

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**

The screenshot displays the FortiGate Web-GUI interface. On the left, the 'User & Authentication' menu is highlighted, with 'TACACS+ Servers' selected. The main panel shows the 'Edit TACACS+ Server' configuration for a server named 'TACACS-SRV'. The 'Authentication Type' is set to 'Auto', and the 'Type' is 'PAP'. The 'Primary Server' section shows the 'Server IP/Name' as '192.168.100.210' and the 'Server Secret' as 'Test123'. The 'Connection status' is 'Error'. The 'Secondary Server' section is currently empty.

Edit TACACS+ Server	
Name	TACACS-SRV
Authentication Type	Auto Specify
Type	PAP
Primary Server	
Server IP/Name	192.168.100.210
Server Secret	Test123
Connection status	Error
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.

The screenshot shows the 'New User Group' configuration page in the FortiGate web interface. The left sidebar has 'User & Authentication' and 'User Groups' highlighted. The main panel is titled 'New User Group' and contains the following fields:

- Name:** AdminGroup
- Type:** Firewall (selected from a dropdown menu that also includes Fortinet Single Sign-On (FSSO), RADIUS Single Sign-On (RSSO), and Guest)
- Members:** A field with a '+' icon for adding members.
- Remote Groups:** A table with columns 'Remote Server' and 'Group Name'. It contains one entry: TACACS-SRV mapped to AdminGroup. Above the table are buttons for '+ Add', 'Edit', and 'Delete'.

The screenshot shows the 'New User Group' configuration page in the FortiGate web interface, similar to the one above but for a different group. The left sidebar is the same. The main panel is titled 'New User Group' and contains the following fields:

- Name:** SupportGroup
- Type:** Firewall (selected from a dropdown menu that also includes Fortinet Single Sign-On (FSSO), RADIUS Single Sign-On (RSSO), and Guest)
- Members:** A field with a '+' icon for adding members.
- Remote Groups:** A table with columns 'Remote Server' and 'Group Name'. It contains one entry: TACACS-SRV mapped to SupportGroup. Above the table are buttons for '+ Add', 'Edit', and 'Delete'. A page number '1' is visible at the bottom right of the table area.

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**.

System

Administrators

Admin Profiles ☆

Firmware

Settings

HA

SNMP

Replacement Messages

FortiGuard

Feature Visibility

Certificates

Policy & Objects

Security Profiles

VPN

User & Authentication

Log & Report

New Admin Profile

Name: AdminProfile

Comments: 0/255

Access Permissions

Access Control	Permissions	Set All ▼
Security Fabric	<input type="radio"/> None <input type="radio"/> Read <input checked="" type="radio"/> Read/Write	
FortiView	<input type="radio"/> None <input type="radio"/> Read <input checked="" type="radio"/> Read/Write	
User & Device	<input type="radio"/> None <input type="radio"/> Read <input checked="" type="radio"/> Read/Write	
Firewall	<input type="radio"/> None <input type="radio"/> Read <input checked="" type="radio"/> Read/Write	<input checked="" type="radio"/> Custom
Log & Report	<input type="radio"/> None <input type="radio"/> Read <input checked="" type="radio"/> Read/Write	<input checked="" type="radio"/> Custom
Network	<input type="radio"/> None <input type="radio"/> Read <input checked="" type="radio"/> Read/Write	<input checked="" type="radio"/> Custom
System	<input type="radio"/> None <input type="radio"/> Read <input checked="" type="radio"/> Read/Write	<input checked="" type="radio"/> Custom
Security Profile	<input type="radio"/> None <input type="radio"/> Read <input checked="" type="radio"/> Read/Write	<input checked="" type="radio"/> Custom
VPN	<input type="radio"/> None <input type="radio"/> Read <input checked="" type="radio"/> Read/Write	
WAN Opt & Cache	<input type="radio"/> None <input type="radio"/> Read <input checked="" type="radio"/> Read/Write	
WiFi & Switch	<input type="radio"/> None <input type="radio"/> Read <input checked="" type="radio"/> Read/Write	

OK

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**.

Dashboard

Security Fabric

Network

System

Administrators

Admin Profiles

Firmware

Settings

HA

SNMP

Replacement Messages

FortiGuard

Feature Visibility

Certificates

Policy & Objects

Security Profiles

VPN

User & Authentication

Log & Report

New Admin Profile

Name

Comments

0/255

Access Permissions

Access Control	Permissions	Set All
Security Fabric	<input checked="" type="radio"/> None <input checked="" type="radio"/> Read <input type="radio"/> Read/Write	
FortiView	<input checked="" type="radio"/> None <input checked="" type="radio"/> Read <input type="radio"/> Read/Write	
User & Device	<input checked="" type="radio"/> None <input checked="" type="radio"/> Read <input type="radio"/> Read/Write	
Firewall	<input checked="" type="radio"/> None <input checked="" type="radio"/> Read <input type="radio"/> Read/Write <input type="radio"/> Custom	
Log & Report	<input checked="" type="radio"/> None <input checked="" type="radio"/> Read <input type="radio"/> Read/Write <input type="radio"/> Custom	
Network	<input checked="" type="radio"/> None <input checked="" type="radio"/> Read <input type="radio"/> Read/Write <input type="radio"/> Custom	
System	<input checked="" type="radio"/> None <input checked="" type="radio"/> Read <input type="radio"/> Read/Write <input type="radio"/> Custom	
Security Profile	<input checked="" type="radio"/> None <input checked="" type="radio"/> Read <input type="radio"/> Read/Write <input type="radio"/> Custom	
VPN	<input checked="" type="radio"/> None <input checked="" type="radio"/> Read <input type="radio"/> Read/Write	
WAN Opt & Cache	<input checked="" type="radio"/> None <input checked="" type="radio"/> Read <input type="radio"/> Read/Write	
WiFi & Switch	<input checked="" type="radio"/> None <input checked="" type="radio"/> Read <input type="radio"/> Read/Write	

OK

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:

Comments: 0/255

Access Permissions

Access Control	Permissions	Set All ▾
Security Fabric	<input type="button" value="None"/> <input type="button" value="Read"/> <input type="button" value="Read/Write"/>	
FortiView	<input type="button" value="None"/> <input type="button" value="Read"/> <input type="button" value="Read/Write"/>	
User & Device	<input type="button" value="None"/> <input type="button" value="Read"/> <input type="button" value="Read/Write"/>	
Firewall	<input type="button" value="None"/> <input type="button" value="Read"/> <input type="button" value="Read/Write"/> <input type="button" value="Custom"/>	
Log & Report	<input type="button" value="None"/> <input type="button" value="Read"/> <input type="button" value="Read/Write"/> <input type="button" value="Custom"/>	
Network	<input type="button" value="None"/> <input type="button" value="Read"/> <input type="button" value="Read/Write"/> <input type="button" value="Custom"/>	
System	<input type="button" value="None"/> <input type="button" value="Read"/> <input type="button" value="Read/Write"/> <input type="button" value="Custom"/>	
Security Profile	<input type="button" value="None"/> <input type="button" value="Read"/> <input type="button" value="Read/Write"/> <input type="button" value="Custom"/>	
VPN	<input type="button" value="None"/> <input type="button" value="Read"/> <input type="button" value="Read/Write"/>	
WAN Opt & Cache	<input type="button" value="None"/> <input type="button" value="Read"/> <input type="button" value="Read/Write"/>	

OK

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.

The screenshot shows the 'Edit Administrator' configuration page for a user named 'admin1'. The left sidebar contains a navigation menu with 'System' and 'Administrators' highlighted. The main form includes the following fields:

- Username:** admin1
- Type:** Match all users in a remote server group (selected from a dropdown menu)
- Comments:** Write a comment... (0/255)
- Administrator Profile:** No-Access (selected from a dropdown menu)
- Remote User Group:** AdminGroup (selected from a dropdown menu)
- Restrict login to trusted hosts:** (unchecked)
- Restrict admin to guest account provisioning only:** (unchecked)

An 'OK' button is located at the bottom right of the form.

The screenshot shows the 'Edit Administrator' configuration page for a user named 'support1'. The left sidebar contains a navigation menu with 'System' and 'Administrators' highlighted. The main form includes the following fields:

- Username:** support1
- Type:** Match all users in a remote server group (selected from a dropdown menu)
- Comments:** Write a comment... (0/255)
- Administrator Profile:** No-Access (selected from a dropdown menu)
- Remote User Group:** SupportGroup (selected from a dropdown menu)
- Restrict login to trusted hosts:** (unchecked)
- Restrict admin to guest account provisioning only:** (unchecked)

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
<pre>FG # config system admin FG (admin) # edit admin1 FG (support1) # set accprofile-override enable FG (support1) # end</pre>
support1 Administrator Account
<pre>FG # config system admin FG (admin) # edit support1 FG (support1) # set accprofile-override enable FG (support1) # end</pre>

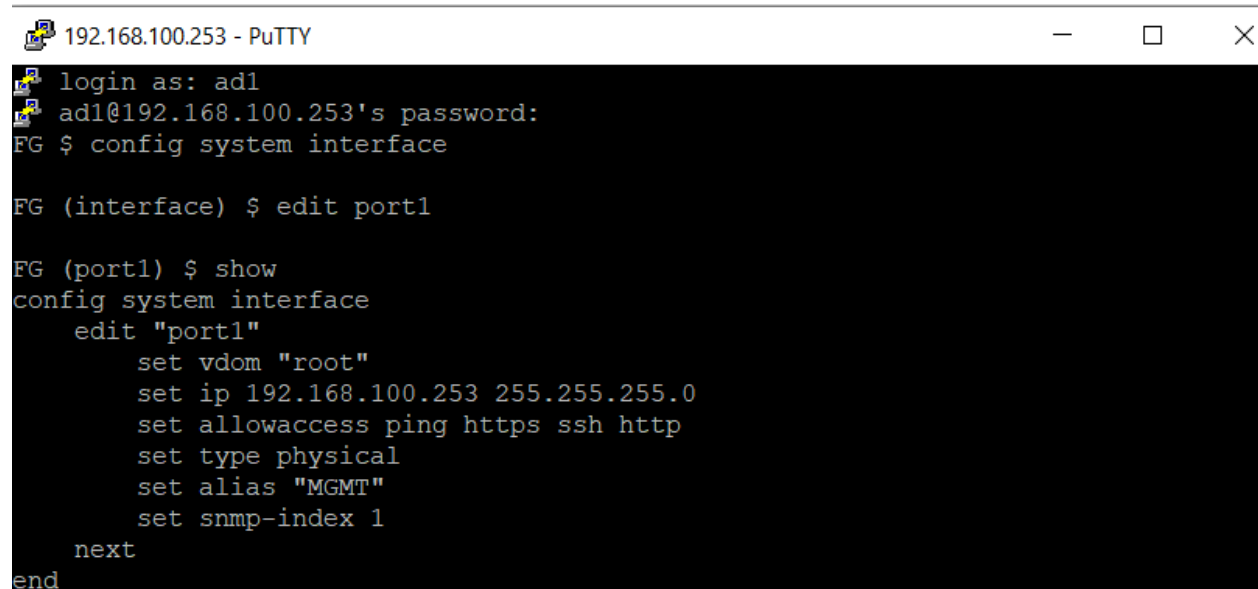
```

CLI Console (1)
FG # config system admin

FG (admin) # show
config system admin
  edit "admin"
    set accprofile "super_admin"
    set vdom "root"
    set password ENC SH2650wxQPM2Yi7NwWNjAjCo4xK2mTika6HPbCq0RmqZiaEH4S15P0ntEwTgEU=
  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.

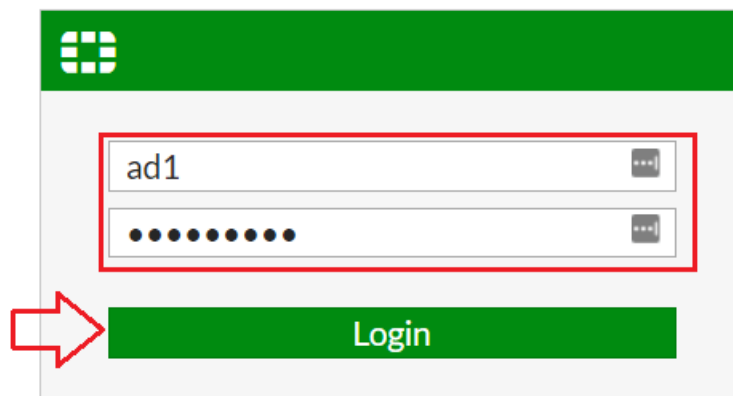


```
192.168.100.253 - PuTTY
login as: ad1
ad1@192.168.100.253's password:
FG $ config system interface

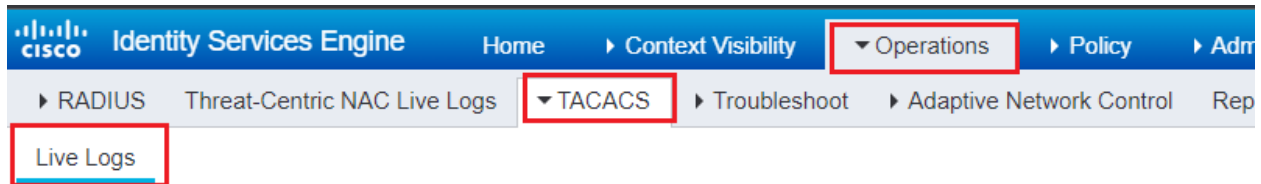
FG (interface) $ edit port1

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**.



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.



Refresh Export To

	Logged Time	Status	Details	Identity	Type
X				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.

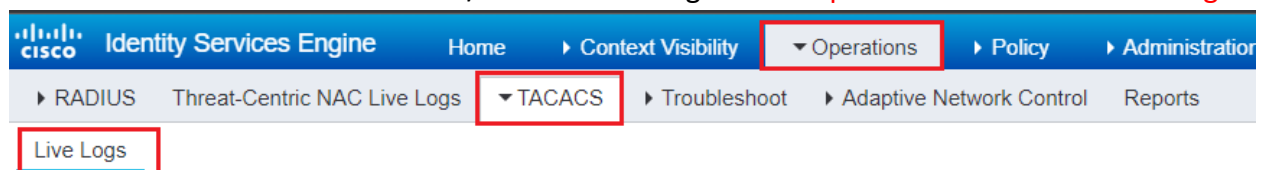
```
192.168.100.253 - PuTTY
login as: sp1
sp1@192.168.100.253's password:
FG $ config system int
Unknown action 0

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**.



Refresh Export To

	Logged Time	Status	Details	Identity	Type	Author
X				Identity		Authen
	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