How to enforce 2 Factor Authentication on user login?

238 admin October 12, 2024 <u>Features & Functionalities</u>, <u>Security Features</u>, <u>Two Factor</u> <u>Authentication (2FA)</u> 10517

Enforce 2fa on user login

Overview: This article provides an overview of <u>Two-Factor Authentication (2FA)</u> implementation options: enforcing 2FA globally for SSH and web interfaces, and selectively for user groups, along with configuration instructions and method setup details.



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

1. Enable 2FA for all users globally.

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

1. Enable 2FA for all users globally.

Enable the **force 2fa** to enforce <u>Two-Factor Authentication (2FA)</u> for both Ezeelogin backend (ezsh) and the web interface, requiring all users to use 2FA globally for added security.

Step 1(A): Under Settings -> General -> Two-factor authentication -> enable force 2fa.

Ezeelogin			Welcome, Administrator Log
i≣ Servers ►	•	General Settings	Authentication Two Earthr Authentication Security Defaults Miscellaneous
🖬 Web Portals 🛛 🕨	er X		Finable Yuhikav @
±t Users ►		×	
🖬 Access Control 🔹 🕨		Enable Duo 💿	Enable Access Keyword 💿
°₀ Settings 🗸 🗸		×	
► General	1.10	Enable Radius 📦	Force Two Factor Authentication
▶ Branding		Vubice Client ID @ Cot Vubice API Key	Vubice Searct Kou
Control Panels Data Centers			
► API		YubiKey Sync Level 🞯	DUO Integration key 🥹
► LDAP	1	0	
► RADIUS	3. 14.	DUO Secret key	DUO API hostname
► SIEM			
 Server Fields 		Allow Reuse Of Google Authenticator Code 🥹	Use Email ID for Duo login
🛞 Cluster		×	×
💿 Command Guard 🔹 🕨	x	Skip Two Factor Authentication For SAML 🥹	Cancel Save

2. Implement Two-Factor Authentication (2FA) for designated user groups

It is possible to activate mandatory Two-Factor Authentication (2FA) selectively for specific user groups based on particular requirements.

Step 2(A): Under Users -> User Groups -> Select the user group -> enable force 2fa -> save

Ezeelogin			Velcome, Administrator Logout
i≣ Servers ►	-		
Web Portals		Eait User Group	
		Name	Description
±t Users ▼		L1 techs	
User Groups		Priority 🐵	Force Two Factor Authentication 🔍
► LDAP		0	
Authentication Log	1	Command Guard 🧐	Cancel Save
▶ SSH Log			
RDP Recording		None 👻	
► SCP Log		Allow Visallow	
Web Proxy Log			
Web Proxy Activity	262		

It is possible to enable the different 2-factor mechanisms that will be available for the gateway user to setup.

Ezeelogin		Welcome, Administrator Logout
t≣ Servers	General Settings	Authentication Security Defaults Microelfaneous
🖬 Web Portals	Enable Google Authenticator 🔍	Enable Yubikay (1)
±t Users ►		
Access Control	Enable Duo 😡	Enable FIDO2 😨
© Settings ▼		
▶ General	Enable Radius 🕡	Enable Access Keyword 🕑
Branding		
 Control Panels 	Yubico Client ID @ Get Yubico API Key	Force Two Factor Authentication 💿
► Data Centers	*****	
► API	YubiKey Sync Level 🞯	Yubico Secret Key 🥹
► LDAP	0	*******
► SAML		
► FIDO2	DUO Secret key	DUO Integration key 🤎
► RADIUS	*****	*****
► SIEM	Allow Reuse Of Google Authenticator Code 2	DUO API hostname
 Server Fields 	×	*****
🛞 Cluster	Skip Two Factor Authentication For SAML 🐵	Use Email ID for Duo login
Command Guard	×	×
Account		Cancel Save

Relogin, into the Ezeelogin GUI, 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

To configure additional <u>Two-Factor Authentication (2FA)</u> methods, log in to the WebGUI and navigate to the **accounts tab** to set up **multiple 2FA** options..

Ezeelogin		Welcome, joh
E Servers	Change password, security code, two factor secret	
🚔 Account 🔹 🔻	New Password	Confirm Password
		Generate
	New Security Code	
► Profile		Confirm Security Code
Password	New Access Keyword	Generate
Google Authenticator	New Access Reyword	
 FID02 Keys 		Confirm Access Keyword
► SSH Log	SSH Private Key 🕑	
		SSH Key Passphrase 📦
J License		
		 Alternate YubiKey 😺
	New YubiKey 🛛 🗲	
Powered by ezeelogin.com		Authorization Password
	24 8	

We have set up Google 2fa and Access Keyword successfully and will be prompted for it. In the example below, we are using <u>Google 2fa</u> 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 267253
Verify

The Ezeelogin backend would look as follows.



- 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.
- The 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.

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