User Roles

Avi Technical Reference (v20.1)

User Roles

view online

Each Avi Vantage user account is associated with a role. The role defines the type of access the user has to each area of the Avi Vantage system.

Roles provide granular Role-Based Access Control (RBAC) within Avi Vantage.

The role, in combination with the tenant (optional), comprise the authorization settings for an Avi Vantage user.

Access Types

For each Avi Vantage system area, the role can be one of the following:

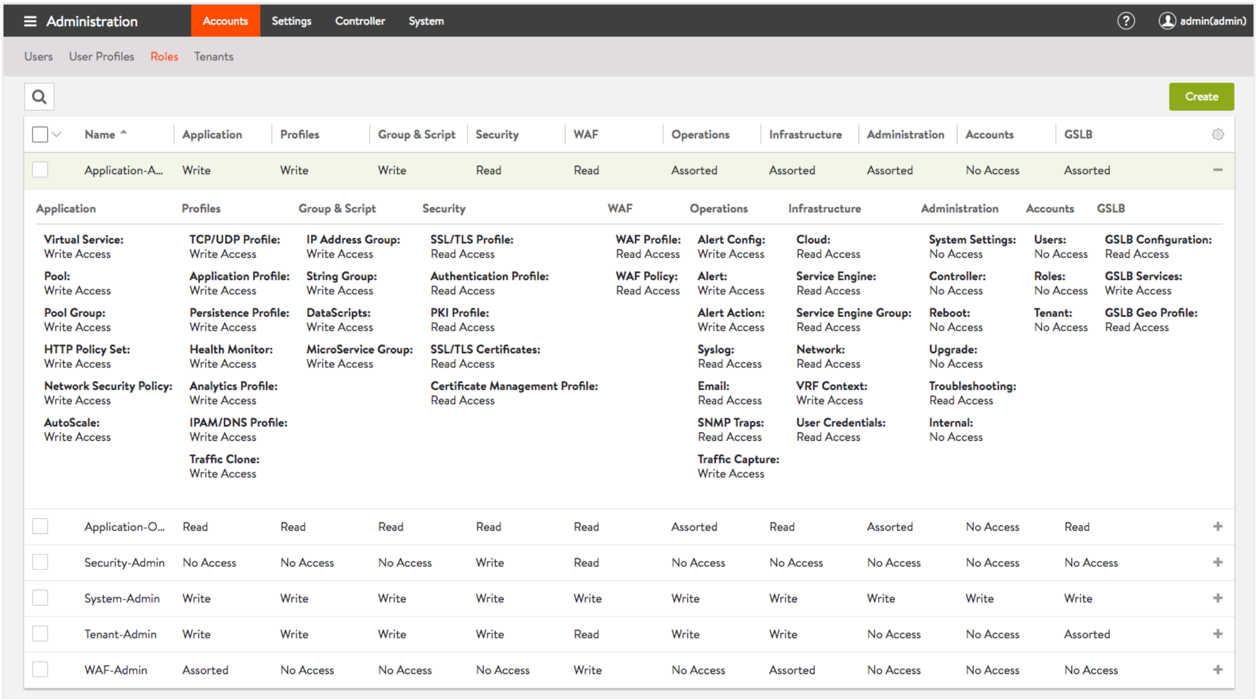
- Write: User has full access to create, read, modify, and delete items. For example, the user may be able to create a virtual service, modify its properties, view its health and metrics, and later delete that virtual service.
- Read: User may only read the existing configuration of the item. For example, the user may see how a virtual service is configured while being unable to view the current metrics, modify, or delete that virtual service.
- No Access: User can neither see nor modify this section of Avi Vantage. For example, the user would be prohibited from creating, modifying, deleting, or even viewing (reading) any virtual services at all.

Pre-defined Avi Vantage User Roles

Avi Vantage comes with the following pre-defined roles:

- Application-Admin: User has write access to the Application and Profiles sections of Avi Vantage, read access to the Infrastructure settings, and no access to the Account or System sections.
- Application-Operator: User has read access to the Application and Profiles sections of Avi Vantage, and no access to the Infrastructure, Account, and System sections.
- Security-Admin: User has read/write access only to the Templates > Security section.
- System-Admin: User has write access to all sections of Avi Vantage.
- Tenant-Admin: User has write access to all sections of Avi Vantage except the System section, to which the user has no access.
- WAF-Admin: User has write access to WAF Profiles and Policies, read access to application VSs, pools and pool groups, read access to clouds, and no access to the rest.

To display a detailed list of the access settings for a role, click on the table row for that role. Here is an example of the detailed information for the Application-Admin role. (The example is truncated on the right side in this example but the information will display in full in the web interface.)



Name	Application	Profiles	Group & Script	Security	WAF	Operations	Infrastructure	Administration	Accounts	GSLB
Application-A...	Write	Write	Write	Read	Read	Assorted	Assorted	Assorted	No Access	Assorted

Application	Profiles	Group & Script	Security	WAF	Operations	Infrastructure	Administration	Accounts	GSLB
Virtual Service: Write Access	**TCP/UDP Profile:** Write Access	**IP Address Group:** Write Access	**SSL/TLS Profile:** Read Access	**WAF Profile:** Read Access	**Alert Config:** Write Access	**Cloud:** Read Access	**System Settings:** No Access	**Users:** No Access	**GSLB Configuration:** Read Access
Pool: Write Access	**Application Profile:** Write Access	**String Group:** Write Access	**Authentication Profile:** Read Access	**WAF Policy:** Read Access	**Alert:** Write Access	**Service Engine:** Read Access	**Controller:** No Access	**Roles:** No Access	**GSLB Services:** Write Access
Pool Group: Write Access	**Persistence Profile:** Write Access	**DataScripts:** Write Access	**PKI Profile:** Read Access		**Alert Action:** Write Access	**Service Engine Group:** Read Access	**Reboot:** No Access	**Tenant:** No Access	**GSLB Geo Profile:** Read Access
HTTP Policy Set: Write Access	**Health Monitor:** Write Access	**MicroService Group:** Write Access	**SSL/TLS Certificates:** Read Access		**Syslog:** Read Access	**Network:** Read Access	**Upgrade:** No Access		
Network Security Policy: Write Access	**Analytics Profile:** Write Access		**Certificate Management Profile:** Read Access		**Email:** Read Access	**VRF Context:** Write Access	**Troubleshooting:** Read Access		
AutoScale: Write Access	**IPAM/DNS Profile:** Write Access				**SNMP Traps:** Read Access	**User Credentials:** Read Access	**Internal:** No Access		
	Traffic Clone: Write Access				**Traffic Capture:** Write Access				

Name	Application	Profiles	Group & Script	Security	WAF	Operations	Infrastructure	Administration	Accounts	GSLB
Application-O...	Read	Read	Read	Read	Read	Assorted	Read	Assorted	No Access	Read
Security-Admin	No Access	No Access	No Access	Write	Read	No Access	No Access	No Access	No Access	No Access
System-Admin	Write	Write	Write	Write	Write	Write	Write	Write	Write	Write
Tenant-Admin	Write	Write	Write	Write	Read	Write	Write	No Access	No Access	Assorted
WAF-Admin	Assorted	No Access	No Access	No Access	Write	No Access	Assorted	No Access	No Access	No Access

Each user must be associated with at least one role. The role can be either predefined or a custom role.

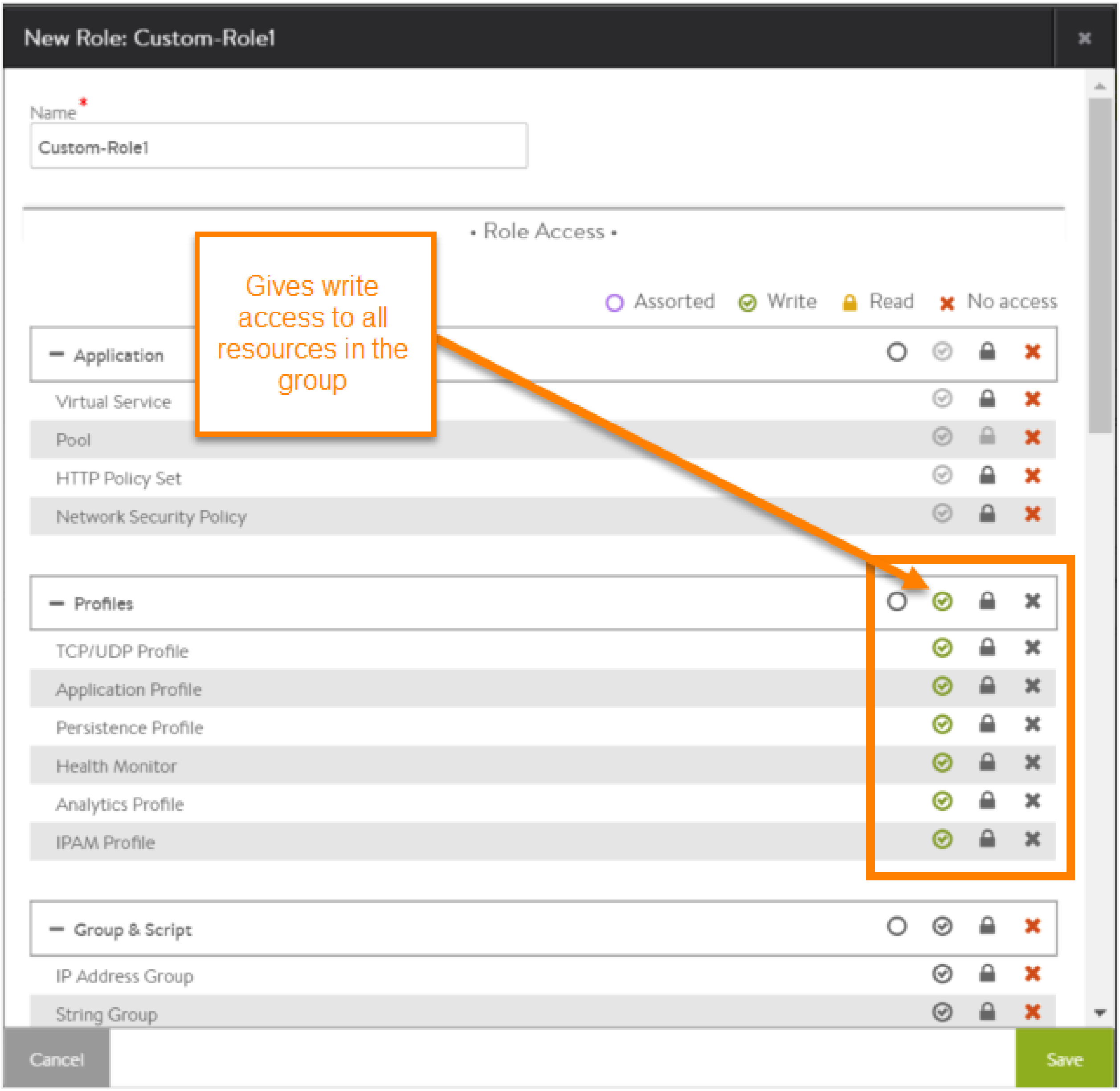
If multitenancy is configured, a user can be assigned to more than one tenant, and can have a separate role for each tenant.

Create a Role

If none of the pre-defined roles exactly fit the access requirements for some user accounts, custom roles can be defined.

By default, access to each system area in a custom role is set to no access. Access can be changed to read or write, for an entire system area or for individual resources within that system area.

For example, to allow write access to all profiles, click the icon in the title row for the Profiles system area as shown in the image.



New Role: Custom-Role1

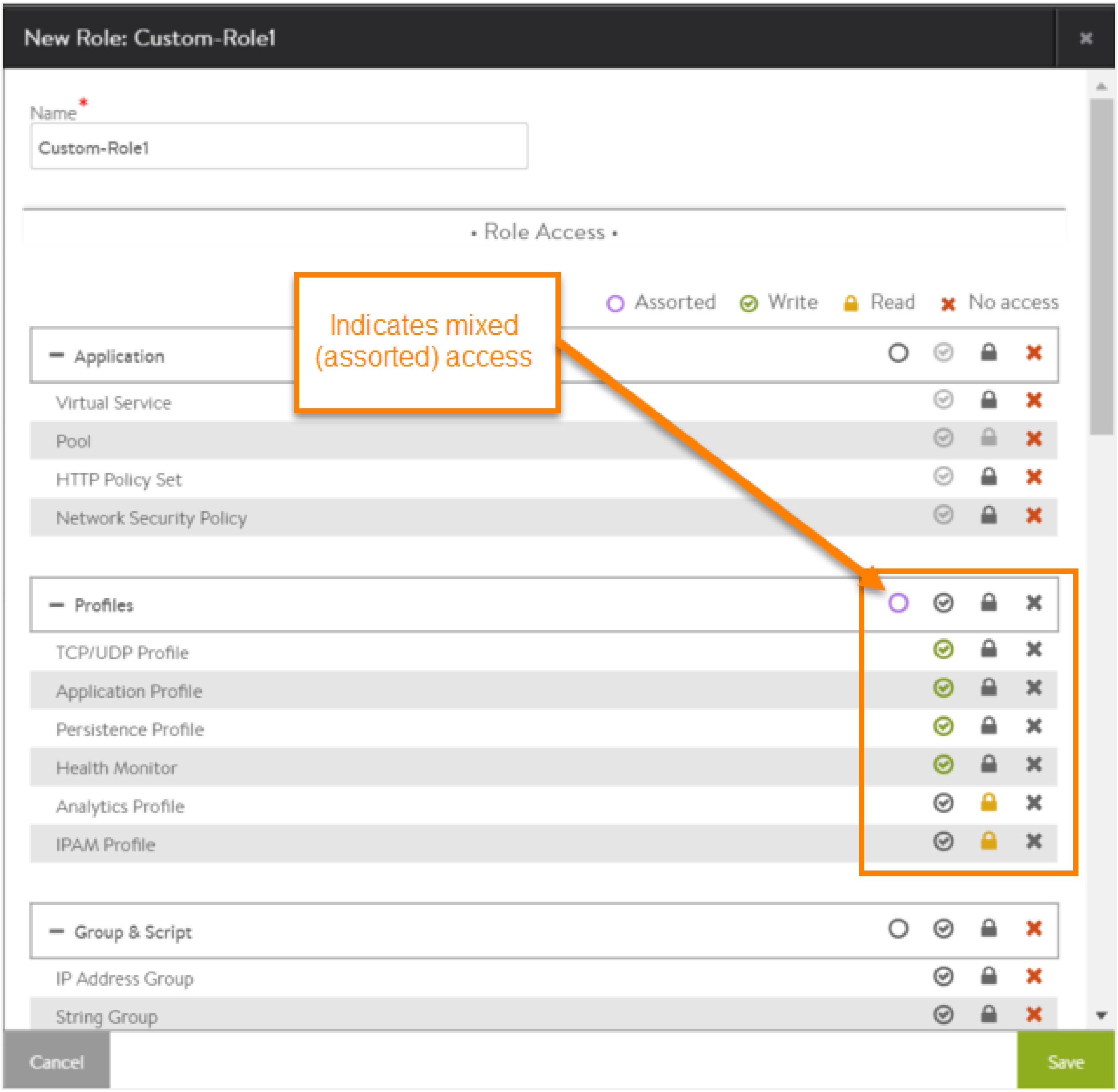
Name* Custom-Role1

• Role Access •

○ Assorted ✓ Write 🔒 Read ✗ No access

Resource	Access
Application	✗ No access
Virtual Service	✗ No access
Pool	✗ No access
HTTP Policy Set	✗ No access
Network Security Policy	✗ No access
Profiles	✓ Write
TCP/UDP Profile	✓ Write
Application Profile	✓ Write
Persistence Profile	✓ Write
Health Monitor	✓ Write
Analytics Profile	✓ Write
IPAM Profile	✓ Write
Group & Script	✗ No access
IP Address Group	✗ No access
String Group	✗ No access

To give access to only some of the resources within a system area, select the access for each area. In this example, the role will have write access to some types of profiles but only read access to the other types:



New Role: Custom-Role1

Name*: Custom-Role1

• Role Access •

Indicates mixed (assorted) access

	○ Assorted	✓ Write	🔒 Read	✖ No access
− Application	○	✓	🔒	[✓ ✖]
Virtual Service		✓	🔒	[✓ ✖]
Pool		✓	🔒	[✓ ✖]
HTTP Policy Set		✓	🔒	[✓ ✖]
Network Security Policy		✓	🔒	[✓ ✖]
− Profiles	[✓ ○]	✓	🔒	✖
TCP/UDP Profile		[✓ ✓]	🔒	✖
Application Profile		[✓ ✓]	🔒	✖
Persistence Profile		[✓ ✓]	🔒	✖
Health Monitor		[✓ ✓]	🔒	✖
Analytics Profile		✓	[✓ 🔒]	✖
IPAM Profile		✓	[✓ 🔒]	✖
− Group & Script	○	✓	🔒	[✓ ✖]
IP Address Group		✓	🔒	[✓ ✖]
String Group		✓	🔒	[✓ ✖]

When there are multiple types of access within a system area, this is indicated by the Assorted icon:

○

To create a custom role:

1. Navigate to Administration > Accounts Roles, and click on Create.
2. Enter a Name for the role.
3. Click on one of the following icons to change access to a system area:

- Write:

  ✓

- Read:

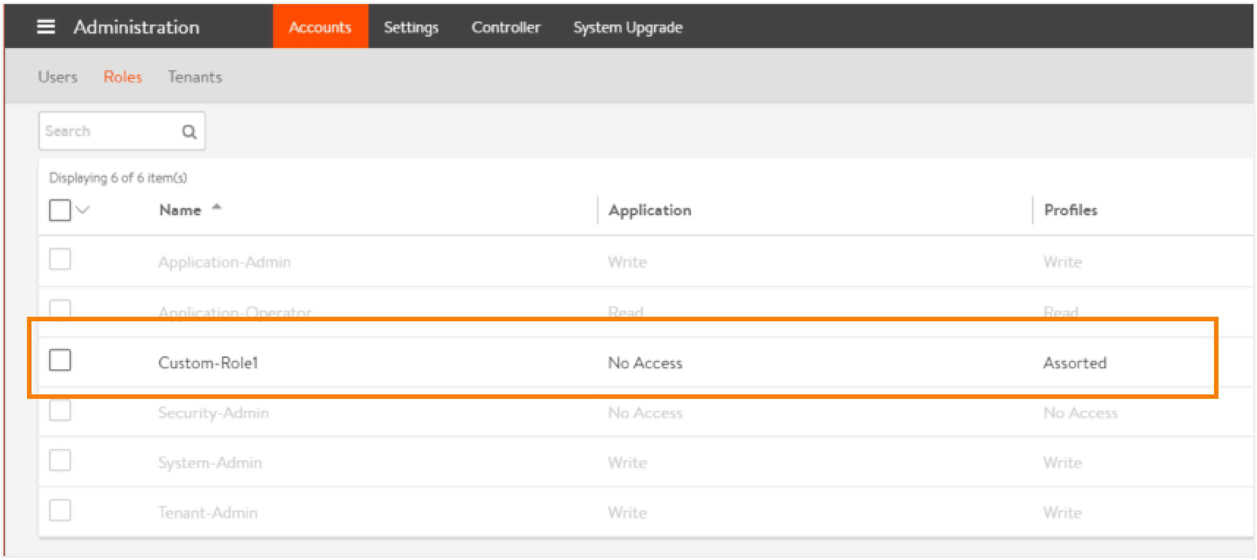
  🔒

- No Access:

  ✖

4. Click on Save.

The new role appears in the table displayed when the Roles tab has been selected.



Displaying 6 of 6 item(s)

Name	Application	Profiles
Application-Admin	Write	Write
Application-Operator	Read	Read
Custom-Role1	No Access	Assorted
Security-Admin	No Access	No Access
System-Admin	Write	Write
Tenant-Admin	Write	Write

To edit a custom role, click the edit icon (not shown in example) to the right of the table entry.

Assigning a Role to a User

Roles can be assigned to both local and remote (LDAP, TACACS+) user accounts. The procedure differs depending on where the account is maintained.

Local User Account

Roles can be assigned to a user account when the account is created or at any time later. In either case, select the role from the Role pull-down list in the configuration popup for the user account.

1. Navigate to Administration > Accounts > Users.
2. If configuring a new account, click on Create. Otherwise, if changing an existing account, click on the Edit icon in the row for the account.
3. Select the role from the Role pull-down list. If a custom role is needed but is not created, click on Create.

Note:
User accounts are case sensitive.

LDAP or TACACS+ User Accounts

If LDAP or TACACS+ remote authentication is used, roles can be assigned to users based on the following:

- LDAP group: A role can be assigned to users in any group, or specifically to users who either are or are not members of specific groups.
- LDAP attributes: For users who match the LDAP group filter, the role is assigned to those users with any attributes and values, or who either do or do not have specific attributes and values.

The mappings are configured within Avi Vantage rather than the LDAP or TACACS+ server.

To map LDAP or TACACS+ users to Avi Vantage roles, use the following steps. Multiple mappings can be configured if needed, for any combination of user group name and attribute:value pair.

Notes: * These steps assume that Avi Vantage authentication/authorization is set to remote, and an LDAP or TACACS+ Auth profile has been applied. * Group names are case sensitive for LDAP mapping.

1. Navigate to Administration > Settings > Authentication/Authorization.
2. Click on New Mapping.
3. Select the filter for the LDAP group:

- Any: Users in any LDAP group match the filter.
- Member: Users must be members of the specified groups. If entering multiple group names, use commas between the names.
- Not a Member: Users must not be members of the specified groups.

4. Select the filter for the LDAP attribute:

- Any: Users match regardless of attributes or their values.
- Contains: User must have the specified attribute, and the attribute must have one of the specified values.
- Does Not Contain: User must not have the specified attribute and value(s).

5. Select the role from the User Role pull-down list:

- From Select List: Displays a Roles pull-down list. Select the role from the list.
- All: Assigns all roles.
- Matching Attribute Value: Assigns the role whose name matches an attribute value from the LDAP server.
- Matching Group Name: Assigns the role whose name matches a group name on the LDAP server.

6. If using multitenancy, users also can be mapped to tenants. Read more about tenants and tenancy tenant.
7. Click on Save. The new mapping appears in the Tenant and Role Mapping table.