How to enforce 2 Factor Authentication on user login?

238 admin November 30, 2023 Features & Functionalities, Security Features, Two Factor Authentication (2FA) 8651

Enforce 2fa on User login

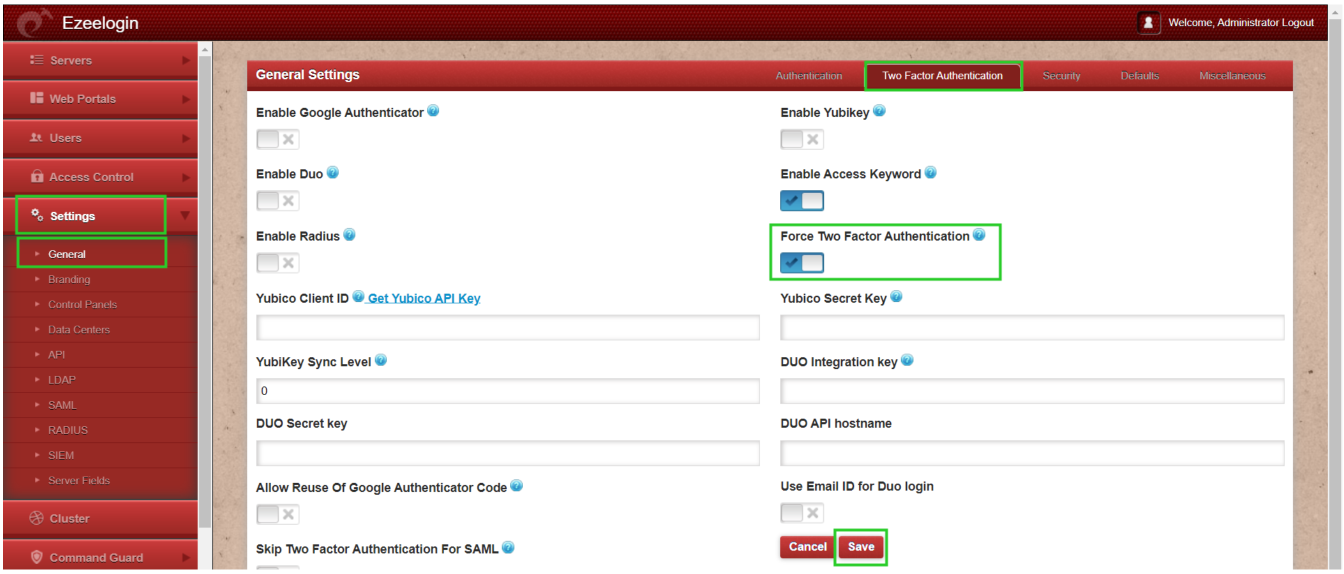
You have two options for implementing Two-Factor Authentication (2FA) for user logins:

1. 1. Enable 2FA for all users globally.
2. 2. Implement Two-Factor Authentication (2FA) for designated user groups as per their specific requirements and access levels.

---

4. Step 1. Activate the specified configurations to ensure that Two-Factor Authentication (2FA) is enforced for both SSH login and the web interface. This measure will require users accessing the SSH gateway to establish two-factor authentication, aligning with recommended security practices.
5. This will enable the users to use 2fa globally.

Under Setting > General > Two-factor authentication > enable force 2fa.



Enable Google Authenticator ☒

Enable Yubikey ☒

Enable Duo ☒

Enable Access Keyword ☑

Enable Radius ☒

Force Two Factor Authentication ☑

Yubico Client ID

Yubico Secret Key

YubiKey Sync Level: 0

DUO Integration key

DUO Secret key

DUO API hostname

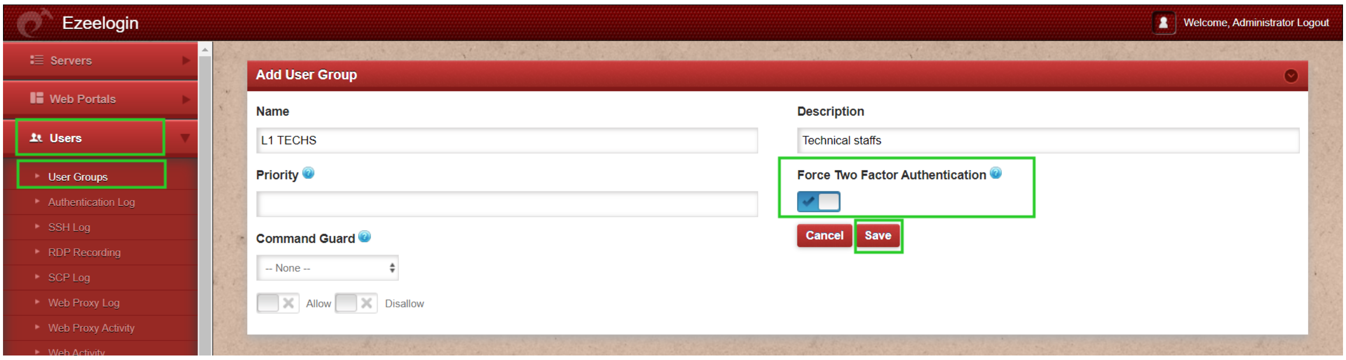
Allow Reuse Of Google Authenticator Code ☒

Use Email ID for Duo login ☒

Skip Two Factor Authentication For SAML

Step 2. You have the option to activate mandatory Two-Factor Authentication (2FA) selectively for particular user groups based on specific requirements.

Under Users > User Groups > Select the user group > enable force 2fa



Add User Group

Name: L1 TECHS

Description: Technical staffs

Priority:

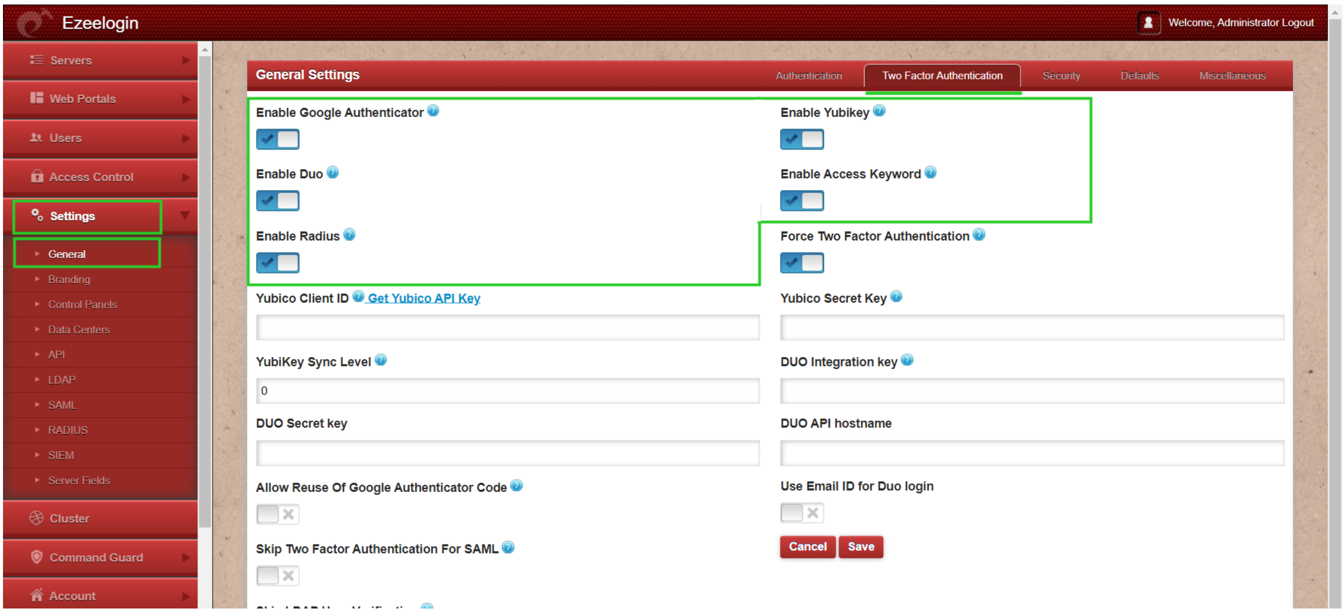
Force Two Factor Authentication: ✓

Command Guard: -- None --

☒ Allow ☒ Disallow

- You can also enable the different 2-factor mechanisms that will be available for the gateway user for setup.

Two-factor Authentication tab is available only from version 7.11.0. If you are running an old version, then 2fa methods configured under Settings->General->Security tab will be available.



General Settings

Enable Google Authenticator: ✓

Enable Yubikey: ✓

Enable Duo: ✓

Enable Access Keyword: ✓

Enable Radius: ✓

Force Two Factor Authentication: ✓

Yubico Client ID:

Yubico Secret Key:

YubiKey Sync Level: 0

DUO Integration key:

DUO Secret key:

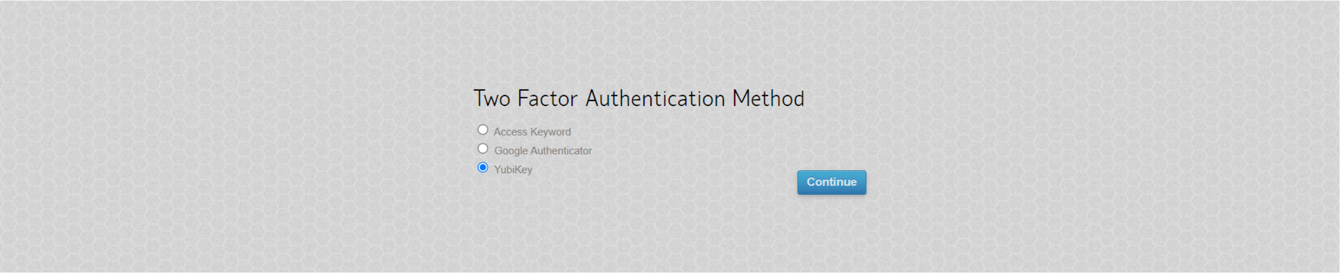
DUO API hostname:

Allow Reuse Of Google Authenticator Code: ☒

Use Email ID for Duo login: ☒

Skip Two Factor Authentication For SAML: ☒

- Relogin, into the WebGUI, and the user will be prompted to set up the 2-factor method if he hasn't set up any. Set up any 2fa method of your choice from here.

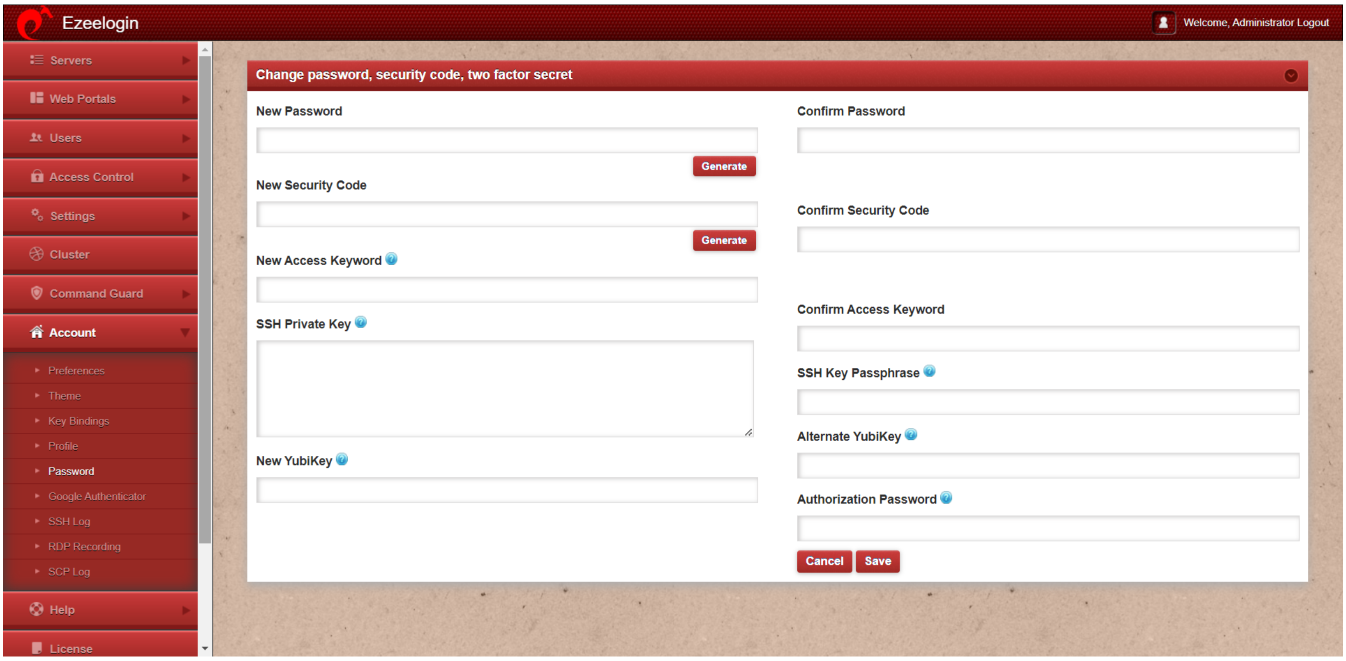


Two Factor Authentication Method

○ Access Keyword
○ Google Authenticator
● YubiKey

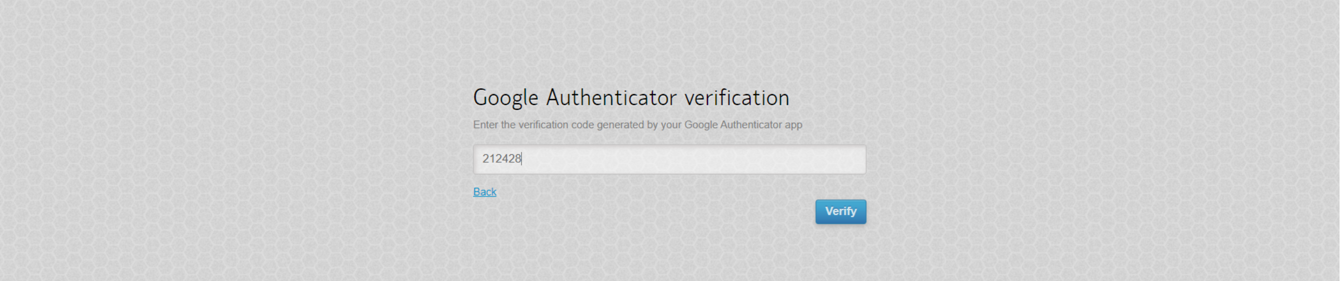
- To configure additional Two-Factor Authentication (2FA) methods, access the WebGUI after logging in and proceed to set up multiple 2FA methods accordingly.

The 2-factor mechanism used for the last login into the WebGUI would be the 2fa method in use in the backend. To change, the 2fa method in use in the backend, log into the WebGUI using the new 2fa method so that it becomes the default 2fa method for the backend.



Change password, security code, two factor secret

- We have set up Google 2fa and Access Keyword successfully and will be prompted for it. In the example below, we are using Google 2fa to log in, and hence the same would be prompted in the backend shell as well.

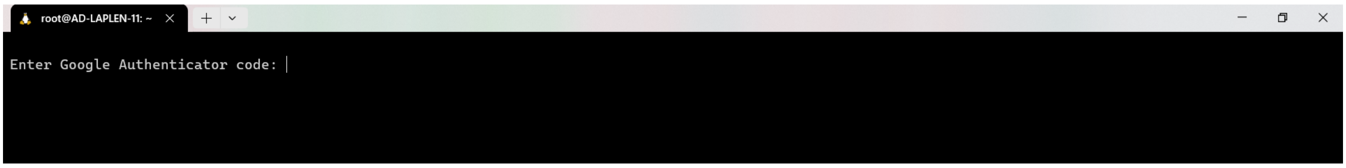


Google Authenticator verification

Enter the verification code generated by your Google Authenticator app

212428

- The **backend** would look as follows.



```
Enter Google Authenticator code:
```

Related Articles:

- [Configure Duo 2fa in JumpServer]
- [Configure Yubikey 2fa in the JumpServer]
- **How to enable Access Keyword 2fa**
- **How to enable Google 2fa in JumpServer**
- **How to configure Radius 2fa in JumpServer**

Online URL:
https://www.ezeelogin.com/kb/article/how-to-enforce-2-factor-authentication-on-user-login-238.html