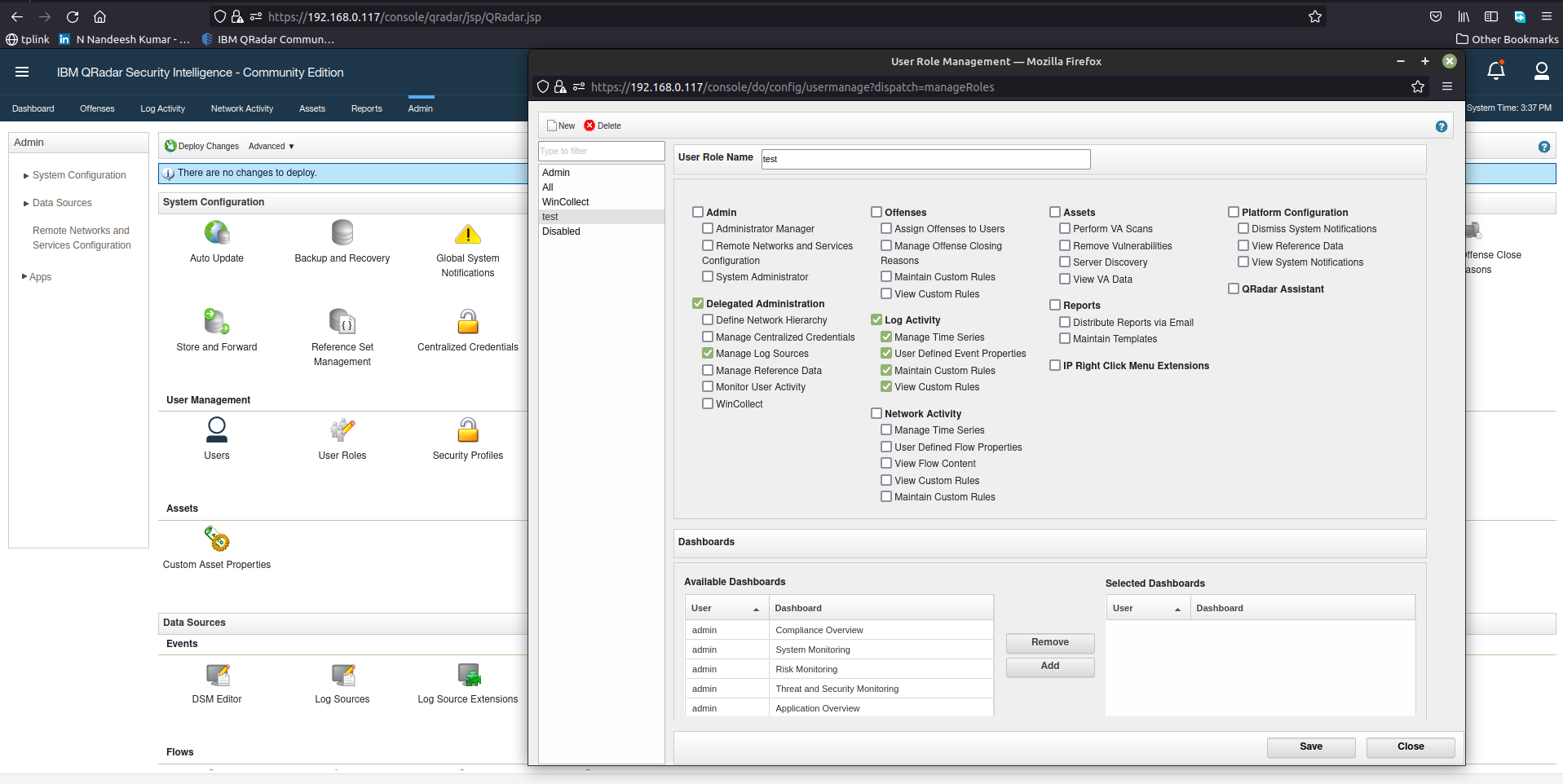
User and roles

1) creating roles

create roles with access to resource which is required for the role

also can provide access to required dashboards

go to admin --> user roles --> new and creating the new role



2) create security profile

The Security Profile Management window defines which networks, log sources, and domains that a user can access.

Permissions precedence

The Permission Precedence setting determines which events and flows appear on the Log Activity and the Network Activity tabs.

For example, if a security profile allows access to events from a log source but the destination network is restricted, the event is displayed on the Log Activity tab if the permission precedence is set to Networks OR Log Sources. If the permission precedence is set to Networks AND Log Sources, the event is not displayed on the Log Activity tab.

The No Restrictions setting permits users of this profile to see all events and flows.

Networks

Use the Networks tab to specify which areas of the deployment users of this profile can access.

Log sources

The log source groupings are nested. If a log source is part of two different groups, the log source appears in the list twice.

The log sources that are assigned to the security profile must also be assigned to the domains that are specified on the Domain tab. You cannot save the security profile if a mismatch exists between the log source assignments and the domain assignments.

Domains

You must define domains on the Domain Management window before the Domains tab is shown on the Security Profile Management window.

Domain assignments take precedence over all settings on the Permission Precedence, Networks, and Log Sources tabs.

If the domain is assigned to a tenant, the tenant name appears in brackets beside the domain name in the Assigned Domains pane.

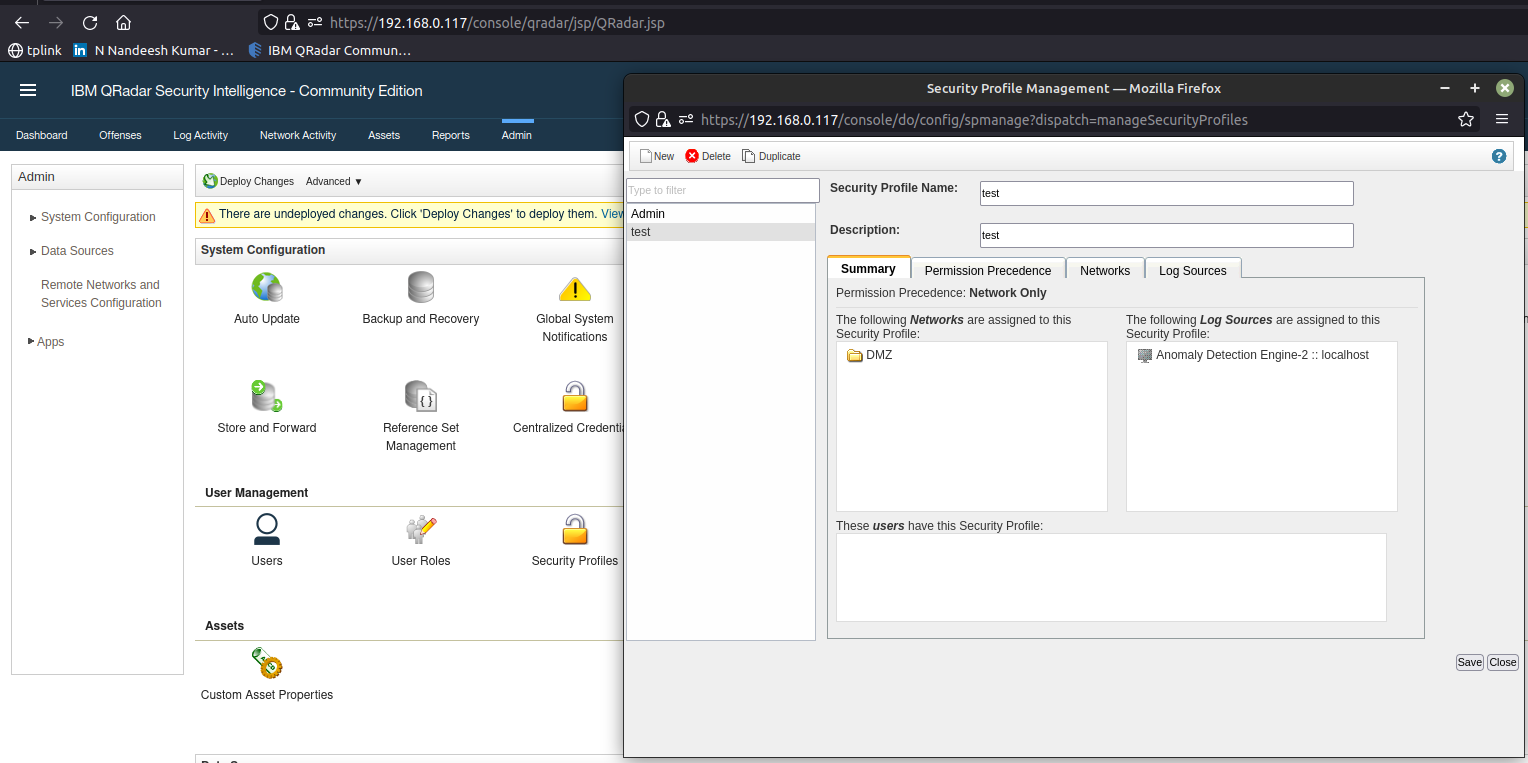
The log sources and domains that are assigned to the security profile must match. You cannot save the security profile if the log sources and domains do not match.

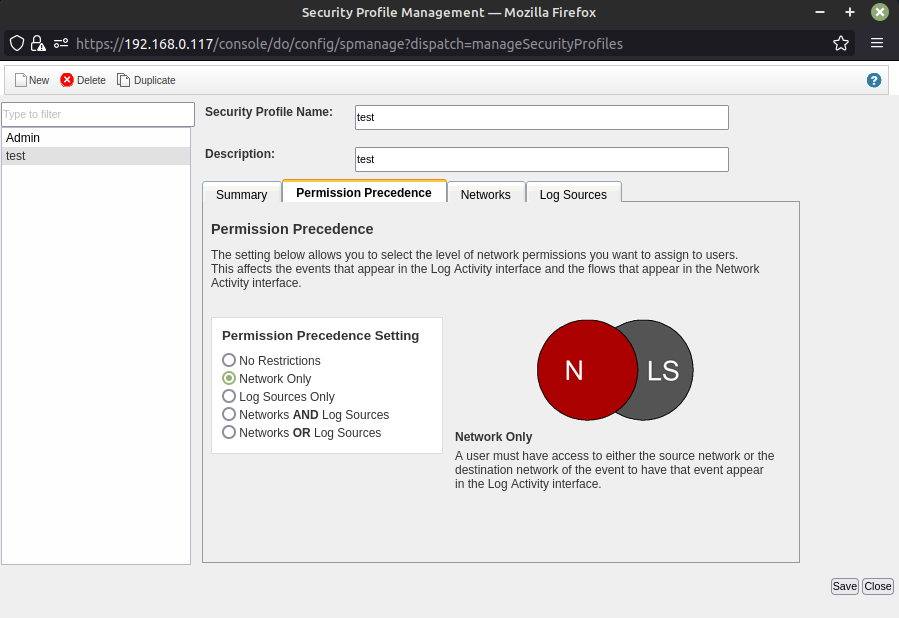
Summary tab

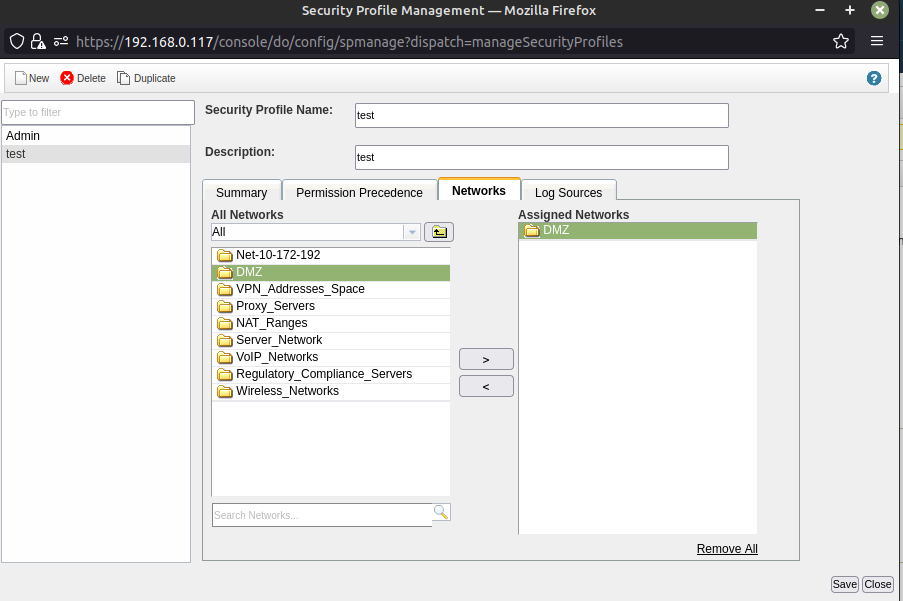
Use the Summary tab to review the settings that you defined and to see the users that have the security profile.

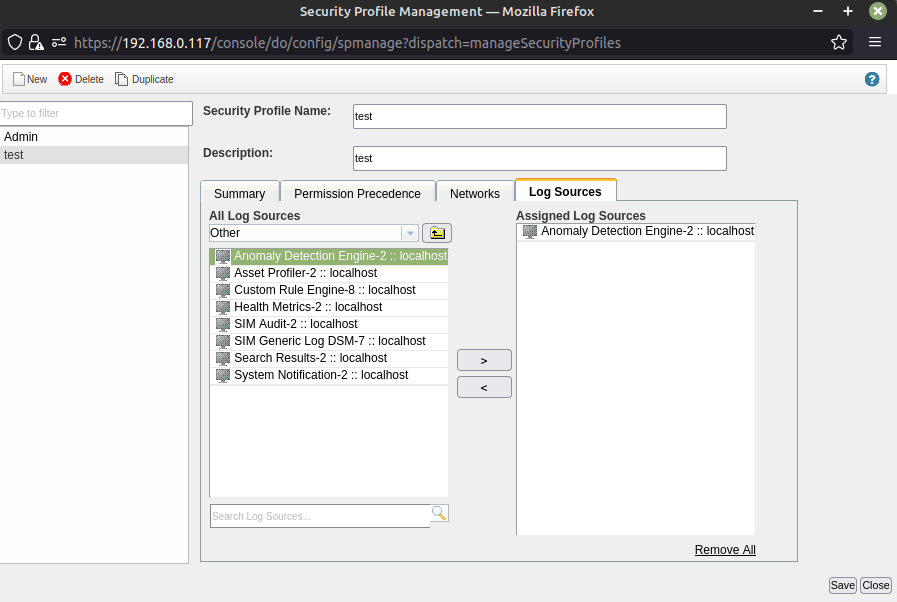
Tenant users are preceded by the tenant name in brackets. Users that have no domain assignments, such as Managed Security Services Provider (MSSP) users, do not show include a tenant name. The user list is sorted alphabetically by user. The tenant name is ignored when the list is sorted.

Note: After you change the security profile, you must click Deploy changes on the Admin tab.

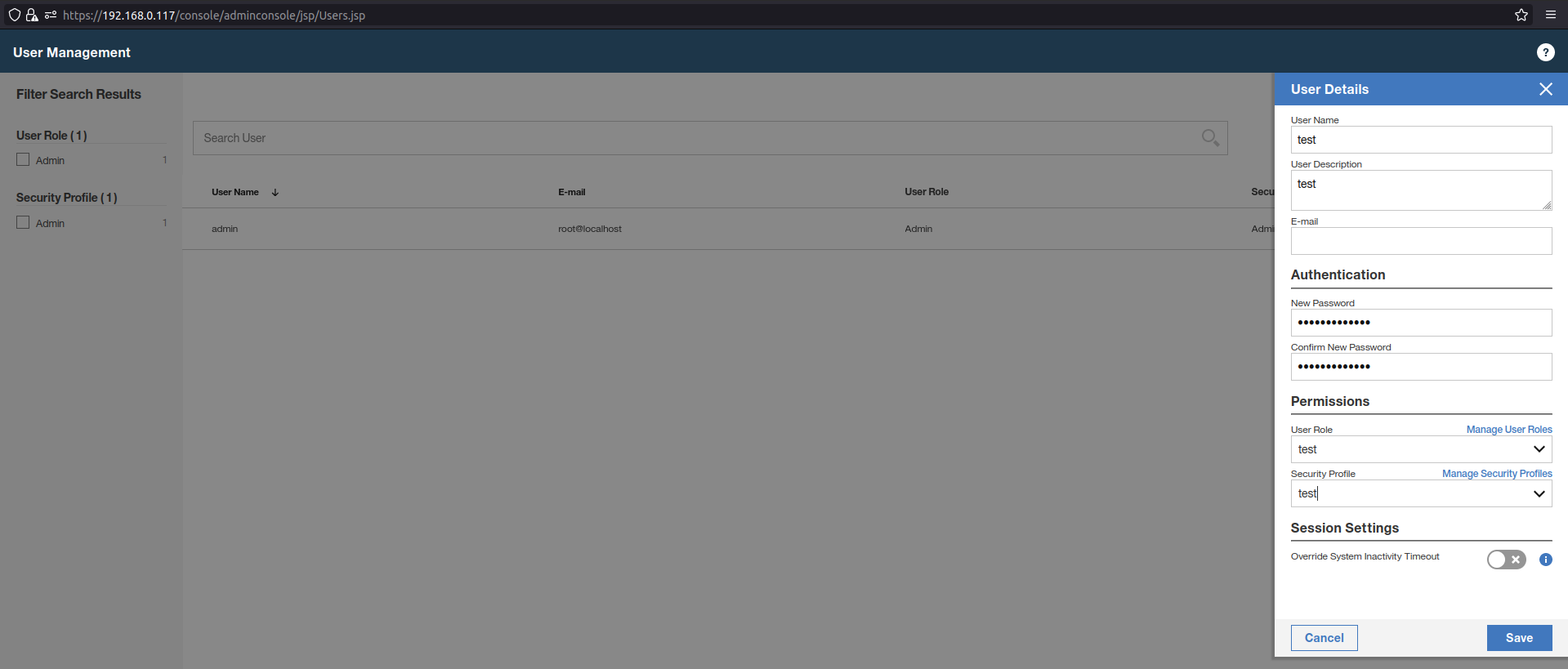




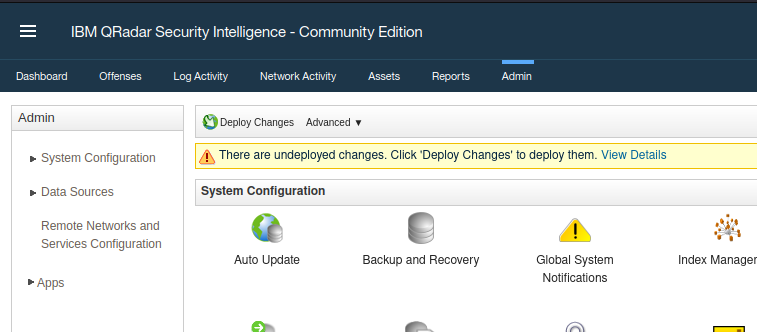




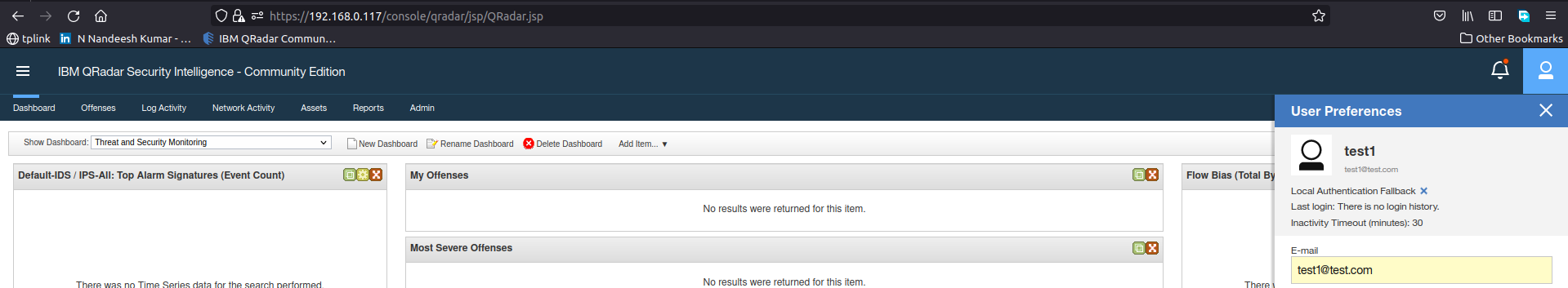
3) create a new user with newly created role and security group



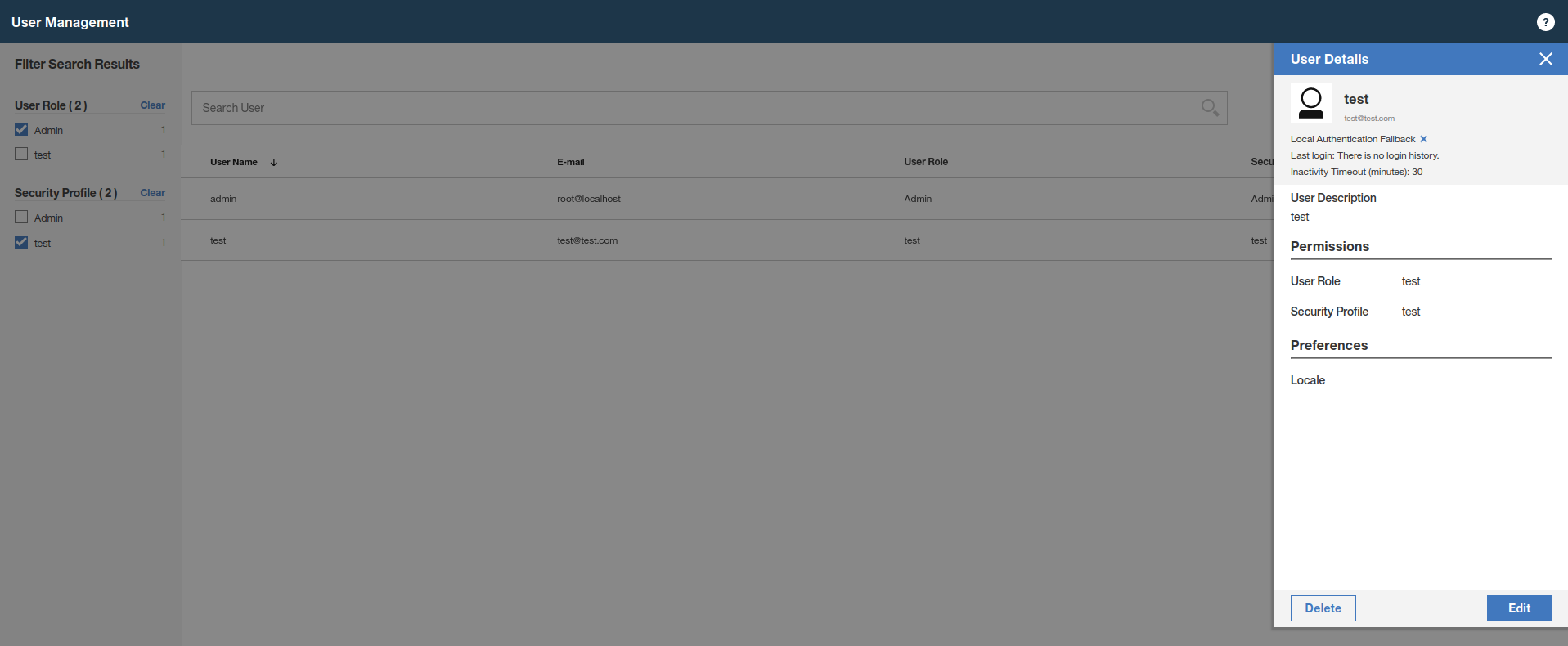
4) deploy the changes to take affect



5) login and check the newly created user



6) can also delete the new created user



7) following list of authentication mechanism is available

[System authentication](https://192.168.0.117/help/en/html/ID_AUTHENTICATION.html" \l "concept_tsn_fc5_rm__sys_auth)

* [RADIUS authentication](https://192.168.0.117/help/en/html/ID_AUTHENTICATION.html" \l "concept_tsn_fc5_rm__radius_auth)
* [TACACS authentication](https://192.168.0.117/help/en/html/ID_AUTHENTICATION.html" \l "concept_tsn_fc5_rm__tacacs_auth)
* [Active Directory](https://192.168.0.117/help/en/html/ID_AUTHENTICATION.html" \l "concept_tsn_fc5_rm__ad_auth)
* [LDAP](https://192.168.0.117/help/en/html/ID_AUTHENTICATION.html" \l "concept_tsn_fc5_rm__ldap_auth)

