Dragon Ourran	FORM	
Process Owner: IT Operations	Configuration Change Request	F-CMG-3.1

Request Information				
Requestor	Ma	Maurice Mendoza		
Implementing Team	Net	work Operations		
Ticket Number/s	201915102			
Change Classification	Х	Major		Minor
After the fact		Yes	Х	No
Emergency		Yes	Х	No
Proposed Change Date	Ma	y 3, 2019		
Proposed Change Start/End Time	4:00 PM – 4:30 PM			
Proposed Change Verification Time	4:20 PM			

Objective of the change

To enable the password policy on all FortiGate Equipment.

Technical/Operational Impact of the change			
Negative:	Beneficial:	Neutral:	
All administrator will reset	Increased in password	Access to FortiGate Web GUI.	
their password after login.	complexity means more		
	security.		

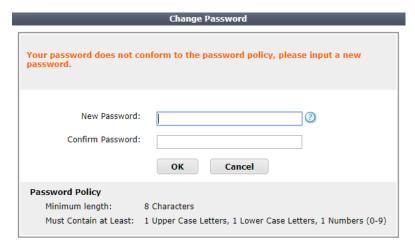
Affected IT Infrastructure components			
Site	Hostname	IP Address	Function
JAKA	THOR	172.16.1.2	Site Firewall
G2	MKT-GL2-FW-1	172.22.0.74	Site Firewall
G2	MKT-GL2-FW-1	172.22.0.75	Site Firewall

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

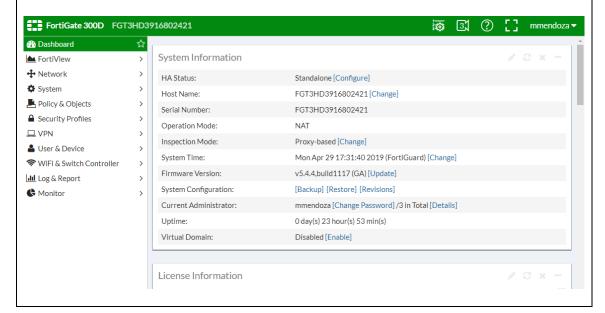
Test Environment implementation and Verification Summary			
Configured the Password Policy in the test FortiGate unit with the following details:			
Password Policy			
Password scope 🕦	Off Admin IPsec Both		
Minimum length	8		
Character requirements C			
Upper case	1		
Lower case	1		
Numbers (0-9)	1		
Special 🐧	0		
Allow password reuse			
Password expiration	60	Days	



After configuring the password policy, the user logged out then logged in again. A change password request appeared:



After changing the password to the required complexity, the user can now access FortiGate.



Test Environment Results Summary

Based on the testing, after configuring the password policy on the test FortiGate, users have been requested to update their passwords in accordance to the policy. After changing, users were now able to access the FortiGate with their updated credentials.



Draces Owner	FORM	
Process Owner: IT Operations	Configuration Change Request	F-CMG-3.1

Configuration Change Template

Baseline File	3.1.401, 3.1.402
Baseline Version	April 30, 2019

Baseline File Changes:

Existing Configuration	Proposed Change	Impact	Section
No existing password policy in FortiGate Equipment.	To enable the password policy on all FortiGate Equipment.	Password Policy	3.1.401, 3.1.402

Physical Implementation Procedures / Advisory

Send an email to all the FortiGate Administrators that will be affected after the implementation.

"Team,

Please be advised that we will changing the Password Policy of all FortiGate Equipment. You are required to change your password based on the complexity.

Thank you.

Regards,"

Backup Procedures

Access FortiGate Jaka and G2 via Web Browser.

Backup the configurations files using the naming conventions:

BACKUP_DEVICENAME_DATE.cfg

Example: BACKUP_THOR_532019.cfg, BACKUP_MKT-GL2-FW-1_532019.cfg

Technical Configuration Procedures

- 1. Access FortiGate Thor via Web (https://172.16.1.2:10443)
- 2. Create an administrator account that will serve as the backup account. Navigate to System > Administrator then create new using the following details:

Username: backupaccount

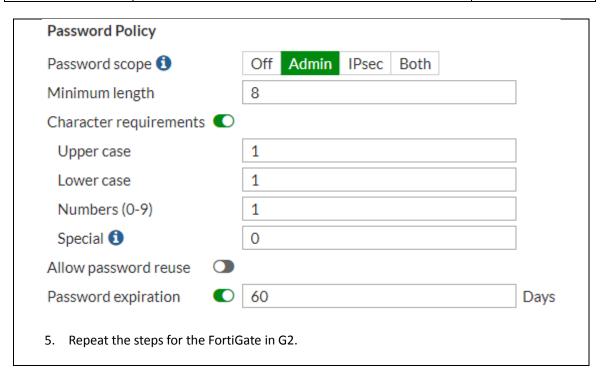
Password: !D3l3cTu5 (password complies to the password policy)

Administrator Profile: super_admin

- 3. Navigate to System > Settings then scroll down to the Password Policy Section.
- 4. Enable the Password Scope to **Admin** then change the details to the following:



Dun anna Outra an	FORM	
Process Owner: IT Operations	Configuration Change Request	F-CMG-3.1



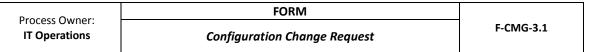
Verification Procedures

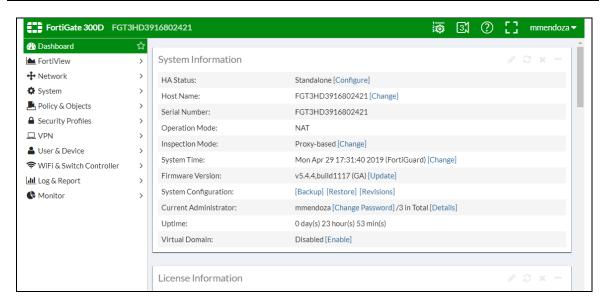
To verify the changes, login to all FortiGate Equipment. A change password request should appear.



After updating the credentials, it should redirect to the FortiGate Dashboard.







Back-out Procedures

1. Login to all FortiGate Equipment using the backup account that was created.

Username: backupaccount Password: !D3l3cTu5

- 2. Navigate to System > Settings then scroll down to the Password Policy Section.
- 3. Turn the Password Scope to OFF.