



Authorization: Tenant and Role Mapping Examples

Avi Technical Reference (v17.1)

Copyright © 2019

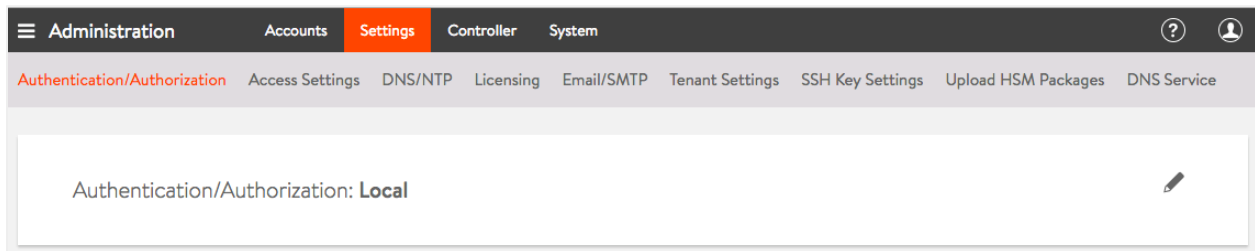
Authorization: Tenant and Role Mapping Examples

[view online](#)

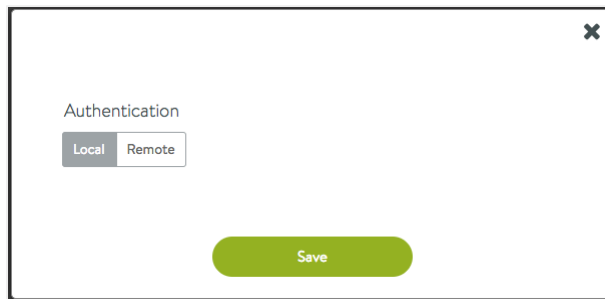
Remote Auth requires assignment of roles and tenants for every user login via the authorization mapping rules. Authorization is assessed on every login and the user record is updated. Upon successful user login via an external authentication server, all mapping rules are evaluated; tenant and role pairs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

Foreword

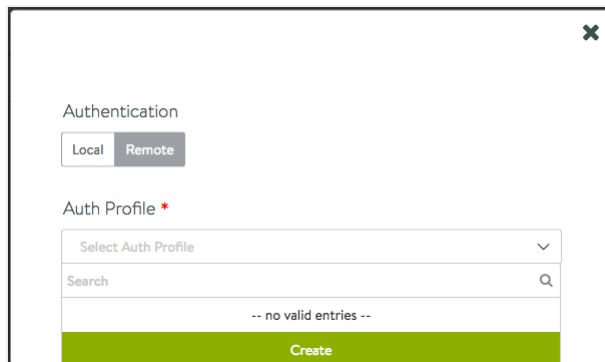
Examples in this article assume the Avi Controller has been set up for remote authentication. By default, a Controller will have only local authentication established, as shown below.



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.

Authorization	Assignment
<input type="checkbox"/> Group Any <input type="checkbox"/> Attribute Any	Tenant All Role From Select List Application-Operator
<input type="checkbox"/> Group Member of technical <input type="checkbox"/> Attribute Any	Super User
<input type="checkbox"/> Group Member of ProdProxyAdmin	Super User

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 be 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.

Tenant and Role Mapping New Mapping

Search

Displaying 3 item(s)

<input type="checkbox"/> Authorization	Assignment
<input type="checkbox"/> Group Any Attribute Any	Tenant From Select List No-Access Tenant Role From Select List No-Access Role

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.

Tenant and Role Mapping New Mapping

Search

Displaying 4 item(s)

<input type="checkbox"/> Authorization	Assignment
<input type="checkbox"/> Group Member of Domain Admins Attribute Any	Super User

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).

Tenant and Role Mapping New Mapping

Search

Displaying 5 item(s)

<input type="checkbox"/> Authorization	Assignment
<input type="checkbox"/> <p>Group Member of Enterprise Admins, Domain Admins</p> <p>Attribute department contains Service Operations</p>	<p>Tenant All</p> <p>Role From Select List System-Admin</p>

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.

Tenant and Role Mapping New Mapping

Search

Displaying 1 item(s)

<input type="checkbox"/> Authorization	Assignment
<input type="checkbox"/> <p>Group Any</p> <p>Attribute Any</p>	<p>Tenant All</p> <p>Role Matching Attribute Value vantageRole</p>

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.

Tenant and Role Mapping
New Mapping

Displaying 1 item(s)

	Authorization	Assignment
<input type="checkbox"/>	<p>Group Any</p> <p>Attribute Any</p>	<p>Tenant Matching Group Name</p> <p>Role From Select List Application-Admin</p>

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.

Tenant and Role Mapping
New Mapping

Displaying 3 item(s)

	Authorization	Assignment
<input type="checkbox"/>	Group Member of Service Operators Attribute Any	Tenant All Role From Select List Application-Operator ↓ ✎
<input type="checkbox"/>	Group Member of Enterprise Admins Attribute Any	Tenant All Role From Select List Application-Admin ↑ ↓
<input type="checkbox"/>	Group Member of Administrators Attribute Any	Super User ↑ ✎

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.

Tenant and Role Mapping				New Mapping
Search <input type="text"/>				
Displaying 7 item(s)				
<input type="checkbox"/> Authorization	Assignment			
<input type="checkbox"/>	Group Member of Service Operators E Attribute Any	Tenant From Select List Role From Select List	Tenant AE, Tenant SE Application-Operator	↓ ↗
<input type="checkbox"/>	Group Member of Service Admins E Attribute Any	Tenant From Select List Role From Select List	Tenant AE, Tenant SE Application-Admin	↑ ↓ ↗
<input type="checkbox"/>	Group Member of Service Admins E Attribute Any	Tenant From Select List Role From Select List	Tenant AW, Tenant SW Application-Operator	↑ ↓ ↗
<input type="checkbox"/>	Group Member of Service Operators W Attribute Any	Tenant From Select List Role From Select List	Tenant AW, Tenant SW Application-Operator	↑ ↓ ↗
<input type="checkbox"/>	Group Member of Service Admins W Attribute Any	Tenant From Select List Role From Select List	Tenant SW, Tenant AW Application-Admin	↑ ↓ ↗
<input type="checkbox"/>	Group Member of Service Admins W Attribute Any	Tenant From Select List Role From Select List	Tenant AE, Tenant SE Application-Operator	↑ ↓ ↗
<input type="checkbox"/>	Group Member of Administrators Attribute Any	Super User		↑ ↗

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.

Tenant and Role Mapping

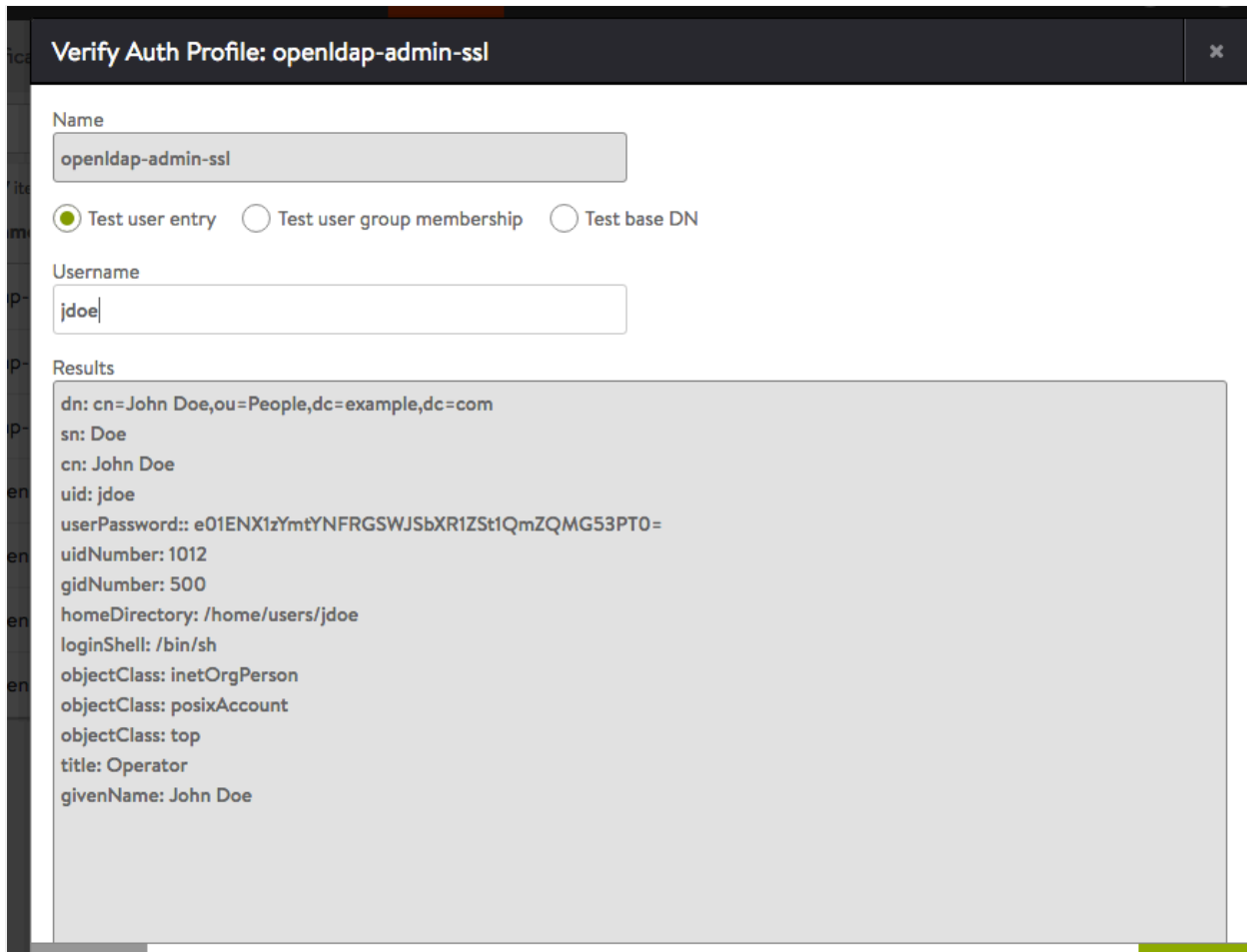
[New Mapping](#)

Search

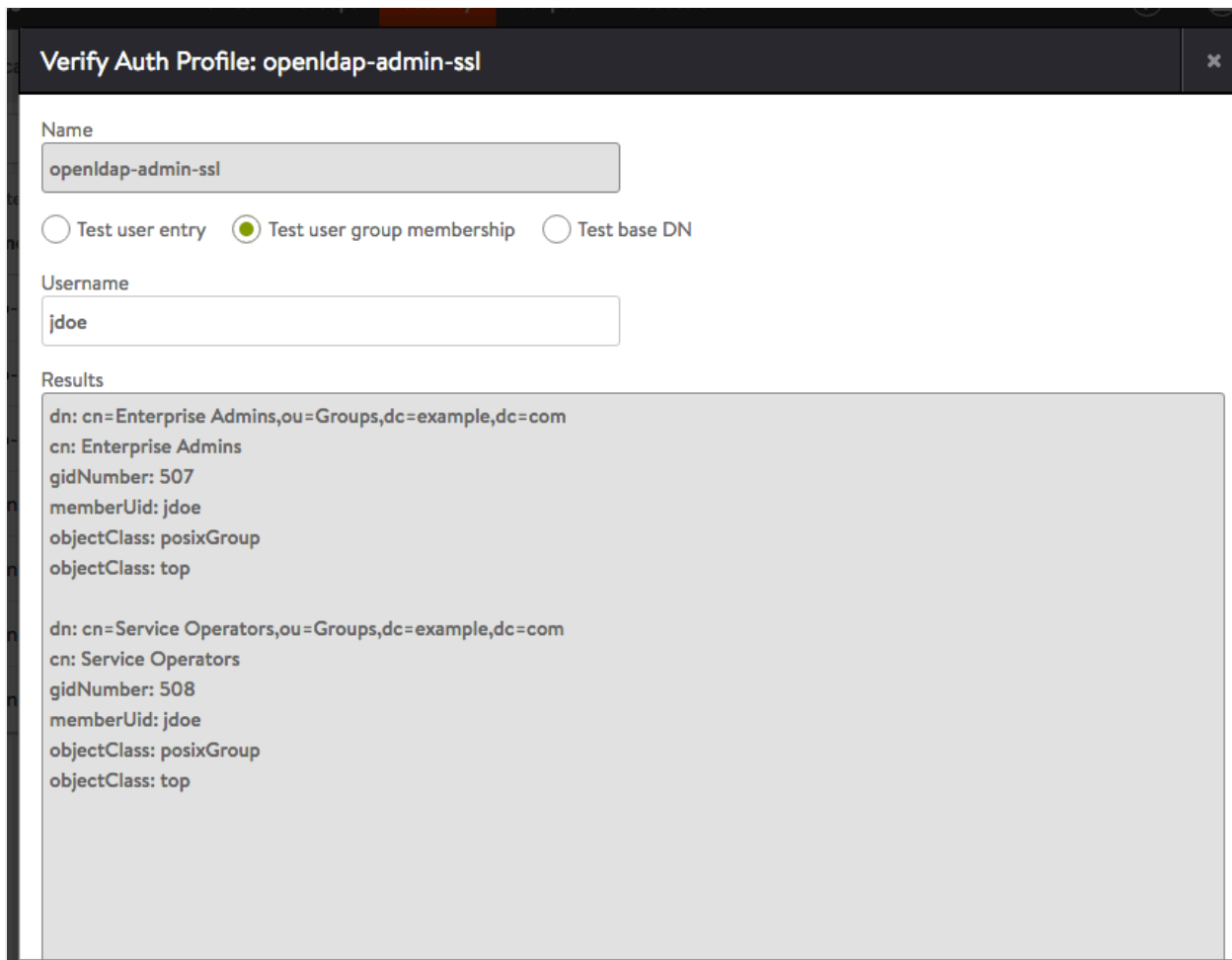
Displaying 4 item(s)

<input type="checkbox"/>	Authorization	Assignment
<input type="checkbox"/>	Group Any Attribute Any	Tenant From Select List No-Access Tenant Role From Select List No-Access Role
<input type="checkbox"/>	Group Any Attribute Any	Tenant Matching Group Name Role From Select List Application-Admin
<input type="checkbox"/>	Group Member of Service Operators Attribute Any	Tenant All Role From Select List Application-Operator
<input type="checkbox"/>	Group Any Attribute givenName contains John Doe	Tenant From Select List Test Lab Role From Select List System-Admin

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.

Tenant and Role Mapping
New Mapping

Displaying 3 item(s)

	Authorization	Assignment	
<input type="checkbox"/>	<p>Group Any</p> <p>Attribute Any</p>	<p>Tenant From Select List</p> <p>Role From Select List</p>	<p>No-Access Tenant</p> <p>No-Access Role</p> <p style="text-align: right;">↓ </p>
<input type="checkbox"/>	<p>Group Member of Service Operators</p> <p>Attribute Any</p>	<p>Super User</p>	<p style="text-align: right;">↑ ↓</p>
<input type="checkbox"/>	<p>Group Any</p> <p>Attribute givenName contains John Doe</p>	<p>Tenant From Select List</p> <p>Role From Select List</p>	<p>Test Lab</p> <p>System-Admin</p> <p style="text-align: right;">↑ </p>

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.

Tenant and Role Mapping

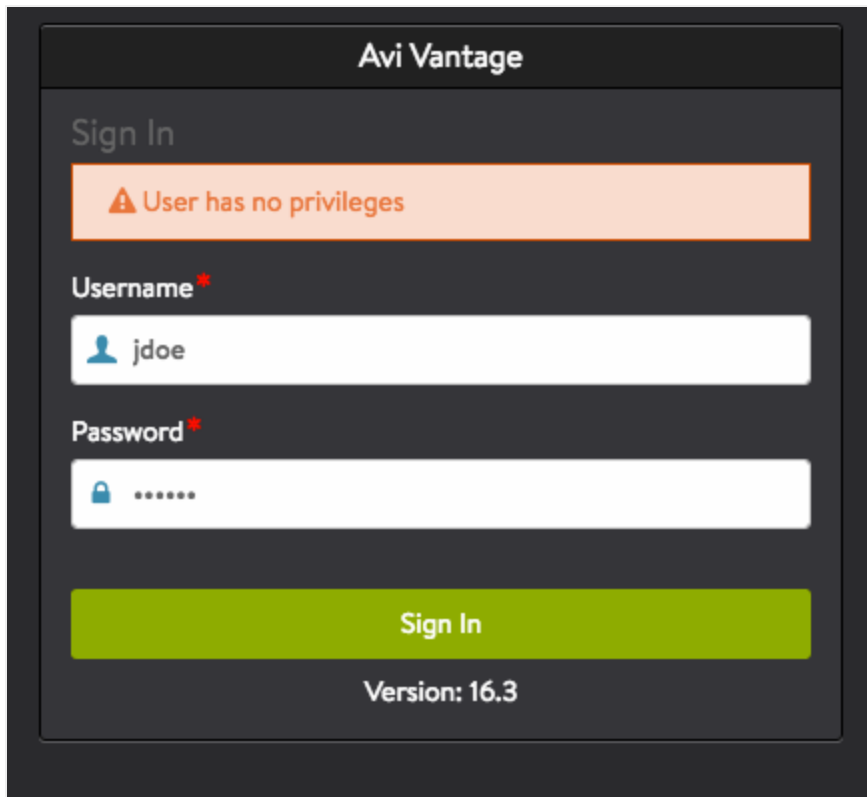
[New Mapping](#)

Search

Displaying 2 item(s)

<input type="checkbox"/>	Authorization	Assignment		
<input type="checkbox"/>	Group Member of Domain Admins	Tenant All		↓
	Attribute Any	Role From Select List	System-Admin	
<input type="checkbox"/>	Group Any	Tenant From Select List	Test Lab	↑
	Attribute givenName does not contain John Doe	Role From Select List	System-Admin	

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

```
: > █
```