



## User Management Commands

---

- [rbac authentication min-pwd-length](#), on page 2
- [rbac authentication password-lifetime](#), on page 3
- [rbac authentication account-inactivity](#), on page 4
- [rbac authentication users](#), on page 5
- [rbac authentication users user activate](#), on page 6
- [rbac authentication users user change-password](#) , on page 7
- [rbac authentication users user change-role](#), on page 8
- [show running-config rbac authentication users](#), on page 9

# 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*

<b>Syntax Description</b>	<i>length</i>	Specifies the minimum length. The minimum length must be between 7 to 128 characters.
<b>Command Default</b>	The default minimum length is 7 characters.	
<b>Command Modes</b>	Global configuration (config)	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	3.7.1	This command was introduced.
<b>Usage Guidelines</b>	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
```

<b>Syntax Description</b>	<b>enforce</b>	Enforces or removes the rule for password lifetime validation. Valid values for this parameter are <b>true</b> and <b>false</b> .
	<b>min-days</b> <i>min-days</i>	Specifies the number of days after which the users can change the password.
	<b>max-days</b> <i>max-days</i>	Specifies the number of days before which the users must change the password.
<b>Command Default</b>	The default minimum lifetime value is set to 1 day and the default maximum lifetime value is set to 60 days.	
<b>Command Modes</b>	Global configuration (config)	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	3.7.1	This command was introduced.
<b>Usage Guidelines</b>	<ul style="list-style-type: none"> <li>• Only the admin user can use this command.</li> <li>• The minimum and maximum lifetime values and the rule to check for these values are not applicable to the admin user.</li> </ul>	

## 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
```

<b>Syntax Description</b>	<b>enforce</b>	Enforces or removes the rule for checking and mark-ing unused user accounts as inactive. Valid values for this parameter are <b>true</b> and <b>false</b> .
	<b>inactivity-days</b> <i>inactivity-days</i>	Specifies the number of days after which an unused account is marked as inactive.
<b>Command Default</b>	None	
<b>Command Modes</b>	Global configuration (config)	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	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
```

<b>Syntax Description</b>	<b>user</b> <i>user-name</i>	Specifies the user name.
	<b>password</b> <i>password</i>	Specifies the password.
	<b>role</b> <i>role-type</i>	Specifies the role of the user. The role can be one of the following: <ul style="list-style-type: none"> <li>Administrators—An administrator can perform all tasks.</li> <li>Operators—An operator can start, stop, and delete a VM, clear logs, and view all information.</li> <li>Auditors—An auditor can view all information, and cannot perform any tasks.</li> </ul>
<b>Command Default</b>	None	
<b>Command Modes</b>	Global configuration (config)	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	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**

<b>Syntax Description</b>	<i>username</i>	Specifies the user name.
<b>Command Default</b>	None.	
<b>Command Modes</b>	Global configuration (config)	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	3.7.1	This command was introduced.
<b>Usage Guidelines</b>	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
```

<b>Syntax Description</b>	<b>user</b> <i>user-name</i>	Specifies the user name.
	<b>old-password</b> <i>password</i>	Specifies the old password.
	<b>new-password</b> <i>password</i>	Specifies the new password.
	<b>confirm-password</b> <i>password</i>	Confirms the new password.
<b>Command Default</b>	None	
<b>Command Modes</b>	Global configuration (config)	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
		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
```

<b>Syntax Description</b>	<hr/> <b>user</b> <i>user-name</i> Specifies the user name. <hr/> <b>old-role</b> <i>role-type</i> Specifies the old role of the user. <hr/> <b>new-role</b> <i>role-type</i> Specifies the new role of the user. <hr/>				
<b>Command Default</b>	None				
<b>Command Modes</b>	Global configuration (config)				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td></td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification		This command was introduced.
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	
<b>user</b> <i>user-name</i>	(Optional) The specified user's details are displayed.
<b>password</b>	(Optional) Username and password are displayed.
<b>role</b> <i>user-role</i>	(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  $7$GVXJbelIYpu4Dtfg4aAkdwxto2CtOf1W
!
rbac authentication users user test1
  role      administrators
  password  $7$Qdmzu2GHhe2zkwP17SvxWNDNH56XV+su
!
```

```
show running-config rbac authentication users
```