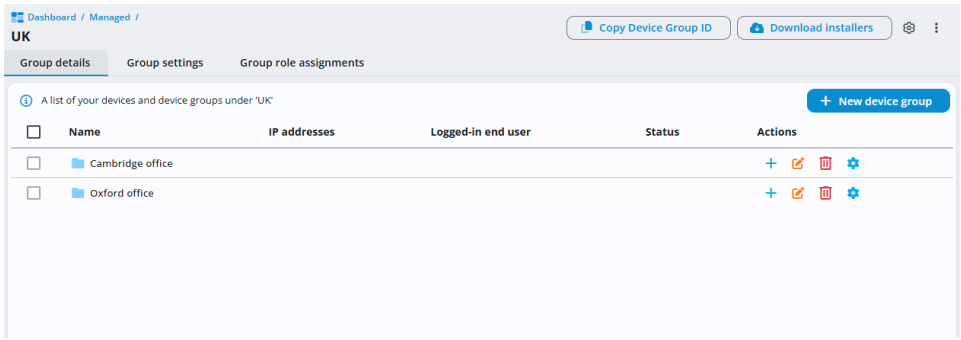
  > **Note:** By default, when you install a Managed Agent on a device, it appears in the Unassigned device group. You can't connect to or interact with managed devices in this group. To enable remote access, move it to a device group. Devices moved out of the Unassigned group cannot return to it for 90 days. You can use device assignment rules to move devices into a selected device group automatically.

- **Favourites:** Devices you've marked for quick access.
- **In session:** Shows devices that are currently being accessed in an active remote control session.
- **Device groups:** Custom folders containing your managed devices. You can create sub-groups to further organise devices by location, department or function.

  > **Note:** A default device group is created automatically for new accounts, named after the company entered during setup.

3. Click a device group to show its contents. Three tabs appear:

## Group details

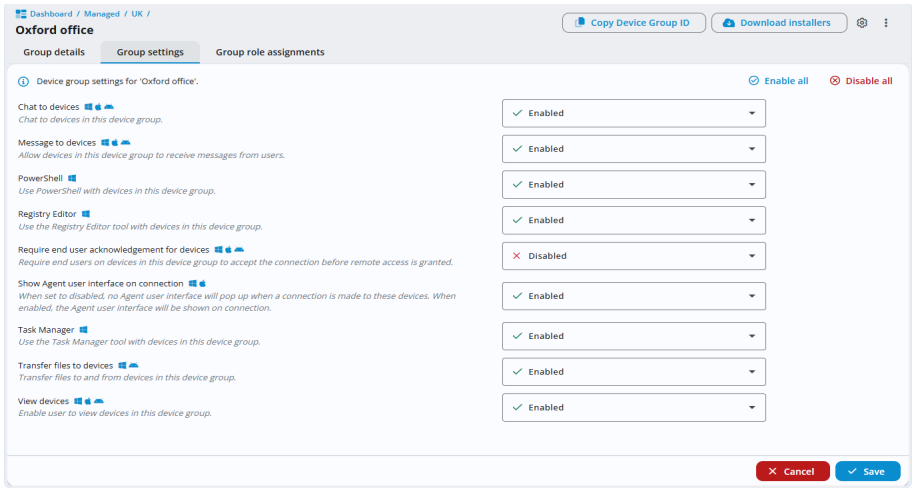



Lists the devices and any sub-groups. Select a sub-group to view its contents, including any nested groups or devices.

If **Enable installer device group assignment** is enabled in **Account** > **Settings**, the following options appear:

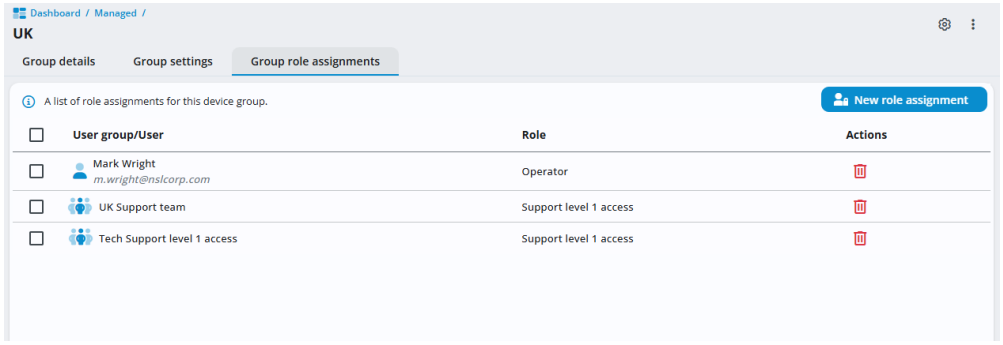
- **Copy Device Group ID:** Copies the unique identifier of the selected device group to the clipboard for use when deploying Managed Agents.
- **Download installers:** Downloads Managed Agent installer pre-configured for the selected device group.

## Group settings




Configure settings specific to the selected device group.

## Group role assignments




Shows which users, user groups and roles are assigned to the device group. To create a new role assignment, click **New role assignment**. To edit a role assignment, click the role assignment and update the assigned roles.

The user group/user icon indicates how the role is assigned:

| | |
|---|---|
| [Single person icon] | The role is assigned by user. |
| [Multiple person icon] | The role is assigned via a user group. |

## Create a device group

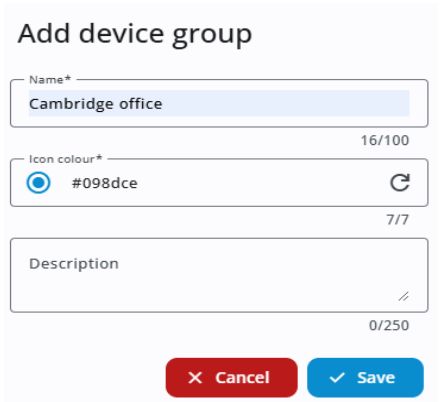
1. Go to **Managed** from the side menu and click **New device group**.

   Or

   Hover over **Managed** in the side menu, click the three dots icon and select **Create**.

   Or

   To create a sub-device group, select an existing device group and click **Create** or hover over the device group in the side menu, click the three dots icon and select **Create**.



2. Enter a name.
3. Select an icon colour. Enter the hex code or click the colour icon [blue circle with blue dot] for preset options (the icon displays the currently selected colour). Click the more colours icon [down arrow with blue dot at upper right] to use the colour picker tool to select a custom colour.
4. (Optional) Add a description to help identify the group.
5. Click **Save**.

## Manage device groups

Use the icons in the Actions column to:

- Add sub-groups.
- Edit the group.
- Delete the group.
- Configure settings specific to the group.

**Note:** You can also access these options from the side menu. Hover over a device group, click the three dots icon and select the required option.

# Device assignment

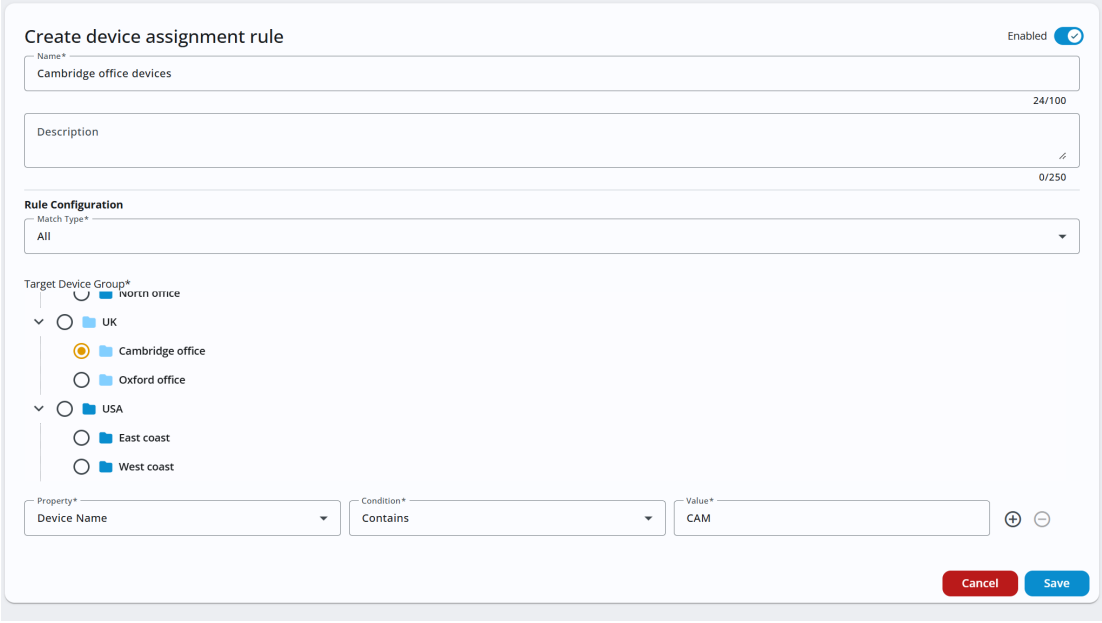
Use device assignment to move new managed devices into the correct device group automatically. When a device appears in Unassigned, 247connect checks it against your rules. If the device matches a rule, it moves it to the device group specified in the rule. You can create several rules and 247connect checks each one in turn.

**Notes:**

- A device can only be assigned once. If you move devices back to the Unassigned group, they are not automatically reassigned.
- Rules are applied in the order they appear in the list. You can reorder as needed.
- If **Enable installer device group assignment** is enabled in the account settings, assignment can be delayed by up to five minutes. Otherwise, assignment rules are processed in batches, so there may be a short delay before a device is moved.

## Create an assignment rule

1. Go to **Account** > **Device assignment** in the side menu.
2. Click **Create**.




3. Enter a name and description for the rule.
4. From the **Rule configuration** drop-down, choose the **Match type**:

- **All:** The device must match every condition.
- **Any:** The device can match any one of the conditions.

5. Select the device group you want matching devices to move to.
6. Add a condition:
   - Choose a property that's used to identify the device (for example, device name, operating system name, device type, etc).

     **Note:** To see the **Entra - Group ID** and **Entra - Group name** properties when creating rules, you need to link your Microsoft Entra account in Settings. Linking your account allows 247connect to retrieve group information from your Microsoft tenant so that these properties can be selected.

   - Choose a condition (for example, contains, does not contain, equals, etc).
   - Enter a value to match when applying the rule.

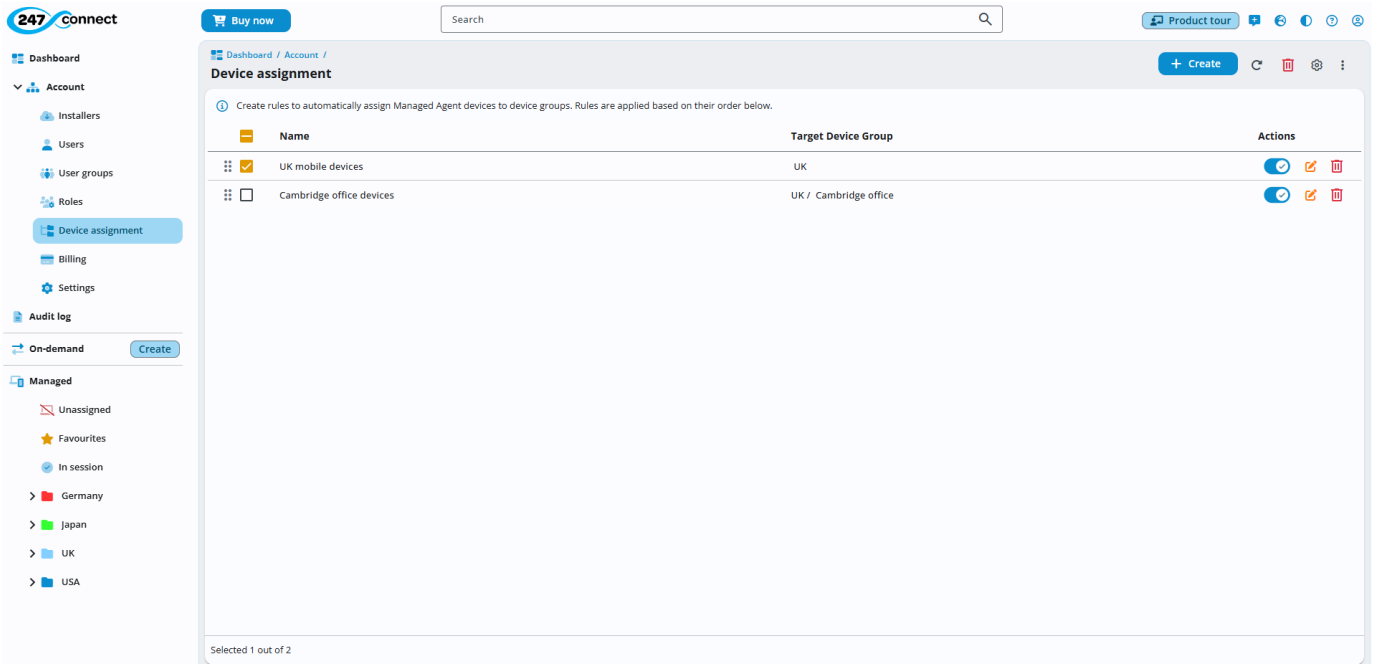
     **Note:** Make sure the value contains no spaces. If it does, the rule won't run. To check, hover over the value - any spaces will appear as an asterisk (*).

7. To add another condition, click the **Add** ⊕ icon.
8. By default, the rule is enabled. Use the **Enabled** toggle to turn it on or off.
9. Click **Save**.

   **Note:** New rules appear at the bottom of the list. Drag and drop them into the order you want 247connect to apply them.

# View and manage assignment rules

A list of your assignment rules and their target device group is shown. Rules are applied in the order that they appear. Click the **Move** icon to drag them into the required order.




From the Actions column, you can:

- Enable or disable a rule.
- Edit a rule.
- Delete a rule.

> **Note:** You can delete multiple rules at once by selecting them and clicking the **Delete** icon at the top of the pane.

# Device group settings

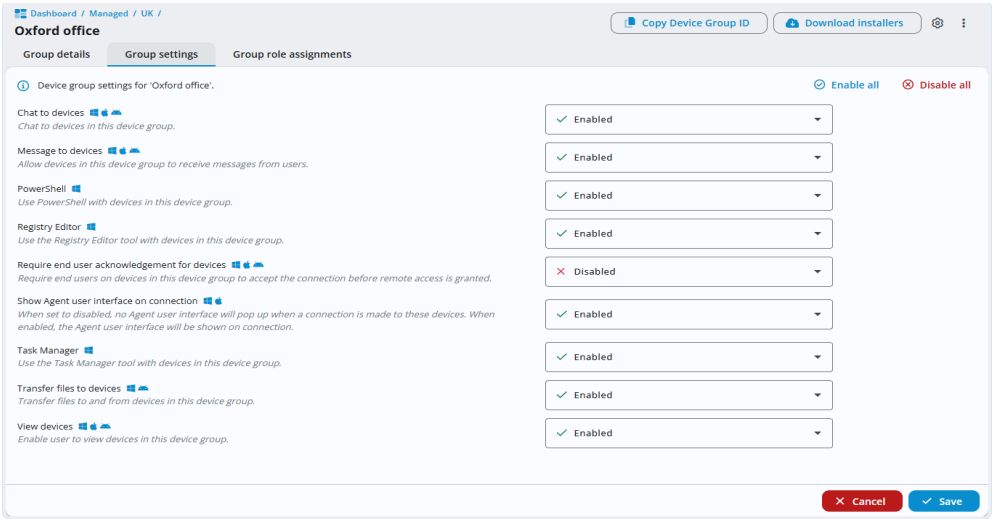
You can use Device group settings to configure certain settings for devices within a specific group. Enabling a feature makes it available to users with the appropriate permissions, while disabling it prevents all users from using that feature, regardless of their permissions.

By default, all settings are enabled, except for **Require end user acknowledgement for devices**.

## Access device group settings

1. Go to **Managed** in the side menu.
2. Select a device group.
3. Click the Group settings tab.

## Available settings




You can enable or disable all options at once by clicking **Enable all** or **Disable all**, or you can use the drop-down menus to set each feature individually:

### Chat to devices

Chat with devices in the group.

**Enabled:** Users with permissions can initiate a chat.

**Disabled:** Chat is unavailable.

### Message to devices

Send messages to devices in the group.

**Enabled:** Users with permissions can send messages.

**Disabled:** No messaging allowed.

### PowerShell (Windows Agents only)

Run PowerShell commands on devices in the group.

**Enabled:** Users with permissions can open a PowerShell window and run commands.

**Disabled:** PowerShell access is unavailable.

### Registry Editor (Windows Agents only)

Access and edit the Windows registry on devices in the group.

**Enabled:** Users with permissions can open the Registry Editor and make changes.

**Disabled:** Registry Editor is unavailable.

### Require end user acknowledgement for devices

Determines whether the end user of a device must approve a remote control session before they start.

**Enabled:** The end user at the device must approve the session.

**Disabled:** Remote control sessions can start without end user approval.

### Show Agent user interface on connection (Windows and macOS)

Specifies whether the Agent window (user interface) appears when a user connects to a device.

**Enabled:** The Agent window opens automatically upon connection.

**Disabled:** The Agent window does not appear when a connection is made.

**Note:** When disabled, the 247connect icon in the system tray turns green to indicate that a user is connected.

### Task Manager (Windows Agents only)

Use the Task Manager with devices in the group.

**Enabled:** Users with permissions can use Task Manager to view and manage applications, processes, services and drivers.

**Disabled:** Task Manager is unavailable.

### Transfer files to devices (Windows and Android)

Transfer files to devices.

**Enabled:** Users with permissions can transfer files.

**Disabled:** File transfer is blocked.

### View devices

View device screens.

**Enabled:** Users with permissions can view devices.

**Disabled:** Users cannot view screens.

Click **Save** to update the settings.

# Managed device remote sessions

You can start a remote session to access and support a managed device from the 247connect Web Portal.

**Note:** You must have the Control component installed (Windows, iOS or macOS) and the appropriate permissions assigned to start a remote control session.

When a session is active, the device appears in the In session folder in the side menu.

## Start a remote session

1. Go to **Managed** in the side menu.
2. Select the required device group, then select the managed device.
3. Choose the remote control action from the toolbar.
4. When prompted, click **Open** to launch the 247connect Control. To skip this step in the future, select **Always allow portal.247connect.cloud to open links of this type in the associated app**.
5. If end user acknowledgement is enabled in Device group settings, the end user at the managed device must approve the connection. While waiting, you'll see a Connecting screen. Click **Cancel** to stop the request.
6. Once connected, the Control component opens (Windows, iOS or macOS).

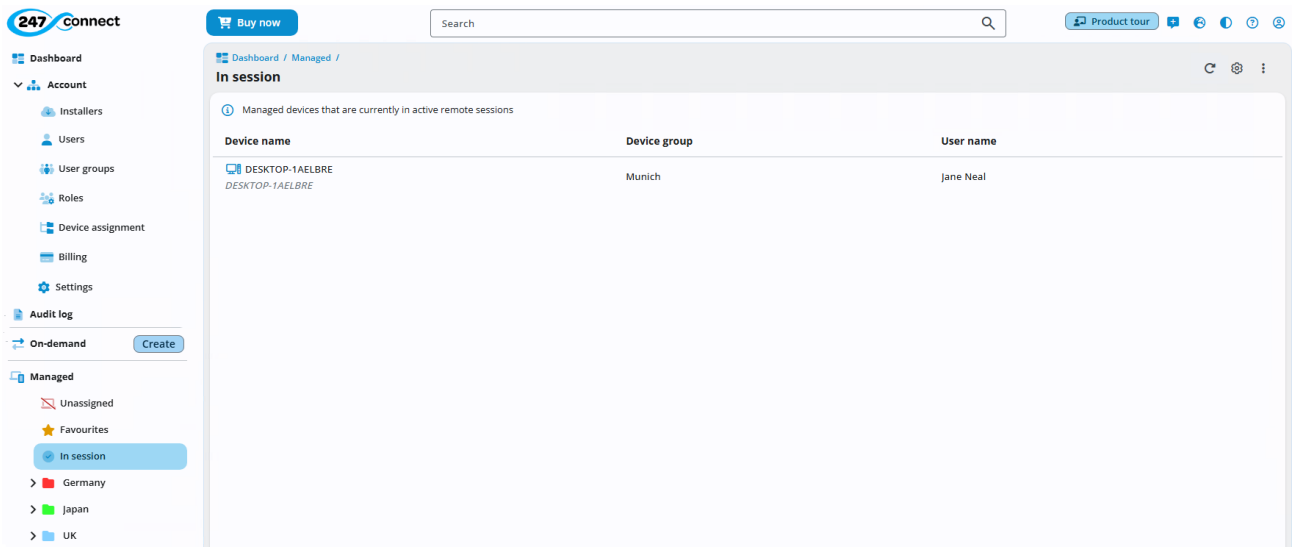
**Notes:**

- On Windows managed devices, the Managed Agent window opens by default when a user connects. You can disable this in the Device group settings. When disabled, the 247connect icon in the system tray turns green to indicate a user is connected.
- You can customise the branding that appears in the Agent window by adding your own logo. Go to **Account** > **Settings** to upload it.
- Remote sessions are automatically disconnected after a period of inactivity. By default, the timeout is 15 minutes, but you can configure this in **Account** > **Settings**.

## View remote sessions

You can view a list of active remote sessions from the Web Portal.

1. Go to **Managed** in the side menu.
2. Click **In session**.




3. A list of managed devices in an active session appears. You can see the device details, device group and the user performing the session.

Click the **Refresh** icon at the top of the display area to update the session list.

**Note:** You can sort the session list by clicking any column header. You can also customise the table using the settings icon and export the list using the three dots icon at the top of the display area.

# Managed Agent window

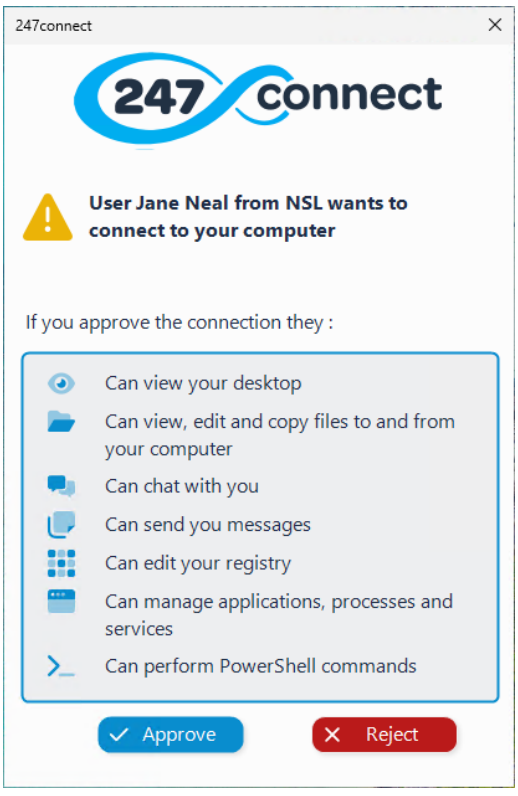
The 247connect Managed Agent window shows real-time session details and user controls during a managed session.

**Notes:**

- The Managed Agent window is available on Windows and macOS. The layout may vary slightly by platform.
- The Managed Agent window opens by default when a user connects. You can disable this in the Device group settings. When disabled, the 247connect icon in the system tray (Windows) or menu bar (macOS) turns green to indicate a user is connected.
- You can customise the branding that appears in the Agent window by adding your own logo. Go to **Account** > **Settings** to upload it.

## Approve connection request

If user acknowledgement is enabled in Device group settings, the end user must approve the connection request before the session starts.

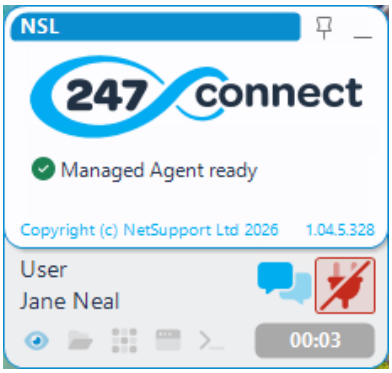


A list of available actions the user can perform when they connect is shown. This only appears for Windows Agents.

The user can't connect unless the end user approves the request.

## Managed Agent during an active session

Once the session is approved and active, the window displays:

- The name of the user running the session (this can be customised in Settings).
- A **Chat** icon for communicating with the user.
- The current remote control action(s) (Windows only).
- A session timer showing how long the session has been active.
- An **End session** icon to disconnect the user.

Ending the session disconnects the user and leaves the Managed Agent ready for the next connection.