

mod05_ex02: Setting Policies for IPA

The purpose of this exercise is to strengthen FreeIPA's password policies and set a rule for sudo access with no password for members of the group admins. You will make changes to the FreeIPA password policy using both the web UI and the command line. This exercise uses a shared account, support, which is a security risk. This will be used during a later exercise.

Reference Information

The following documents provide information related to this exercise.

- See password policy attribute descriptions in the “Supported Password Policy Attributes” section of the [Linux Domain Identity, Authentication, and Policy Guide](#).
- [systemd unit files](#) (mirrors official RHEL and CentOS documentation on creating custom unit files)

1. Login into FreeIPA as the security administrator, sam_sec.

```

Mate Terminal
File Edit View Search Terminal Help
[sam_sec@cmhost ~]$ ipa sudorule-add admins_sudo --hostcat=all --runasusercat=all
l --runasgroupcat=all --cmdcat=all
-----
Added Sudo Rule "admins_sudo"
-----
Rule name: admins_sudo
Enabled: TRUE
Host category: all
Command category: all
RunAs User category: all
RunAs Group category: all
[sam_sec@cmhost ~]$ █

```

1.1 On the Firefox browser bookmark toolbar select Identity Management. Login with the security administrative user, sam_sec, and password <password>. Click Login or press Enter.

Username *

Password *

[Login Using Certificate](#) [Sync OTP Token](#) [Login](#)

2. Test current password policies.

2.1 Review the Active users on the Identity tab. All of these users, except support, use <password> to log in.

Identity	Policy	Authentication	Network Services	IPA Server
Users	Hosts	Services	Groups	ID Views Automember
User categories				
Active users				
Stage users				
Preserved users				

Active users						
	User login	First name	Last name	Status	UID	Email address
<input type="checkbox"/>	admin		Administrator	✓ Enabled	1780600000	
<input type="checkbox"/>	allan_admin	Allan	Adm	✓ Enabled	1780600001	allan_admin@example.com
<input type="checkbox"/>	bo_biz	Bo	Biz	✓ Enabled	1780600003	bo_biz@example.com
<input type="checkbox"/>	dana_dev	Dana	Dev	✓ Enabled	1780600004	dana_dev@example.com
<input type="checkbox"/>	denis_deng	Denis	Deng	✓ Enabled	1780600005	denis_deng@example.com
<input type="checkbox"/>	fina_fin	Fina	Fin	✓ Enabled	1780600006	fina_fin@example.com
<input type="checkbox"/>	grace_gov	Grace	Gov	✓ Enabled	1780600007	grace_gov@example.com
<input type="checkbox"/>	hamal_hr	Hamal	Hr	✓ Enabled	1780600008	hamal_hr@example.com
<input type="checkbox"/>	omar_ops	Omar	Ops	✓ Enabled	1780600009	omar_ops@example.com
<input type="checkbox"/>	steff_sci	Steff	Sci	✓ Enabled	1780600010	steff_sci@example.com
<input type="checkbox"/>	support	Shared	Admin_acct	✓ Enabled	1780600011	support@example.com

Showing 1 to 11 of 11 entries.

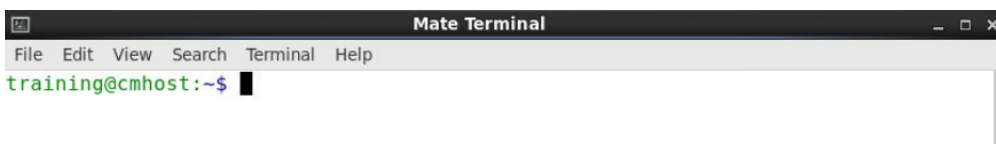
2.2 Select the user support. Review the properties page.

The screenshot shows the IPA web interface for the user 'support'. The top navigation bar includes 'Identity', 'Policy', 'Authentication', 'Network Services', and 'IPA Server'. Below this, a breadcrumb trail shows 'Active users > support'. The user 'support' is selected, and the 'Settings' tab is active. The 'Identity Settings' section includes fields for Job Title (Support account), First name (Shared), Last name (Admin_acct), Full name (Shared Admin_acct), Display name (Shared Admin_acct), Initials (SA), GECOS (Shared Admin_acct), and Class. The 'Account Settings' section includes fields for User login (support), Password (masked with asterisks), Password expiration (2021-12-04 17:42:00Z), UID (1780600011), GID (1780600011), Principal alias (support@EXAMPLE.COM), Kerberos principal expiration (YYYY-MM-DD), and Login shell (/bin/bash).

2.3 Select Actions > Reset Password. Reset the password to 'letmein'. Click Reset Password.

The screenshot shows the 'Reset Password' dialog box. It has two input fields: 'New Password' and 'Verify Password', both containing masked text (asterisks). Below the fields are 'Reset Password' and 'Cancel' buttons.

2.4 On the remote desktop in workspace 1 open a Mate terminal.



2.5 Use the su command to become the user support with password 'letmein'. Change the password to letmein. The password will not be displayed as you type. This demonstrates a number of security risks. The password is too short, the password does not contain any special characters, the password will be easy to guess, and the user was not required to change the password.



```
$ su - support
```

3. Using the IPA web UI to change password policy.

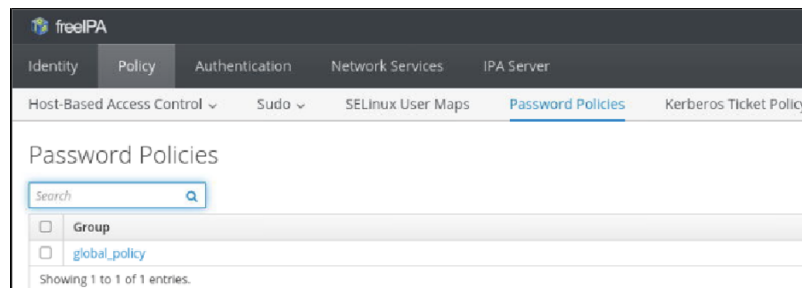
As the previous example demonstrates the FreeIPA server begins with a weak password policy. You will modify the global password policy on the FreeIPA server to improve password security.

Password policies are controlled by classes. A class could set a requirement for the length of the password, or the number of capital letters required in the password. There are six classes:

- Upper-case characters
- Lower-case characters
- Digits
- Special characters (for example, punctuation)
- 8-bit characters (characters whose decimal code starts at 128 or below)
- Number of repeated characters

You can also set the required number of classes to be applied to a password. Setting a value to 3 requires a password to have characters from at least three classes. The default value is zero (0), meaning there are no required classes.

3.1 Return to workspace 2. Return to the Firefox browser. Return to IPA. Select Policy. Select Password Policies.



3.2 Select global_policy. This contains the default password settings for all users.

Password Policy: global_policy

Settings

Refresh

Revert

Save

Password Policy

Group	global_policy
Max lifetime (days)	<input type="text" value="9999"/>
Min lifetime (hours)	<input type="text" value="1"/>
History size (number of passwords)	<input type="text" value="0"/>
Character classes	<input type="text" value="0"/>
Min length	<input type="text" value="7"/>
Max failures	<input type="text" value="200"/>
Failure reset interval (seconds)	<input type="text" value="60"/>
Lockout duration (seconds)	<input type="text" value="600"/>

Note: For this exercise environment **Max failures** was changed from the default of 6 to 200. In a later exercise this will allow the hacking tool ncrack enough attempts during penetration testing to correctly guess the password letmein.

See descriptions of all password policy in “Supported Password Policy Attributes” section of the [Linux Domain Identity, Authentication, and Policy Guide](#).

3.3 In the Max lifetime (days) field, enter 90 (ninety). The Max lifetime (days) is changed to force a password reset every 90 days.

3.4 In the Min lifetime (hours) field, enter 0 (zero). The Min lifetime (hours) is changed to allow for multiple password changes in a short period of time.

3.5 In the Character classes field, enter 4. This will require four password classes each time a password is changed.

3.6 In the Min length field, enter 12. For this exercise environment, the Min length was changed from the default value of 8 to 7. This allows the user support password of letmein.

3.7 Validate the policy settings. Click Save.

Password Policy: global_policy

Settings
Refresh
Revert
Save

Password Policy

Group	global_policy
Max lifetime (days)	90 Undo
Min lifetime (hours)	0 Undo
History size (number of passwords)	0
Character classes	4 Undo
Min length	12 Undo
Max failures	200
Failure reset interval (seconds)	60
Lockout duration (seconds)	600

3.8 Return to the Mate terminal where you are logged in as the user support. Use the `passwd` command to change the password for support. First attempt a password of 'changeme', which will fail. After your attempts are rejected, changing the password to `BadPassWord@1`, which does conform to the new rules. The password characters are shown here but they will not be displayed on your screen.

```
$ passwd
Current Password: letmein
New password: changeme
Retype new password: changeme
Password change failed. Server message: Password is too short
Password not changed.
passwd: Authentication token manipulation error
```

```
$ passwd
```

3.9 Exit from the user support.

```
$ exit
```

4. Using the IPA command line interface to change password policy.

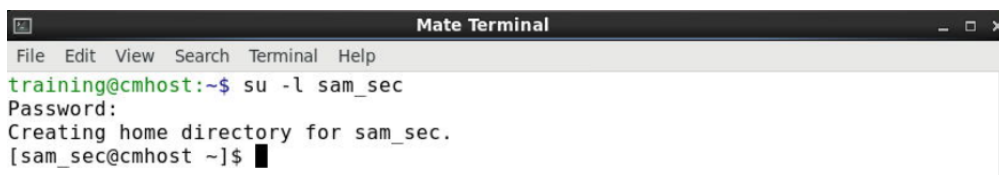
4.1 Setting Password Aging Policy.

You can use the ipa command line to check and to make changes to password policy. The ipa command must be run as the IPA admin user.

LDAP sets a password lifetime to enforce password aging. Use the ipa command to change password lifetime.

Note: For local Linux accounts, this is set per user and there is no global setting. The *chage* command is used to set policy for local users. See *man chage* to view options for this command.

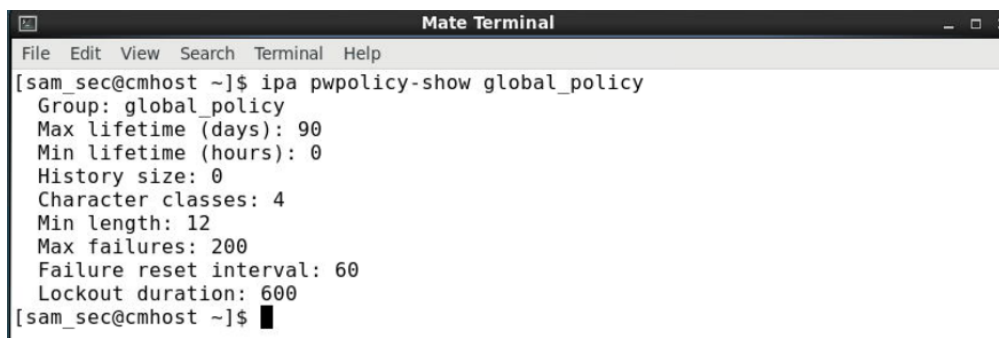
4.2 In a Mate terminal change to security administrative user, sam_sec, with password <password>.



```
Mate Terminal
File Edit View Search Terminal Help
training@cmhost:~$ su -l sam_sec
Password:
Creating home directory for sam_sec.
[sam_sec@cmhost ~]$
```

```
$ su -l sam_sec
```

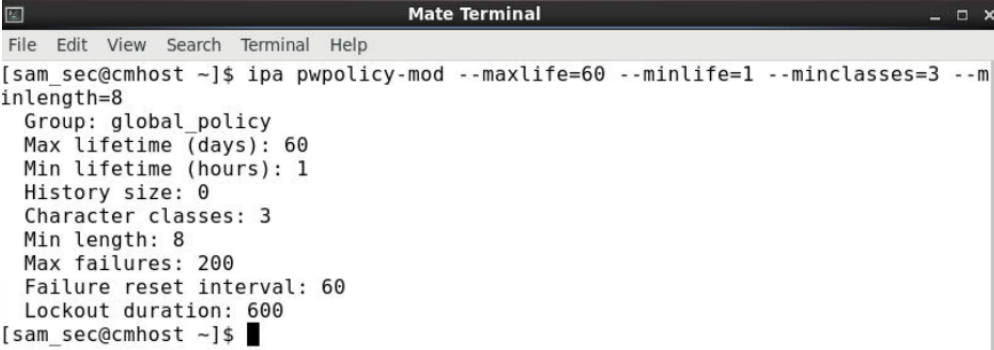
4.3 List the global policy.



```
Mate Terminal
File Edit View Search Terminal Help
[sam_sec@cmhost ~]$ ipa pwpolicy-show global_policy
Group: global_policy
Max lifetime (days): 90
Min lifetime (hours): 0
History size: 0
Character classes: 4
Min length: 12
Max failures: 200
Failure reset interval: 60
Lockout duration: 600
[sam_sec@cmhost ~]$
```

```
$ ipa pwpolicy-show global_policy
```

4.4 Change the Min lifetime to 1 hour and the Character Classes to require 3 classes. We will leave the Max lifetime at 90 days. Set the min length to the default of 8 to allow the exercise environment to use <password>. If a policy group is not specified, the global_policy is the default. Exit from the user admin.



```
[sam_sec@cmhost ~]$ ipa pwpolicy-mod --maxlife=60 --minlife=1 --minclasses=3 --minlength=8
Group: global_policy
Max lifetime (days): 60
Min lifetime (hours): 1
History size: 0
Character classes: 3
Min length: 8
Max failures: 200
Failure reset interval: 60
Lockout duration: 600
[sam_sec@cmhost ~]$
```

```
$ ipa pwpolicy-mod --maxlife=60 --minlife=1 --minclasses=3 --minlength=8
```

With FreeIPA, the **global_policy** affects all users unless other policies have been configured for user groups.

Note: For local Linux users, you can adjust the defaults to be used when creating a new user by editing the `/etc/login.defs` file. See `man login.defs` for details on available settings. Settings in `login.defs` only affects user settings as a local user is being created. All local user changes post-creation is done with `chage`.

4.5 Return to the Firefox browser. Refresh the page. Review the change to the global_password policy.

Password Policy: global_policy

Settings

Refresh Revert Save

Password Policy

Group	global_policy
Max lifetime (days)	60
Min lifetime (hours)	1
History size (number of passwords)	0
Character classes	3
Min length	8
Max failures	200
Failure reset interval (seconds)	60

4.6 When changing passwords, it is important to determine the source of the user. The user will either be stored on the local host `/etc/passwd` file or the user will be stored in the LDAP database. The user training is local on each host. The user training is stored in `/etc/passwd` and the password is stored in `/etc/shadow`. When the user training uses the `passwd` command to change the password the change is made to the local host `/etc/shadow` file, not to the LDAP database. The user support is sourced from the LDAP database. The user support is not found in the local host `/etc/passwd` file. When the user support uses the `passwd` command to change the password the change is made to the LDAP database. Because the user support is configured in the LDAP database, the `passwd` command will apply the password policy defined in FreeIPA.

See the [ldappasswd man page](#) for details.

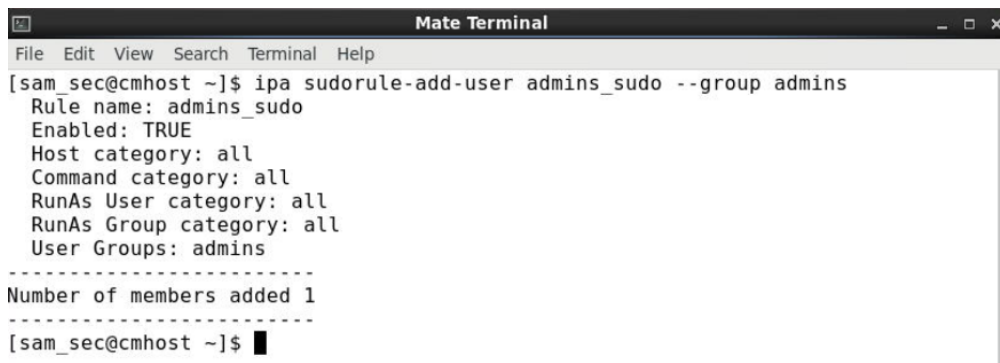
5. Using IPA command line interface to set sudo policy.

5.1 Create the sudo rule for `admins_sudo`. Grant access to all hosts, users, and groups for all commands.

```
[admin@ipa ~]$ ipa sudorule-add admins_sudo --hostcat=all --runasusercat=all
--runasgroupcat=all --cmdcat=all
```

```
$ ipa sudorule-add admins_sudo --hostcat=all --runasusercat=all --
runasgroupcat=all --cmdcat=all
```

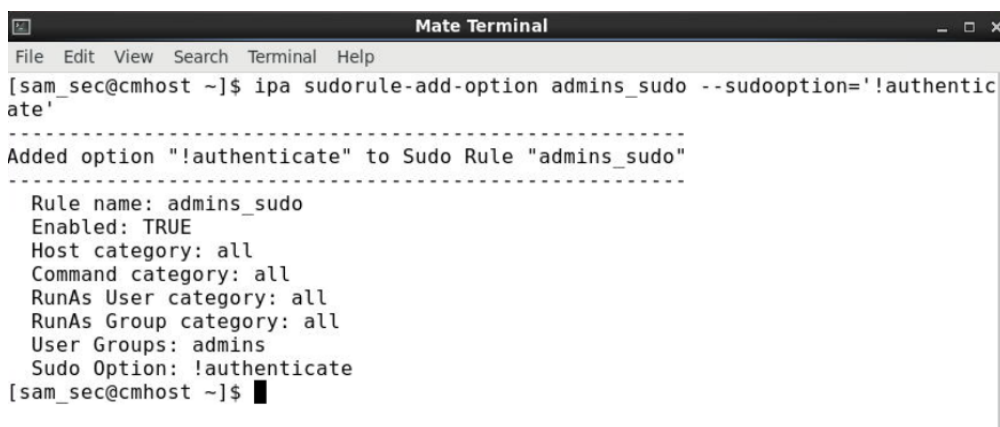
5.2 Add the group admins to the sudo rule.



```
Mate Terminal
File Edit View Search Terminal Help
[sam_sec@cmhost ~]$ ipa sudorule-add-user admins_sudo --group admins
Rule name: admins_sudo
Enabled: TRUE
Host category: all
Command category: all
RunAs User category: all
RunAs Group category: all
User Groups: admins
-----
Number of members added 1
-----
[sam_sec@cmhost ~]$
```

```
$ ipa sudorule-add-user admins_sudo --group admins
```

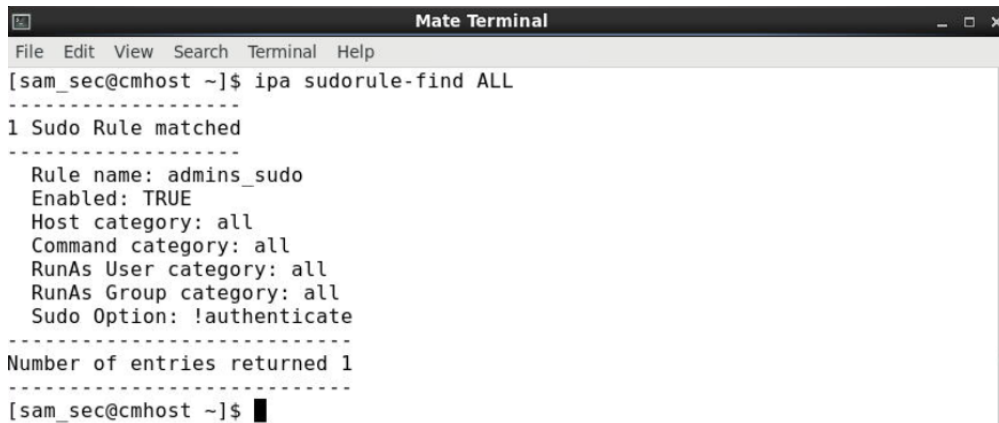
5.3 Add the option to sudo without a password.



```
Mate Terminal
File Edit View Search Terminal Help
[sam_sec@cmhost ~]$ ipa sudorule-add-option admins_sudo --sudoooption='!authenticate'
Added option "!authenticate" to Sudo Rule "admins_sudo"
-----
Rule name: admins_sudo
Enabled: TRUE
Host category: all
Command category: all
RunAs User category: all
RunAs Group category: all
User Groups: admins
Sudo Option: !authenticate
[sam_sec@cmhost ~]$
```

```
$ ipa sudorule-add-option admins_sudo --sudoooption='!authenticate'
```

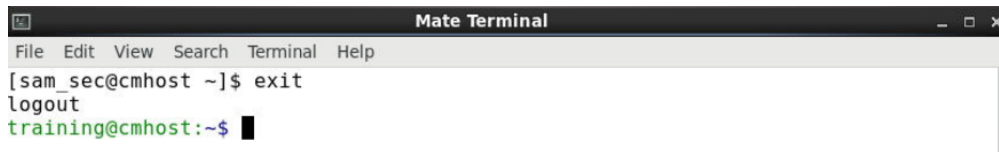
5.4 Validate the rule.



```
Mate Terminal
File Edit View Search Terminal Help
[sam_sec@cmhost ~]$ ipa sudorule-find ALL
-----
1 Sudo Rule matched
-----
Rule name: admins_sudo
Enabled: TRUE
Host category: all
Command category: all
RunAs User category: all
RunAs Group category: all
Sudo Option: !authenticate
-----
Number of entries returned 1
-----
[sam_sec@cmhost ~]$
```

```
$ ipa sudorule-find All
```

5.5 Exit from the security administrative user, sam_sec. Return to the local administrative user, training.



```
Mate Terminal
File Edit View Search Terminal Help
[sam_sec@cmhost ~]$ exit
logout
training@cmhost:~$
```

```
$ exit
```

5.6 The sssd service must be restarted for the rule to take affect. This restart of sssd would have to be done on every host.

```
training@cmhost:~$ sudo systemctl restart sssd
training@cmhost:~$
```

```
$ sudo systemctl restart sssd
```

5.7 Test sudo with no password for the administrative user, allan_admin.

```
training@cmhost:~$ su -l allan_admin
Password:
Last login: Sat Jan  1 13:32:37 PST 2022 on pts/0
[allan_admin@cmhost ~]$ sudo id
uid=0(root) gid=0(root) groups=0(root)
[allan_admin@cmhost ~]$ exit
logout
training@cmhost:~$
```

```
$ su -l allan_admin
Password: <password>
allan_admin$ sudo id
```

5.8 Type exit to logout of allan_admin. Return to the user training.



```
Mate Terminal
File Edit View Search Terminal Help
[allan_admin@cmhost ~]$ exit
logout
training@cmhost:~$
```

```
$ exit
```

6. Return to the Firefox browser.