

Password Recovery Procedure for the Cisco NAC Appliance (Cisco Clean Access)

Document ID: 71159

Contents

Introduction

Prerequisites

- Requirements

- Conventions

Step-by-Step Procedures

- NAC Appliance Version 3.5.x and Earlier

- NAC Appliance Version 3.6.x and Later

CAM WEB GUI Password Recovery

- Create a New User

- Delete the Admin Account

Related Information

Introduction

This document describes how to recover a password on a Cisco Clean Access Manager (CAM) and Cisco Clean Access Server (CAS).

Prerequisites

Requirements

There are no specific requirements for this document.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Step-by-Step Procedures

The Cisco Network Admission Control (NAC) Appliance contains these built-in administrative user account passwords:

- Clean Access Manager installation machine root user
- Clean Access Server installation machine root user
- Clean Access Server web console admin user
- Clean Access Manager web console admin user

The first three passwords are initially set at installation time (the default password is cisco123). In order to change these passwords at a later time, access the Clean Access Manager or Clean Access Server machine by SSH and log in as the user whose password you want to change. Use the Linux **passwd** command in order to change the user password. In order to recover the root password for the Clean Access Manager/Clean Access Server, you can use the Linux procedure to boot to single user mode and change the root password.

NAC Appliance version 3.5.x and earlier used LILO as the boot loader. Version 3.6.x and later uses GRUB as the boot loader and hence the password recovery procedure is different. These are the two different procedures.

- NAC Appliance Version 3.5.x and Earlier
- NAC Appliance Version 3.6.x and Later

NAC Appliance Version 3.5.x and Earlier

Complete these steps:

1. Connect to the CAM/CAS machine via console.
2. Power-cycle the machine in order to display GUI mode.
3. Press **Ctrl-x** in order to switch to text mode. This displays a **boot :** prompt.
4. At the prompt type **linux single** in order to boot the machine into single user mode.
5. Type **passwd** and press **Enter**.
6. Change the root password and reboot the machine using the **reboot** command.

Note: It is important to provide secure passwords for the user accounts in the Cisco NAC Appliance system, and to change them from time to time in order to maintain system security. The suite does not generally impose standards for the passwords you choose, but it is advised that you use strong passwords. That is, passwords with at least six characters, mixed letters and numbers, and so on. Strong passwords reduce the likelihood of a successful password guessing attack against your system.

NAC Appliance Version 3.6.x and Later

Complete these steps:

1. Power up the machine, the NAC Appliance, or server.
2. Press any key when the boot loader screen appears with the "Press any key to enter the menu&" message in order to enter the GRUB menu.

The GRUB menu appears with one item in the list:

- ◆ Cisco Clean Access (2.6.11-perfigo)

3. Press **e** in order to edit.

These multiple choices appear:

```
root (hd0,0)
kernel /vmlinuz-2.6.11-perfigo ro root=LABEL=/ console=tty0 console=ttyS0,9600n8
Initrd /initrd-2.6.11-perfigo.img
```

4. Scroll to the second entry (the line that starts with **kernel**&) and press **e** in order to edit the line.
5. Delete **console=ttyS0,9600n8**, add the word **single** to the end of the line, and then press **Enter**.

The line appears similar to this example:

```
kernel /vmlinuz-2.6.11-perfigo ro root=LABEL=/ console=tty0 single
```

6. Press **b** in order to boot the machine in single user mode.

You are presented with a root shell prompt after boot-up.

Note: You are not prompted for a password.

7. At the prompt type **passwd**, press **Enter**, and follow the instructions.

8. After the password is changed, enter **reboot** in order to reboot the box.

CAM WEB GUI Password Recovery

Create a New User

There is no standard procedure to recover the admin password. The only procedure available is for the CLI ROOT password.

1. Connect to the CLI and issue these commands:

```
[root@cca-3390-cam ~]# psql -h 127.0.0.1 controlsmartdb -U postgres
controlsmartdb=# select * from admin_account;
```

You should now see a list of users, similar to this:

id	name	password	group_name	enable	admin_desc
0	admin	96208ed2256706e8d8b29c1bf58d10c4a07267b4c1	Full-Control Admin	1	Primary admin account
1	localadmin	b0f3e23dcd1046d1dbf4e095186d5cb54e47963690	GuestLobby	1	only local users
2	admin1	96208ed225670d688bs29c1bf58d10c4a07267b4c1	Full-Control Admin	1	admin test user

(3 rows)

2. You need to see the highest id value and increment it (in this example, the new value is 3).
3. Insert the new user with the command:

```
insert into admin_account(id, name, password, group_name, enable)
values ('3', 'recover', 'cisco123', 'Full-Control Admin', '1');
```

4. Verify if the recover user is in the DB:

```
controlsmartdb=# select * from
admin_account;
      id |      name      |      password      |      group_name      | enable |
      admin_desc
-----+-----+-----+-----+-----+-----
      0 | admin          | 96208ed225670688b29c1bf58d10c4a07267b4c1 | Full-Control Admin |      1 | Primary admin account
      1 | localadmin     | b0f3e23dcd10461db4e095186d5cb54e47963690 | GuestLobby         |      1 | only local users
      2 | admin1         | 96208ed225670688b29c1bf58d10c4a07267b4c1 | Full-Control Admin |      1 | admin test user
      3 | recover        | cisco123           | Full-Control Admin |      1 |
(4 rows)
```

5. Login to the GUI with this new user.

Delete the Admin Account

Use the SQL command to delete the admin user.

1. Enter the SQL command line:

```
[root@cca-3390-cam ~]# psql -h 127.0.0.1 controlsmartdb -U postgres
```

2. Delete the admin user (id=0).

```
controlsmartdb=# delete from admin_account where id='0';
```

3. Verify that id 0 was deleted.

```

controlsmartdb=# select * from admin_account;
 id |      name      |      password      |
group_name | enable |      admin_desc
-----+-----+-----+
  1 | localadmin | b0f3e23dcd10461db4e095186d5cb54e47963690 |
GuestLobby |      1 | only local users
  2 | admin1 | 96208ed225670688b29c1bf58d10c4a07267b4c1 |
Full-Control Admin |      1 | admin test user
  3 | recover | 96208ed225670688b29c1bf58d10c4a07267b4c1 |
Full-Control Admin |      1 |
(3 rows

```

4. You can now create a new 'admin' user on id '0'.

```

controlsmartdb=# insert into
admin_account(id,name,password,group_name,enable) values('0', 'admin',
'cisco123', 'Full-Control Admin', 1);
INSERT 0 1
controlsmartdb=# select * from admin_account
controlsmartdb=# ;

```

id	name	password	group_name	enable	admin_desc
1	localadmin	b0f3e23dcd10461db4e095186d5cb54e47963690	GuestLobby	1	only local users
2	admin1	96208ed225670688b29c1bf58d10c4a07267b4c1	Full-Control Admin	1	admin test user
3	recover	96208ed225670688b29c1bf58d10c4a07267b4c1	Full-Control Admin	1	
0	admin	cisco123	Full-Control Admin	1	

```

(4 rows)

```

5. Verify if the new user is in the DB.

Related Information

- Cisco NAC Appliance Product Documentation
- Technical Support & Documentation – Cisco Systems