



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

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.

Process Owner: IT Operations	FORM	F-CMG-3.1
	<i>Configuration Change Request</i>	

### 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:

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

### Password Policy

Password scope ⓘ Off **Admin** IPsec Both

Minimum length

Character requirements ☒

Upper case

Lower case

Numbers (0-9)

Special ⓘ

Allow password reuse ☐

Password expiration ☒  Days

5. Repeat the steps for the FortiGate in G2.

### Verification Procedures

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

Change Password

Your password does not conform to the password policy, please input a new password.

New Password:  ⓘ

Confirm Password:

OK Cancel

**Password Policy**

Minimum length: 8 Characters

Must Contain at Least: 1 Upper Case Letters, 1 Lower Case Letters, 1 Numbers (0-9)

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

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

The screenshot displays the FortiGate 300D web interface for device FGT3HD3916802421. The left sidebar contains navigation links: Dashboard, FortiView, Network, System, Policy & Objects, Security Profiles, VPN, User & Device, WiFi & Switch Controller, Log & Report, and Monitor. The main content area is divided into two sections: 'System Information' and 'License Information'. The 'System Information' section lists various system parameters with links to configure or change them.

System Information	
HA Status:	Standalone <a href="#">[Configure]</a>
Host Name:	FGT3HD3916802421 <a href="#">[Change]</a>
Serial Number:	FGT3HD3916802421
Operation Mode:	NAT
Inspection Mode:	Proxy-based <a href="#">[Change]</a>
System Time:	Mon Apr 29 17:31:40 2019 (FortiGuard) <a href="#">[Change]</a>
Firmware Version:	v5.4.4,build1117 (GA) <a href="#">[Update]</a>
System Configuration:	<a href="#">[Backup]</a> <a href="#">[Restore]</a> <a href="#">[Revisions]</a>
Current Administrator:	mmendoza <a href="#">[Change Password]</a> /3 in Total <a href="#">[Details]</a>
Uptime:	0 day(s) 23 hour(s) 53 min(s)
Virtual Domain:	Disabled <a href="#">[Enable]</a>

The 'License Information' section is partially visible at the bottom of the screen.

#### Back-out Procedures

1. Login to all FortiGate Equipment using the backup account that was created.  
  
Username: backupaccount  
Password: !D3I3cTu5
2. Navigate to System > Settings then scroll down to the Password Policy Section.
3. Turn the Password Scope to **OFF**.