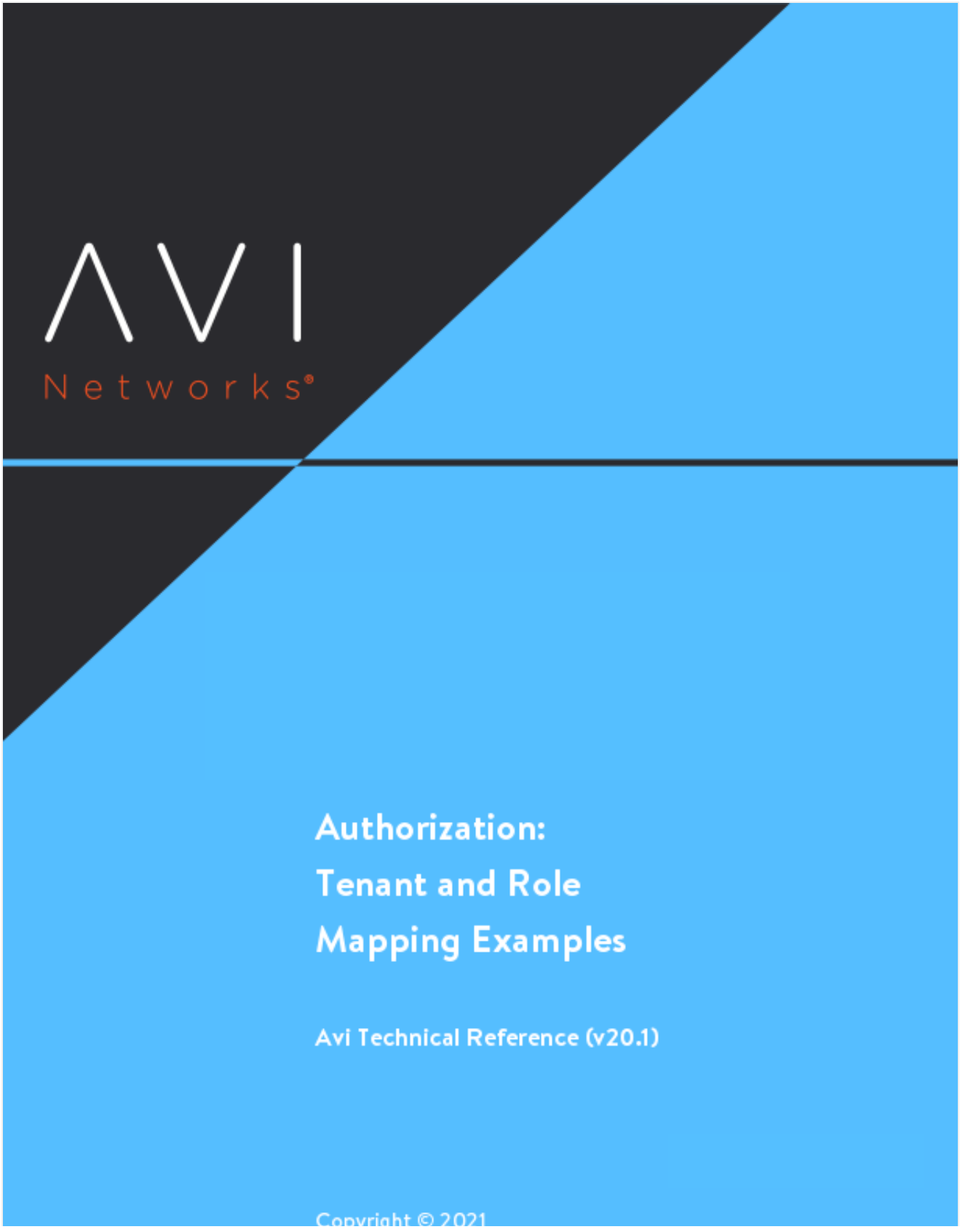


Authorization: Tenant and Role Mapping Examples

Avi Technical Reference (v20.1)

Authorization: Tenant and Role Mapping Examples

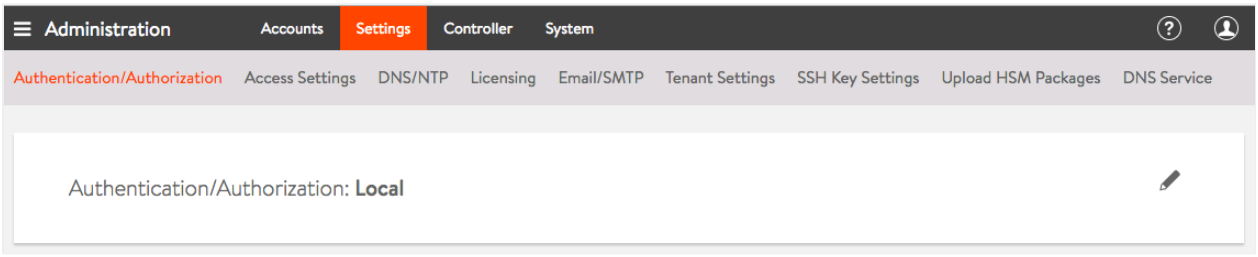
view online

Remote Auth requires assignment of roles and tenants for every user login via the authorization mapping rules. Authorization is assessed on every login and the user record is updated. Upon successful user login via an external authentication server, all mapping rules are evaluated; tenant and role pairs are added to user access list.

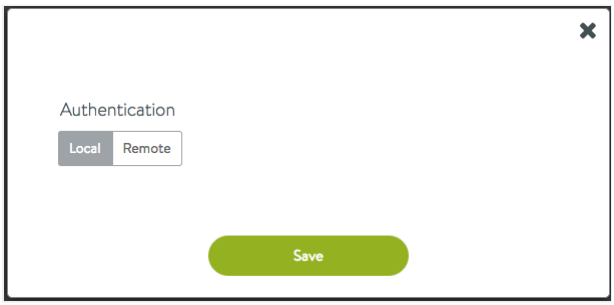
Starting with Avi Vantage 20.1.3, user profile mapping user profile mapping for remote users is supported.

Foreword

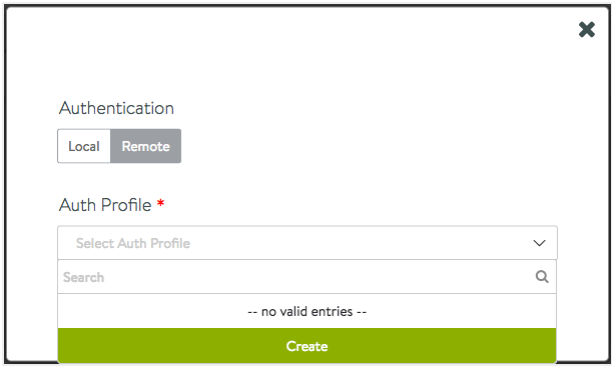
Examples in this article assume the Avi Controller has been set up for remote authentication. By default, a Controller will have only local authentication established, as shown below.



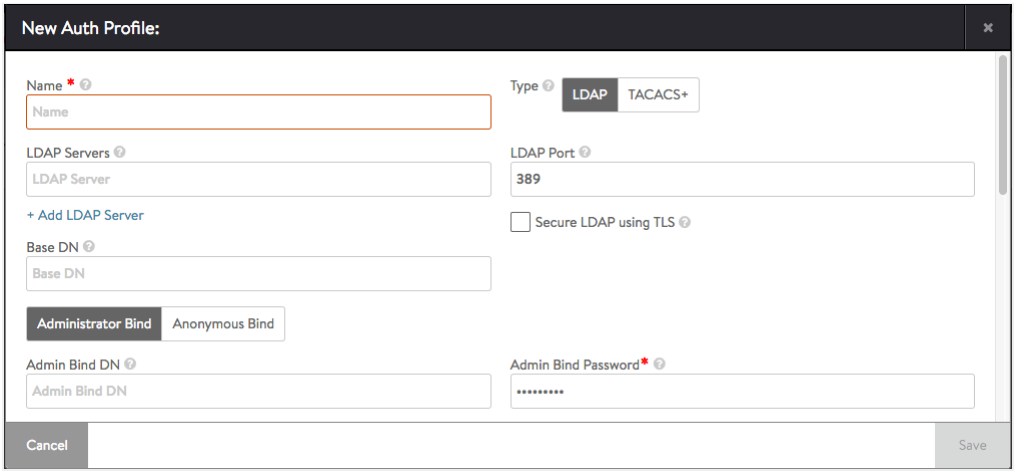
Tenant and role mapping is only available when Administration > Settings > Authentication/Authorization is configured with a Remote server as opposed to the default Local. Clicking on the pencil icon allows you to edit the Authentication process.



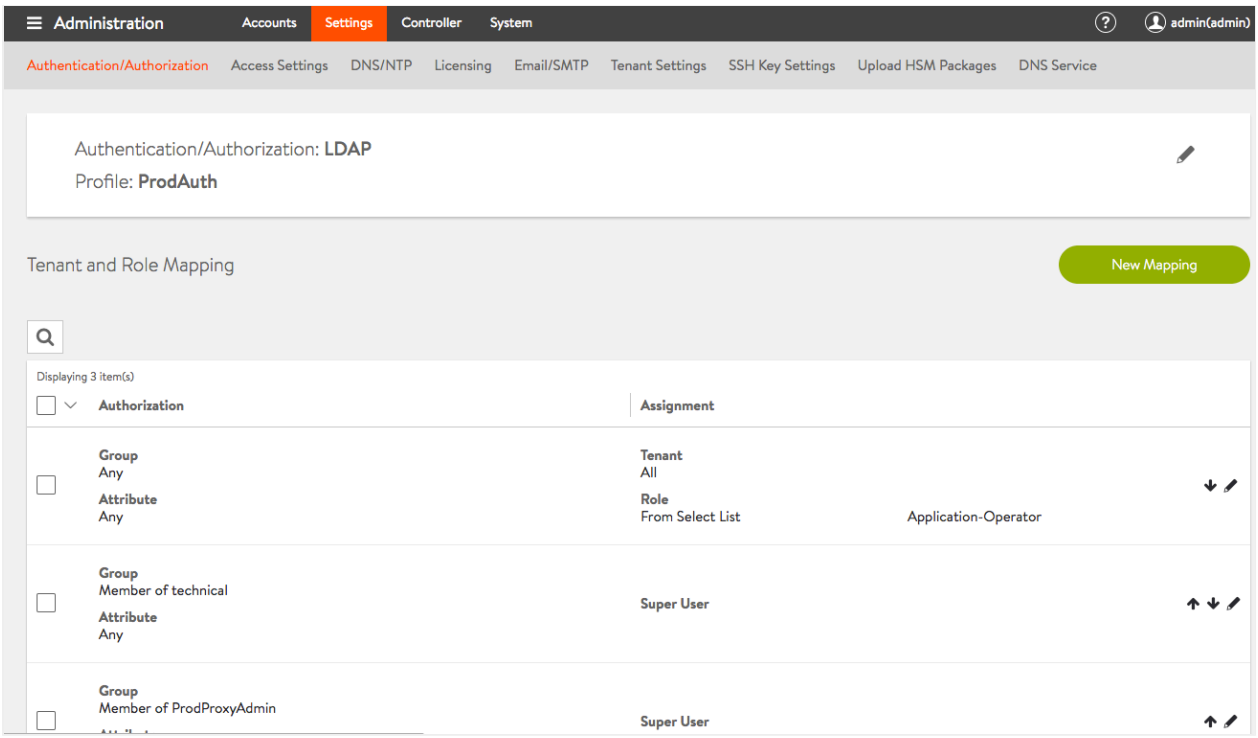
Clicking Remote enables you to either select a pre-existing remote auth profile from the drop-down, or define a new profile by clicking on Create button.



Clicking Create above causes the New Auth Profile editor to pop up:



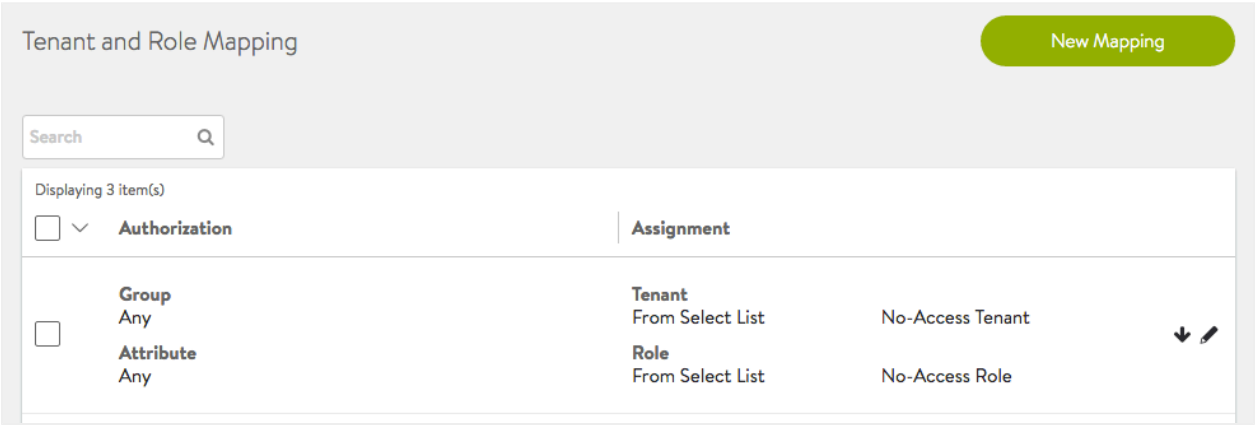
Once the LDAP or TACACS+ remote auth profile has been established, navigating to Administration > Settings > Authentication/Authorization yields a window from which tenant and role mappings may be viewed and/or created.



When the remote server is LDAP, the mapping table can be edited and the options allow us to select Group or Attribute based mapping. When the remote server is TACACS+, the allowed mapping is only based on user Attribute.

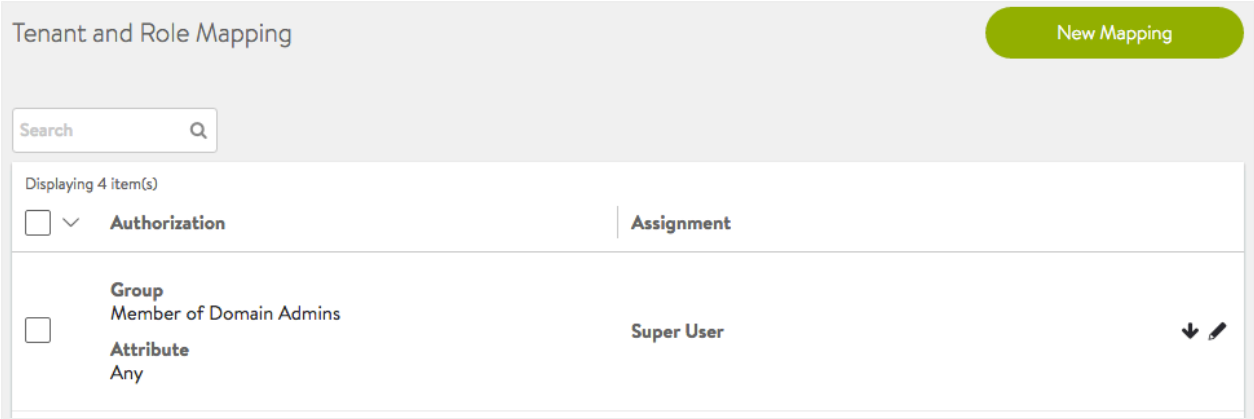
Any Group/Any Attribute Rule

A rule with any group or any attribute applies to all users and can be used as a default option. The rule below assigns every user to a least privileged role and tenant (Note, the role and tenant need to configured to only allow least privileges). If the user is not assigned any more role/tenant pairs, the least privileged access will take effect after login.



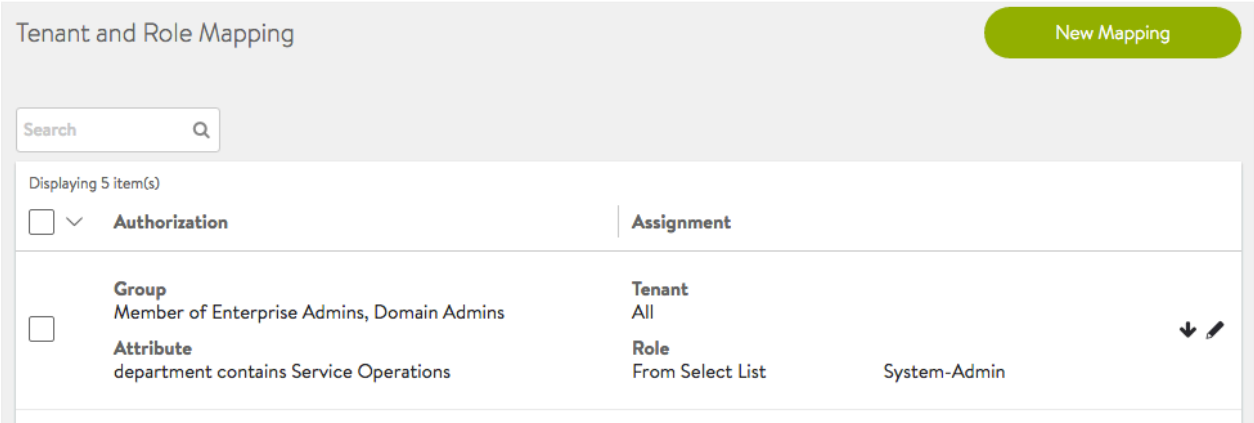
Super User Rule

A rule can be configured to assign Super User privileges to a user. This user will have access to all tenants with the most privileged role. Once a user is super user, no other tenant/role mapping assignments will make a difference to the user's access.



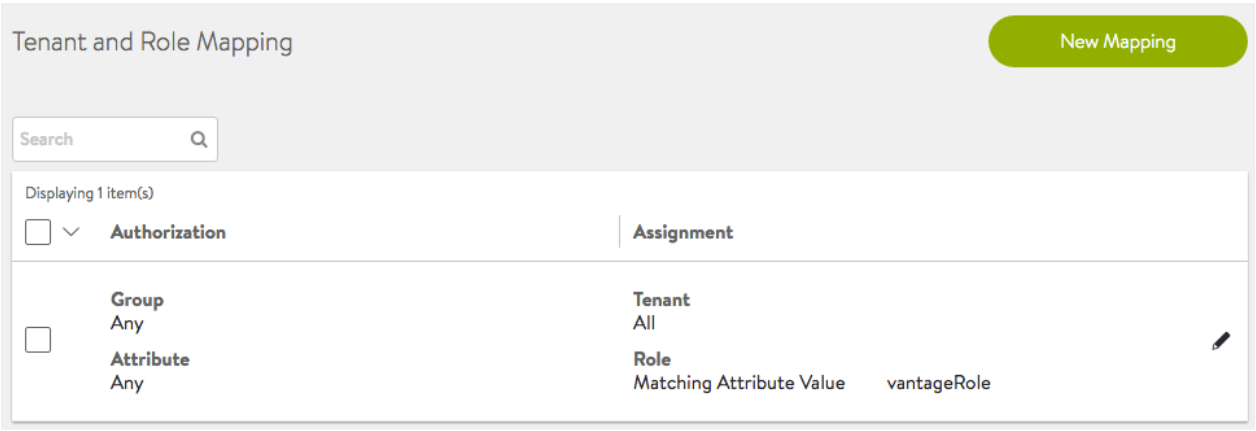
Attribute and Group Match

A mapping rule can be required to match both an attribute and group requirement. This will ensure a more specific assignment of role(s) and tenant(s).



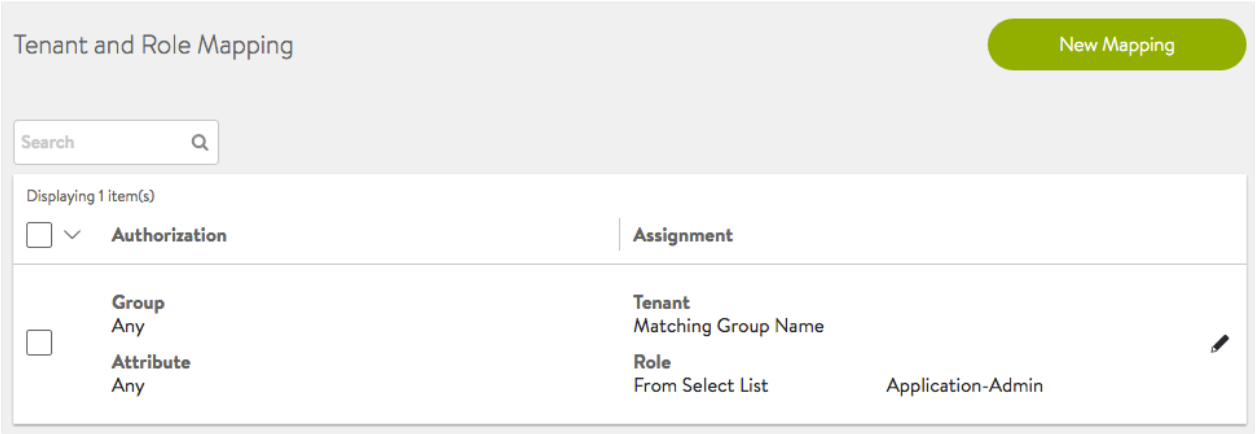
Assign Matching Attribute Values

LDAP/TACACS+ attribute "vantageRole" for a user can have one or more values. For each value, if there is a configured role with the same name, the role is assigned to the user with access to all tenants. A user session can end up with multiple roles and the most privileged role will take effect.



Assign Matching Group Names

A user can be a member of multiple LDAP/AD groups. For each group, if there is a configured tenant, the user will be given access to the tenant, along with any other tenants the user may already have obtained access via matching rules.



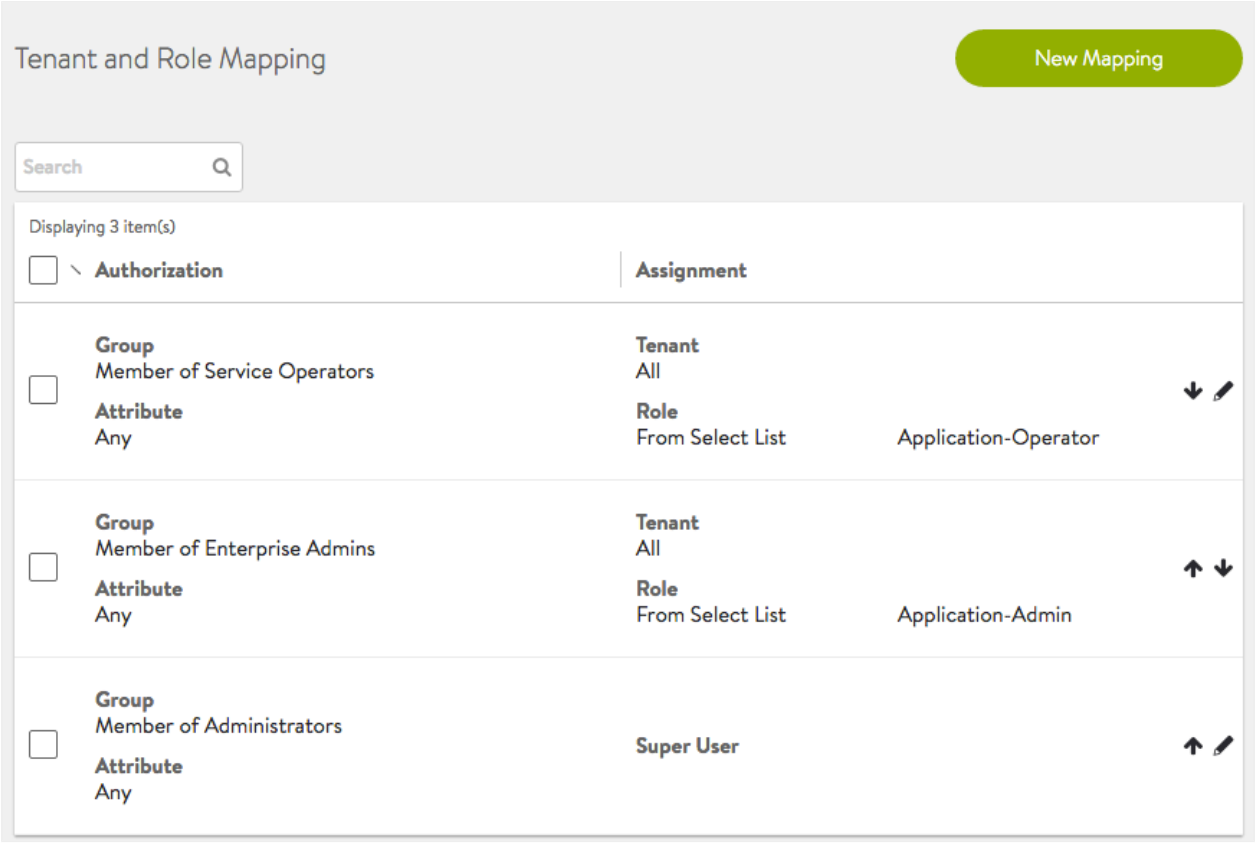
Examples

Multiple Groups Mapping to Different Roles

This example illustrates the case of an IT team with three user groups ? super-admins, app-admins, operations ? where the following applies:

- Super Admins: may access all tenants, all settings, hence, they are super users.
- Application Admins:
  - may only create, read, update and delete virtual services and other profiles.
  - may not create clouds.
- Application Operators: have read-only access.

Separate mapping rules are required to map users from each group to different role/tenant assignments.

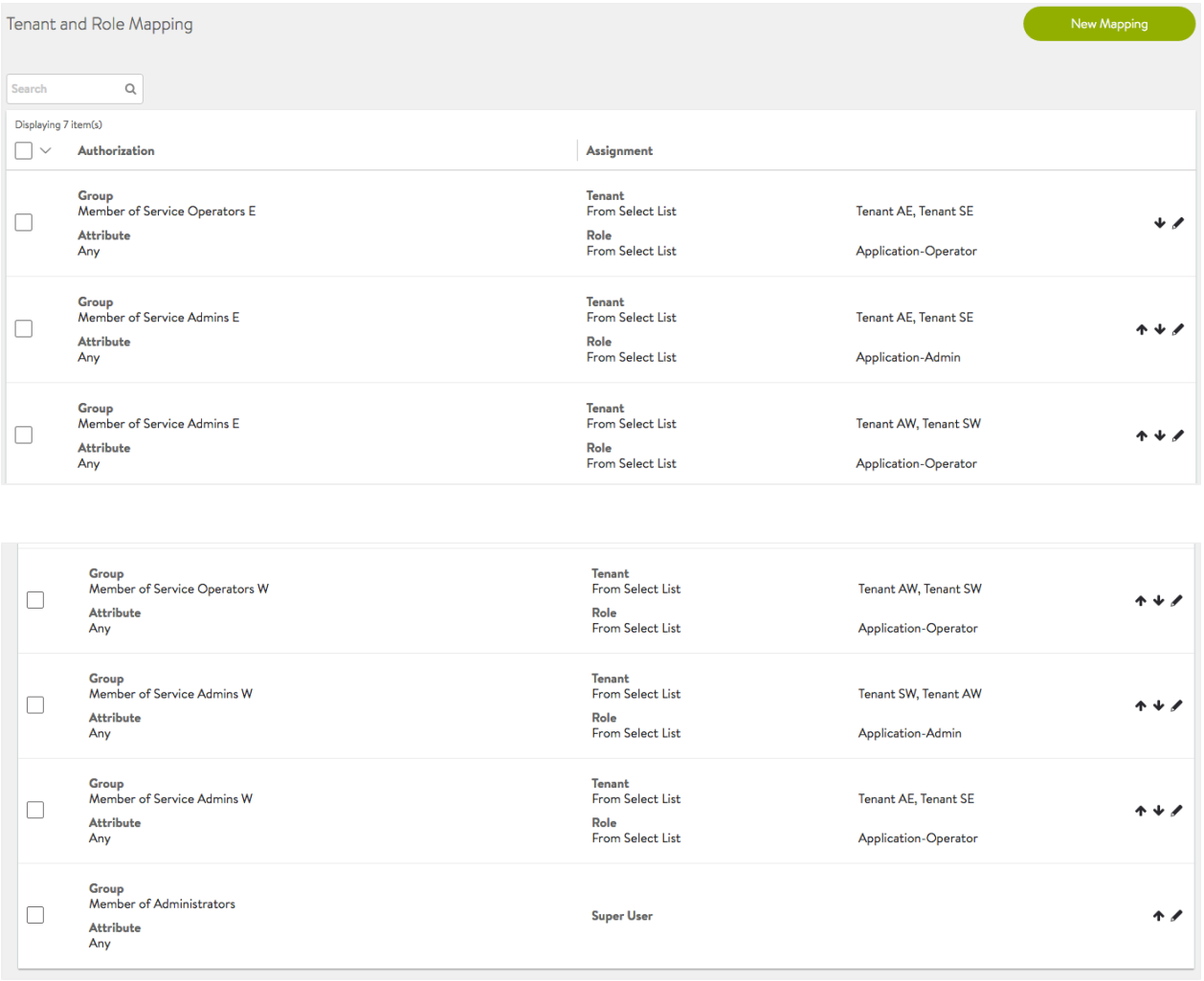


Multiple Groups Mapping to Different Tenants

This example illustrates settings for an IT team that expects tenant isolation except for a few super users.

- Super Admins: can access all tenants, all settings, hence, they are super users.
- Tenant Application Admins: have access to a few tenants ? app owner for few tenants
- Tenant Application Operators: have access to a few tenants ? cannot modify anything
- Tenant Application Admins/Operators: have access to a few tenants as app owners and other tenants as app operator folks.

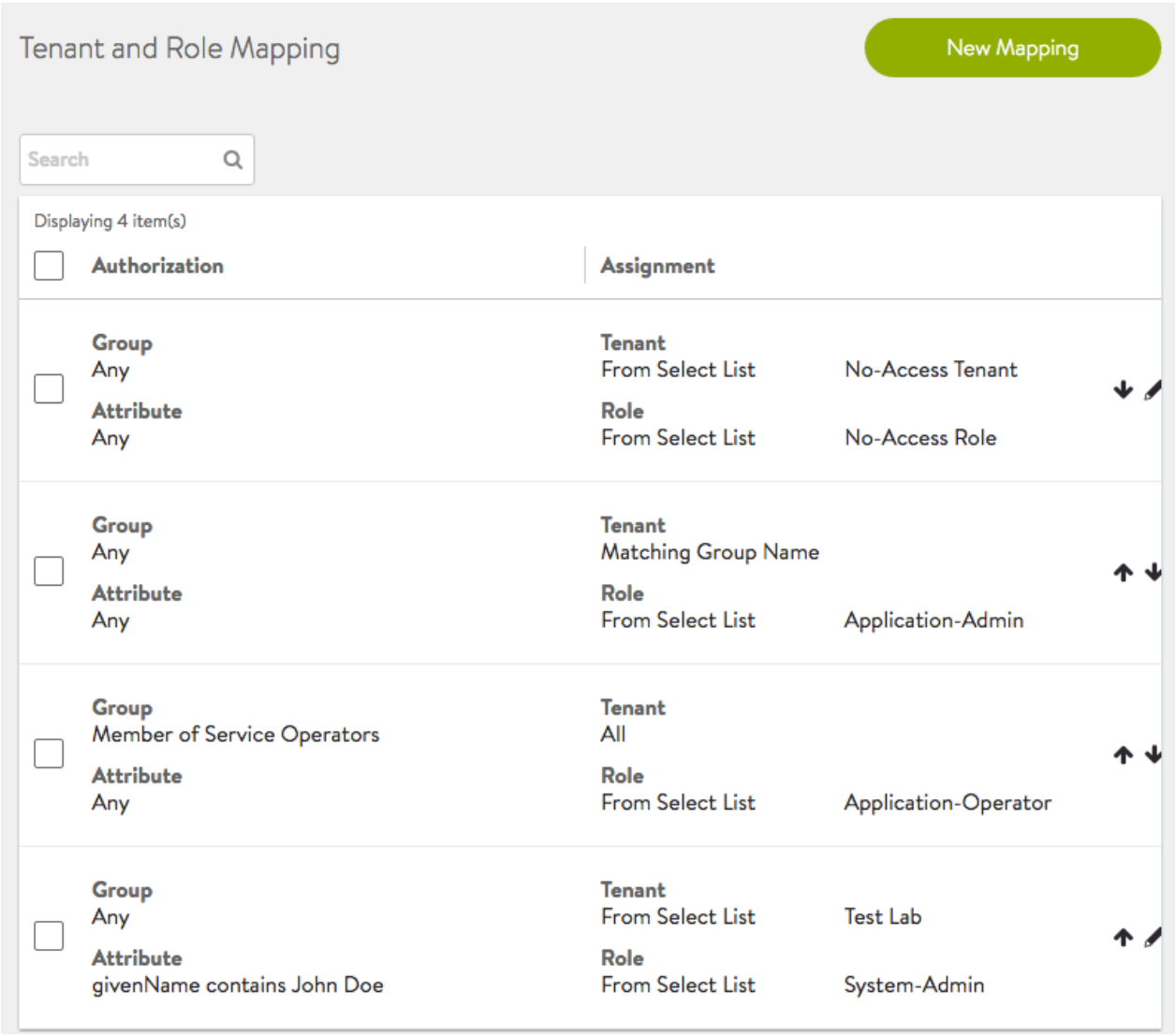
In this example, members of group "Service Admins E" have read/write access (Application-Admin role) in tenants Tenant AE and Tenant SE, while they have read only access (Application-Operator role) in a few other tenants. "Service Operators" have only read-only access in their respective tenants.



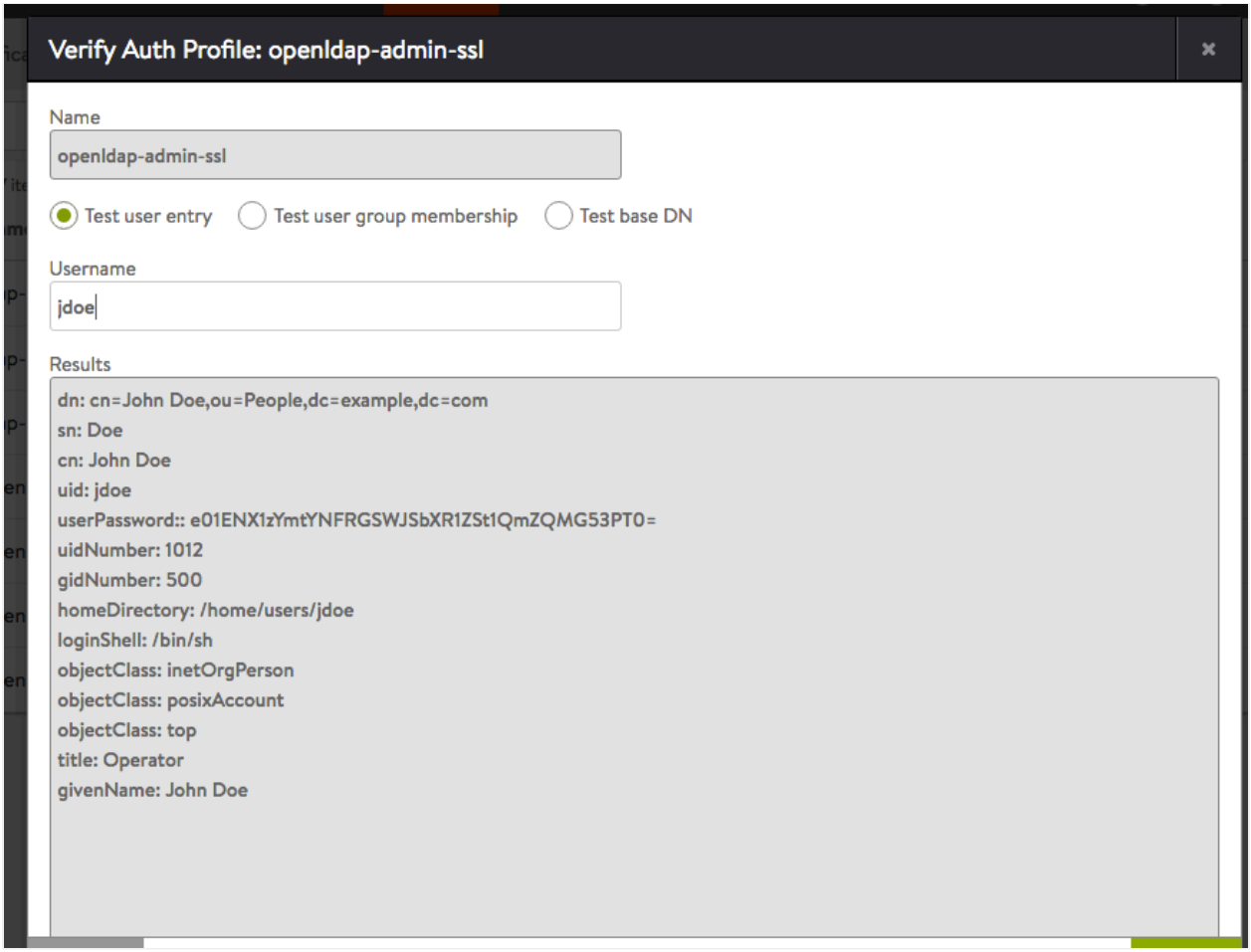
Multiple Authorizations for a Single User

In this example, login of user John Doe results in the user gaining access via multiple authorization mapping rules.

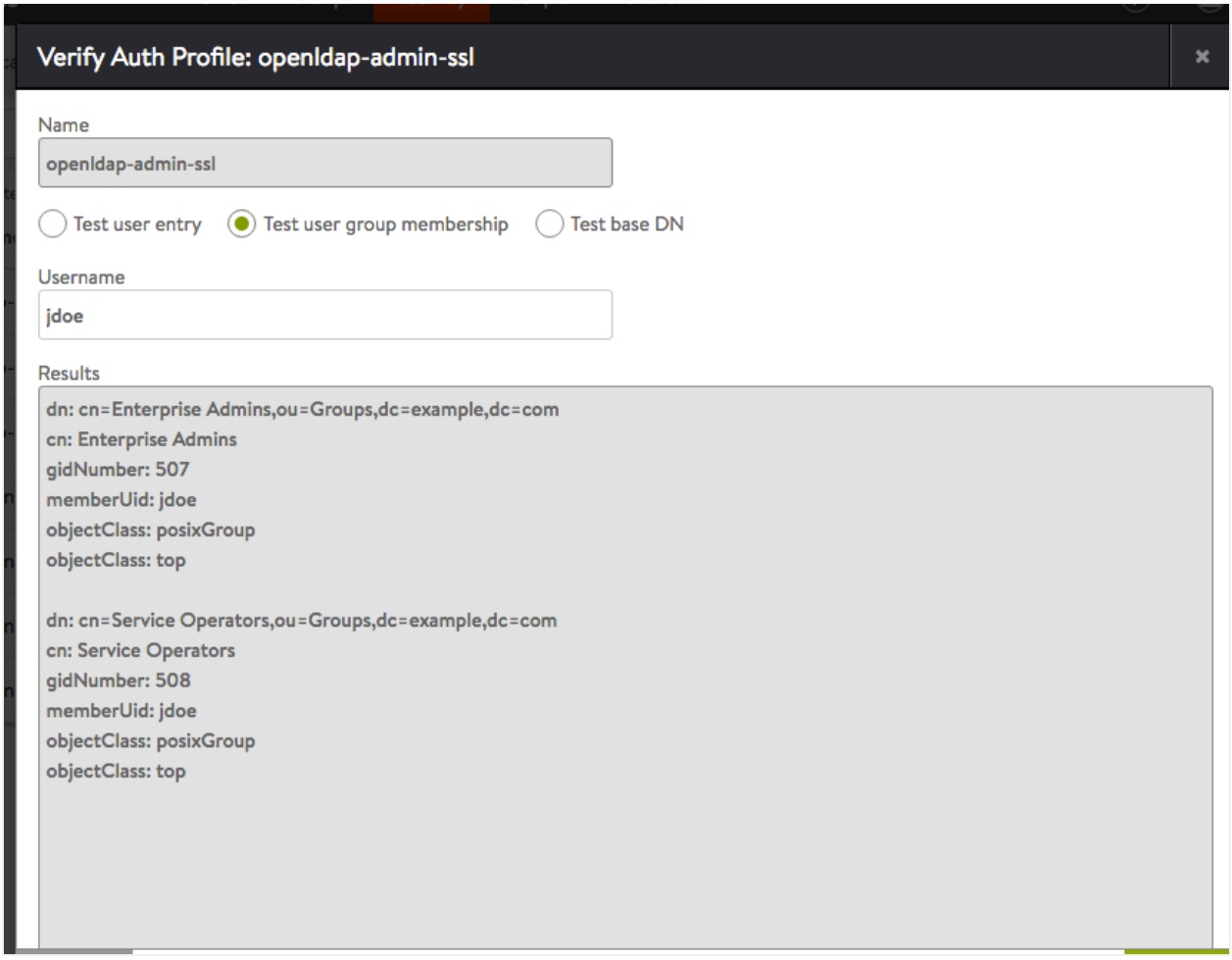
Multiple mapping rules are configured based on various group and attribute criteria.



The LDAP server is configured with user John Doe.



The LDAP server is configured with John Doe as a member of the groups Enterprise Admins and Service Operators.



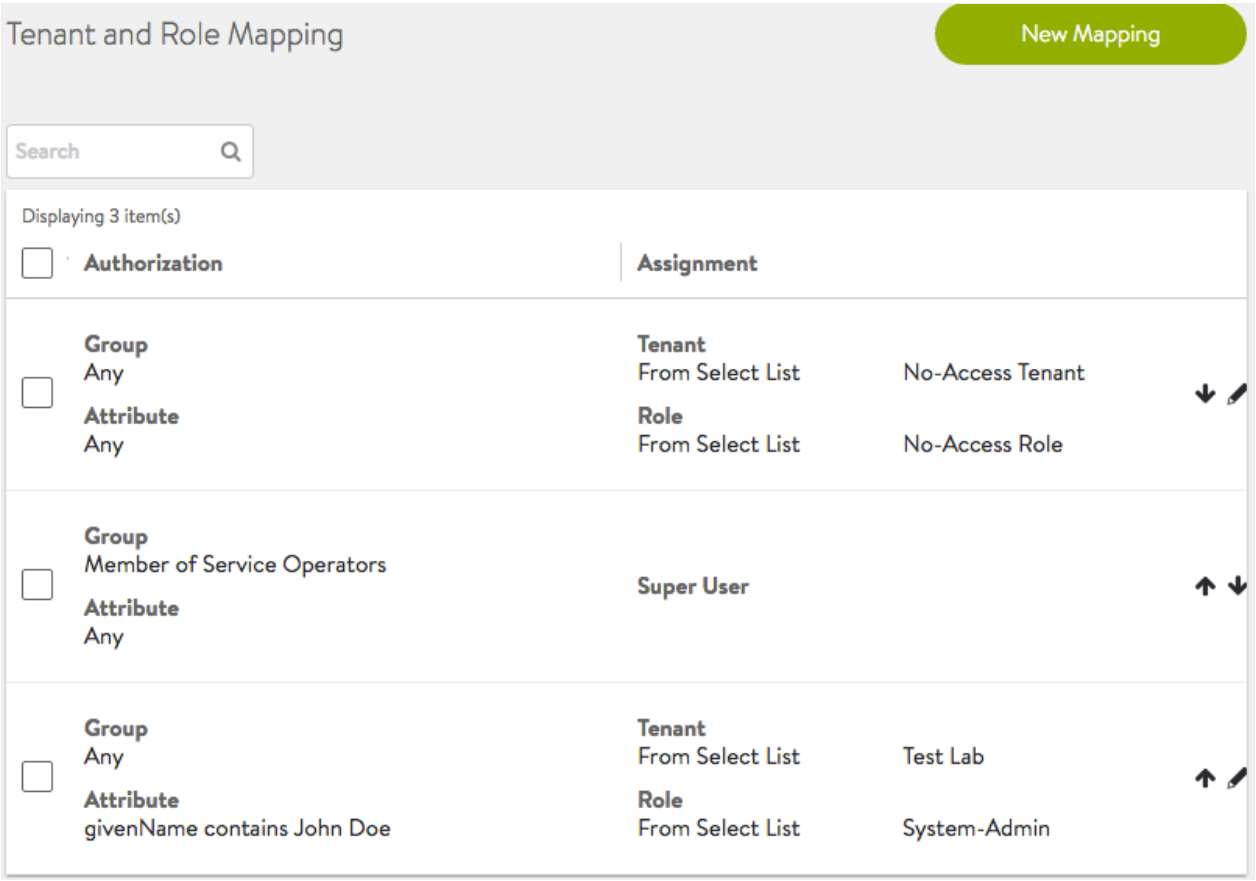
After user John Doe logs in and all authorization rules are applied on the user session. Multiple role/tenant combinations are used to determine user privileges during user login. The user record shows the user successfully matched all 4 rules and role /tenant pairs were appropriately applied.

```
[: > show user jdoe
+----------------------+------------------------------------------+
| Field                | Value                                    |
+----------------------+------------------------------------------+
| uuid                 | user-fe20bd42-8448-49a8-a684-a8bddf772ab6 |
| username             | jdoe                                     |
| name                 | jdoe                                     |
| email                |                                          |
| access[1]            |                                          |
|   role_ref           | No-Access Role                           |
|   tenant_ref         | No-Access Tenant                         |
|   all_tenants        | False                                    |
| access[2]            |                                          |
|   role_ref           | Application-Admin                        |
|   tenant_ref         | Enterprise Admins                        |
|   all_tenants        | False                                    |
| access[3]            |                                          |
|   role_ref           | Application-Operator                     |
|   all_tenants        | True                                     |
| access[4]            |                                          |
|   role_ref           | System-Admin                             |
|   tenant_ref         | Test Lab                                 |
|   all_tenants        | False                                    |
| is_superuser         | False                                    |
| last_login_ip        | 10.10.221.128                            |
| last_login_timestamp | 2016-08-06 08:20:37                      |
| logged_in            | True                                     |
| local                | False                                    |
| full_name            | John Doe                                 |
| default_tenant_ref   | No-Access Tenant                         |
+----------------------+------------------------------------------+
: >
```

Multiple Authorizations Resulting in a Super User

In this example, login of user John Doe results in the user becoming super user.

Mapping rules make a member of the group Service Operators a super user.



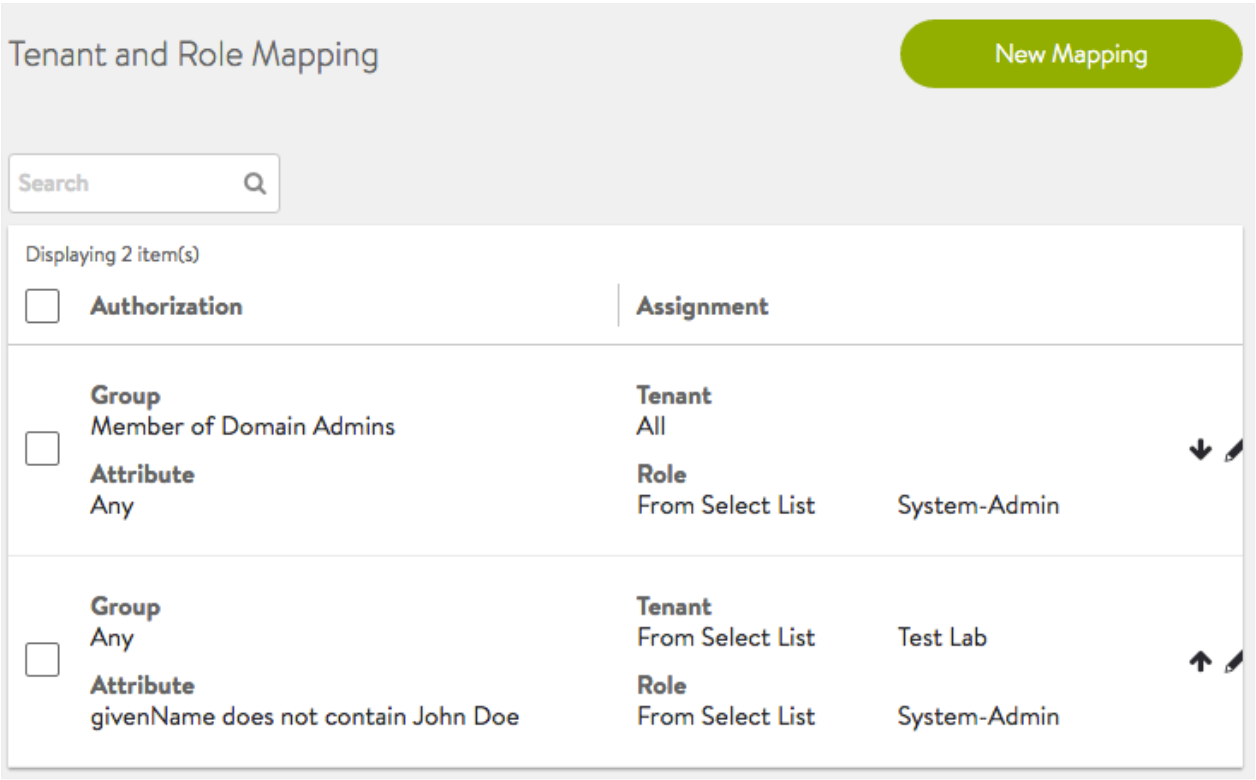
Due to the super user access, user John Doe gets access to all tenants with every role.

```
: > show user jdoe
+----------------------+------------------------------------------+
| Field                | Value                                    |
+----------------------+------------------------------------------+
| uuid                 | user-2d4348f3-fcf6-4af3-9c8b-ff54476ad7f6 |
| username             | jdoe                                     |
| name                 | jdoe                                     |
| email                |                                          |
| access[1]            |                                          |
|   role_ref           | No-Access Role                           |
|   tenant_ref         | No-Access Tenant                         |
|   all_tenants        | False                                    |
| access[2]            |                                          |
|   role_ref           | Application-Admin                        |
|   all_tenants        | True                                     |
| access[3]            |                                          |
|   role_ref           | Tenant-Admin                             |
|   all_tenants        | True                                     |
| access[4]            |                                          |
|   role_ref           | System-Admin                             |
|   all_tenants        | True                                     |
| access[5]            |                                          |
|   role_ref           | Application-Operator                     |
|   all_tenants        | True                                     |
| access[6]            |                                          |
|   role_ref           | Security-Admin                           |
|   all_tenants        | True                                     |
| access[7]            |                                          |
|   role_ref           | Operator                                 |
|   all_tenants        | True                                     |
| access[8]            |                                          |
|   role_ref           | No-Access Role                           |
|   all_tenants        | True                                     |
| access[9]            |                                          |
|   role_ref           | System-Admin                             |
|   tenant_ref         | Test Lab                                 |
|   all_tenants        | False                                    |
| is_superuser         | True                                     |
| last_login_ip        | 10.10.221.128                            |
| last_login_timestamp | 2016-08-06 18:28:39                      |
| logged_in            | True                                     |
| local                | False                                    |
| full_name            | John Doe                                 |
| default_tenant_ref   | No-Access Tenant                         |
+----------------------+------------------------------------------+
: >
```

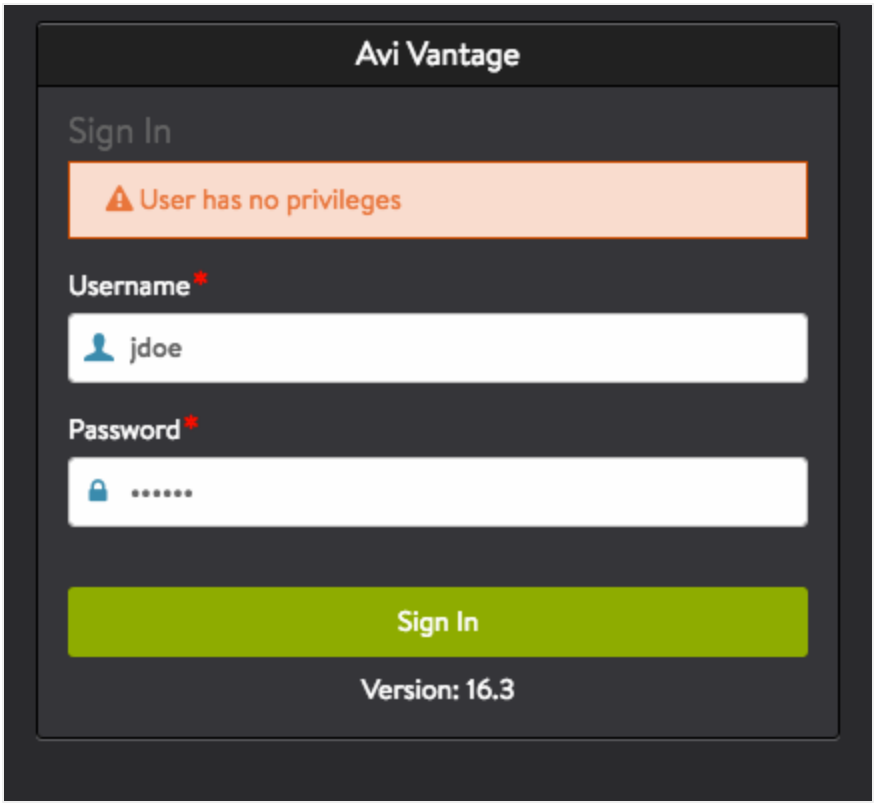
No Authorizations for a Single User

In this example, login of user John Doe results in the user not getting any roles or tenants.

Mapping rules are updated to keep user John Doe from having any privileges.



When user John Doe logs in, the user interface reports no privileges to login.



User record does not have any access entries.

```
[: > show user jdoe
+----------------------+------------------------------------------+
| Field                | Value                                    |
+----------------------+------------------------------------------+
| uuid                 | user-2d4348f3-fcf6-4af3-9c8b-ff54476ad7f6 |
| username             | jdoe                                     |
| name                 | jdoe                                     |
| email                |                                          |
| is_superuser         | False                                    |
| last_login_ip        | 10.10.221.128                            |
| last_login_timestamp | 2016-08-07 06:08:42                      |
| logged_in            | True                                     |
| local                | False                                    |
| full_name            | John Doe                                 |
+----------------------+------------------------------------------+
: >
```

Tenant to Role Mappings

Avi Vantage supports dynamically assigning tenant and role name based on a regex match. This requires a tenant or role variable to be configured in the regex to assign tenant/role name based on the regex. The variables must be in the `(?P{tenant}regex)` form

Example:

LDAP DATA

user: test_user

test_user is a member of the following groups:

- lb_ap1234_test
- lb_ap7890_test

Mapping Rule Configuration:

The following is the CLI format:

```
"attribute_match": {
           "values": [ "lb_?P{tenant}\\w*)_test" ],
           "name": "tenant",
           "criteria": "AUTH_MATCH_REGEX"
         }
 "assign_tenant": "ASSIGN_MATCHING_ATTRIBUTE_REGEX",
 "assign_role": "ASSIGN_FROM_SELECT_LIST"
 "role_refs": ["https://10.10.24.204/api/role/[Role-UUID]" ],
}
```

Result:

With this rule mapping and LDAP configuration, test_user will get `<role-uuid></role-uuid>` (say, Tenant-admin) assigned in tenants `ap1234` and `ap7890`.

You can configure the above rule in the CLI as follows:

```
configure systemconfiguration
admin_auth_configuration
mapping_rules index 2
group_match criteria auth_match_regex groups adcs_(?P{tenant}\\w*)_fa
save
assign_tenant assign_matching_group_regex assign_role assign_from_select_list role_refs Tenant-Admin
save
mapping_rules index 3
group_match criteria auth_match_regex groups adcs_(?P{tenant}\\w*)_ra
save
assign_tenant assign_matching_group_regex assign_role assign_from_select_list role_refs Application-Admin
save
mapping_rules index 4
group_match criteria auth_match_regex groups adcs_(?P{tenant}\\w*)_ro
save
assign_tenant assign_matching_group_regex assign_role assign_from_select_list role_refs Application-Operator
save
save
save
```

User Profile Mapping

With user profile mapping, it is possible to choose a user profile for remote users based on certain conditions.

To configure the user profile,

```
[admin:123]: systemconfiguration> admin_auth_configuration
[admin:123]: systemconfiguration:admin_auth_configuration> mapping_rules index 1
[admin:123]: systemconfiguration:admin_auth_configuration:mapping_rules> assign_userprofile assign_from_select_list
[admin:123]: systemconfiguration:admin_auth_configuration:mapping_rules> userprofile_ref Tacacs-Userprofile
[admin:123]: systemconfiguration:admin_auth_configuration:mapping_rules> save
```

Note: Ensure the user profile is already created. To know more about how to create and configure a user profile, click here.

View the user profile configuration as shown below:

```
[admin:123]: > show systemconfiguration
|---------------------------------|-----------------------------------|
|Field                            |    Value                          |
|---------------------------------|-----------------------------------|
|                         Truncated Output                            |
| admin_auth_configuration        |                                   |
|   auth_profile_ref              | tacacs1                           |
|   mapping_rules[1]              |                                   |
|     index                       | 1                                 |
|     assign_tenant               | ASSIGN_FROM_SELECT_LIST           |
|     tenant_attribute_name       |                                   |
|     tenant_refs[1]              | admin                             |
|     assign_role                 | ASSIGN_FROM_SELECT_LIST           |
|     role_attribute_name         |                                   |
|     role_refs[1]                | Application-Admin                 |
|     is_superuser                | False                             |
|     assign_userprofile          | ASSIGN_FROM_SELECT_LIST           |
|     userprofile_ref             | Tacacs-Userprofile                |
|   allow_local_user_login        | True                              |
|---------------------------------|-----------------------------------|
```