Default Passwords and Policies

Table of contents

BMC Passwords

The BMC password must comply with the following policy parameters:

- Using ASCII and Unicode characters is permitted
- Minimum length: 12
- Maximum length: 20
- Maximum number of consecutive character pairs: 4

> **Info**
>
> Two characters are consecutive if |hex(char_1)-hex(char_2)|=1.
>
> Examples of passwords with 5 consecutive character pairs (invalid): DcBa123456AbCd!; ab1XbcYcdZdeGef!; Testing_123abcgh!.

The following is a valid example password:

- HelloNvidia3D!

> **Note**
>
> A user account is locked for 10 minutes after 10 consecutive failed attempts.

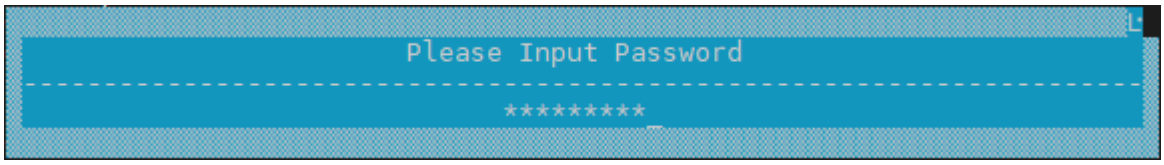
UEFI Menu Password

A password is required to enter the UEFI menu during BlueField bootup. The UEFI menu contains various settings which impact BlueField behavior. Therefore, it is very important

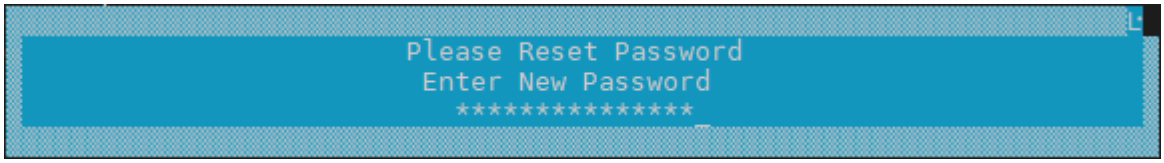
to keep that password secure.

Default Password

1. A first-time user accessing the UEFI menu must enter the default password for the UEFI menu, bluefield:

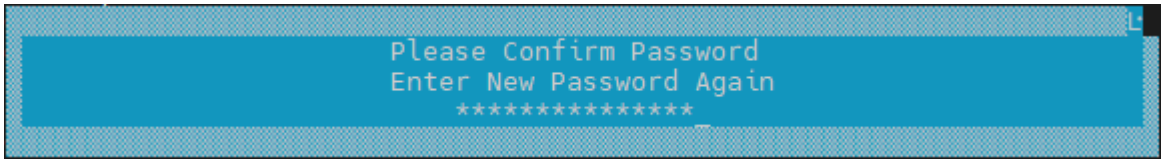


2. The user is prompted to provide a new password:



> **Note**
>
> The new password entered above must be in compliance with the password policy:
>
> - The password must be between 12 and 64 characters (inclusive)
> - There are no requirements for upper/lower case, or special characters. Spaces are allowed.

3. The user is prompted to confirm the new password:

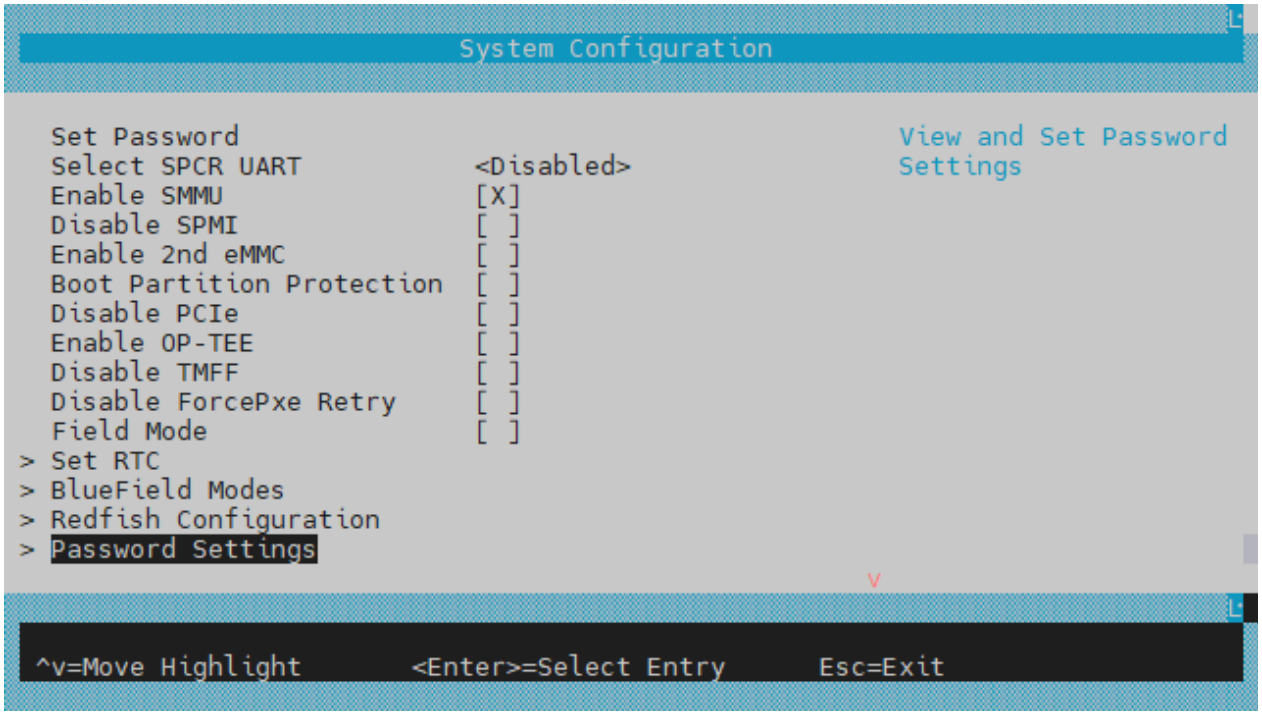


Default Password Policy

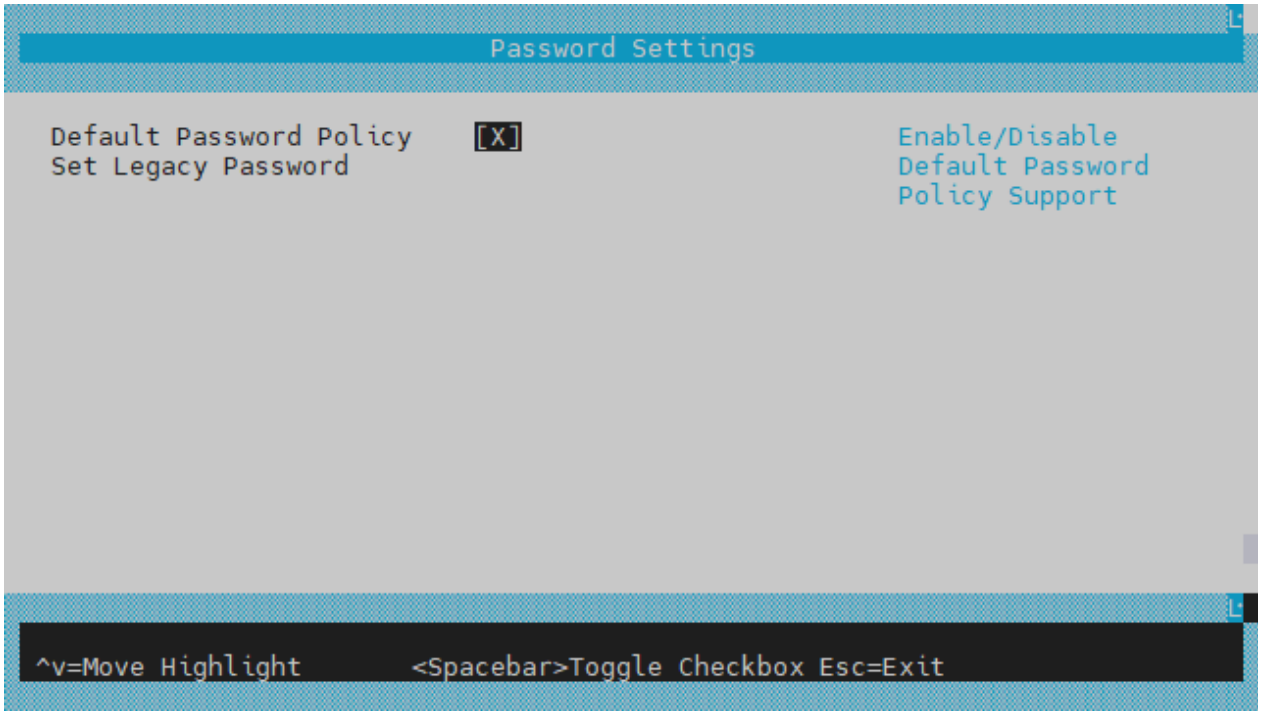
The user can enable/disable the UEFI password policy. The default password policy is enabled by default using a checkbox in the UEFI menu.

The user can browse the UEFI menu and disable as follows:

1. Navigate to "Device Configuration" > "System Configuration" > "Password Settings":



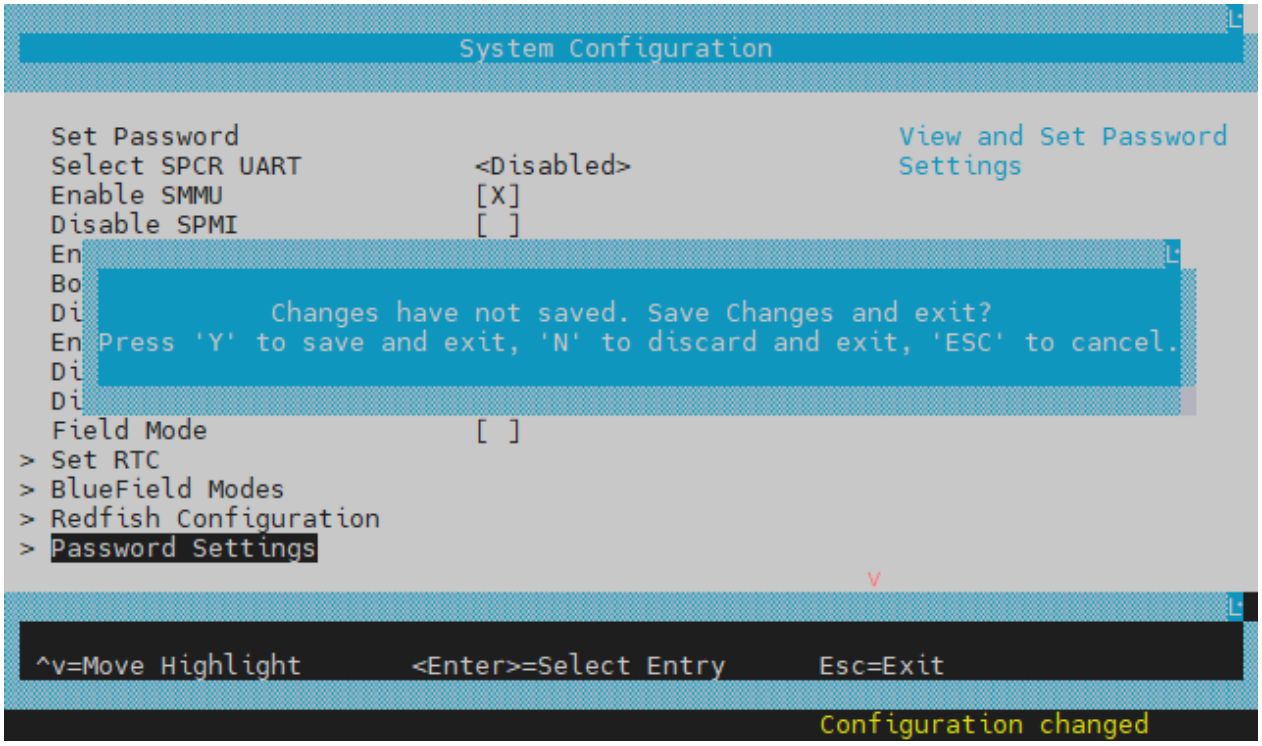
2. The "Default Password Policy" checkbox controls whether the more secure password policy is enabled:



Info

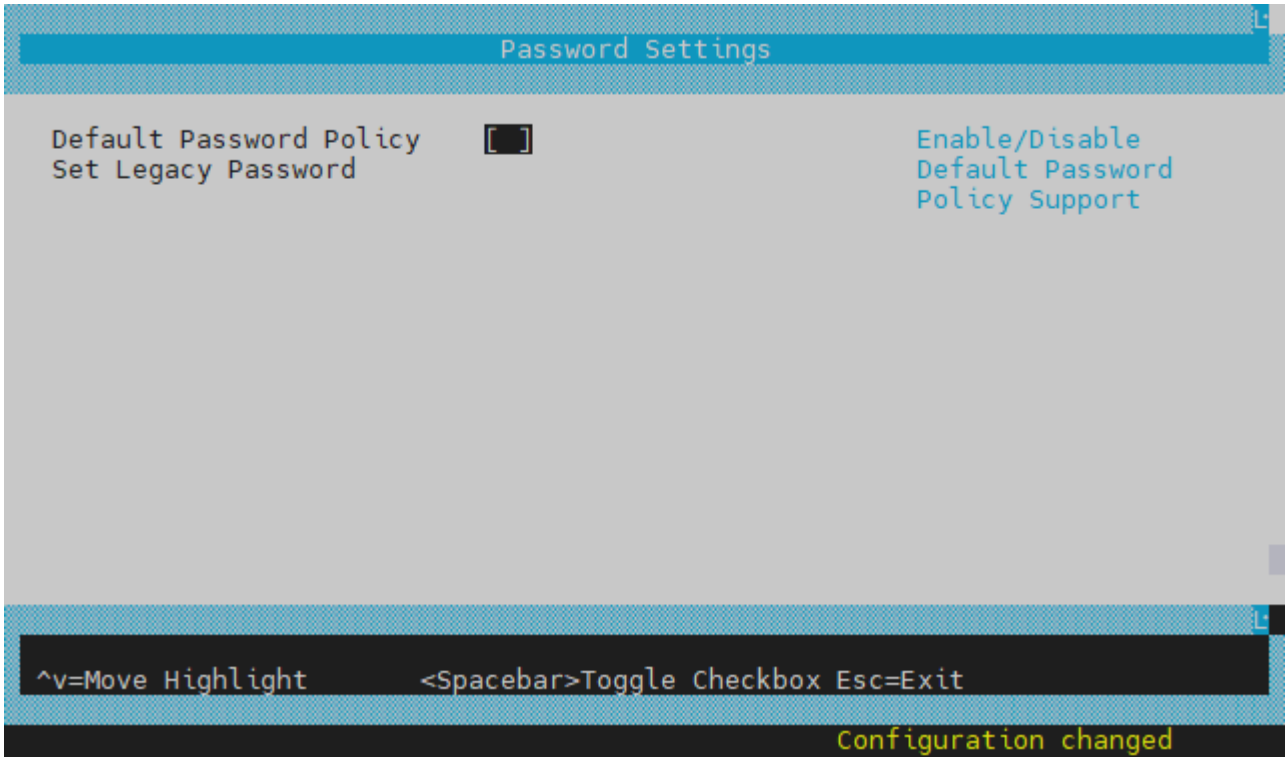
To disable the Default Password Policy, hit the spacebar to clear the checkbox.

3. The user must hit ESC ESC and answer "Y" to save the configuration change.



Disabling Default Password Policy

To disable the Default Password Policy, hit the spacebar to clear the checkbox.



Info

If the Default Password Policy is disabled, the password entered must be between 1 and 64 characters.

Software Downgrade

The UEFI's password policy is not backward compatible. Although downgrade is not recommended, users are allowed to downgrade their software while their password is set. But , if and only if the password is set, users must configure the legacy password prior to performing any downgrade.

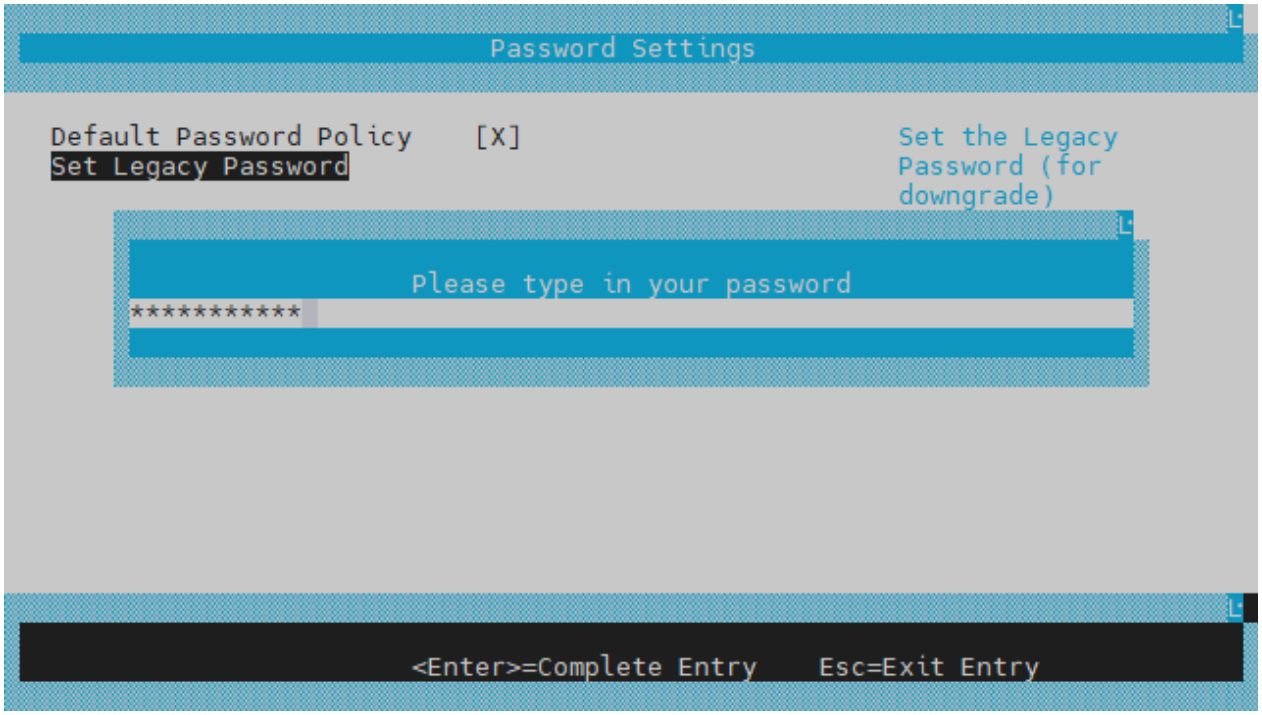
For BSP 4.6.0 (DOCA 2.6.0) or higher, users must change the UEFI password saved to the older "Legacy" format.

Warning

If this procedure is not followed before performing a software downgrade, users would not be able to enter the UEFI menu.

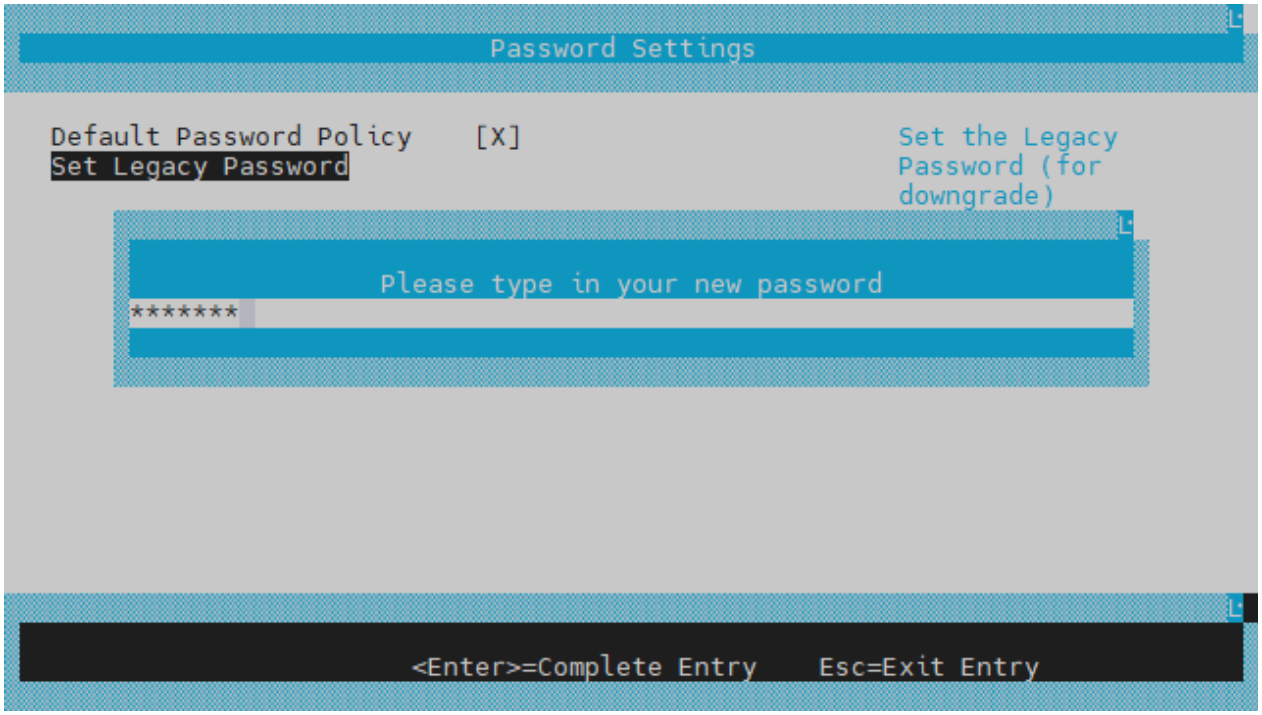
In the UEFI menu:

1. Navigate to "Device Manager" > "System Configuration" >"Password Settings" >" Set Legacy Password".
2. Select " Set Legacy Password ".
3. Enter your current password:

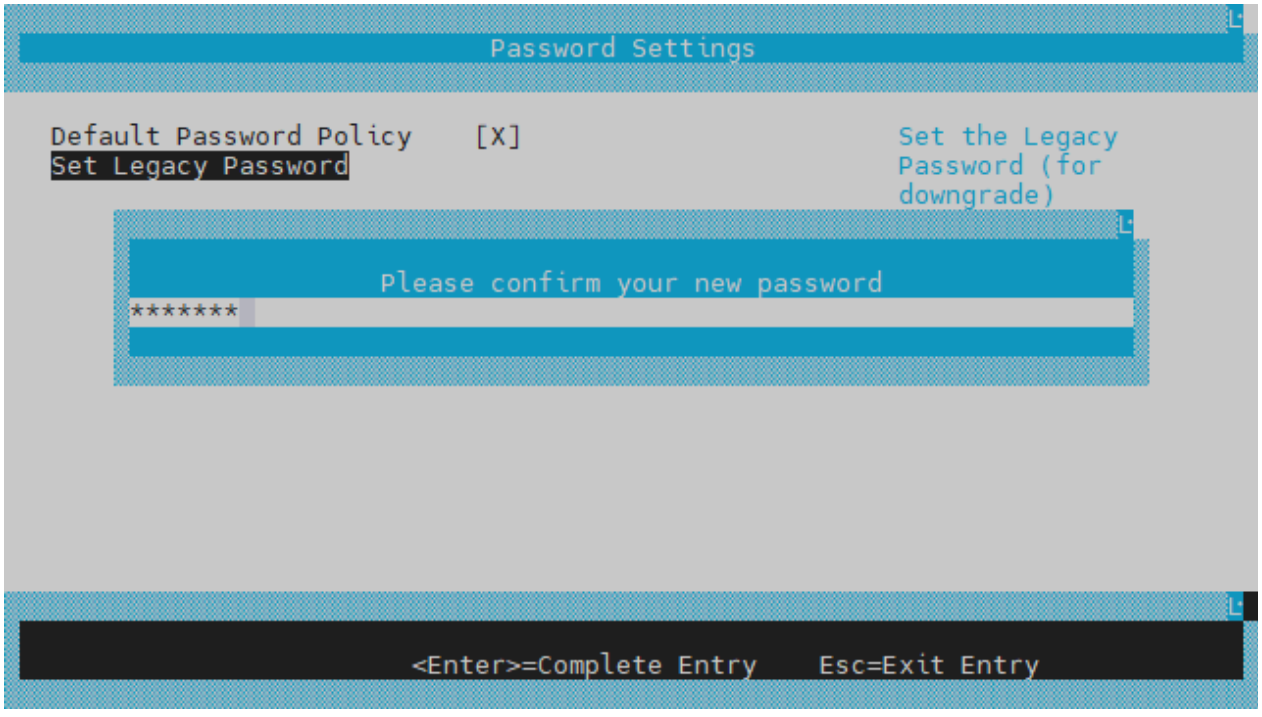


4. Type in a new legacy password between 1 and 20 characters:

> **Note**
>
> The password format allows up to 64 characters but anything greater than 20 characters is not backward compatible.



5. Confirm the new password:



Now, you may downgrade your BlueField image.

Password Reset

To reset the UEFI menu password, users may use the ready to use capsule file EnrollKeysCap installed under /lib/firmware/mellanox/boot/capsule/EnrollKeysCap on the BlueField DPU file system. From the BlueField console, execute the following command, then reboot:

```
ubuntu@localhost:~$ bfrec --capsule /lib/firmware/mellanox/boot/capsule/EnrollKeysCap
```

On the next reboot, the capsule file is processed, and the UEFI password is reset to bluefield.

GRUB Password

GRUB menu entries are protected by a username and password to prevent unwanted changes to the default boot options or parameters.

The default credentials are as follows:

Username	admin
Password	BlueField

The password can be changed during BFB installation by providing a new grub_admin_PASSWORD parameter in bf.cfg:

```
# vim bf.cfg
grub_admin_PASSWORD='
grub.pbkdf2.sha512.10000.5EB1FF92FDD89BDAF3395174282C77430656A6DBEC1F9289D5F5DAD17811A
```

To get a new encrypted password value use the command grub-mkpasswd-pbkdf2.

After the installation, the password can be updated by editing the file /etc/grub.d/40_custom and then running the command update-grub which updates the file /boot/grub/grub.cfg.

Ubuntu Password Policy

Upon first login, the username ubuntu must enter the default password ubuntu if this was not changed during the OS installation process. Users are then required to change the default password according to the following password policy:

The following table details the password policy parameters:

> **Info**
>
> Each of these parameters is configurable in its respective config file indicated in the "Config File Path" column.

Config File Path	Parameter	Value	Description
/etc/security/pwquality.conf	minlen	12	Minimum password length
/etc/pam.d/common-password	remember	3	The number of previous passwords which cannot be reused
/etc/security/faillock.conf	silent	Uncommented	Prevents printing informative messages to the user
	deny	10	The number of authentication attempts permitted before the user is locked out
	unlock_time	600	The duration of the lockout period, in seconds