Use case 1

Companies who sell their installations directly to customers

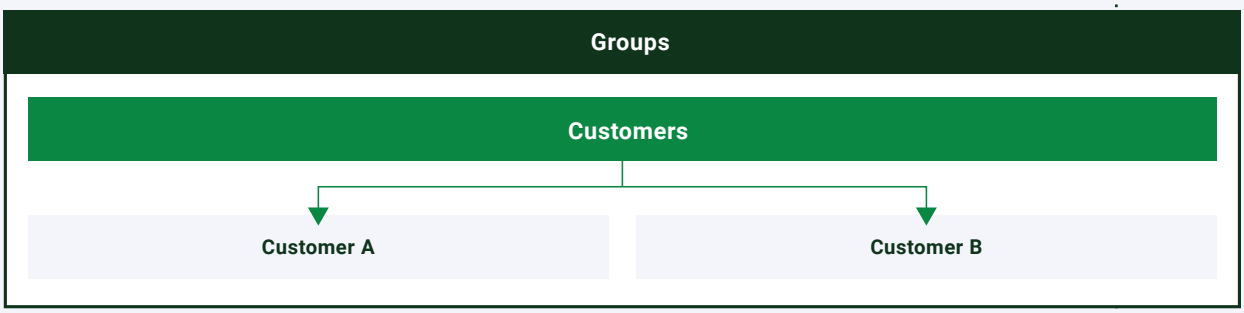
In this scenario a machine manufacturer sells directly to their customers and their engineers provide support. Platform administrators manage their StrideLinx Cloud account and users.

All engineers can configure devices and get access to all devices for troubleshooting over VPN and VNC. Each customer can manage their users (operators) and each operator can access the VNC of their machine.

Step 1

Configure groups

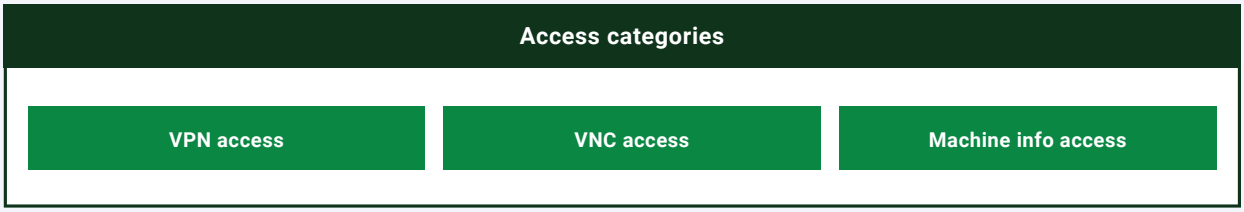
A group is a selection of devices and users.
You can divide groups in different group types.



Step 2

Configure access categories

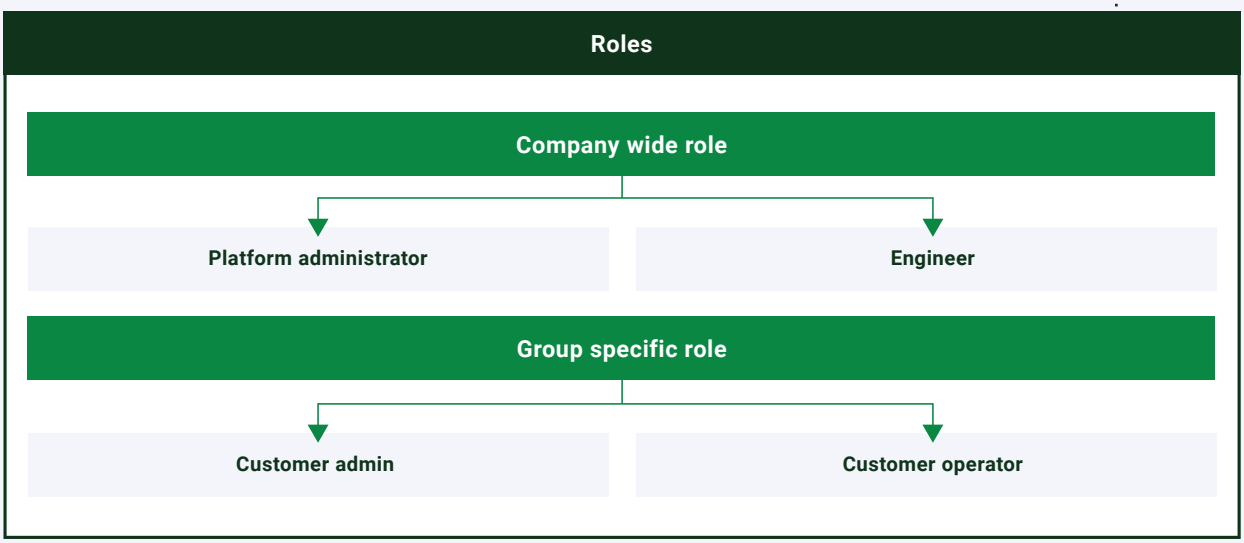
An access category is a selection of pages and services.



Step 3

Define roles

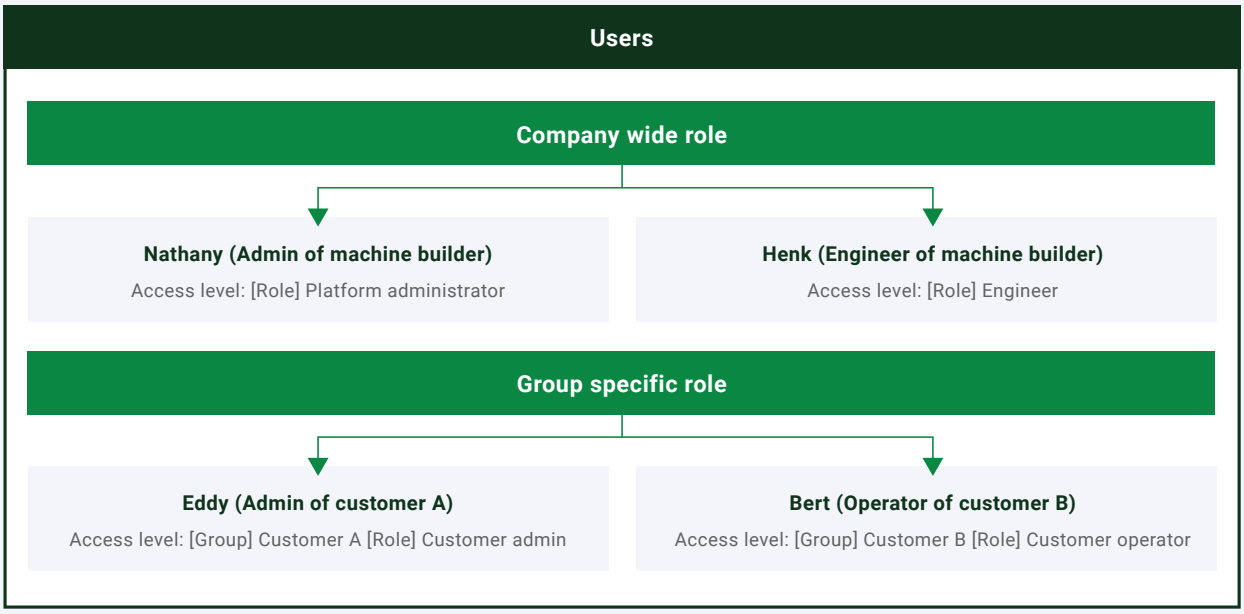
A role is a selection of permissions. You can set admin and device permissions, and you can add access categories.



Step 4

Add users

Now the roles, groups and access categories are ready, you can add users and set their access level.



Use case 2

Companies who sell their installations via a partner channel to customers and provide support

In this scenario a machine manufacturer sells his machines via a partner to their customers and their engineers provide support. Platform administrators manage their StrideLinx Cloud account and users.

All engineers can configure devices and get access to all devices for troubleshooting over VPN, HTTP and VNC. They also have access to the maintenance dashboard. Each partner can manage their devices and customers. Each customer can manage their users (operators) and each operator can access the VNC of their machine.

Step 1

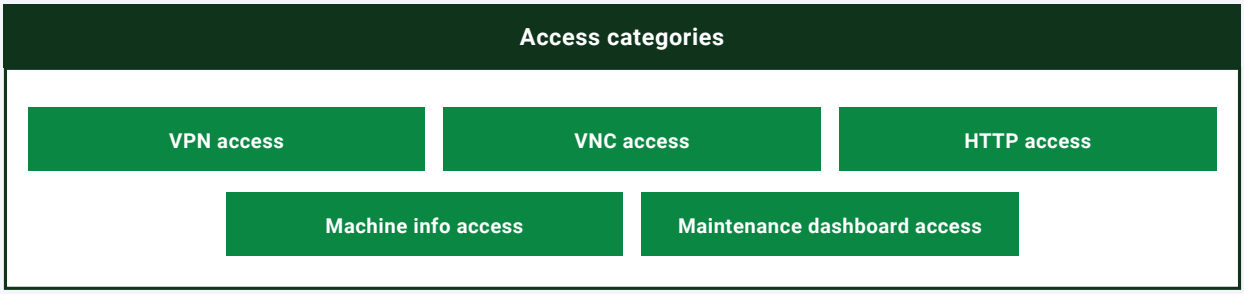
Configure groups

A group is a selection of devices and users.
You can divide groups in different group types.

Step 2

Configure access categories

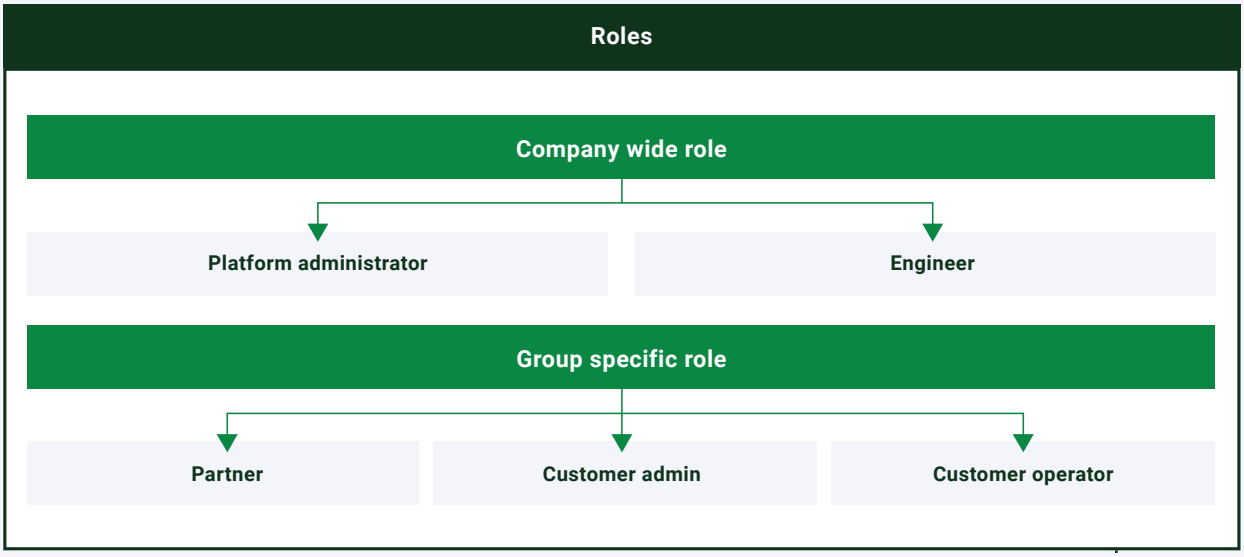
An access category is a selection of pages and services.



Step 3

Define roles

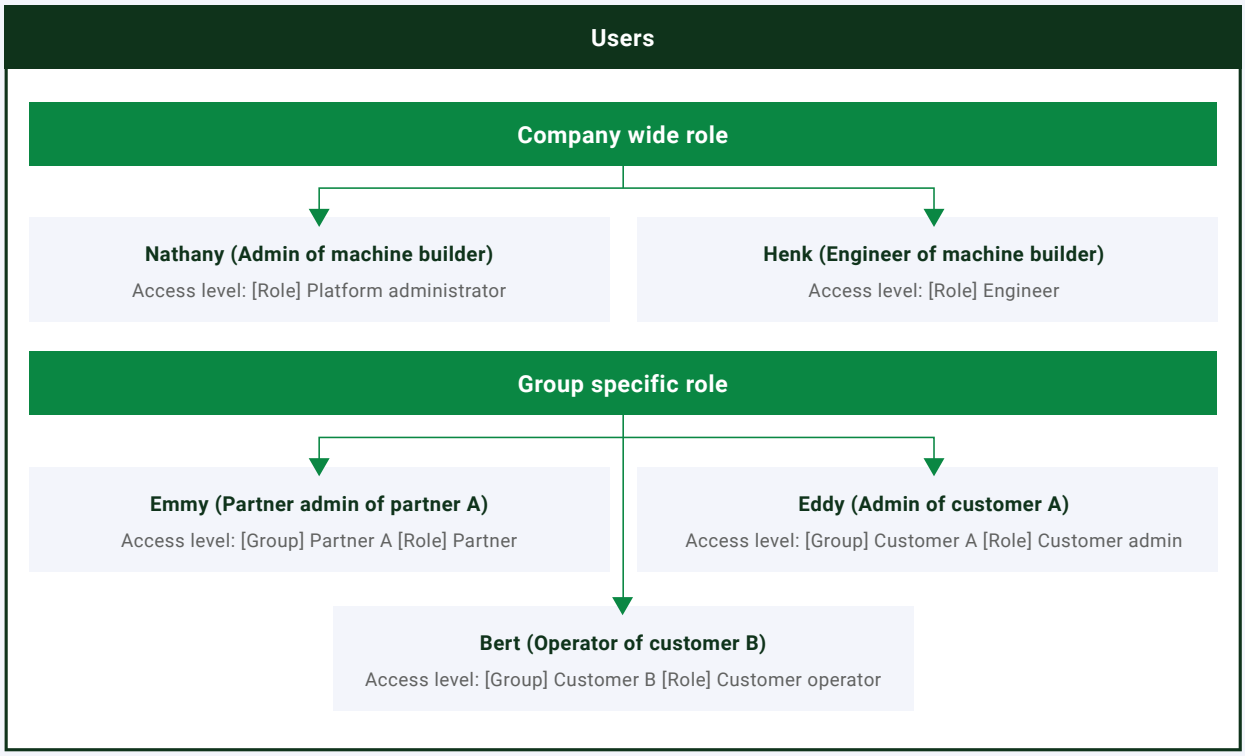
A role is a selection of permissions. You can set admin and device permissions, and you can add access categories.



Step 4

Add users

Now the roles, groups and access categories are ready, you can add users and set their access level.



Use case 3

Companies (worldwide active) with multiple divisions providing support via local service teams

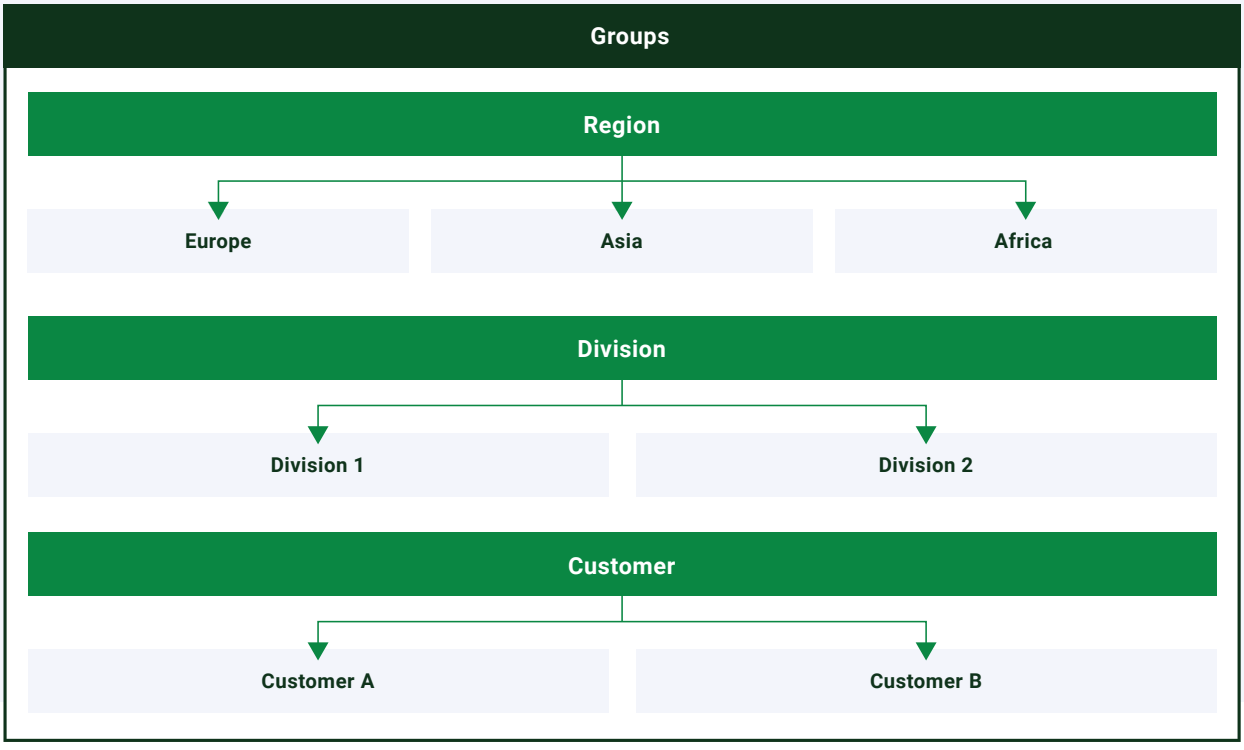
In this scenario the machine manufacturer is divided into multiple regions and divisions worldwide. They cooperate with their local service teams for support. Each machine is allocated to a specific region, division and customer. Platform administrators manage the StrideLinx Cloud account and users.

Each division has a service manager who owns the users and devices of their own division and allocates devices to support engineers. Each support engineer gets access to all allocated devices for troubleshooting over VPN for their own customers. Within the devices, they can also access a machine info dashboard. In this case the customer isn't yet allowed to access his machine via the StrideLinx Cloud platform.

Step 1

Configure groups

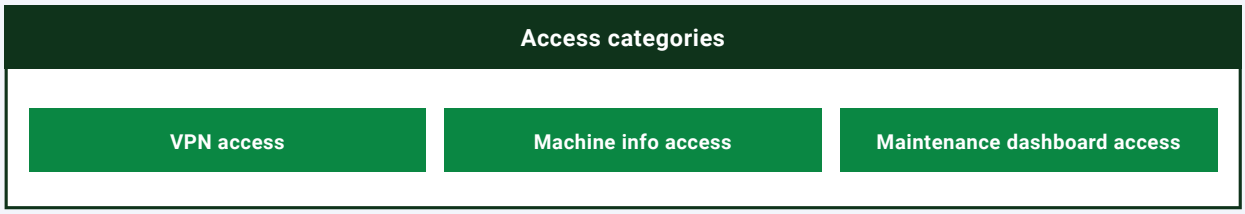
A group is a selection of devices and users.
You can divide groups in different group types.



Step 2

Configure access categories

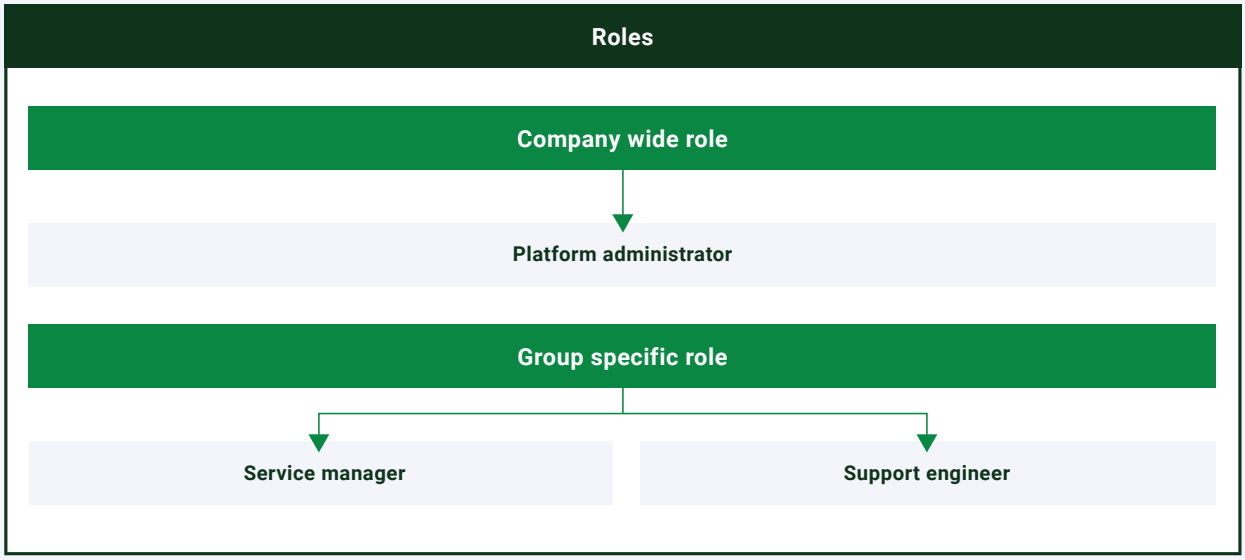
An access category is a selection of pages and services.



Step 3

Define roles

A role is a selection of permissions. You can set admin and device permissions, and you can add access categories.



Step 4

Add users

Now the roles, groups and access categories are ready, you can add users and set their access level.