Enable MFA for Remote Server and Network Device Access

824 Jisna Joseph October 30, 2026 Features & Functionalities 330

How to configure Two-Factor Authentication (2FA / MFA) for remote server access and network devices, including routers and switches.

Overview: Ezeelogin provides an additional layer of security by requiring users to complete two-factor authentication (2FA) before accessing remote servers and network devices. With this step-up MFA, engineers must verify their identity when connecting to protected devices such as switches, routers, and firewalls, even when those devices cannot run a PAM agent.

This approach requires no agents, firmware modifications, or changes to the network devices. The **Ezsh 2FA Interval** setting controls how long a successful verification remains valid before users must authenticate again when accessing remote devices through the Ezeelogin shell (`ezsh`). This uses the same two factor authentication method that is configured for the initial ezsh login.

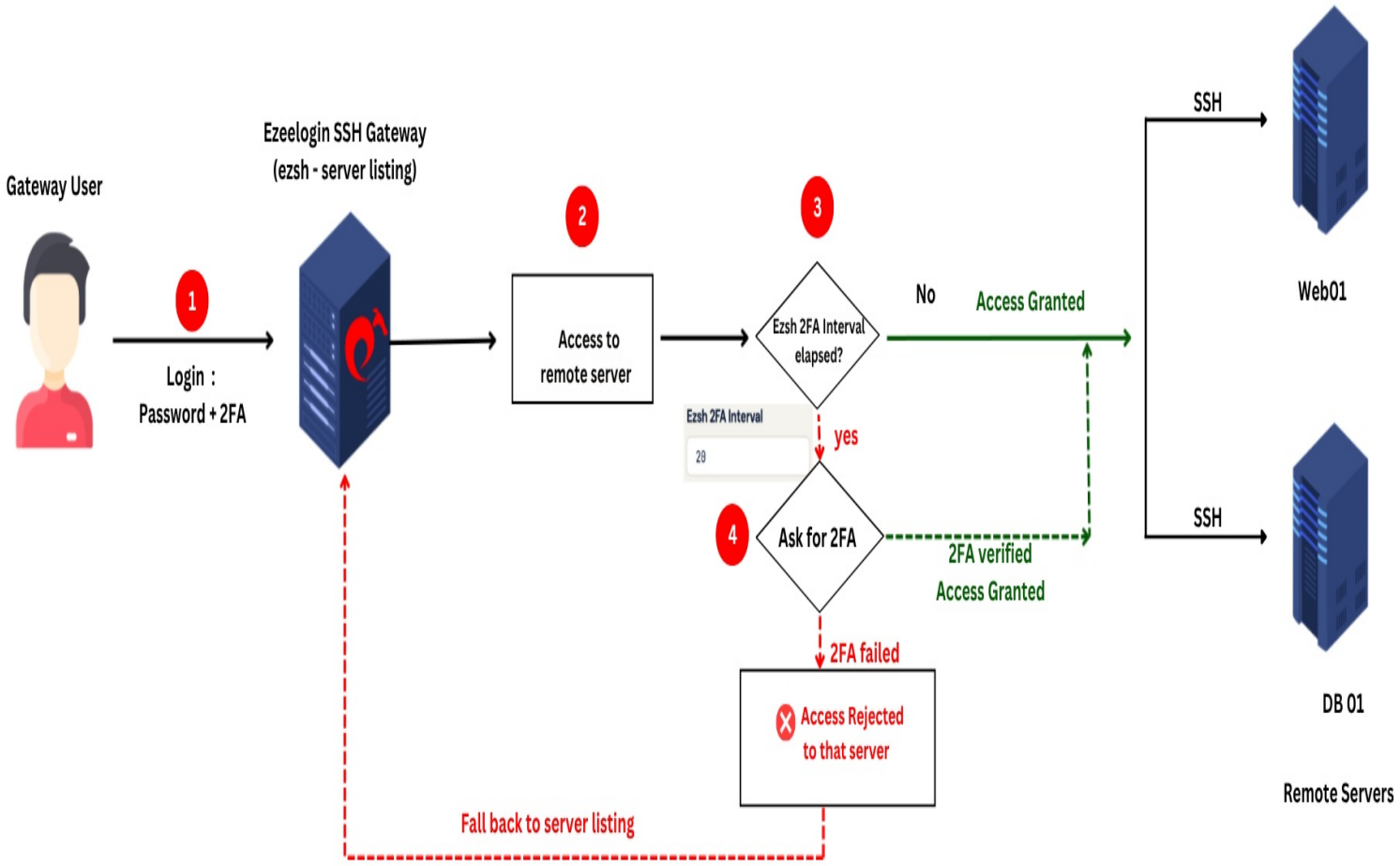
This article explains how to configure MFA for remote servers and network devices and strengthen privileged access security in Ezeelogin version 7.48.0 and later.

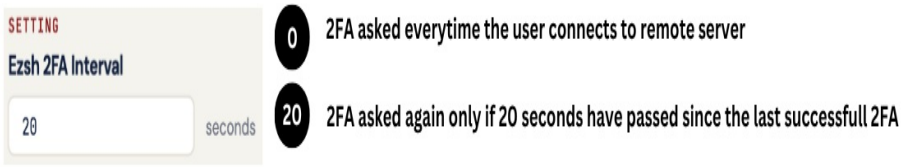
Note: This feature requires **Ezeelogin 7.48.0 or later**. Not sure which version you have? Check it in the Ezeelogin UI. If you're on an earlier release, upgrade Ezeelogin first

Prerequisites:

Ezeelogin version 7.48.0 or later.
2FA already enabled and working for ezsh login (for example, Google Authenticator).
Administrator access to the Ezeelogin UI.

How two factor authentication (2FA) before remote server access works?





Step 1: Log in to the Ezeelogin SSH Gateway.

The user logs in to the gateway using their password and 2FA. This verification is required once per gateway session.

Step 2: Select a remote server.

The gateway displays the available remote servers. The user selects the server they want to access.

Step 3: Check whether the 2FA interval has elapsed.

If the configured 2FA interval has elapsed, the user must complete 2FA verification again. Proceed to Step 5.
If the interval has not elapsed, the user is granted access to the remote server without additional 2FA verification.

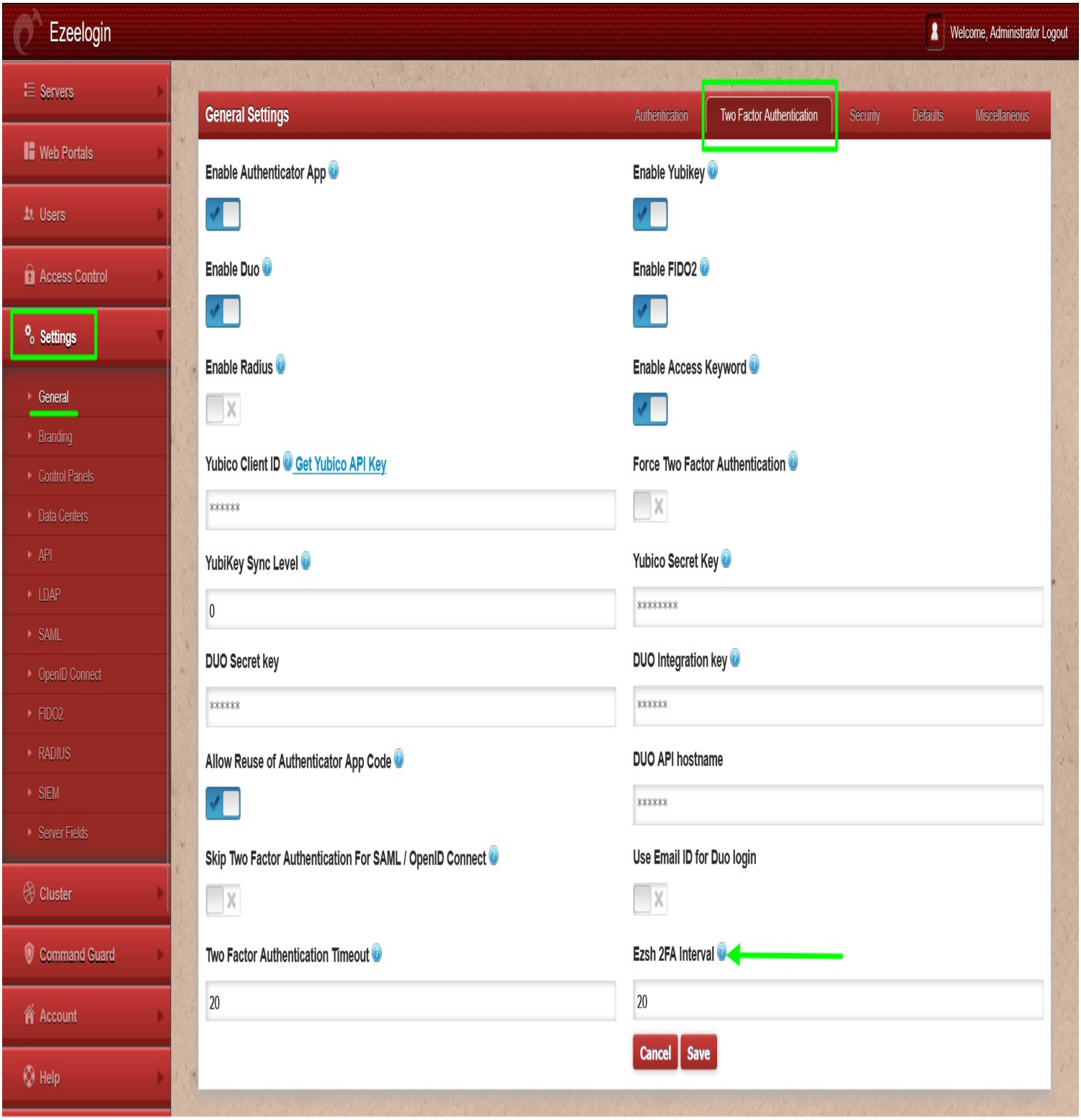
Step 5: Enter the 2FA code.

The user enters their 2FA code to verify their identity.

Steps to configure 2FA (MFA) before remote server access

Step 1: Open the Ezsh 2FA Interval setting.

Log in to the Ezeelogin UI and navigate to **Settings** -> **General** -> **Two Factor Authentication** -> **Ezsh 2FA Interval**.



Step 2: Set the interval and save

> **Note: The default value of the Ezsh 2FA Interval is 86400 seconds (24 hours)**

Enter the required value in seconds and click Save. This value controls how often 2FA is rechecked when users access remote servers through ezsh. For example:

If the value is **20**: 2FA is rechecked after 20 seconds have passed since the last verification.

If the value is **0**: 2FA is rechecked every time a user connects to a remote server.

Step 3: Verify the 2FA prompt in ezsh

Log in to the backend (ezsh) and connect to a remote server. The 2FA method used for the initial ezsh login is prompted again, based on the configured interval.

In the example below, Google Authenticator is used for the initial ezsh login. The same method prompts for the code before the connection to the remote server is made. Once the interval expires, 2FA is required again for the next remote access.

Why use 2FA before remote server access?

Logging in to the jump server is only the first checkpoint. Requiring 2FA again before each remote server connection adds a second layer of protection for sensitive systems such as production databases, payment servers, and hosts that hold customer data. If a user’s session is left open or hijacked, the attacker still can’t reach your servers without the second factor.

Frequently Asked Questions:

1.What does the ezsh 2FA Interval setting do?

It specifies, in seconds, how long a successful 2FA verification remains valid before Ezeelogin requests 2FA verification again when accessing remote servers.

2. What happens if the ezsh 2FA Interval is set to 0?

2FA verification is required every time a user connects to a remote server.

3. Which Ezeelogin version supports this feature?

This feature is supported in Ezeelogin version 7.48.0 and later.

4. Does remote 2FA use a different authentication method from the initial login?

No. Remote 2FA uses the same 2FA method configured for the initial ezsh login.

5. Is remote 2FA supported with RDP?

No. Remote 2FA is currently not supported with RDP connections.

6. Does remote 2FA apply to parallel shell sessions?

Yes. Remote 2FA applies to parallel shell sessions. Users are prompted for 2FA verification before switching to a parallel shell session. However, 2FA is requested only when switching to the parallel shell and not for every individual server login.

7. Does remote 2FA apply to interactive shell sessions?

Yes. Remote 2FA applies to interactive shell sessions. Users are prompted for 2FA verification before switching to an interactive shell session. However, 2FA is requested only when switching to the interactive shell and not for every individual server login.

8. Is remote 2FA required when connecting to a remote server for the first time?

It depends on the configured ezsh 2FA Interval.
- If the ezsh 2FA Interval is set to 0, 2FA verification is required when connecting to the remote server for the first time.
- If the interval is set to a specific duration in seconds, 2FA verification is not required if the user connects to the remote server within that configured validity period following a successful 2FA verification, even if it is the first connection to that server.

9. Is remote 2FA required for secure copy (SCP) operations through ezsh?

Yes. Remote 2FA applies to secure copy (SCP) operations through ezsh. Users are prompted for 2FA verification before switching to the secure copy operation.

10. Is remote 2FA supported for web-based file transfers?

No. Remote 2FA is currently not supported for file transfers performed through the Ezeelogin web interface.

11. Is remote 2FA supported when transferring files from a desktop to a remote server using SCP or SFTP?

No. Remote 2FA is not supported when transferring files from a desktop to a remote server using SCP or SFTP.

12. Is remote 2FA supported when using WebSSH?

Yes. Remote 2FA is supported when accessing remote servers through WebSSH.

Conclusion

Requiring two-factor authentication before remote server access gives your jump server a second checkpoint without forcing users to log in to the gateway again. Set the Ezsh 2FA Interval to 0 for maximum security, or use a longer interval if users connect to many servers in a short time.

Need help with the setup? Contact Ezeelogin support and our team will help you configure it.

Related Articles:

Enable/Disable 2FA

Enforce 2fa on user login

Disable 2fa from web interface

How to reset 2fa on ezeelogin user?

Online URL: https://www.ezeelogin.com/kb/article/enable-mfa-for-remote-server-and-network-device-access-824.html