Fortigate Firewall Configuration:

First define TACACS+ server in Fortigate Firewall. By default, TACACS+ settings are not shown in Fortigate Firewall Web-GUI. Configure it from Command Line Interface CLI. After configuration from the Command Line Interface CLI the settings are shown in Web-GUI.

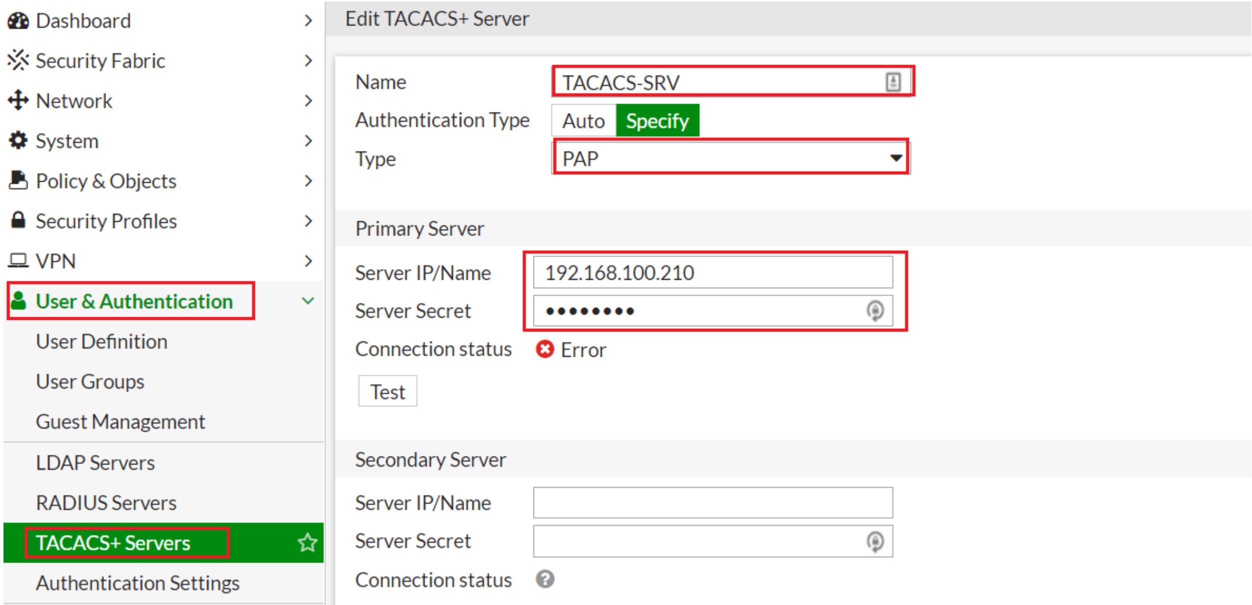
Enable http through CLI

```
FortiGate-VM64-KVM # config system interface
FortiGate-VM64-KVM (interface) # edit port1
FortiGate-VM64-KVM (port1) # set allowaccess pin https http ssh
FortiGate-VM64-KVM (port1) # end
```

Enable TACACS+ through CLI

```
FG # config user tacacs+
FG (tacacs+) # edit "TACACS-SRV"
FG (TACACS-SRV) # set server "192.168.100.210"
FG (TACACS-SRV) # set key Test123
FG (TACACS-SRV) # set authen-type pap
FG (TACACS-SRV) # set authorization enable
FG (TACACS-SRV) # next
FG (tacacs+) # end
```

After that TACACS options are available in GUI. Navigate to User & Authentication>TACACS+ Servers



Edit TACACS+ Server

Name	TACACS-SRV
Authentication Type	Auto **Specify**
Type	PAP

Primary Server

Server IP/Name	192.168.100.210
Server Secret	••••••••
Connection status	✖ Error

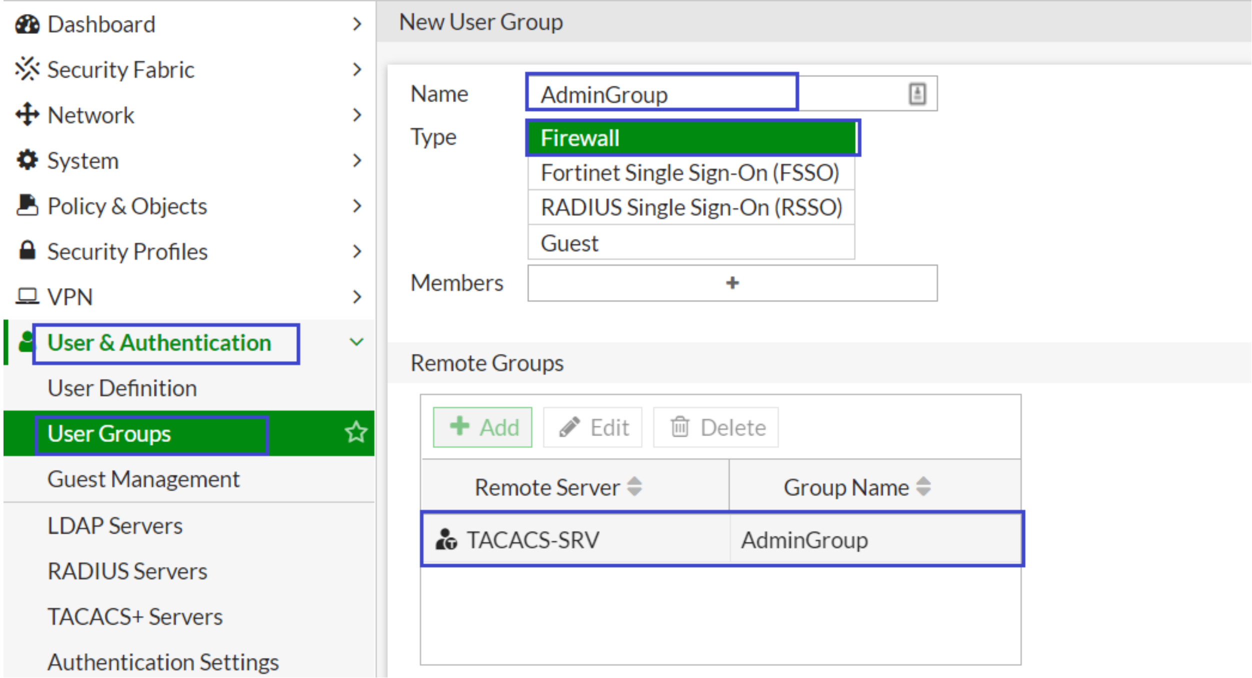
Test

Secondary Server

Server IP/Name	
Server Secret	
Connection status	?

User Groups:

Now we need two user groups configured in the Fortigate Firewall (Read-Only and Read-Write). Navigate to User & Authentication > User Groups > Create New provide the information.



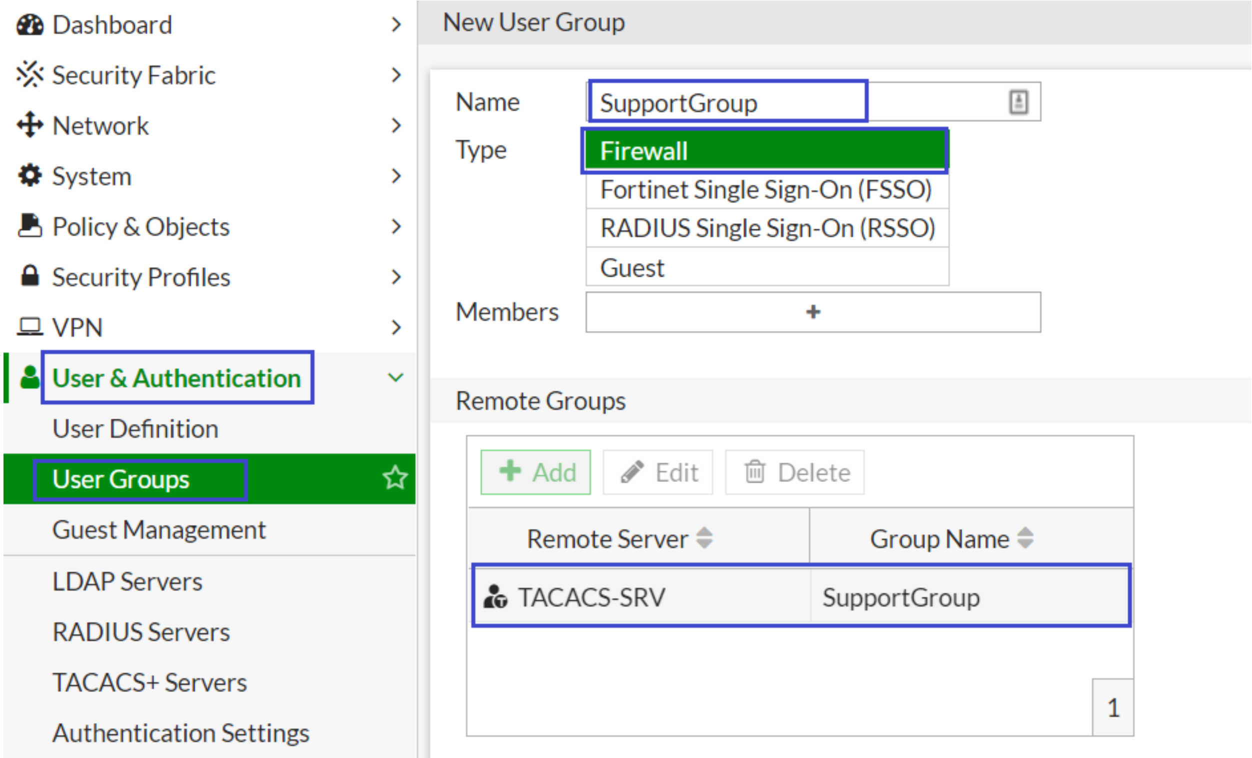
Name: AdminGroup

Type: Firewall / Fortinet Single Sign-On (FSSO) / RADIUS Single Sign-On (RSSO) / Guest

Members: +

Remote Groups

Remote Server	Group Name
TACACS-SRV	AdminGroup



Name: SupportGroup

Type: Firewall / Fortinet Single Sign-On (FSSO) / RADIUS Single Sign-On (RSSO) / Guest

Members: +

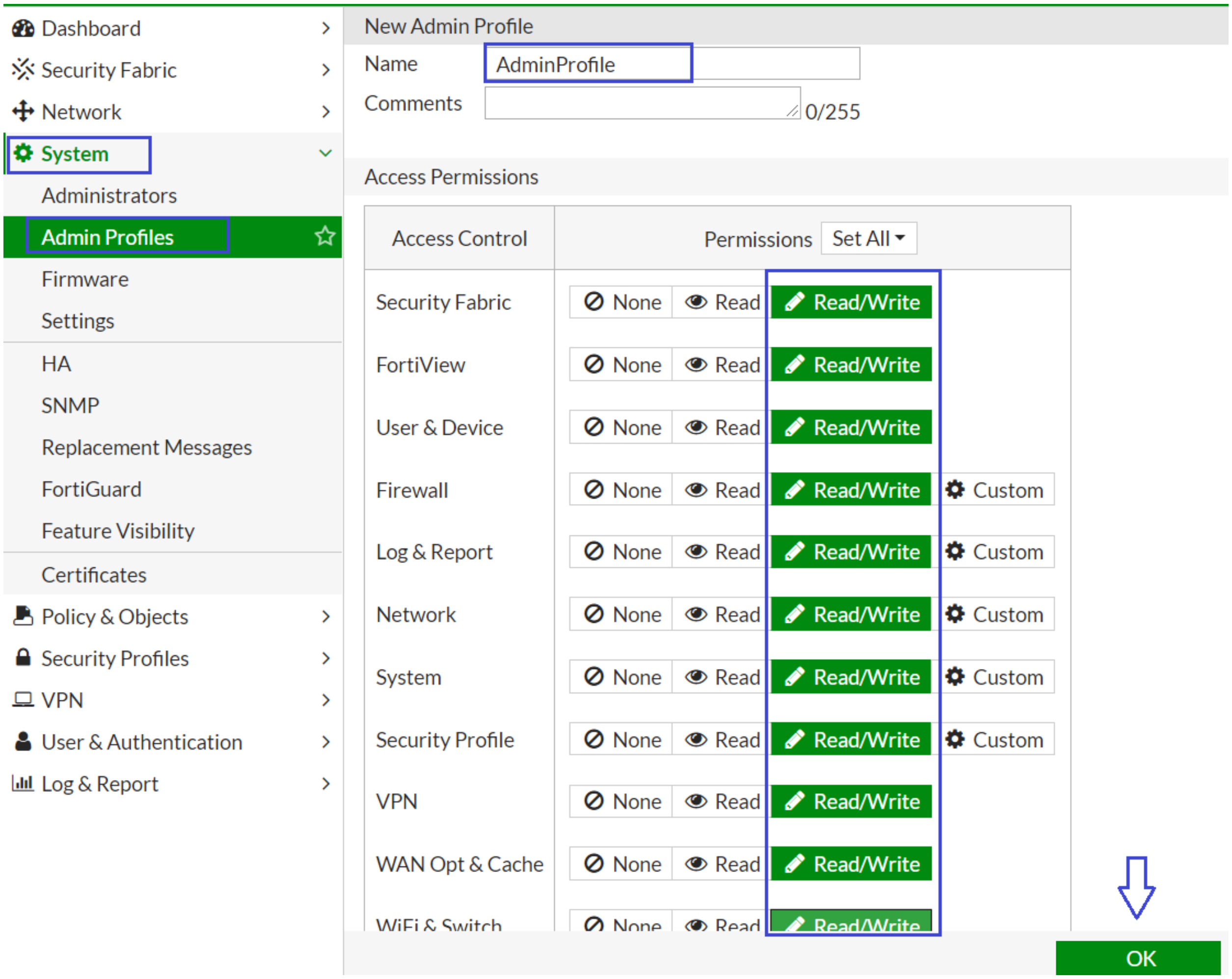
Remote Groups

Remote Server	Group Name
TACACS-SRV	SupportGroup

Admin Profiles:

Now, Let’s configure three Admin Profiles in Fortigate Firewall - No-Access (No Permission), AdminProfile (All Permissions), SupportProfile (Read-Only Permission).

Navigate to System>Admin Profiles > Create New Set the permissions as per profile in the case of AdminProfile allow all Read/Write access and Click OK.



New Admin Profile

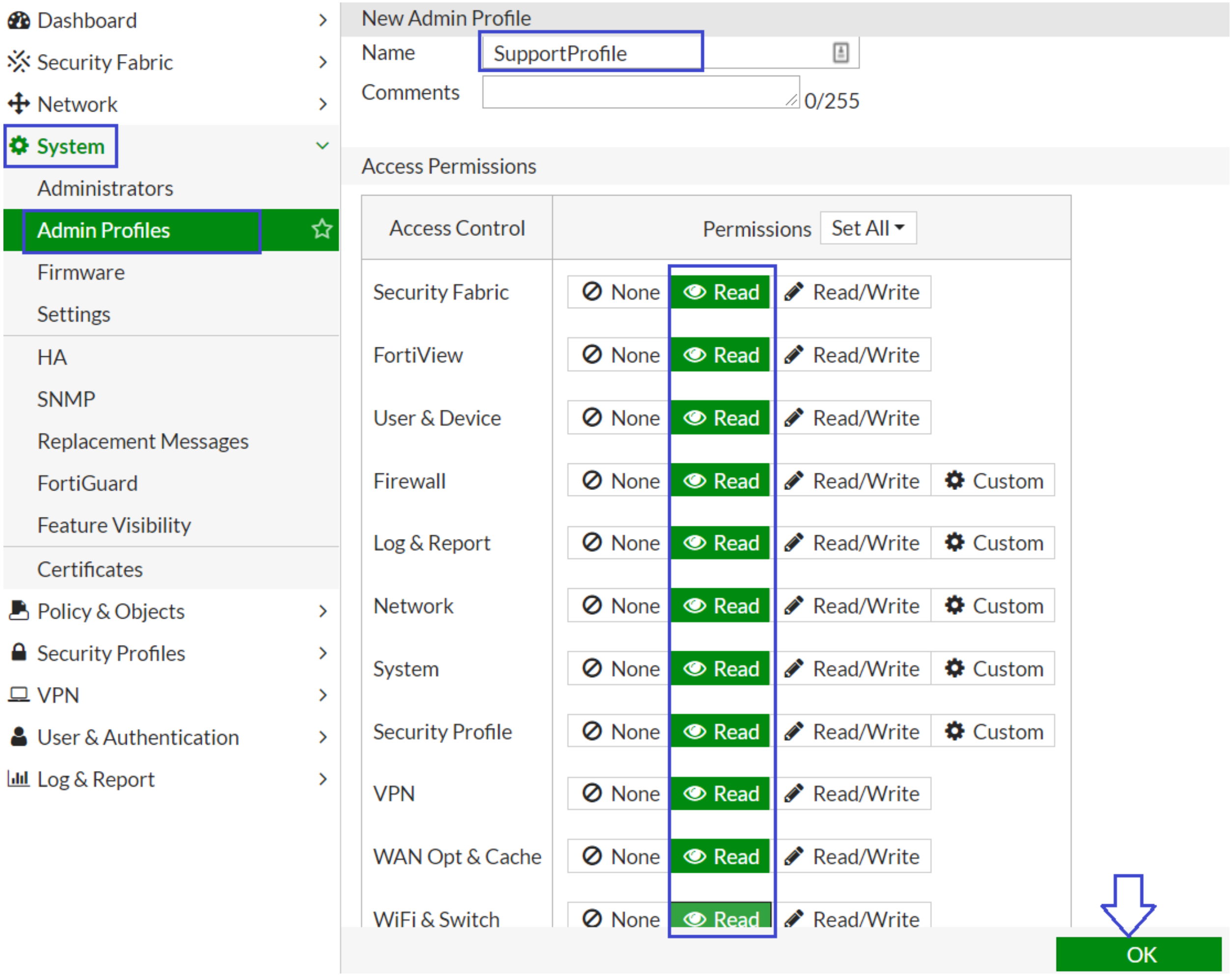
Name: AdminProfile

Comments: 0/255

Access Permissions

Access Control	Permissions Set All ▾
Security Fabric	⊘ None 👁 Read [✓ Read/Write]
FortiView	⊘ None 👁 Read [✓ Read/Write]
User & Device	⊘ None 👁 Read [✓ Read/Write]
Firewall	⊘ None 👁 Read [✓ Read/Write] Custom
Log & Report	⊘ None 👁 Read [✓ Read/Write] Custom
Network	⊘ None 👁 Read [✓ Read/Write] Custom
System	⊘ None 👁 Read [✓ Read/Write] Custom
Security Profile	⊘ None 👁 Read [✓ Read/Write] Custom
VPN	⊘ None 👁 Read [✓ Read/Write]
WAN Opt & Cache	⊘ None 👁 Read [✓ Read/Write]
WiFi & Switch	⊘ None 👁 Read [✓ Read/Write]

Navigate to System>Admin Profiles > Create New Set the permissions as per profile in the case of SupportProfile allow all Read access and Click OK.



New Admin Profile

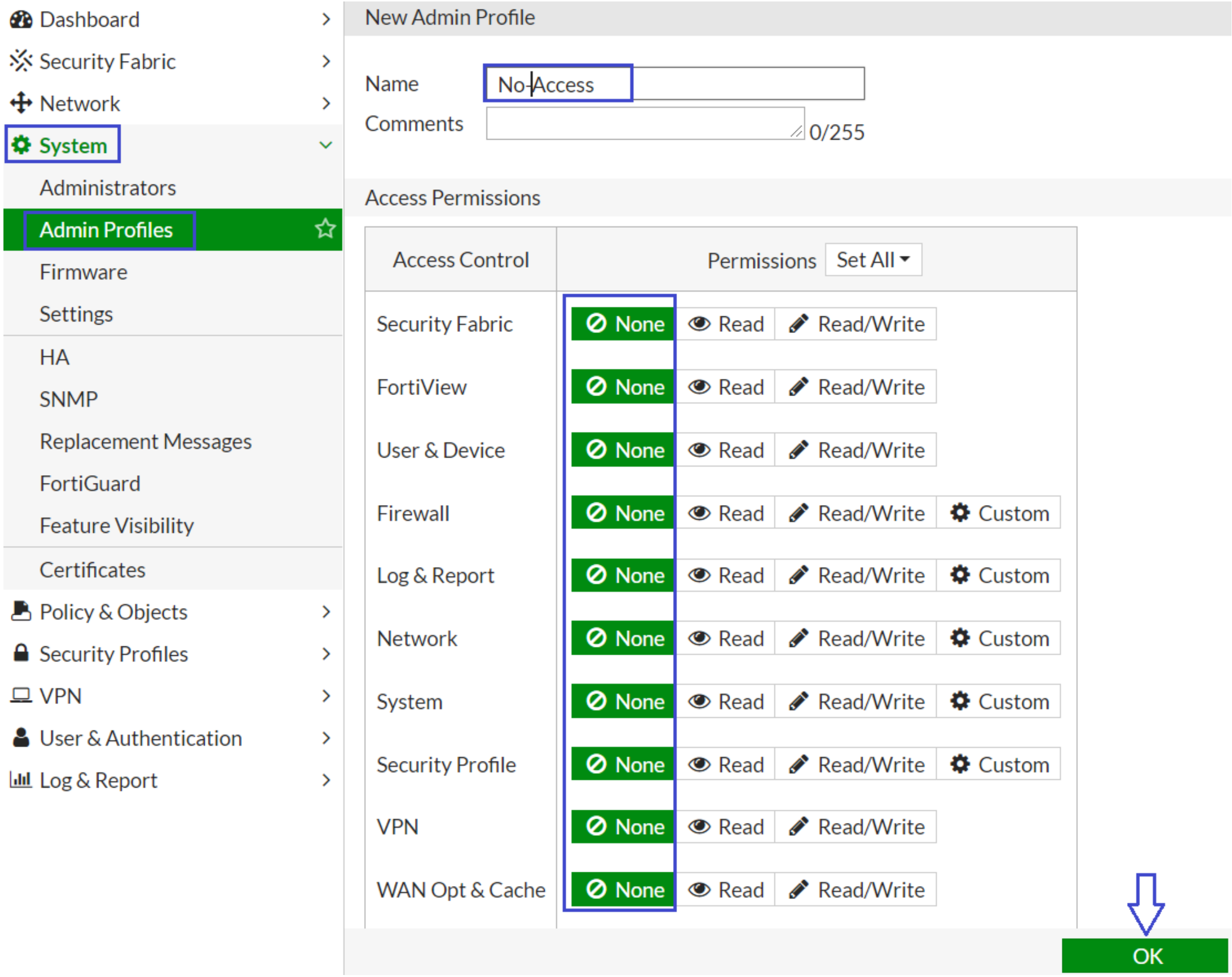
Name: SupportProfile

Comments: 0/255

Access Permissions

Access Control	Permissions Set All
Security Fabric	None [✓ Read] Read/Write
FortiView	None [✓ Read] Read/Write
User & Device	None [✓ Read] Read/Write
Firewall	None [✓ Read] Read/Write Custom
Log & Report	None [✓ Read] Read/Write Custom
Network	None [✓ Read] Read/Write Custom
System	None [✓ Read] Read/Write Custom
Security Profile	None [✓ Read] Read/Write Custom
VPN	None [✓ Read] Read/Write
WAN Opt & Cache	None [✓ Read] Read/Write
WiFi & Switch	None [✓ Read] Read/Write

Navigate to System>Admin Profiles > Create New Set the permissions as per profile in the case of No-Access allow all None access and Click OK.



New Admin Profile

Name: No-Access

Comments: 0/255

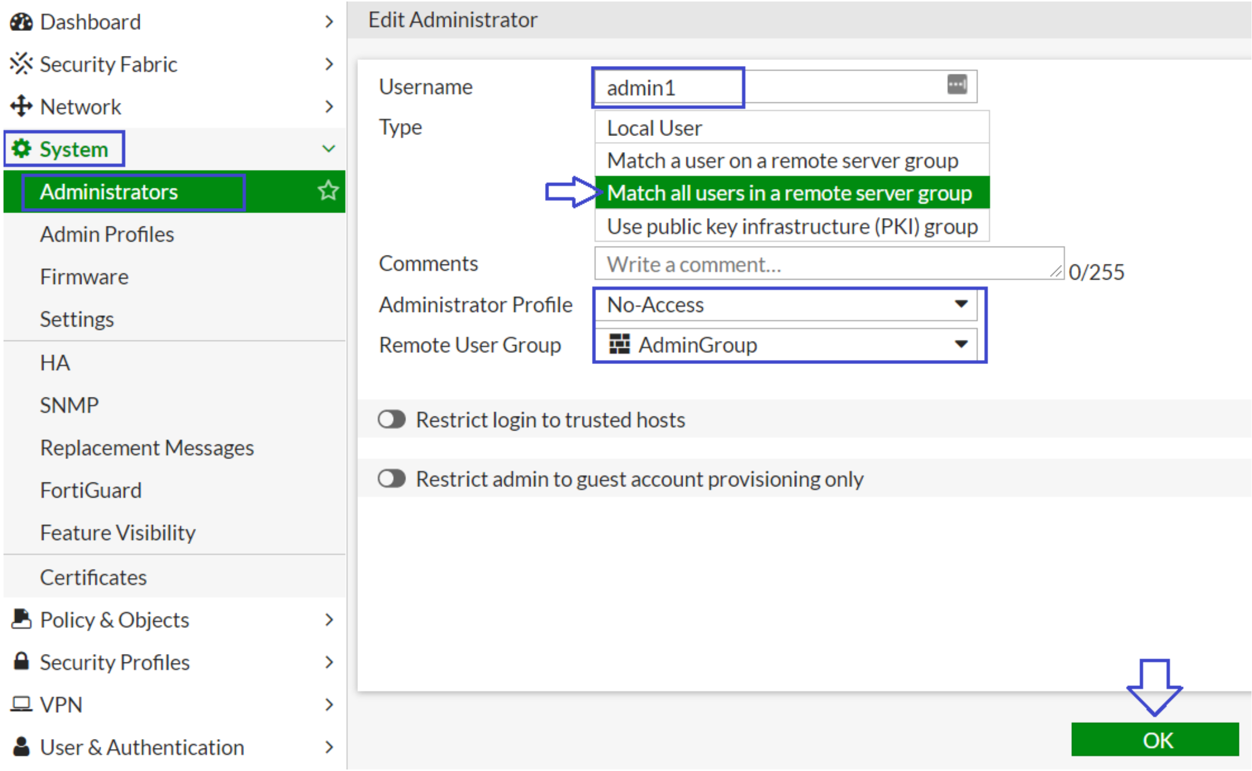
Access Permissions

Access Control	Permissions Set All
Security Fabric	[✓ None] Read Read/Write
FortiView	[✓ None] Read Read/Write
User & Device	[✓ None] Read Read/Write
Firewall	[✓ None] Read Read/Write Custom
Log & Report	[✓ None] Read Read/Write Custom
Network	[✓ None] Read Read/Write Custom
System	[✓ None] Read Read/Write Custom
Security Profile	[✓ None] Read Read/Write Custom
VPN	[✓ None] Read Read/Write
WAN Opt & Cache	[✓ None] Read Read/Write

Administrator Accounts:

Now, Let’s create Administrators accounts which in turn will be assigned one of those "Admin Profiles" after successful authentication. We will create two "Administrators" - one for read-write and another Administrator for read-only.

Navigate to System >Administrators > Create New provide the information.



Username: admin1

Type:
- Local User
- Match a user on a remote server group
- Match all users in a remote server group
- Use public key infrastructure (PKI) group

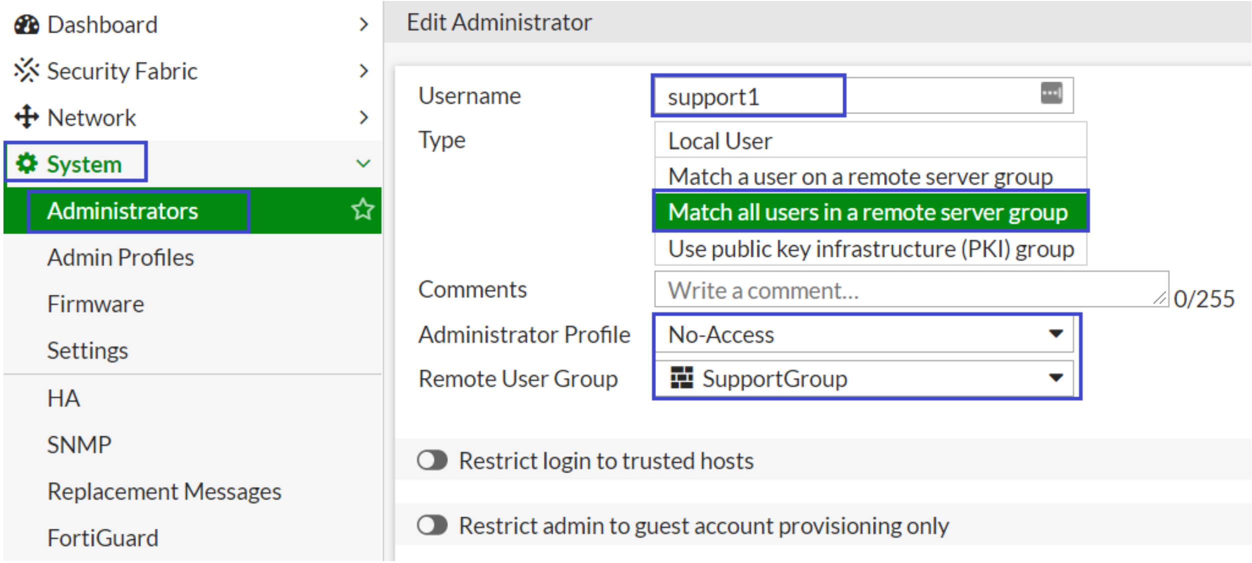
Comments: Write a comment... 0/255

Administrator Profile: No-Access

Remote User Group: AdminGroup

Restrict login to trusted hosts

Restrict admin to guest account provisioning only



Username: support1

Type:
- Local User
- Match a user on a remote server group
- Match all users in a remote server group
- Use public key infrastructure (PKI) group

Comments: Write a comment... 0/255

Administrator Profile: No-Access

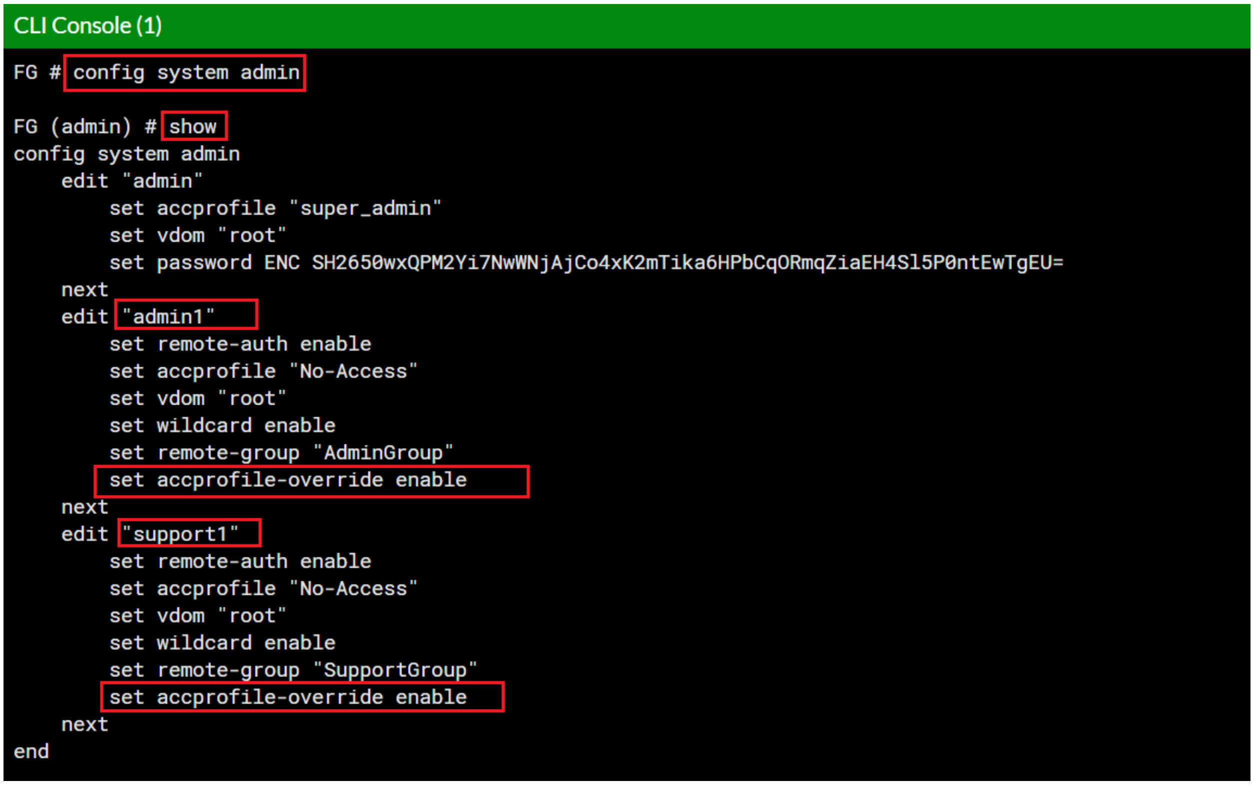
Remote User Group: SupportGroup

Restrict login to trusted hosts

Restrict admin to guest account provisioning only

Initially every user is assigned "No-Access" profile. However, after successful authentication, Cisco ISE TACACS will override that profile and tell the Fortigate Firewall to authorize a proper profile according to a user's access level. How this override works - TACACS server will send a "Admin Profile" name and the Fortigate firewall will match that profile's name to one of its locally defined profiles and assigned it to the user by overriding the "No-Access" profile.

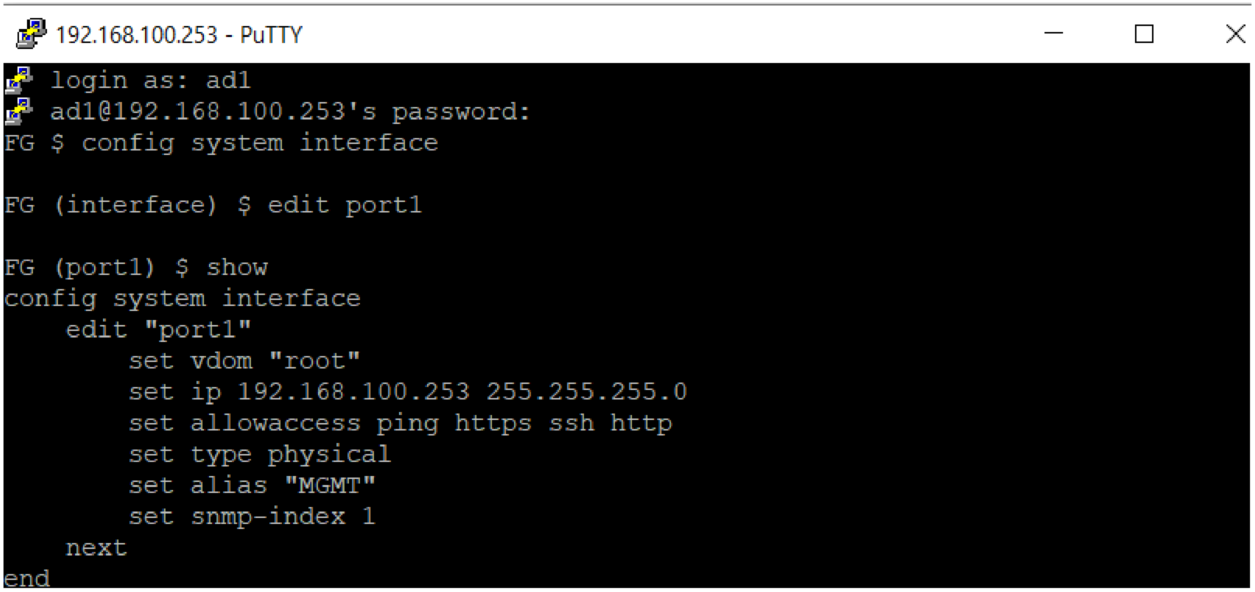
Admin1 Administrator Account
FG # config system admin FG (admin) # edit admin1 FG (support1) # set accprofile-override enable FG (support1) # end
support1 Administrator Account
FG # config system admin FG (admin) # edit support1 FG (support1) # set accprofile-override enable FG (support1) # end



```
FG # config system admin

FG (admin) # show
config system admin
    edit "admin"
        set accprofile "super_admin"
        set vdom "root"
        set password ENC SH2650wxQPM2Yi7NwWNjAjCo4xK2mTika6HPbCqORmqZiaEH4Sl5P0ntEwTgEU=
    next
    edit "admin1"
        set remote-auth enable
        set accprofile "No-Access"
        set vdom "root"
        set wildcard enable
        set remote-group "AdminGroup"
        set accprofile-override enable
    next
    edit "support1"
        set remote-auth enable
        set accprofile "No-Access"
        set vdom "root"
        set wildcard enable
        set remote-group "SupportGroup"
        set accprofile-override enable
    next
end
```

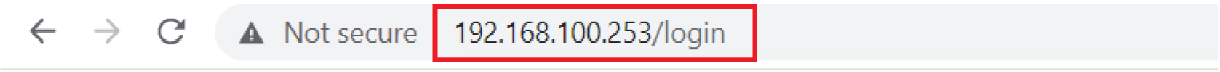
Testing and Verification:

We can test our configuration by login into the Fortigate Firewall by SSH. Let's try using the ad1 user credential.

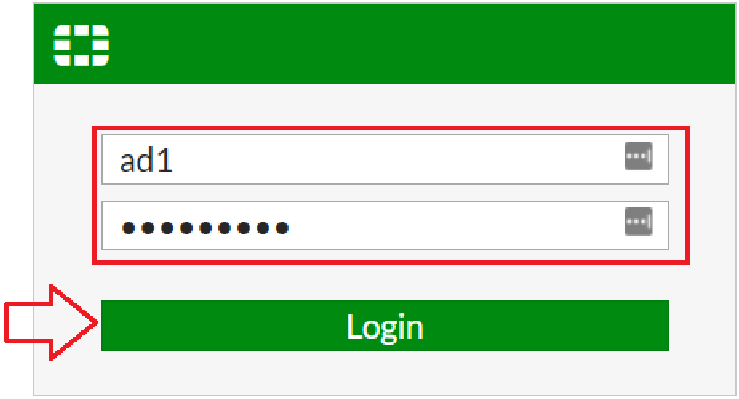


```
login as: ad1
ad1@192.168.100.253's password:
FG $ config system interface

FG (interface) $ edit port1

FG (port1) $ show
config system interface
    edit "port1"
        set vdom "root"
        set ip 192.168.100.253 255.255.255.0
        set allowaccess ping https ssh http
        set type physical
        set alias "MGMT"
        set snmp-index 1
    next
end
```

Let's login through Web-GUI type the Active Directory AdminGroup username ad1/Abc@12345.



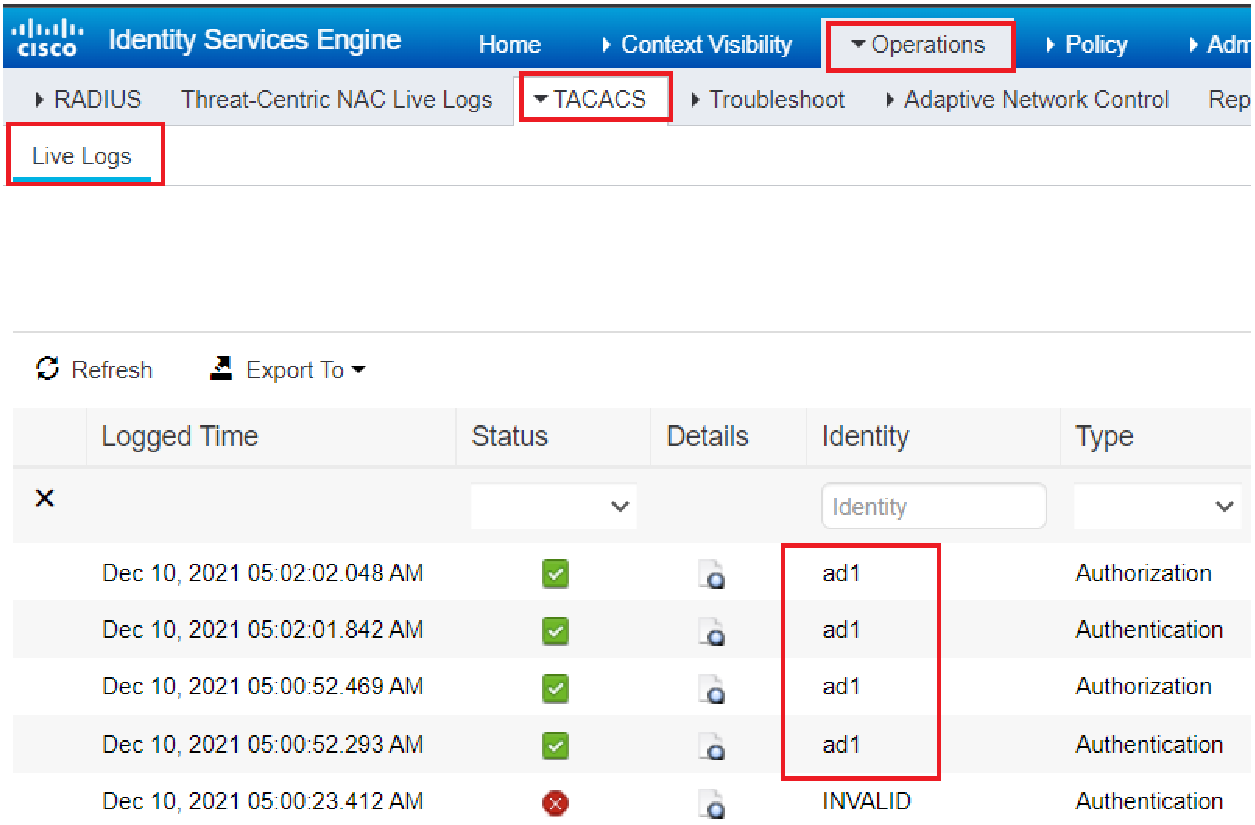
192.168.100.253/login



ad1

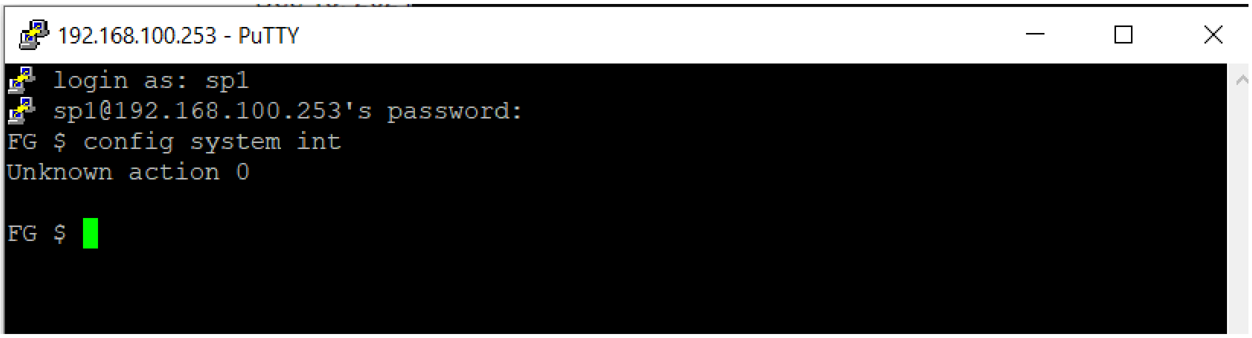
••••••••••

We can monitor the authentication/authorization logs on ISE Operations > TACACS > Live Logs. The ad1 user was successfully authenticated and authorized to run privileged commands.



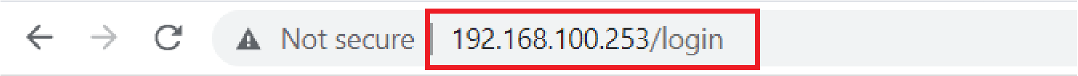
	Logged Time	Status	Details	Identity	Type
✕				Identity	
	Dec 10, 2021 05:02:02.048 AM	✓	🔍	ad1	Authorization
	Dec 10, 2021 05:02:01.842 AM	✓	🔍	ad1	Authentication
	Dec 10, 2021 05:00:52.469 AM	✓	🔍	ad1	Authorization
	Dec 10, 2021 05:00:52.293 AM	✓	🔍	ad1	Authentication
	Dec 10, 2021 05:00:23.412 AM	✗	🔍	INVALID	Authentication

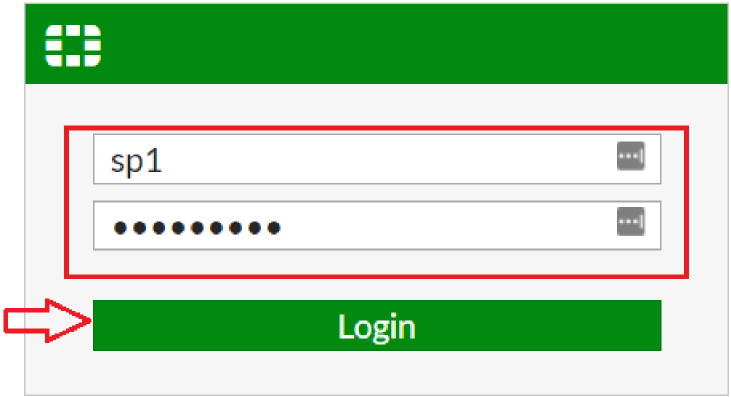
Now let's try again using support account users sp1. The user sp1 was successfully authenticated but wasn't authorized to run more commands.



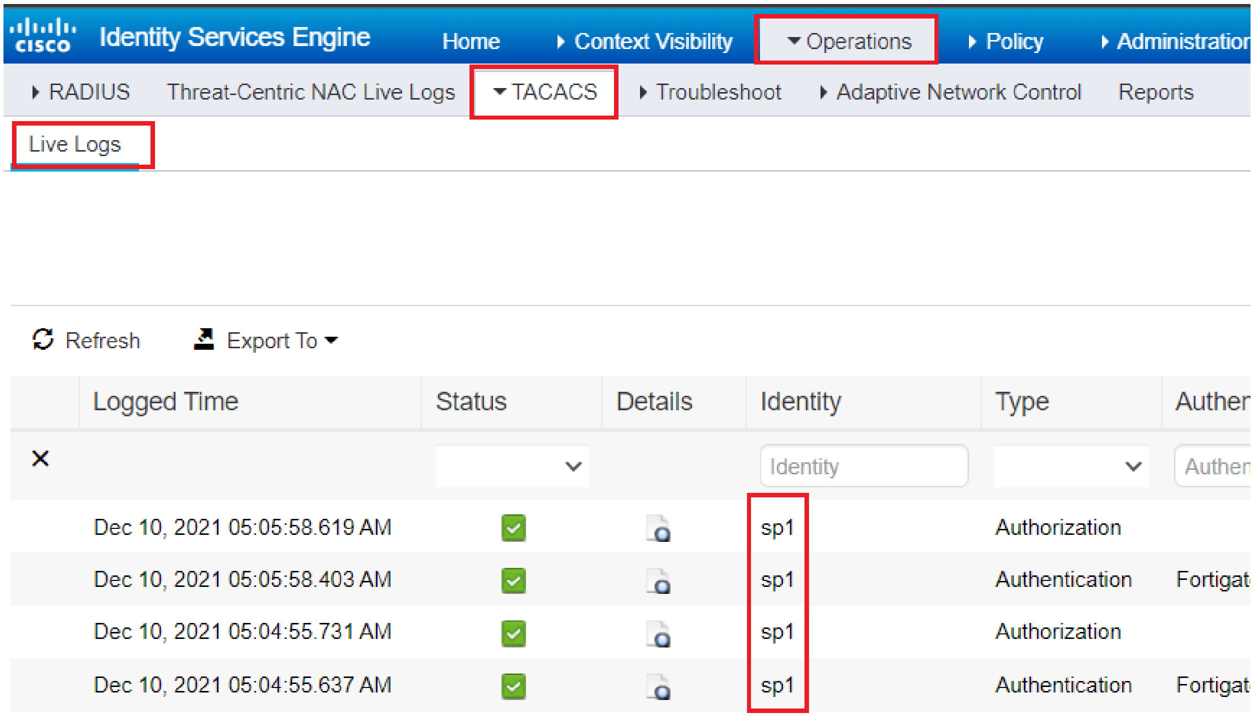
```
login as: sp1
sp1@192.168.100.253's password:
FG $ config system int
Unknown action 0

FG $
```

Let’s login through Web-GUI type the Active Directory AdminGroup username sp1/Abc@12345.





We can monitor the authentication/authorization logs on ISE Operations > TACACS > Live Logs.



Logged Time	Status	Details	Identity	Type	Auther
Dec 10, 2021 05:05:58.619 AM	✓		sp1	Authorization	
Dec 10, 2021 05:05:58.403 AM	✓		sp1	Authentication	Fortigat
Dec 10, 2021 05:04:55.731 AM	✓		sp1	Authorization	
Dec 10, 2021 05:04:55.637 AM	✓		sp1	Authentication	Fortigat