Resetting a lost administrator password

Periodically a situation arises where your FortiMail unit needs to be accessed or the administrator account's password needs to be changed but no one with the existing password is available. If physical access to the device is possible and with a few other tools, the password can be reset.

This procedure will require the reboot of the FortiMail unit.

FortiMail versions 6.0.8 and 6.2.3 introduce a new CLI command allowing you to enable or disable administrator password recovery:

```
config system global
   set admin-maintainer {enable | disable}
end
```

The following procedure requires `admin-maintainer` to be set to `enable`.

Administrators with physical access to a FortiMail unit can use a console cable and the maintainer administrator account to log into the CLI. The maintainer account allows you to log into a FortiMail unit if you have lost all administrator passwords.

Once logged into the FortiMail unit with the maintainer account, you can reset the passwords of super-admin profile accounts, or enter the `execute factoryreset` command to return the FortiMail unit 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 to 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 causes 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 `admin-maintainer` command is enabled by default. The methodology for using the maintainer account is publicly available. As long as someone with physical access to the device has the serial number of the device, which is labeled on the device, the admin administrator account password can be changed and access to the FortiMail unit is granted.

If this is an unacceptable risk to your specific environment (especially where the hardware is not physically secured), you can disable the command. However, if the feature is disabled, and the password gets lost without having someone else that can log in as a super-admin, you will have no options to restore access.

Requirements:

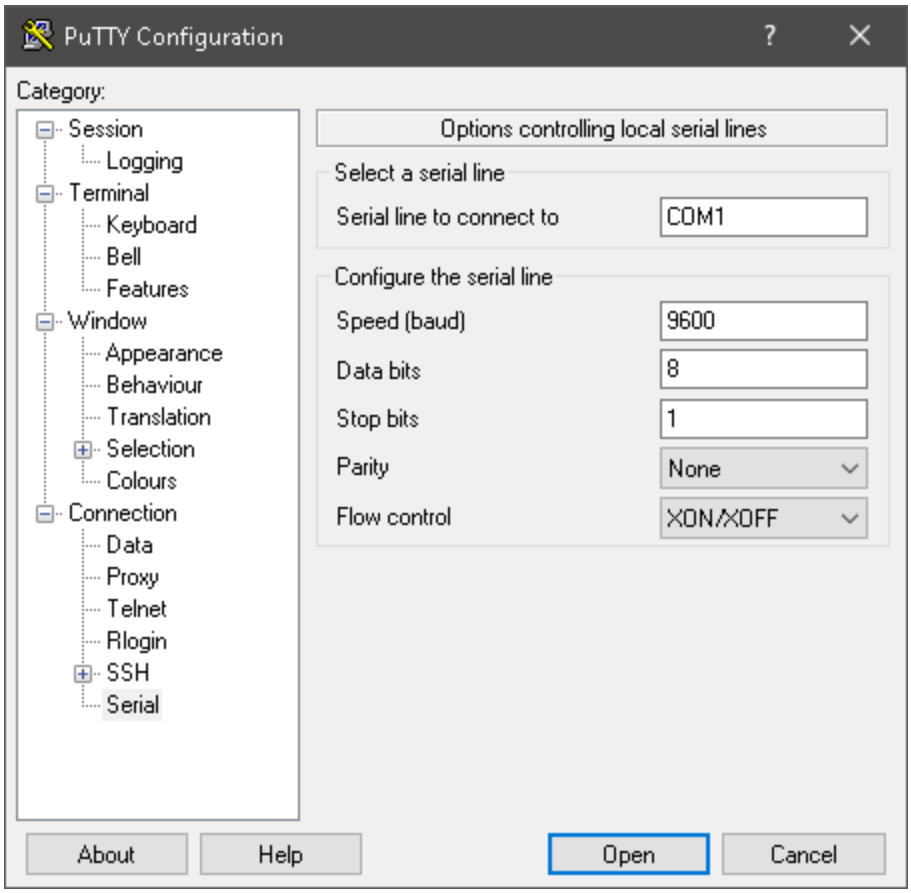
- Console cable
- Terminal software such as Putty.exe (Windows) or Terminal (MacOS)
- Serial number of the FortiGate device

Physically connect the FortiMail unit

1. Connect the computer to the FortiMail via the Console port on 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.
2. For virtual instances of FortiMail (that do not have any physical port to connect) use the supplied VM Hosts' console connection utility.

Connect to the FortiMail unit using terminal software

1. Start the terminal software, for example PuTTY.
2. Open the serial connection settings and enter the following:
   - **COM port/serial line**: The appropriate COM port
   - **Speed (baud)**: 9600
   - **Data bits**: 8
   - **Stop bits**: 1
   - **Parity**: None
   - **Flow control**: No hardware flow control
3. Click **Open**.



4. The FortiMail unit should then respond with its name or hostname (if it does not try pressing “Enter”).
5. Reboot the FortiMail unit. 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.

Log in using the maintainer account

1. Once the FortiMail unit has finished rebooting, on the login prompt, enter `maintainer`.
2. The password is `bcpb` plus the serial number of the unit. Make sure to enter the serial number in upper-case format. For example:
`bcpbFE900FT918******`

On some FortiMail units, after the device reboots, there is only 14 seconds or less to type in the username and password. It is recommended to have the credentials ready in a text editor to copy and paste them into the login screen when required. There is no indicator of when the time runs out so it might take more than one attempt to succeed.

Change the admin password

1. Once logged in as the maintainer, enter the following CLI command:

```
config system admin
   set password <password_str>
end
```

If the administrator account has somehow been deleted, enter the followng command to reset the FortiMail unit to its factory default configuration:

```
execute factoryreset
```