# Procedimiento para recuperación de contraseña para el dispositivo NAC de Cisco (acceso limpio de Cisco)

## Contenido



## Introducción

Este documento describe cómo recuperar una contraseña en Cisco Clean Access Manager (CAM) y Cisco Clean Access Server (CAS).

## prerrequisitos

### Requisitos

No hay requisitos específicos para este documento.

### Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

## Procedimientos paso a paso

El dispositivo del Cisco Network Admission Control (NAC) contiene estas contraseñas de la cuenta incorporadas del usuario administrador:

- Limpie al usuario raíz de la máquina de la instalación del Access Manager

- Limpie al usuario raíz de la máquina de la instalación del servidor de acceso
- Limpie al Usuario administrador de la consola Web del servidor de acceso
- Limpie al Usuario administrador de la consola Web del Access Manager

Las primeras tres contraseñas se fijan inicialmente en el momento de la instalación (la contraseña predeterminada es cisco123). Para cambiar estas contraseñas en otro momento, acceda el Access Manager limpio o la máquina limpia del servidor de acceso por SSH y inicie sesión como el usuario cuya contraseña usted quiere cambiar. Utilice el **comando passwd de** Linux para cambiar la contraseña del usuario. Para recuperar la contraseña de raíz para el Access Manager limpio/el servidor de acceso limpio, usted puede utilizar el procedimiento de Linux para iniciar al modo de usuario único y para cambiar la contraseña de raíz.

LILO usado versión 3.5.x y anterior del dispositivo NAC como el cargador de arranque. Las aplicaciones de la versión 3.6.x y posterior CAVAN pues el cargador de arranque y por lo tanto el procedimiento para recuperación de contraseña es diferente. Éstos son los dos diversos procedimientos.



## Versión 3.5.x y anterior del dispositivo NAC

Complete estos pasos:

1. Conecte con la máquina CAM/CAS vía la consola.
2. Ciclo de la potencia la máquina para visualizar al modo GUI.
3. Presione el **Ctrl-x** para conmutar al Modo de texto. Esto visualiza un `inicio:` mensaje
4. En el **linux del** tipo de prompt **solo** para iniciar la máquina en el modo de usuario único.
5. **Passwd** y Presione ENTER del tipo.
6. Cambie la contraseña de raíz y reinicie la máquina usando el **comando reboot**.**Note**: Es importante proporcionar las contraseñas seguras para las cuentas de usuario en el sistema del dispositivo NAC de Cisco, y cambiarlas de vez en cuando para mantener la seguridad del sistema. La habitación no impone generalmente los estándares para las contraseñas que usted elige, pero se aconseja que usted utiliza las contraseñas fuertes. Es decir, contraseñas con por lo menos seis caracteres, cartas mezcladas y números, y así sucesivamente. Las contraseñas fuertes reducen la probabilidad de una contraseña acertada que conjetura el ataque contra su sistema.

## Versión 3.6.x y posterior del dispositivo NAC

Complete estos pasos:

1. Accione para arriba la máquina, el dispositivo NAC, o el servidor.
2. Pulse cualquier tecla cuando la pantalla del cargador de arranque aparece con la “prensa cualquier clave para ingresar el menú…” mensaje para ingresar el menú de la COMIDA.El menú de la COMIDA aparece con un elemento en la lista:Acceso limpio de Cisco (2.6.11-perfigo)
3. Presione **e** para editar.Estas opciones múltiples aparecen:

```
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. Navegue a la segunda entrada (la línea que comienza con el `corazón…`) y prensa **e** para editar la línea.
5. Borre **console=ttyS0,9600n8**, agregue la palabra **sola** al final de la línea, y entonces el Presione ENTER.La línea aparece similar a este ejemplo:
   `kernel /vmlinuz-2.6.11-perfigo ro root=LABEL=/ console=tty0 single`
6. Presione **b** para iniciar la máquina en el modo de usuario único.Le presentan con un prompt del shell raíz después del arranque inicial.**Note**: Le no indican para una contraseña.
7. En el **passwd del** tipo de prompt, el Presione ENTER, y sigue las instrucciones.
8. Después de que se cambie la contraseña, ingrese la **reinicialización** para reiniciar el rectángulo.

# Recuperación de contraseña de la RED GUI CAM

## Cree a un usuario nuevo

No hay procedimiento estándar para recuperar la clave del administrador. El único procedimiento disponible está para la contraseña de raíz CLI.

1. Conecte con el CLI y publique estos comandos:
   ```
   [root@cca-3390-cam ~]#  psql -h 127.0.0.1 controlsmartdb -U postgres
   controlsmartdb=# select * from admin_account;
   ```
   Usted debe ahora ver una lista de usuarios, similar a esto:
   ```
   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. Usted necesita ver el valor del ID identificación y incrementarlo (en este ejemplo, el nuevo valor es 3).
3. Inserte al usuario nuevo con el comando:
   ```
   insert into admin_account(id, name, password, group_name, enable)
   values ('3', 'recover', 'cisco123', 'Full-Control Admin', '1');
   ```
4. Verifique si el usuario de la recuperación está en el 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. Inicie sesión al GUI con este usuario nuevo.

## Borre la cuenta de administración

Utilice el comando sql de borrar al Usuario administrador.

1. Ingrese la línea de comando sql:
```
[root@cca-3390-cam ~]#  psql -h 127.0.0.1 controlsmartdb -U postgres
```
2. Borre al Usuario administrador (id=0).
```
controlsmartdb=# delete from admin_account where id='0';
DELETE 1
```
3. Verifique que la identificación 0 fuera borrada.
```
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. Usted puede ahora crear a un nuevo usuario “admin” el '0' identificación.
```
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. Verifique si el usuario nuevo está en el DB.

# Información Relacionada

- Documentación del Producto del dispositivo NAC de Cisco
- Soporte Técnico y Documentación - Cisco Systems