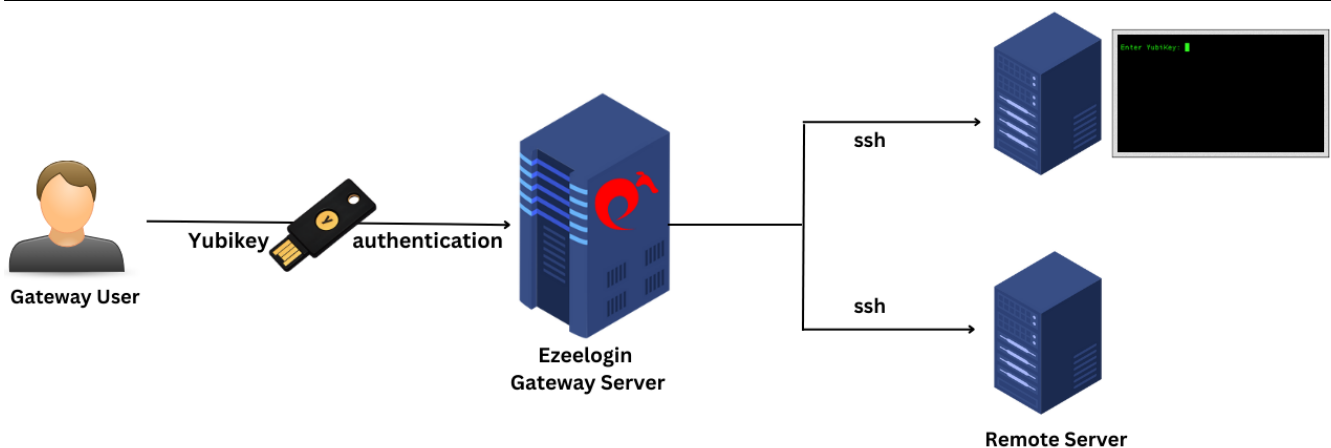


# How to configure Yubikey two factor authentication in ssh ?

75 admin July 2, 2024 [Features & Functionalities](#), [Tweaks & Configuration](#) 16198

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

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



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

**Step 1: Enable Yubikey 2FA in the Ezeelogin Web Interface with an admin privileged User.**

- Login into Ezeelogin web GUI as an Admin user.
- Navigate to **Settings -> General -> Two Factor Authentication**.
- Enable Yubikey by clicking on "Get Yubico API Key" to obtain the Client and Secret for 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

DUO Secret key

Allow Reuse Of Google Authenticator Code ☐

Skip Two Factor Authentication For SAML ☐

Enable Yubikey ☒

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 2: Set Up Yubikey for User Authentication

- Navigate to Account > Password > New Yubikey and follow the prompts to complete the setup for each user.

**Ezeelogin** Welcome, Administrator Logout

**Change password, security code, two factor secret**

New Password

New Security Code

SSH Private Key

New Yubikey

Confirm Password

Confirm Security Code

SSH Key Passphrase

Alternate YubiKey

Authorization Password

Generate Generate

Cancel Save

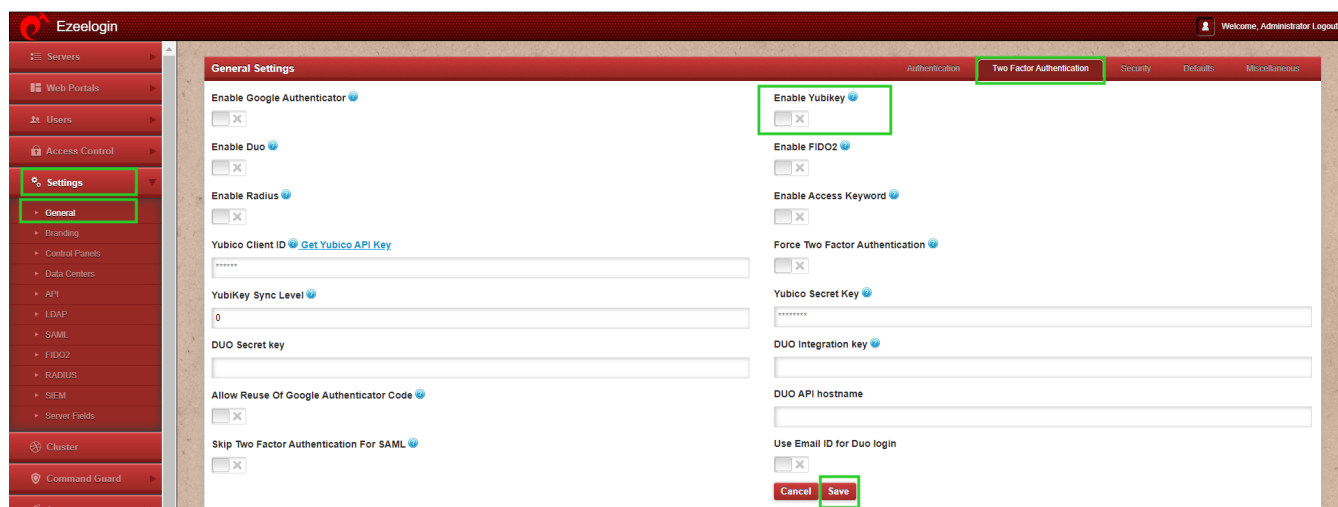
## Step 3: Usage in Web Interface

- Log in to the Ezeelogin web interface using the Yubikey 2FA method.
- The last successful 2FA method used in the web interface will automatically be applied to the backend SSH or ezsh shell.



## Step to Disable Yubikey 2FA from the GUI.

- Navigate to **Settings > General > Two-factor Authentication** and [disable Yubikey](#).



### Emergency CLI Method:

- How to 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

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 URL's 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](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>