

# 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.

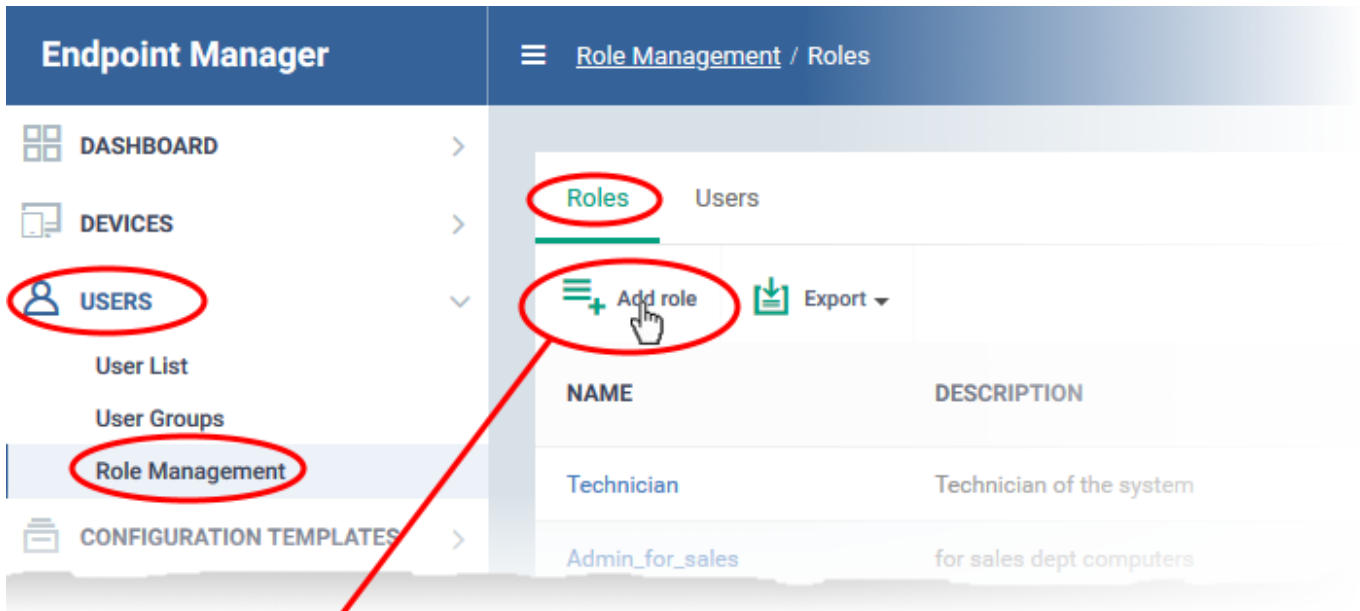
Use the links below to jump to the task you need help with:

- [Add a new role](#)
  - [Select access rights and privileges for the role](#)
  - [Assign the new role to selected users](#)
  - [Select which companies and device groups can be accessed by the role](#)

## Add a new role

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





### Create New Role

Name \*

Description \*

OK

- 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.



Roles Users

+ Add role Export

NAME ▲	DESCRIPTION
Account Admin	Account Admin of the system
<b>Admin_Device_Management</b>	Admins for managing devices only
Admin_for_sales	for sales dept computers

**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	Access to "User Settings" page, "Log in to portal", "Sending user creation email" and "Reset password" actions.	ON

Dashboard

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

**Devices**

devices	Access to "Device List" page.	<input checked="" type="checkbox"/> ON
devices.actions	Access to "Device List" actions. Parent permission is "devices".	<input type="checkbox"/> OFF
devices.actions.enroll-device	Access to "Enroll Device" action at devices list page. Parent permissions are "devices.actions" and "users.enroll-devices".	<input type="checkbox"/> OFF
devices.actions.remote-tool	Access to "Remote Management Tools" action at devices list and device properties pages. Parent permission "devices.actions".	<input type="checkbox"/> OFF
devices.actions.remote-tool.process-explorer	Access to "Process Explorer" (viewing and managing processes). Parent permission is "devices.actions.remote-tool".	<input type="checkbox"/> OFF
devices.actions.remote-tool.service-explorer	Access to "Service Explorer" (viewing and managing processes). Parent permission is "devices.actions.remote-tool".	<input type="checkbox"/> OFF
devices.actions.remote-tool.command-tools	Access to "Command Tools" (using remote device's Command Interface). Parent permission is "devices.actions.remote-tool".	<input type="checkbox"/> OFF
devices.actions.remote-tool.file-explorer	Access to "File Explorer" (viewing remote device's files). Parent permission is "devices.actions.remote-tool".	<input type="checkbox"/> 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".	<input type="checkbox"/> 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".	<input type="checkbox"/> OFF
	Access to "File Explorer" (uploading files and folders to	



- 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:

### Admin\_Device\_Management

[Make Default](#)

Delete Role Edit

Role Permissions **Assign Users** Access Scope

NAME	EMAIL	ACTION
admin	herculespopular22@gmail.com	<a href="#">Assign to Role</a>
Alice	aliceroadster@gmail.com	<a href="#">Assign to Role</a>
Avanti	avantistude@gmail.com	<a href="#">Assign to Role</a>
Dyanora	dyanorat481@gmail.com	<a href="#">Assign to Role</a>
dyanora@yopmail.com	dyanora@yopmail.com	<a href="#">Assign to Role</a>
fsregionaltransport@gmail.com	fsregionaltransport@gmail.com	<a href="#">Assign to Role</a>

- **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.

COMPANY	GROUP	ACTION
Default Company		<input checked="" type="checkbox"/> ON
Default Comp...	Default Group	<input type="checkbox"/> ON
Default Comp...	Default Group - Default Company	<input type="checkbox"/> ON
Coyote		<input checked="" type="checkbox"/> ON
Coyote	Sales	<input type="checkbox"/> ON
Coyote	Default Group	<input type="checkbox"/> ON

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.

user\_137447

- Enroll Device
- Manage Profiles
- Send Password Recovery Email
- Change Password
- Delete User
- Run Procedure
- Reset 2FA Token

- User Info
- Associated Devices
- User Tokens
- Groups

Personal

Edit

Username

user\_137447

Email

Phone number

Phone number is not set

Roles

Role\_1, Role\_2

Customer

KGF

Change password time

2020/12/09 01:34:28 PM

Time add

2020/12/09 01:33:49 PM

Last login

2020/12/10 12:22:17 PM

In Role\_1, KGF customer is turned off in access scope

Endpoint Manager | Role Management / Roles / Role\_1 / Access Scope

License Options | ? | Logout

Role\_1  
Make Default

Delete Role | Edit

Role Permissions | Assign Users | **Access Scope**

Save | Apply to all:  ON

CUSTOMER	GROUP	ACTION
Default Customer		<input checked="" type="checkbox"/> ON
Default Customer	Default Group - Default Customer	<input checked="" type="checkbox"/> ON
Default Customer	Customers	<input checked="" type="checkbox"/> ON
cloudconnect		<input checked="" type="checkbox"/> ON
cloudconnect	Default Group - cloudconnect	<input checked="" type="checkbox"/> ON
cloudconnect	test	<input checked="" type="checkbox"/> ON
cloudconnect	Test_devices	<input checked="" type="checkbox"/> ON
cloudconnect	Chennaconnect	<input checked="" type="checkbox"/> ON
KGF		<input type="checkbox"/> OFF
KGF	Default Group - KGF	<input type="checkbox"/> OFF
KGF	Group21	<input type="checkbox"/> OFF
Steve_Smith		<input checked="" type="checkbox"/> ON
Steve_Smith	Default Group - Steve_Smith	<input checked="" type="checkbox"/> ON
Carey		<input checked="" type="checkbox"/> ON
Carey	Default Group - Carey	<input checked="" type="checkbox"/> ON
Carey	chennaconnect	<input checked="" type="checkbox"/> ON

Results per page: 20 | Displaying 1-16 of 16 results

In Role\_2, KGF customer is only turned on in the access scope.

Endpoint Manager | Role Management / Roles / Role\_2 / Access Scope

License Options | ? | Logout

Role\_2  
Make Default

Delete Role | Edit

Role Permissions | Assign Users | **Access Scope**

Save | Apply to all:  ON

CUSTOMER	GROUP	ACTION
Default Customer		<input type="checkbox"/> OFF
Default Customer	Default Group - Default Customer	<input type="checkbox"/> OFF
Default Customer	Customers	<input type="checkbox"/> OFF
cloudconnect		<input type="checkbox"/> OFF
cloudconnect	Default Group - cloudconnect	<input type="checkbox"/> OFF
cloudconnect	test	<input type="checkbox"/> OFF
cloudconnect	Test_devices	<input type="checkbox"/> OFF
cloudconnect	Chennaconnect	<input type="checkbox"/> OFF
KGF		<input checked="" type="checkbox"/> ON
KGF	Default Group - KGF	<input checked="" type="checkbox"/> ON
KGF	Group21	<input checked="" type="checkbox"/> ON
Steve_Smith		<input type="checkbox"/> OFF
Steve_Smith	Default Group - Steve_Smith	<input type="checkbox"/> OFF
Carey		<input type="checkbox"/> OFF
Carey	Default Group - Carey	<input type="checkbox"/> OFF
Carey	chennaconnect	<input type="checkbox"/> OFF

Results per page: 20 | Displaying 1-16 of 16 results

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

COMODO ONE MSP APPLICATIONS MANAGEMENT REPORTS STORE TOOLS Become a Partner EN

**Endpoint Manager** Device List License Options Logout

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

<input type="checkbox"/>	OS	NAME	ACTIVE COMPONENTS	VIRTUAL DESKTOP	PATCH STATUS	CUSTOMER	LOGGED IN USER
<input type="checkbox"/>	Windows	DESKT...	AG AV FW CO	🚫	🟡 1	cloudconnect	DESKT...
<input type="checkbox"/>	Windows	win73...	AG CCS	🚫	🟢	cloudconnect	WIN732...
<input type="checkbox"/>	Windows	DESKT...	AG AV FW CO	🚫	🟡 1	cloudconnect	DESKT...
<input type="checkbox"/>	Windows	DESKT...	AG AV FW CO	🚫	🟢	cloudconnect	DESKT...
<input type="checkbox"/>	Windows	WIN-4...	AG CCS	🚫	🔴 3	KGF	N/A