User Management Commands

rbac authentication min-pwd-length

To configure the minimum length required for passwords of all users, use the **rbac authentication min-pwd-length** command in global configuration mode. To set the minimum password length to default value, use the no form of the command.

rbac authentication min-pwd-length *length*

Syntax Description

length	Specifies the minimum length. The minimum length must be between 7 to 128 characters.

Command Default

The default minimum length is 7 characters.

Command Modes

Global configuration (config)

Command History

Release	Modification
3.7.1	This command was introduced.

Usage Guidelines

Only the admin user can use this command.

Example

```
nfvis(config)# configure terminal
nfvis(config)# rbac authentication min-pwd-length 14
nfvis(config)# commit
nfvis(config)# end
```

rbac authentication password-lifetime

To configure the minimum and maximum lifetime values for passwords of all users and enforce a rule to check these values, the admin user can use the **rbac authentication password-lifetime** command in global configuration mode. To set the minimum password length to default value, use the no form of the command.

rbac authentication password-lifetime enforce { **true** | **false**} **min-days** *min-days* **max-days** *max-days*

Syntax Description

enforce	Enforces or removes the rule for password lifetime validation. Valid values for this parameter are **true** and **false**.
min-days *min-days*	Specifies the number of days after which the users can change the password.
max-days *max-days*	Specifies the number of days before which the users must change the password.

Command Default

The default minimum lifetime value is set to 1 day and the default maximum lifetime value is set to 60 days.

Command Modes

Global configuration (config)

Command History

Release	Modification
3.7.1	This command was introduced.

Usage Guidelines

- Only the admin user can use this command.
- The minimum and maximum lifetime values and the rule to check for these values are not applicable to the admin user.

Example

```
nfvis(config)# configure terminal
nfvis(config)# rbac authentication password-lifetime enforce true min-days 1 max-days 30
nfvis(config)# commit
nfvis(config)# end
```

rbac authentication account-inactivity

To configure the number of days after which an unused user account is marked as inactive and to enforce a rule to check the configured inactivity period, the admin user can use the **rbac authentication account-inactivity** command in global configuration mode.

rbac authentication account-inactivity enforce { **true** | **false**} **inactivity-days** *inactivity-days*

Syntax Description

enforce	Enforces or removes the rule for checking and mark-ing unused user accounts as inactive. Valid values for this parameter are **true** and **false**.
inactivity-days *inactivity-days*	Specifies the number of days after which an unused account is marked as inactive.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
3.7.1	This command was introduced.

Usage Guidelines

- Only the admin user can use this command.
- The inactivity period and the rule to check the inactivity period are not applicable to the admin user.
- When marked as inactive, a user cannot login to the system. To allow the user to again login to the system, the ad-min user must reactivate the user account by using the **rbac authentication users user** *username* **activate** command.

Example

```
nfvis(config)# configure terminal
nfvis(config)# rbac authentication account-inactivity enforce true inactivity-days 2
nfvis(config)# commit
nfvis(config)# end
```

rbac authentication users

To create a new user, use the **rbac authentication users** command in global configuration mode. To delete a user, use the **no** form of the command.

rbac authentication users user *user-name* **password** *password* **role** *role-type*
no rbac authentication users user *user-name* **password** *password* **role** *role-type*

Syntax Description

user *user-name*	Specifies the user name.
password *password*	Specifies the password.
role *role-type*	Specifies the role of the user. The role can be one fo the following: • Administrators—An administrator can perform all tasks. • Operators—An operator can start, stop, and delete a VM, clear logs, and view all information. • Auditors—An auditor can view all information, and cannot perform any tasks.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
3.5.1	This command was introduced.

Example

The following example shows how to create a new user:

```
nfvis(config)# rbac authentication users user admin2 password Cisco123* role administrators
nfvis(config)# commit
```

rbac authentication users user activate

To activate the account of an inactive user, the admin user can use the **rbac authentication users user activate** command in global configuration mode.

rbac authentication users user *username* **activate**

Syntax Description

username	Specifies the user name.

Command Default

None.

Command Modes

Global configuration (config)

Command History

Release	Modification
3.7.1	This command was introduced.

Usage Guidelines

Only the admin user can use this command.

Example

```
nfvis(config)# configure terminal
nfvis(config)# rbac authentication users user guest_user activate
nfvis(config)# commit
nfvis(config)# end
```

rbac authentication users user change-password

To change the existing password of a user, use the **rbac authentication users user change-password** command in global configuration mode.

rbac authentication users user *user-name* **change-password old-password** *password* **new-password** *password* **confirm-password** *password*

Syntax Description

user *user-name*	Specifies the user name.
old-password *password*	Specifies the old password.
new-password *password*	Specifies the new password.
confirm-password *password*	Confirms the new password.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
	This command was introduced.

Example

The following example shows how to change the password of an existing user:

```
nfvis(config)# rbac authentication users user admin2 change-password old-password Cisco123*
 new-password Cisnfv453# confirm-password **********
nfvis(config)#commit
```

rbac authentication users user change-role

To change the role of an existing user, use the **rbac authentication users user change-role** command in global configuration mode.

rbac authentication users user *user-name* **change-role old-role** *role-type* **new-role** *role-type*

Syntax Description

user *user-name*	Specifies the user name.
old-role *role-type*	Specifies the old role of the user.
new-role *role-type*	Specifies the new role of the user.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
	This command was introduced.

Example

The following example shows how to change the user role:

```
nfvis(config)# rbac authentication users user admin2 change-role old-role administrators
new-role operators
nfvis(config)# commit
```

show running-config rbac authentication users

To display details of all users, use the **show running-config rbac authentication users** command in privileged EXEC mode.

show running-config rbac authentication users [**user** *user-name* **password role**]

Syntax Description

user *user-name*	(Optional) The specified user's details are displayed.
password	(Optional) Username and password are displayed.
role *user-role*	(Optional) Username and role are displayed.

Command Default

Details of all users are displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
3.5.1	This command was introduced.

Example

The following is a sample output of the **show running-config rbac authentication users** command:

```
nfvis# show running-config rbac authentication users
rbac authentication users user admin
 role     administrators
 password $7$GVXJbe1IYpu4Dtfg4aAkdwxto2CtOFlW
!
rbac authentication users user test1
 role     administrators
 password $7$Qdmzu2GHhe2zkwPl7SvxWNDNH56XV+su
!
```