Dragoss Owners	FORM	
Process Owner:  IT Operations	2FA for FortiGate SSL VPN using DUO	F-CMG-3.1

Request Information					
Requestor		Maurice Mendoza			
Implementing Team	Network Operations				
Ticket Number/s		.915572			
Change Classification	Χ	Major		Minor	
After the fact		Yes	Х	No	
Emergency		Yes	Х	No	
Proposed Change Date		May 17, 2019			
Proposed Change Start/End Time		18:00 – 21:00			
Proposed Change Verification Time		20:00			

# Objective of the change

To point all Network Equipment to Syslog Server

Technical/Operational Impact of the change				
Negative:	Beneficial:	Neutral:		
No known negative impact.	Improved security: By requiring a second form of identification.	Additional cabling and utilization of switchport of DMZ switch		
		Additional power for Duo Auth Proxy and Radius server in Rack A		

Affected	Affected IT Infrastructure components				
Site	Hostname	IP Address	Function		
JAKA	ODYSSEUS	10.1.0.100	VPN Device		

Affected Departments and corresponding contact persons				
Department Contact Name Contact Info				
IT	Rynel Yanes	09178535630		
Network Operations	Maurice Mendoza	09176328103		

# Test Environment implementation and Verification Summary

Configured FortiGate 101E with SSL VPN, installed Duo Authentication proxy and daloRadius in the test server. Followed all the steps provided by Duo for FortiGate SSL VPN with Duo integration. <a href="https://duo.com/docs/fortinet">https://duo.com/docs/fortinet</a>

## Test Environment Results Summary

Upon testing, whenever a user logs in to the FortiClient SSL VPN, DUO sends a Login request message to the registered device. If accepted, user will be logged in successfully. If not, FortiGate will drop and revert to the login page.

OPENACCESS WE SHAK YOUR LANGUAGE	Proprietary and Confidential	Effectivity: April 1, 2019	Page 1
	and community		Template Version : <b>02</b>

Dragoss Owners	FORM	
Process Owner: IT Operations	2FA for FortiGate SSL VPN using DUO	F-CMG-3.1

## Configuration Change Template

Baseline File	3.1.407
Baseline Version	April 3, 2019

#### Baseline File Changes:

Existing Configuration	Proposed Change	Impact	Section
No existing 2 Factor	Improved security: By adding	SSL-VPN portal and	3.1.407
Authentication	the Factor Authentication using	settings, Radius	
configured in the VPN	Duo	Server, User and	
Device		Groups	

#### Physical Implementation Procedures / Advisory

- 1. Place the configured Duo Authentication Proxy and Radius server in Rack A.
- 2. Connect a LAN cable from Radius server to port fa0/3 of DMZ Switch.
- 3. Connect a monitor, keyboard, and mouse to the Radius server.

#### **Backup Procedures**

Access Odysseus via web (https://10.1.0.100:10443)

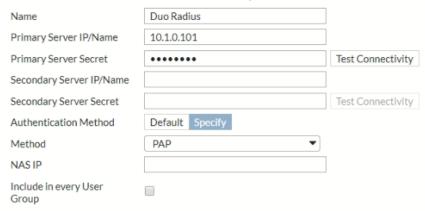
Backup the configurations files using the naming conventions:

BACKUP\_DEVICENAME\_DATE.cfg

Example: BACKUP\_ODYSSEUS\_5172019.cfg

#### **Technical Configuration Procedures**

- 1. Access Odysseus via web(<a href="https://10.1.0.100:10443">https://10.1.0.100:10443</a>)
- 2. Navigate to User & Device > Radius Servers
- 3. Create new Radius Server with the following details:



- 4. Navigate to User & Device > User Groups
- 5. Create new User Group with the following details:

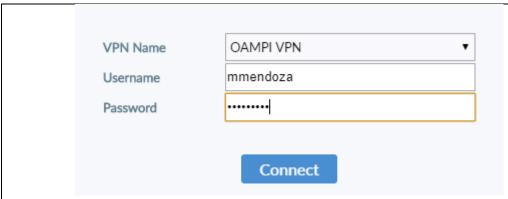


# Process Owner: IT Operations FORM F-CMG-3.1





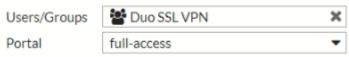




- 3. A login request message will appear on the registered device via Duo Mobile App.
- 4. If accepted, user will be logged in successfully. If not, FortiGate will drop and revert to the login page.
- 5. If the user logs in successfully, ping or access the device via web <a href="https://172.17.3.101:10443">https://172.17.3.101:10443</a>. It should be reachable.

#### **Back-out Procedures**

- 1. Go to VPN > SSL-VPN Settings. Scroll down to Authentication/Portal Mapping
- 2. Delete the previously created mapping with the following details:



- 3. Remove the configured Duo Authentication Proxy and Radius server from Rack A.
- 4. Unplug the LAN cable from Radius server to port fa0/3 of DMZ Switch.

