Permissions Menu

Summary

Configuring Tachyon users, roles and management groups.

Settings can be reached directly using the following URL:

```
https://<tachyon DNS Name FQDN>/Tachyon/App/#/platform/
```

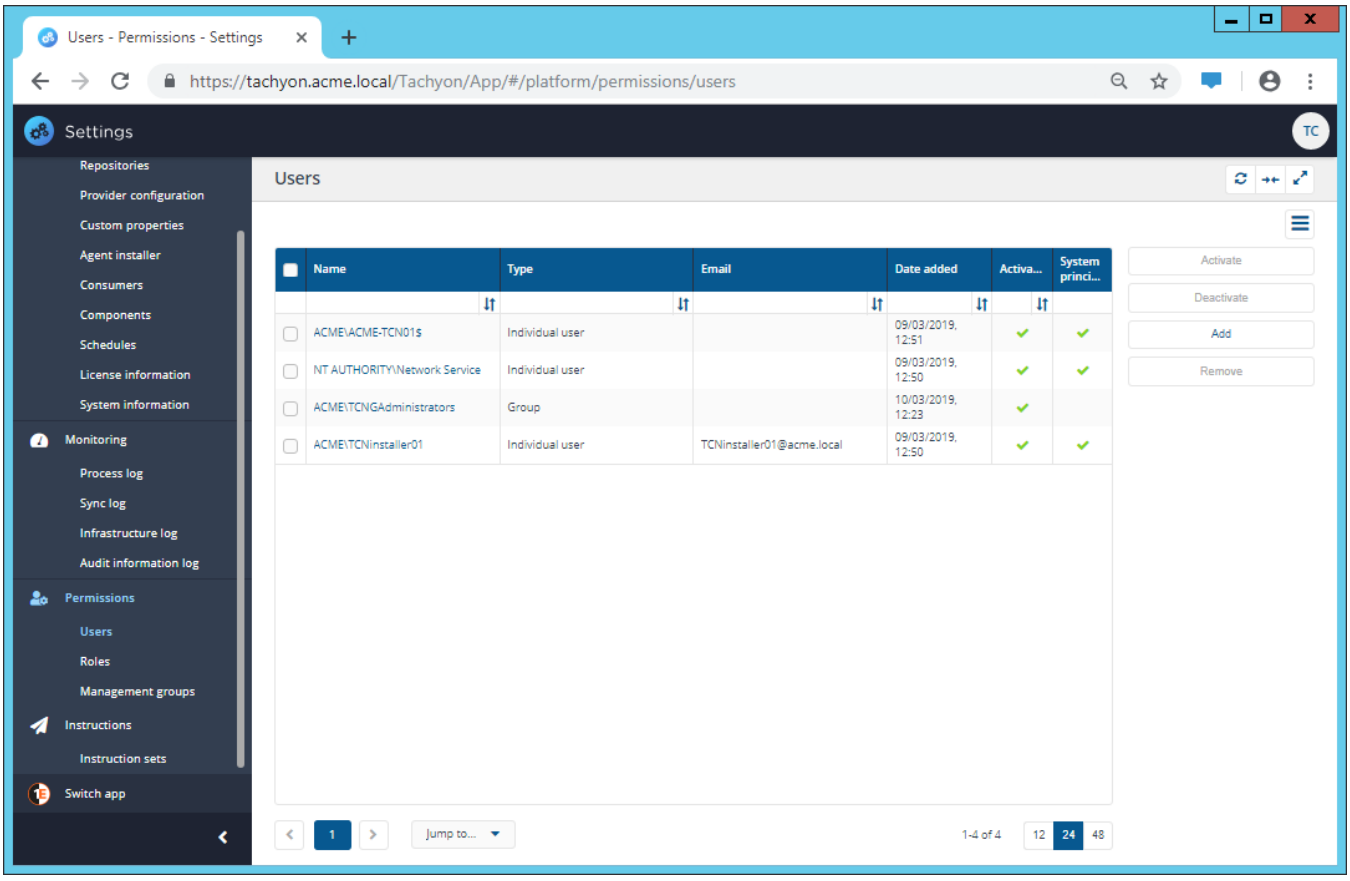
where <tachyon DNS Name FQDN> is the one set up during the preparation phase, as described under the heading Preparation: DNS Names.

In this section...

Users page

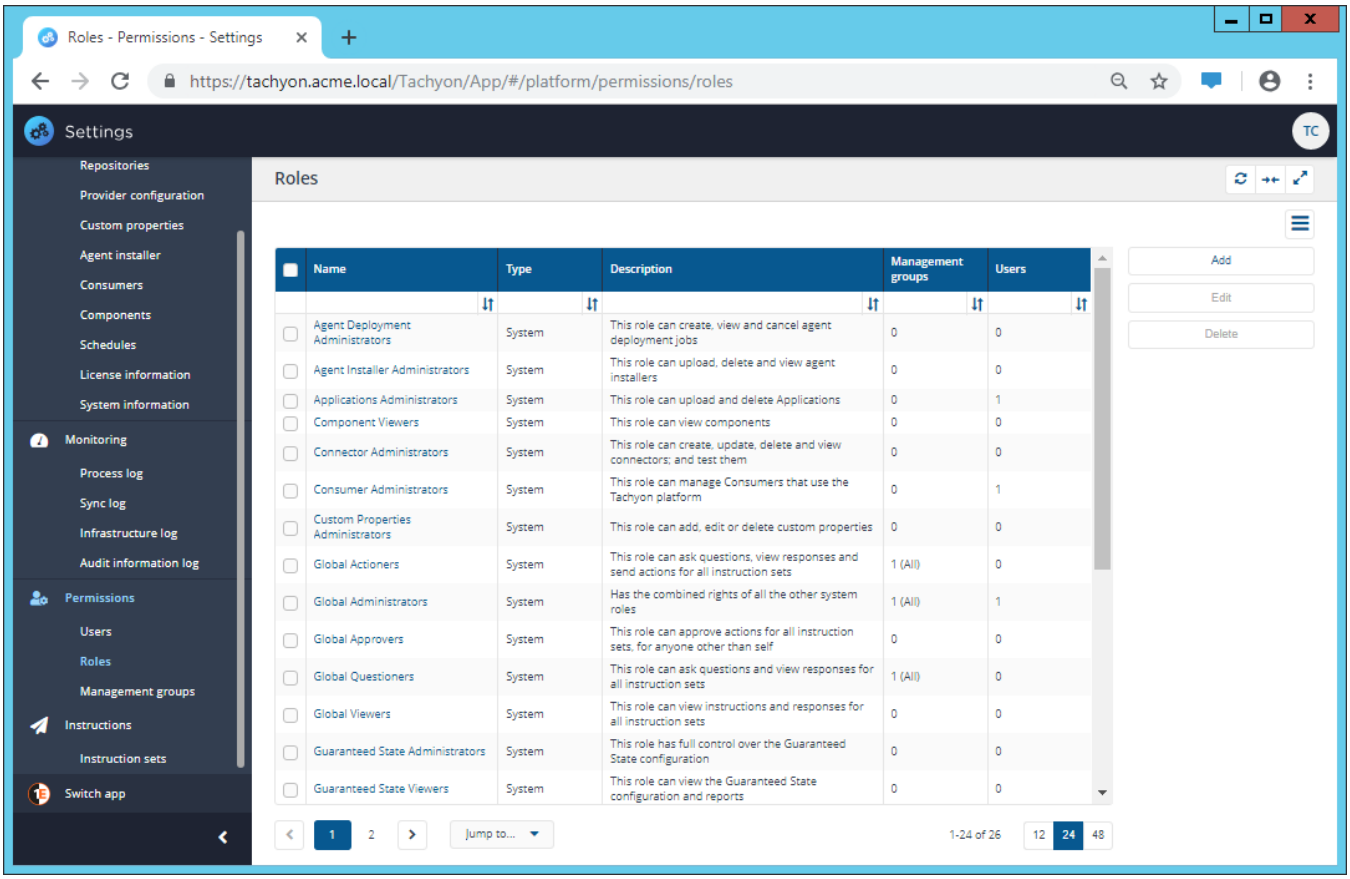
The **Users** page lets you view and manage the current users of Tachyon.
From this page you can:

- Reactivate deactivated users
- Deactivate selected users
- Add new users
- Remove users
- View the details for particular users and set their roles.



Roles page

The **Roles** page lets you view the system roles and currently defined custom roles. From here you can also go into each role to set its membership and any associated management groups.



Configuring Access Rights - tutorial

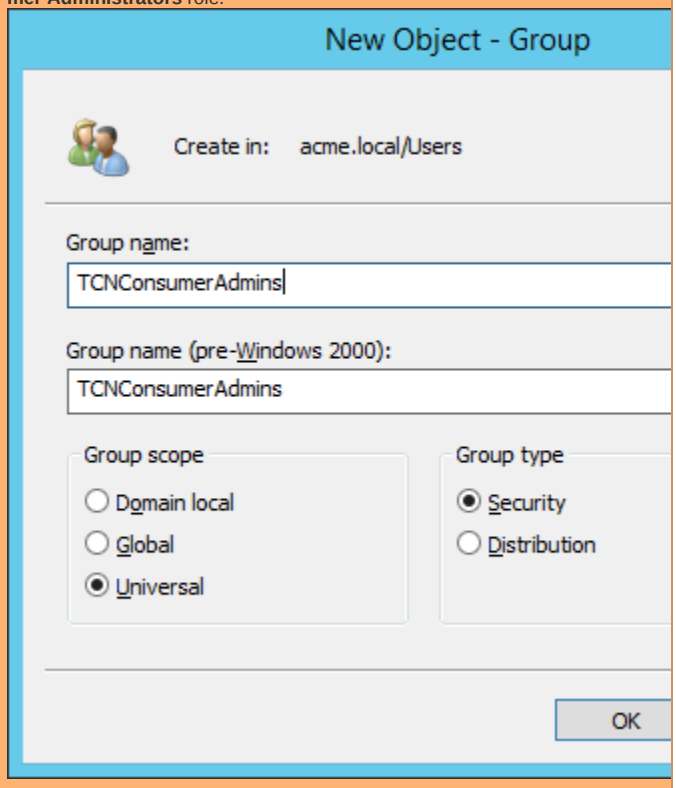
A quick tutorial on configuring access rights for Tachyon. Using a scenario where access to Tachyon will be managed through Active Directory groups, the tutorial illustrates the general setup required and the particular steps needed to add the necessary Tachyon users.

In this tutorial

In this tutorial we demonstrate a process for creating Active Directory (AD) managed permissions to the Tachyon portal. We use specifically created AD groups for each of the Tachyon system roles and create Tachyon users for each one, we then define a custom role for a specific Instruction Set and create a Tachyon user with an existing AD group that provides access to running actions in the Instruction Set.

Example AD groups for the Tachyon system roles

As mentioned in Requirements: Active Directory requirements, we recommend that the AD security groups used for defining access to the Tachyon portal features are defined as **Universal** groups. The picture opposite shows an example **TCNConsumerAdmins** AD security group intended for the **Consumer Administrators** role.



Management groups page

Management groups are containers used to group devices and the software installed on those devices. Management groups are defined using configurable rules that look at various properties of the devices and their installed software, these are then evaluated to determine the group membership. This means that Management group membership adapts to changes to the devices and software in your environment.

Management groups are used by Tachyon to:

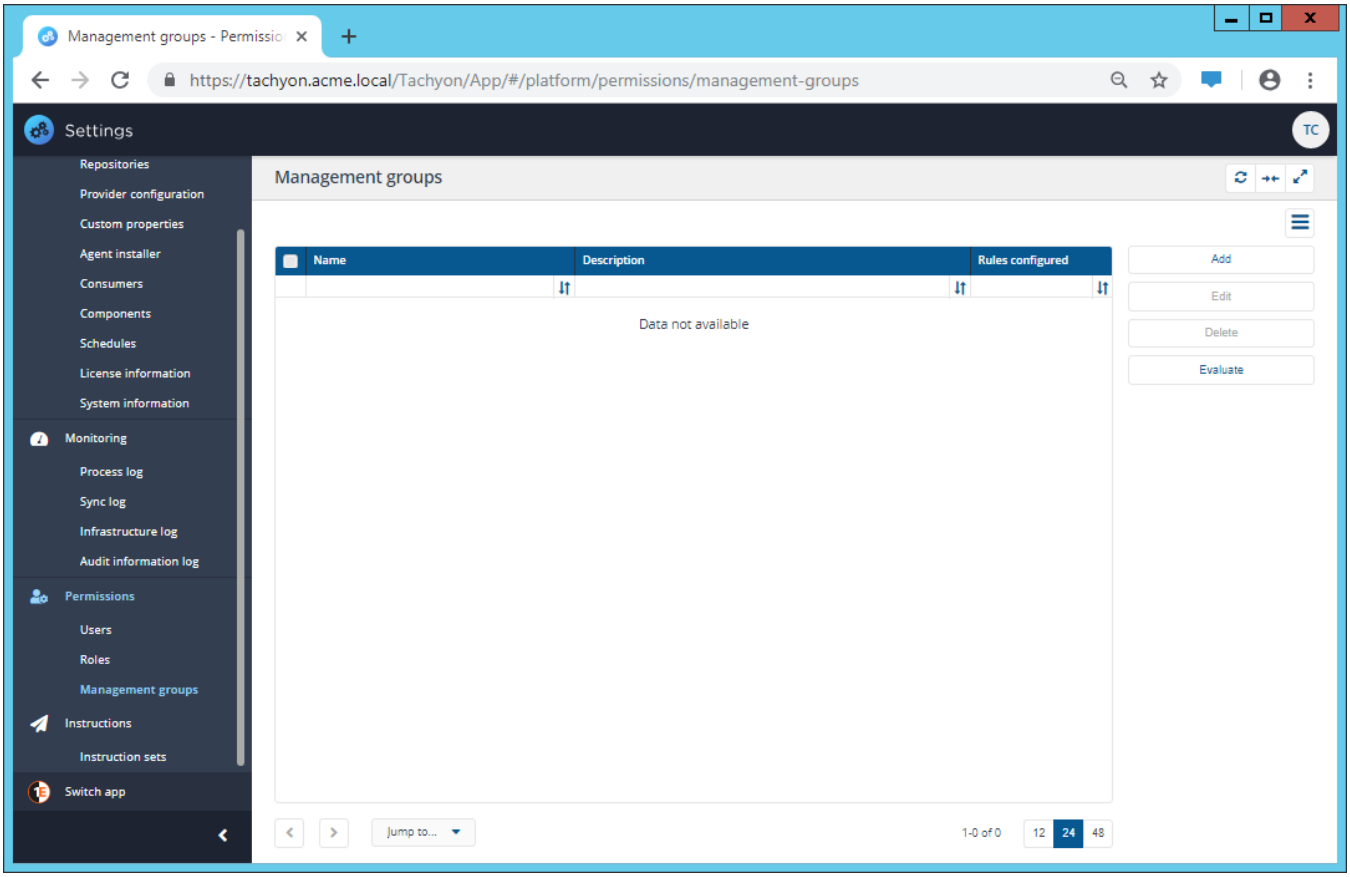
- Determine the targets for questions, actions and reporting.
- Determine user permissions for targeting on particular devices based on Management group membership.

In terms of permissions for determining how Tachyon users interact with the devices in your network, Management groups work alongside Instruction sets. Management groups define *where* users can act. Instruction sets define *what* users can do.

The **Management groups** page lets you add, edit, delete and evaluate management groups.

Management groups have the following properties:

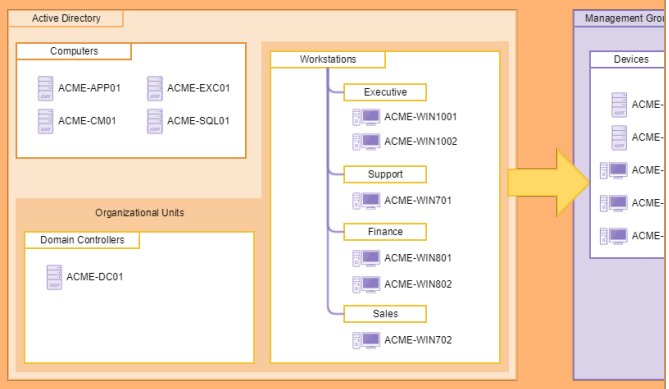
- Each device known to Tachyon can be assigned to any number of management groups, or be left unassigned. Devices not assigned to any management group will still be accessible, subject to permissions.
- Roles can be associated with specific management groups, so that users with those roles will only be able to target the devices in their management groups.
- Management groups can only contain devices and they are completely independent from any other management group, even if they contain the same devices.
- Each Management Group must have a unique name which is not case sensitive.



Management groups - tutorial

In this tutorial

In this tutorial we add a number of management groups for the ACME organization: one that uses the name of the devices and several that use the Organizational Unit (OU) the devices belong to. The following picture shows what we have in our example Active Directory and how this will appear as management groups in Tachyon. Here you can see there are four servers in the AD Computers group, an additional Domain Controller server and six workstations in the OU.



By the end of this example you will have added six management groups:

- Devices - this management group will use the names of the devices to bring them all into a single management group.
- Workstations, Executive, Support, Finance and Sales - these management groups will use an OU rule to separate the devices according to the OU they belong to.