SOPHOS UTM: ADMIN, LOGINUSER, AND ROOT ŞİFRE YENİLEME

OVERVİEW

This article contains steps to reset the password of the accounts `admin`, `loginuser`, and `root`.

PRODUCT AND ENVİRONMENT

Sophos UTM

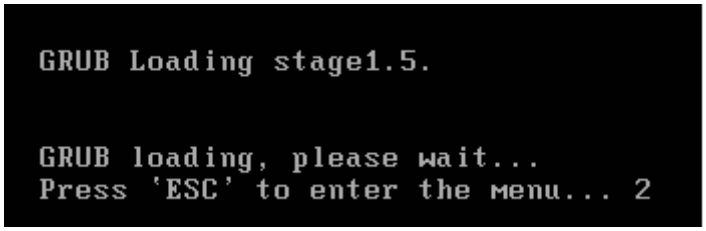
RESETTİNG PASSWORD FOR ADMİN, LOGİNUSER, AND ROOT

RESET THE LOGİNUSER AND ROOT PASSWORDS VİA CLI

1. Power off Sophos UTM.
2. Do either of the following:
   - Connect a monitor and a keyboard to Sophos UTM.
   - Connect a computer to Sophos UTM via a serial cable and use a terminal emulator application such as PuTTY and configure it to connect to `COM1` with a baud rate of `38400`. For more information, see Sophos UTM: Access the UTM shell via SSH using

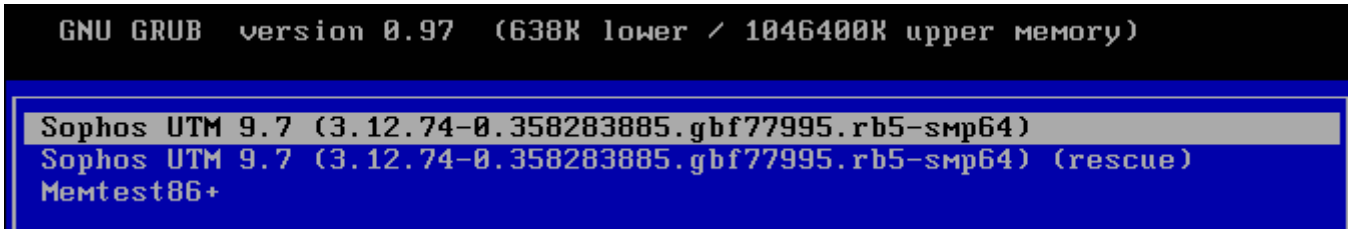
PuTTY.

3. Power on Sophos UTM and press **ESC** once the GRUB boot loader shows:



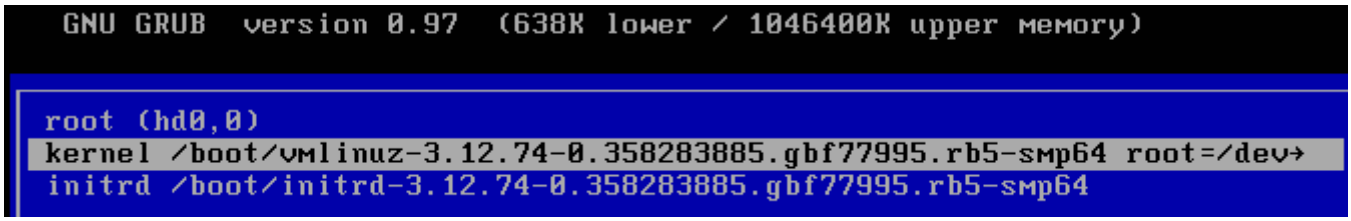
4. Select the running Sophos UTM version that does not have the words `previous` or `rescue` listed and press **E**.

   Example:



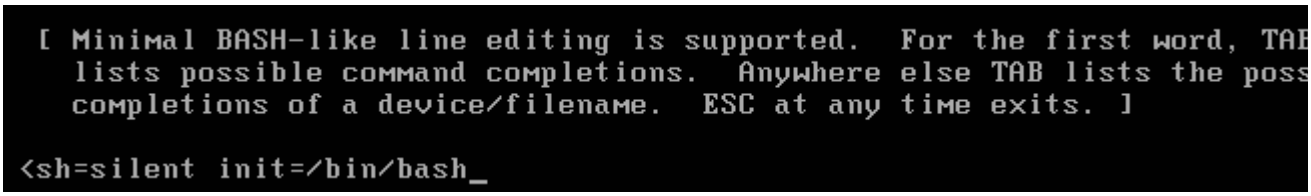
5. Select the option that starts with the word `kernel` and press **E**.

   Example:



6. Run the following commands:
   - Connected via a monitor and keyboard or if you are using a virtual machine: `init=/bin/bash`

     Example:



- Connected via a laptop and serial cable: `init=/bin/bash console=ttyS0,38400`

7. Press **Enter** to return to the previous screen.
8. Press **B** to restart Sophos UTM.

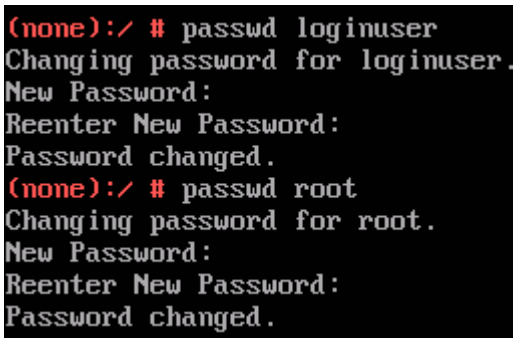
   The keyboard layout may change when going through the GRUB boot loader, and this may cause passwords to be different than what you entered. Avoid using the following:

   - Letters `s`, `y`, and `z`
   - Short passwords like `test`

   You can use a simple password like `ClosedDoor` and change its complexity later via WebAdmin.

9. Run the command `passwd loginuser`
10. Confirm the password for the account `loginuser`.
11. Run the command `passwd root`

    Note:
    Step 11 and onwards may not work with certain firmware versions due to a known issue with USB keyboard drivers not loading correctly when accessing the bash recovery environment. Ensure your Sophos UTM is updated to the latest firmware version.
    Affected versionsNon-affected versions9.104-9.1119.1129.205-9.2099.2109.300-9.307 for SG-series UTMs9.308+
12. Enter and confirm the password for the account `root`:



13. Press Ctrl+Alt+Del to restart Sophos UTM or run the command `./etc/init.d/rc6.d/S10reboot`

    Note: Do not enter the GRUB CLI that will be displayed.

14. Run the command `root` and enter its newly-set password.
15. Run the command `cc`
16. Run the command `RAW`
17. Run the command `system_password_reset`

Example:

```
All configuration is done with WebAdmin. Go to https://192.168.2.1:4444
in your browser.

192.168.2.1
login: root
Password:


Sophos UTM
(C) Copyright 2000-2020 Sophos Limited and others. All rights reserved.
Sophos is a registered trademark of Sophos Limited and Sophos Group.
All other product and company names mentioned are trademarks or registered
trademarks of their respective owners.

For more copyright information look at /doc/astaro-license.txt
or http://www.astaro.com/doc/astaro-license.txt

NOTE: If not explicitly approved by Sophos support, any modifications
      done by root will void your support.

noahutm:/root # cc
Confd command-line client.  Maintainer: <Ingo.Schwarze@sophos.com>

Connected to 127.0.0.1:4472, SID = WvawGQNaMXQiBaIHFAdl.
Available modes: MAIN OBJS RAW WIZARD.
Type mode name to switch mode.
Typing 'help' will always give some help.
127.0.0.1 MAIN > RAW
Switched to RAW mode.
127.0.0.1 RAW > system_password_reset
Calling Confd function system_password_reset()
result: 1
127.0.0.1 RAW > _
```

18. Ensure your computer:
    - is connected to Sophos UTM's local area network (LAN) port.
    - is on the same LAN as that of Sophos UTM.
    - has the Sophos UTM's IP address configured as its gateway.

19. Open a browser on your computer and connect to your Sophos UTM via `https://IP address:4444`

    Example: `https://192.168.2.1:4444`

20. Enter a new password for the account `admin` and click **Apply**.

Note:
If resetting the password fails on Sophos UTM appliances that are online and in high availability (HA) setup, power off the secondary appliance and reset the password of the primary appliance. Once successful with the password reset, power on the other appliance to sync the updated passwords.

RESET THE WEBADMİN PASSWORD

Follow the steps here if you cannot sign in to WebAdmin using the account `admin` but you know the password for the account `root`.

1. Access Sophos UTM via the following:
   - Connect a monitor and keyboard and sign in using the account `root`.
   - Connect a computer to Sophos UTM via a serial cable and use a terminal emulator application such as PuTTY and configure it to connect to `COM1` with a baud rate of `38400`. For more information, see Sophos UTM: Access the UTM shell via SSH using PuTTY.

2. Sign in via the following:
   - CLI: Use the account `root`
   - PuTTY: Use the account `loginuser` then run the command `su` to go to the account `root`

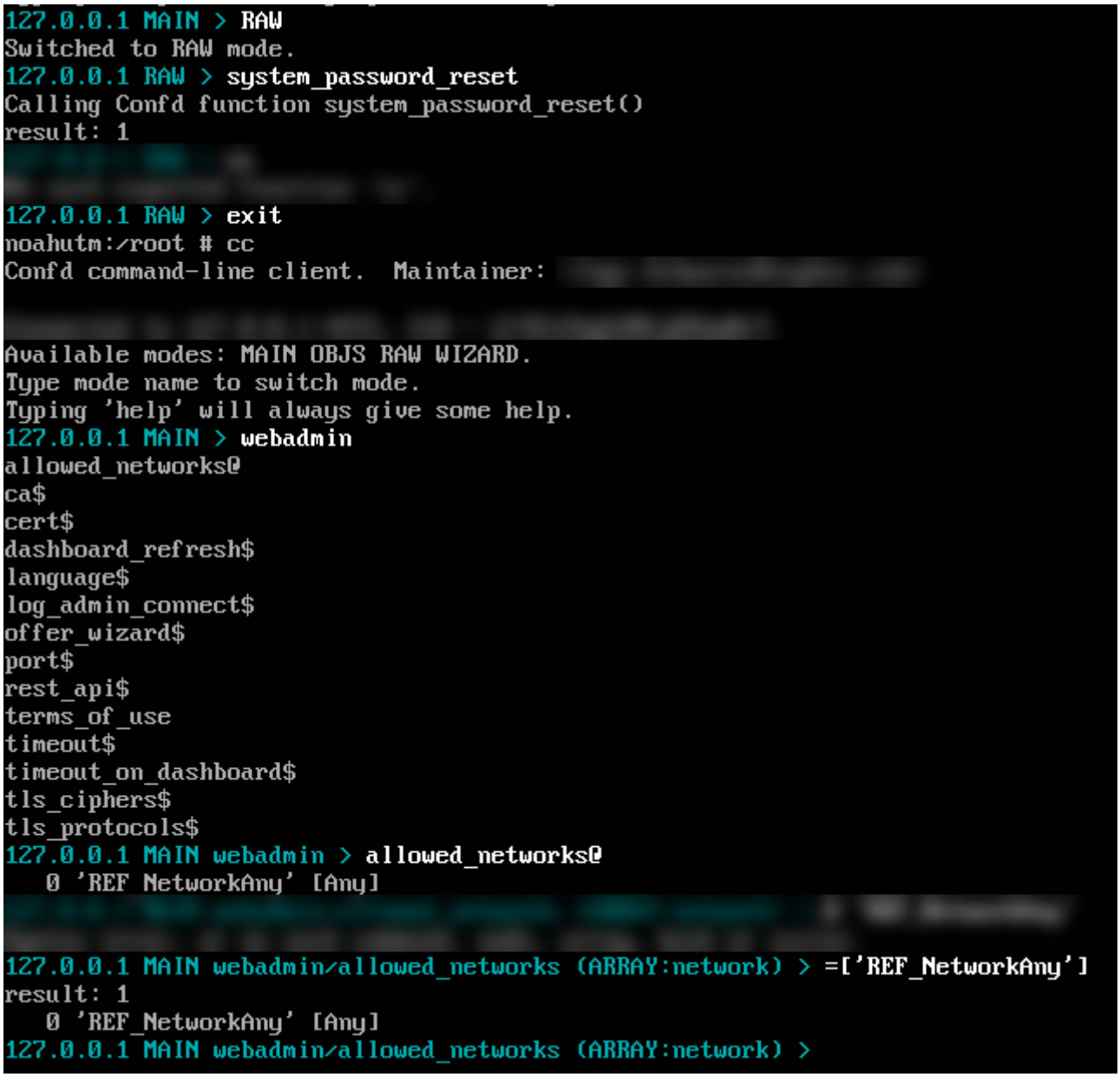
3. Follow step 15 onwards of the section Reset the loginuser and root passwords via CLI.

Note: This procedure will also reset the `loginuser` and `root` SSH passwords. Do either of the following to enter new passwords:

- Go to **Management** > **System Settings** > **Shell Access** > **Shell user passwords**
- Run the commands `passwd loginuser` and `passwd root` on the console, while signed in as `root`

If you cannot access the WebAdmin sign-in page, the allowed networks may have changed. Run the following commands and press **Enter** to fix the access:

1. `cc`
2. `webadmin`
3. `allowed_networks@`
4. `=['REF_NetworkAny']`



Kaynak: https://support.sophos.com/support/s/article/KB-000034260?language=en_US

Revision #2
Created 29 April 2024 21:39:56 by Teletek
Updated 19 July 2024 01:43:02 by Teletek