

How to configure Yubikey two factor authentication in ssh ?

75 admin November 22, 2024 [Features & Functionalities](#), [Tweaks & Configuration](#) 20965

How to enable/disable Yubikey 2FA (Two-factor Authentication) in Ezeelogin?

Overview: This article provides a comprehensive guide on configuring and managing Yubikey two-factor authentication (2FA) for SSH jump host.

Refer to the YouTube video to [Configure Yubikey's two-factor authentication](#) in ssh jump host.

1. How to enable Yubikey?

Step 1(A): Log in to the Ezeelogin GUI as an admin privileged user, navigate to **Settings -> General -> Two Factor Authentication**, and enable Yubikey.

Ezeelogin Welcome, Administrator Logout

General Settings Authentication **Two Factor Authentication** Security Defaults Miscellaneous

Enable Google Authenticator ☐

Enable Duo ☐

Enable Radius ☐

Yubico Client ID [Get Yubico API Key](#)

YubiKey Sync Level 0

DUO Secret key

Allow Reuse Of Google Authenticator Code ☐

Skip Two Factor Authentication For SAML ☐

Enable Yubikey ☒

Enable FIDO2 ☐

Enable Access Keyword ☐

Force Two Factor Authentication ☐

Yubico Secret Key

DUO Integration key

DUO API hostname

Use Email ID for Duo login ☐

Cancel Save

Step 1(B): Click on "Get Yubico API Key" to obtain the Yubico Client ID and secret key.

Ezeelogin Welcome, Administrator Logout

General Settings Authentication **Two Factor Authentication** Security Defaults Miscellaneous

Enable Google Authenticator ☐

Enable Duo ☐

Enable Radius ☐

Yubico Client ID [Get Yubico API Key](#)

YubiKey Sync Level 0

DUO Secret key

Allow Reuse Of Google Authenticator Code ☐

Skip Two Factor Authentication For SAML ☐

Enable Yubikey ☒

Enable FIDO2 ☐

Enable Access Keyword ☐

Force Two Factor Authentication ☐

Yubico Secret Key

DUO Integration key

DUO API hostname

Use Email ID for Duo login ☐

Cancel Save

Step 1(C): To set up Yubikey for user authentication, navigate to **Account** -> **Password** -> **New Yubikey** and click on **save** after providing the authorization password(password of the currently logged in user).

Ezeelogin Welcome, mike Logout

Servers

Account

- Preferences
- Theme
- Key Bindings
- Profile
- Password**
- Google Authenticator
- Duo Authenticator
- FIDO2 Keys
- SSH Log
- SCP Log
- License

Change password, security code, two factor secret

New Password Generate

New Security Code Generate

New Access Keyword

SSH Private Key

New YubiKey

Confirm Password

Confirm Security Code

Confirm Access Keyword

SSH Key Passphrase

Alternate YubiKey

Authorization Password

Cancel Save

Step 1(D): Log in to the Ezeelogin GUI using the Yubikey 2FA method.

YubiKey verification

Insert your YubiKey into a USB port and touch the YubiKey button

YubiKey

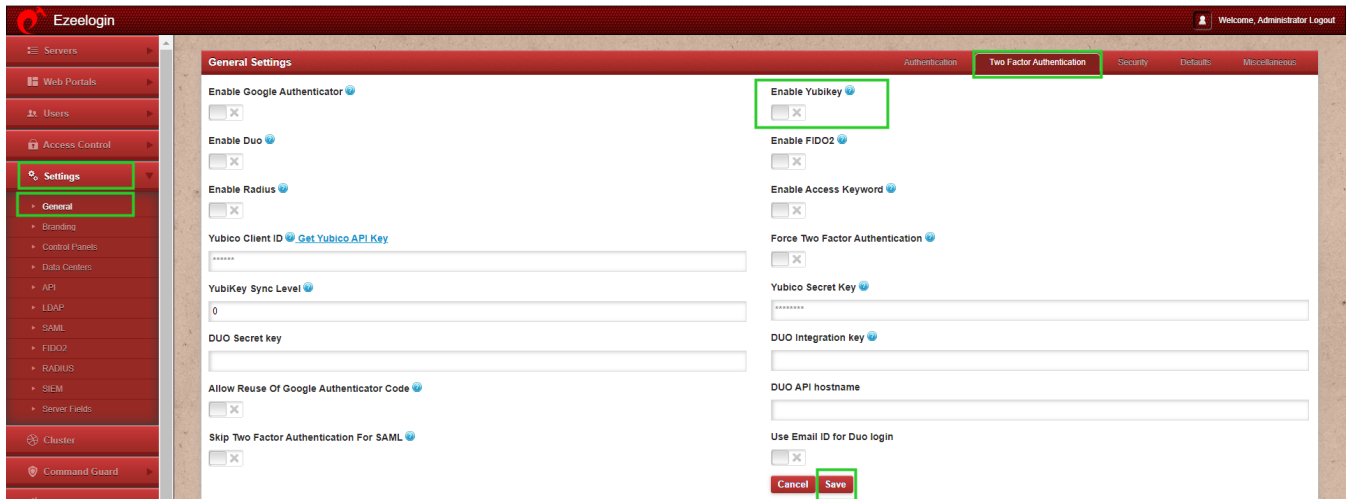
Verify

Step 1(E): The backend 2fa method will also be now using Yubikey.

```
Enter YubiKey: 
```

2. Disable Yubikey 2FA from the GUI.

Step 2(A): To disable Yubikey from Ezeelogin GUI, navigate to **Settings -> General -> Two-factor Authentication** and [disable Yubikey](#).



Emergency CLI Method:

1. How do we disable Yubikey 2FA (Two-factor Authentication) from the backend?

Run the below commands to [disable and clear Google authenticator](#). Replace the username to disable Yubikey for that user.

```
root@gateway:~# php /usr/local/ezlogin/ez_queryrunner.php "update prefix_settings set value='N'
where(name='enable_yubikey')"
```

```
root@gateway:~# php /usr/local/ezlogin/ez_queryrunner.php "update prefix_users set eyk=NULL
where username='ezadmin'"
```

No Two-factor Authentication enabled

2. This error happens when we enforce Two-Factor authentication without enabling any of the Two-Factor authentications. Run the following command to disable **Force Two Factor Authentication**.

```
root@gateway:~# php /usr/local/ezlogin/ez_queryrunner.php "update prefix_settings SET value = 0
WHERE name = 'two_factor_auth'"
```

```
root@gateway:~# php /usr/local/ezlogin/ez_queryrunner.php "update prefix_usergroups SET
```

```
force_tfa = 'N'
```

Yubikey outbound URLs to be whitelisted:

Following are the Yubikey outbound URLs to be whitelisted in the firewall.

1. <https://api.yubico.com/wsapi/2.0/verify>
2. <https://api2.yubico.com/wsapi/2.0/verify>
3. <https://api3.yubico.com/wsapi/2.0/verify>
4. <https://api4.yubico.com/wsapi/2.0/verify>
5. <https://api5.yubico.com/wsapi/2.0/verify>

Yubikey Library requires access to the above URLs. Also, do check out the article for the list of YubiKey API servers that the YubiKey client would utilize https://developers.yubico.com/yubikey-val/Getting_Started_Writing_Clients.html

Related Articles:

[Disable all 2fa from the backend.](#)

[Enforce 2fa on user login.](#)

[Reset 2fa on Ezeelogin user.](#)

Online URL:

<https://www.ezeelogin.com/kb/article/how-to-configure-yubikey-two-factor-authentication-in-ssh-75.html>