

Password Recovery Procedure for the CNS Configuration Registrar

Document ID: 28960

Introduction

Prerequisites

Requirements

Conventions

Step-by-Step Procedure

Versions Prior to 1.2

Version 1.2

Version 1.3 and Later

Related Information

Introduction

This document describes how to recover a password on a CNS Configuration Registrar.

Prerequisites

Requirements

To perform this procedure you must:

- be connected to the IE 2100 appliance through the serial port (console).
- determine a strong password, that cannot be easily guessed.

Conventions

For more information on document conventions, refer to Cisco Technical Tips Conventions.

Step-by-Step Procedure

Versions Prior to 1.2

This procedure is only valid for appliances running earlier versions of the software. It requires that you first clear the password and enter a new one later.

1. Reboot the appliance. At boot time (on the console), you see a message instructing you to press **Esc** for a menu. The following menu appears:

```
Current Boot Device: SCSI Hard Disk
1-Change boot order to Bootflash
2-Exit without saving changes
3-Save changes and exit
```

2. Press **1** and configure the system to boot from the bootflash. Then, press **3** to boot it from the bootflash.
3. Once the machine is rebooted, you are running a tiny Linux system (as root), based in memory. You must mount the partition that contains the **/etc** directory (in this example the partition is the 11th on

the first SCSI disk, but it may vary between versions):

```
[root@CiscoMaintImage /]# mount -t ext2 /dev/sdall /mnt
```

4. Once the partition is mounted, you must edit the file **/mnt/etc/shadow** to give the root no password. Using a file editor, edit the file and remove the second field in the line corresponding to the root account (if you are not familiar with an editor, ask your local UNIX administrator for help).

Change:

```
root:$1$uukl7Gto$XHk5c42C6EH6Qn.0dBJFA1:12229:0:99999:7:-1:-1:134539580
```

To:

```
root::12229:0:99999:7:-1:-1:134539580
```

Note: The second field in the shadow file contains an encrypted password. The value of this field may be different between two identical systems. Removing this field makes sure that there is no password configured for the root account.

5. Next, unmount the disk, as follows:

```
[root@CiscoMaintImage /]# unmount /mnt
```

This assures that the changes are saved to the disk.

6. Reload the appliance by typing **reboot** or by pressing the **reset** button, and let the appliance boot normally.
7. When you are prompted for a user name, type **root**.
8. When prompted for the password, press **Enter**.
9. Once logged into the system, set a new strong password for the root to prevent unauthorized access. This can be done through the command **passwd** at the shell prompt:

```
sh-2.04# passwd
New UNIX password:
Retype new UNIX password:
passwd: all authentication tokens updated successfully
sh-2.04#
```

Version 1.2

The example shown here is password recovery on a IE 2100 version 1.2.

1. First, reboot the appliance. The console port displays messages stating that the system is shutting down. Once the appliance restarts, you get the boot prompt:

```
LILO
boot:
```

2. Press the **Tab** key, and you see a list of all the images that are installed on the machine (usually, there is only one image installed). For the purposes of this document, assume that one of the images is called *ie2100*.
3. Boot the appliance in single user mode by typing the following at the prompt:

```
ie2100 single
```

The IE 2100 will boot in single user mode, and after the system initialization, you get a root prompt, without having to type in a username or password:

```
[... sys init messages ...]
```

```
Turning on user and group quotas for local filesystems: [ OK ]
Enabling swap space: [ OK ]
sh-2.04#
```

4. At this prompt, type the command **passwd** and enter the new (strong) password for the root user:

```
sh-2.04# passwd
New UNIX password:
Retype new UNIX password:
passwd: all authentication tokens updated successfully
sh-2.04#
```

5. Once you change the password, type **reboot**.
6. When prompted for a name, type **root**.
7. When prompted for the password, type the new password.

Version 1.3 and Later

The example shown here is password recovery on a IE 2100 version 1.3 and later.

1. Reboot the appliance. The system shuts down, and restarts. Once the appliance restarts, you should see the following screen:

```
GRUB version 0.91 (631K lower / 1047472K upper memory)

+-----+
| Red Hat Linux (2.4.18-17.7.x) |
+-----+

Use the ^ and v keys to select which entry is highlighted.
Press enter to boot the selected OS, 'e' to edit the
commands before booting, 'a' to modify the kernel arguments
before booting, or 'c' for a command-line.

The highlighted entry will be booted automatically in 9 seconds.  H■
```

2. Press the key **e** to edit the boot parameters. The following screen is displayed:

GRUB version 0.91 (631K lower / 1047472K upper memory)

```
+-----+
| root (hd0,0)                                     |
| kernel /vmlinuz-2.4.18-17.7.x ro root=/dev/sda7 console=ttyS0,9600n8 |
| initrd /initrd-2.4.18-17.7.x.img               |
+-----+

Use the ^ and v keys to select which entry is highlighted.
Press 'b' to boot, 'e' to edit the selected command in the
boot sequence, 'c' for a command-line, 'o' to open a new line
after ('O' for before) the selected line, 'd' to remove the
selected line, or escape to go back to the main menu.
The highlighted entry will be booted automatically in 2 seconds.  H■
```

3. Using the arrows, select the entry **kernel /vmlinuz-2.4.18-17.7.x ro root=/dev/sda7 console=ttyS0,9600n8**.
4. Press the key **e** to enter the editor.
5. Go to the end of the line, and add **single** after the parameter **console=ttyS0,9600n8**:

```
kernel /vmlinuz-2.4.18-17.7.x ro root=/dev/sda7 console=ttyS0,9600n8 single
```

6. Press **Enter** once you have added the parameter **single** (you may not see this parameter added to the previous screen due to screen size).

Note: This parameter tells the kernel to start in single user mode.

7. Press **b** to boot in single user mode. After the system initialization, you see a root prompt, without having to type in a username or password:

```
[... sys init messages ...]
Turning on user and group quotas for local filesystems: [ OK ]
Enabling swap space: [ OK ]
sh-2.04#
```

8. At this prompt, type the command **passwd** and enter the new (strong) password for the root user:

```
sh-2.04# passwd
New UNIX password:
Retype new UNIX password:
passwd: all authentication tokens updated successfully
sh-2.04#
```

9. Once you change the password, type **reboot**, and let the machine boot normally.
10. When prompted for a name, type **root**.
11. When prompted for the password, type the new password.

Related Information

- [Cisco CNS Configuration Engine Documentation](#)
 - [Technical Support – Cisco Systems](#)
-

