Fortigate Password Recovery

Once logged into the FortiGate with the maintainer account (as described below), if the FortiGate is running FortiOS 6.0.3 or later, enter the execute factoryreset command to return the FortiGate to its default configuration.
This can be useful if the admin administrator account was deleted.

In newer versions of the BIOS, expect some changes to the behavior of the maintainer account. These changes will include:

- The countdown timer for how log enter the credentials has increased. Starting from when the device powers up, there will be 60 seconds instead of 30.
- Using the maintainer account and resetting a password cause a log to be created; making these actions traceable for security purposes.
- The account will be able to reset the password for any super-admin profile user in addition to the default admin user. This takes into account the possibility that the default account has been renamed.
- The only thing the maintainer account has permissions to do is reset the passwords of super-admin profile accounts.

What is needed:

- Console cable
- Terminal software such as Putty.exe (Windows) or Terminal (MacOS)
- Serial number of the FortiGate device

Procedure:

Step 1

Connect the computer to the firewall via the Console port on the back of the unit.
In most units this is done either by a Serial cable or a RJ-45 to Serial cable. There are some units that use a USB cable and FortiExplorer to connect to the console port.

Resetting a lost admin password for the VM-s using the maintainer account is not possible.
In this case, reverting to a snapshot or re-provisioning the VM and restoring the configuration (without a password for the admin account) is the only solution.

Step 2

Start the terminal software.

Step 3

Connect to the firewall using the following:

- Setting - Value
- SpeedBaud - 9600
- Data Bits - 8 Bit
- Parity - None
- Stop Bits - 1
- Flow Control - No Hardware Flow Control
- Com Port - the correct COM port

Step 4

The firewall should then respond with its name or hostname. (If it doesn’t try pressing “enter”.)

Step 5

Reboot the firewall.
If there is no power button, disconnect the power adapter and reconnect it after 10 seconds. Plugging in the power too soon after unplugging it can cause corruption in the memory in some units.

Step 6

Wait for the Firewall name and login prompt to appear. The terminal window should display something similar to the following:

> FortiGate-60C (18:52-06.18.2010)
> Ver:04000010
> Serial number: FGT60C3G10xxxxxx
> CPU(00): 525MHz
> Total RAM: 512 MB
> NAND init... 128 MB
> MAC Init... nplite#0
> Press any key to display configuration menu...
> ......
> reading boot image 1163092 bytes.
> Initializing firewall...
> System is started.
> login:

Step 7

Type in the username: maintainer

Step 8

The password is bcpb + the serial number of the firewall (letters of the serial number are in UPPERCASE format)
Example: bcpbFGT60C3G10xxxxxx

Note: On some devices, after the device boots, there is only 14 seconds or less to type in the username and password.
It might, therefore, be necessary to have the credentials ready in a text editor, and then copy and paste them into the login screen.
There is no indicator of when the time runs out so it is possible that it might take more than one attempt to succeed.

Step 9

Now there should be a connection to the firewall.
To change the admin password, type the following…

In a unit where VDOMs are not enabled:

> **# config system admin**
> edit admin
> set password
> end

In a unit where VDOMs are enabled:

> **# config global**
> config system admin
> edit admin
> set password
> end

If the FortiGate is running FortiOS 6.0.3 or later, enter the following command to reset the FortiGate to its factory default configuration.
This can be useful if the admin administrator account has been deleted.

> **# execute factoryreset**

Warning:
Good news and bad news. Some might be worried that there is a backdoor into the system.
The maintainer feature/account is enabled by default, but the good news is that there is an option to disable this feature. The bad news is that if the feature is disabled and the password get lost without having someone else that can log in as a superadmin profile administrator, there will be no

options.

If an attempt to use the maintainer account and there is the following message on the console, “PASSWORD RECOVERY FUNCTIONALITY IS DISABLED”, this means that the maintainer account has been disabled.

Disabling the maintainer feature/account:

Use the following command in the CLI to change the status of the maintainer account

To disable

> **# config system global**
> set admin-maintainer disable
> end

To enable

> **# config system global**
> set admin-maintainer enable
> end

Revision #1
Created 2024-01-08 19:05:51 UTC by Miles Menninga
Updated 2024-01-08 19:06:32 UTC by Miles Menninga