

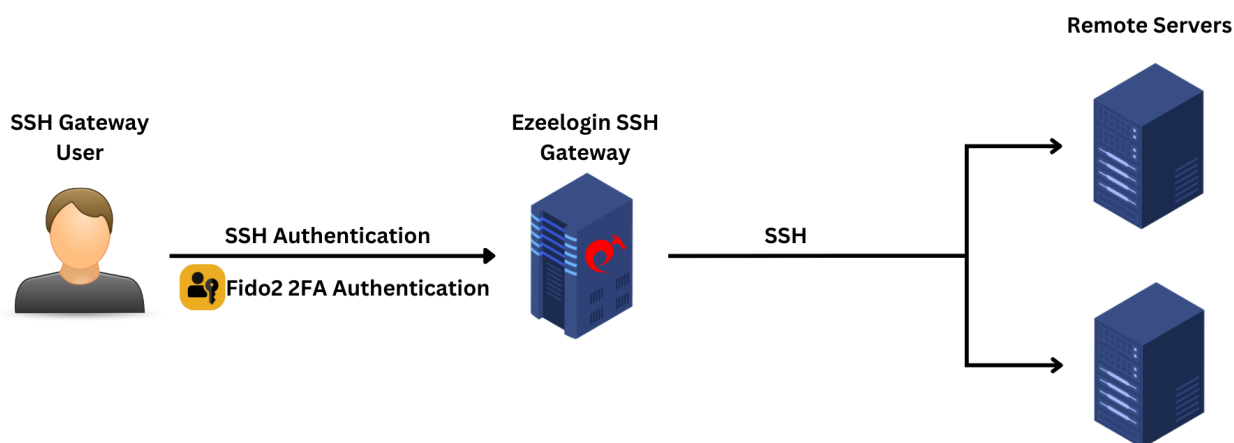
Configure FIDO2 with Ezeelogin

651 Nesvin KN April 17, 2025 [Security Features](#) 1263

How to enable/disable FIDO2 authentication with Ezeelogin?

Overview: This article explains how to enable and configure FIDO2 authentication in Ezeelogin from version 7.37.0, including steps to troubleshoot common errors and disable it from the backend if needed.

FIDO2, shorthand for Fast Identity Online, comprises open standards designed for secure and convenient authentication. By diminishing dependence on passwords and incorporating robust authentication methods such as biometrics and hardware tokens, FIDO2 seeks to enhance the overall security of online accounts and services.



This feature is available from Ezeelogin version 7.37.0. [How to upgrade the Ezeelogin version to the latest?](#)

SSL Certificate to enable FIDO2 authentication, as self-signed certificates and IP addresses are not supported

Step 1: Login to Ezeelogin GUI and navigate to **Settings -> General -> Two Factor Authentication -> Enable FIDO2.**

The screenshot shows the Ezeelogin administration interface. On the left, a navigation menu has 'Settings' highlighted with a green box. The main content area is titled 'General Settings' and has a sub-tab 'Two Factor Authentication' also highlighted in green. The settings are organized into two columns. The left column includes: 'Enable Google Authenticator' (checkbox), 'Enable Duo' (checkbox), 'Enable Radius' (checkbox), 'Yubico Client ID' (text input with a link to 'Get Yubico API Key'), 'YubiKey Sync Level' (text input with value '0'), 'DUO Secret key' (text input), 'Allow Reuse Of Google Authenticator Code' (checkbox), and 'Skip Two Factor Authentication For SAML' (checkbox). The right column includes: 'Enable Yubikey' (checkbox), 'Enable FIDO2' (checkbox, checked, with a green arrow pointing to it), 'Enable Access Keyword' (checkbox), 'Force Two Factor Authentication' (checkbox), 'Yubico Secret Key' (text input), 'DUO Integration key' (text input), 'DUO API hostname' (text input), and 'Use Email ID for Duo login' (checkbox). At the bottom right, there are 'Cancel' and 'Save' buttons.

Step 2: Enable the Authenticator Types and Save the settings.

Ezeelogin Welcome, Administrator Logout

- Servers
- Web Portals
- Users
- Access Control
- Settings**
 - General
 - Branding
 - Control Panels
 - Data Centers
 - API
 - LDAP
 - SAML
 - FIDO2**
 - RADIUS
 - SIEM
 - Server Fields
- Cluster
- Command Guard
- Account
- Help
- License

Collapse

Powered by ezeelogin.com

FIDO2 Settings

FIDO2 Relying Party

User Verification

Match Root Certificate

Client-side Discoverable Credentials

Require User Present

Attestation

CTS Profile Match

Cancel Save

Authenticator Types

USB

Bluetooth

Internal

NFC

Hybrid

Cancel Save

Attestation Statement Formats

Android Key

Apple

None

TPM

Android SafetyNet

FIDO U2F

Packed

Cancel Save

Attestation Root Certificates

FIDO Alliance Metadata Service

Yubico

Hypersecu

Apple

SoloKeys

Google

Microsoft

Cancel Save

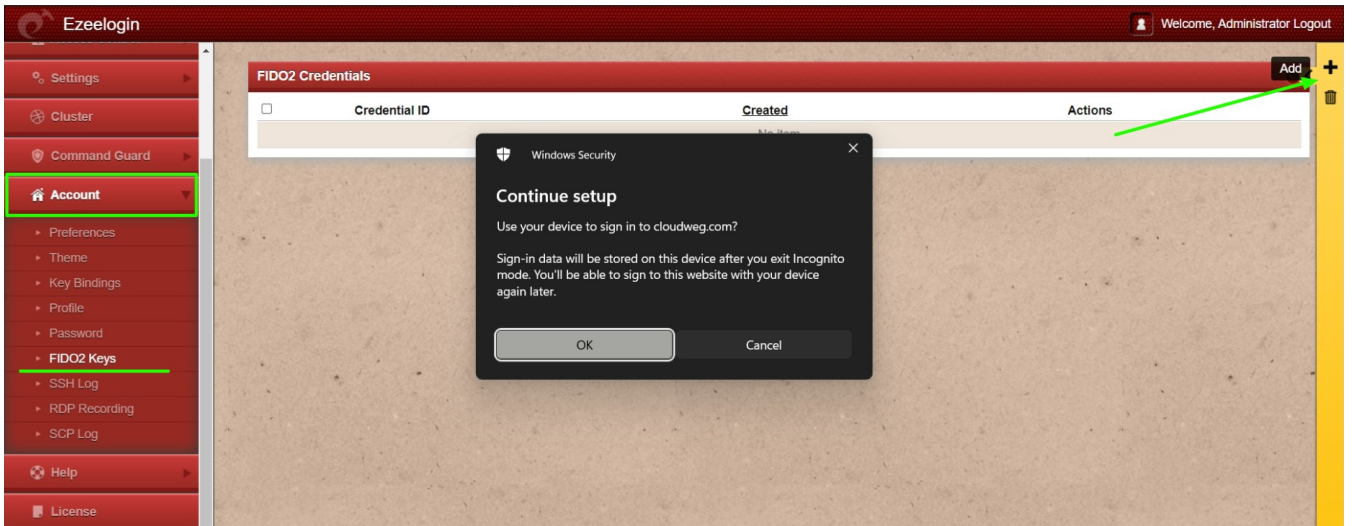
Note: Nothing checked = accept all

If you select a root certificate authority, direct attestation is required to validate the client with the root.

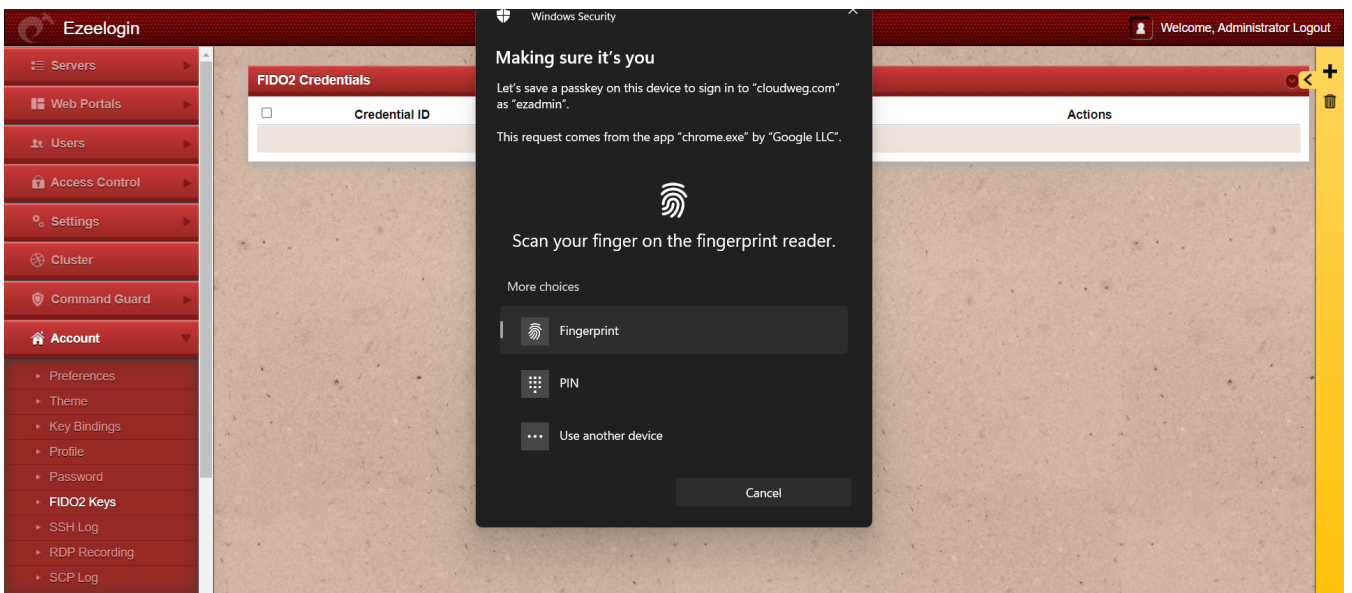
The browser may warn you that it will provide information about the user device.

When not checking against any root certificate authority (deselect all certificates), the client may change the assertion from the authenticator (for instance, using an anonymization CA), the browser may not warn about providing information about the user device.

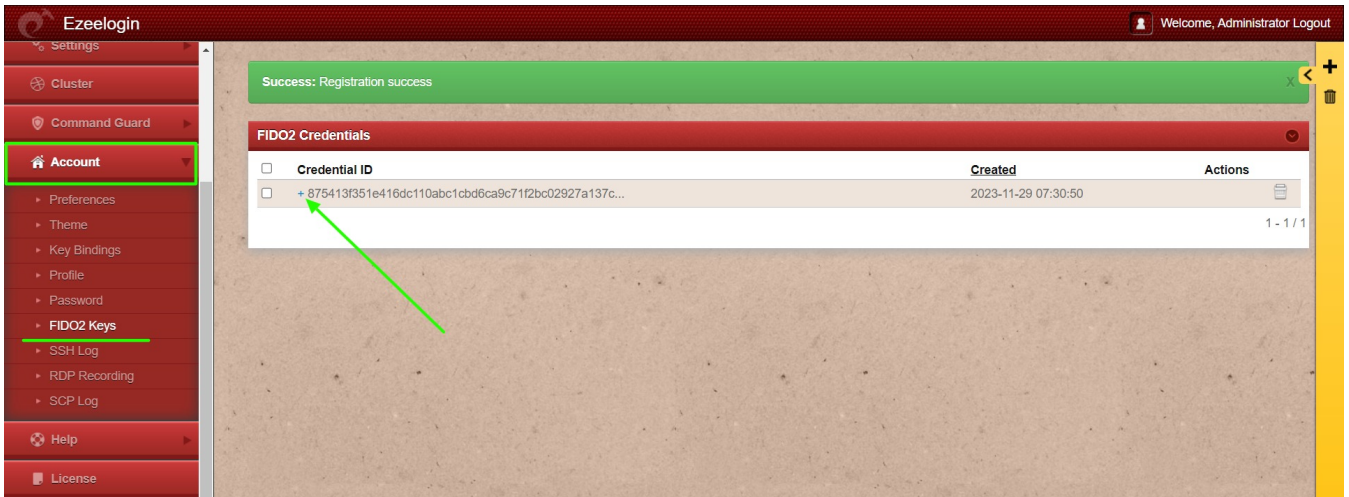
Step 3: Navigate to **Accounts** -> **Fido2 Keys** -> **Add new**. Click on **OK** to continue setup to add FIDO2 keys.



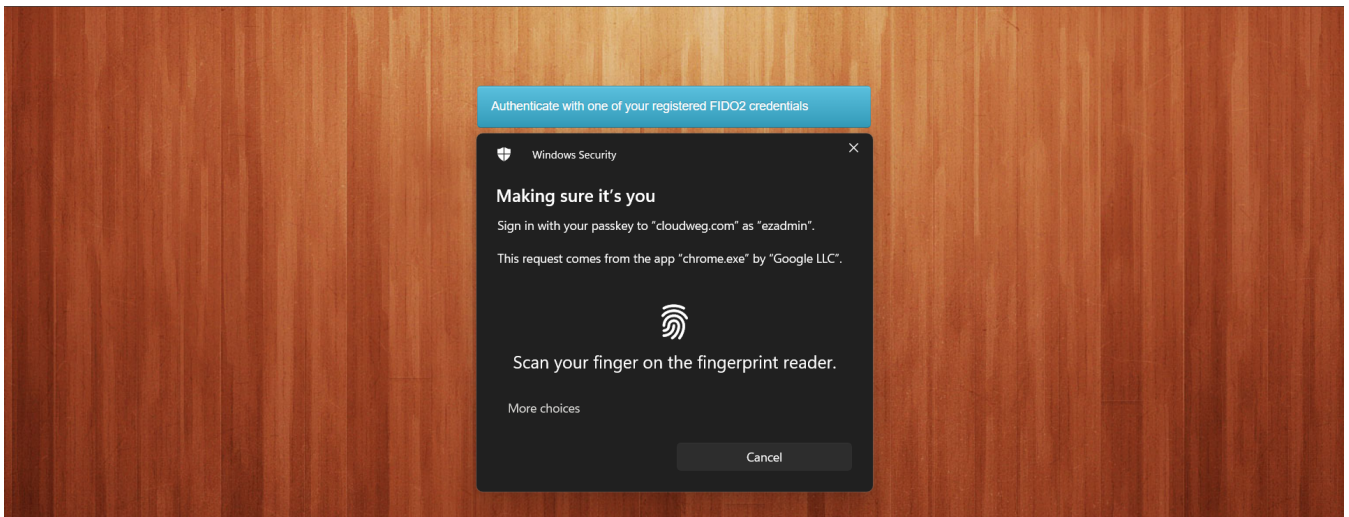
Step 4: Continue with your **fingerprint, PIN, security key, or Android device** to complete the setup, and the new FIDO2 ID will appear in the FIDO2 keys tab.



Step 5: If registration is successful, the user can see the message '**Success: Registration success.**' More registration details can be seen using the **view** button.



Step 6: Log out and log back into the GUI to confirm that FIDO2 authentication is working correctly with the method chosen in the above step.



Step 7: Log in to the backend (ezsh) and confirm that FIDO2 authentication works there as well. Copy the link to the browser, use the authentication method, and press any key in the shell to authenticate to ezsh.

```
Open the following URL in a web browser for FIDO2 authentication:
https://cloudweg.com/ezlogin/index.php/auth/fido2_ezsh/b83f45b7-776e-499e-b8a1-92b4e926d8f2
Valid for 3 minutes.
Press 'x' to exit.
After authenticating, press any other key to continue. |
```

How to disable FIDO2 2FA (Two-factor Authentication) from the backend?

Run the below commands to disable FIDO2.

```
root@gateway ~]# php /usr/local/ezlogin/ez_queryrunner.php "update prefix_settings set value='N' where(name='enable_fido2')"
```

Run the below commands to clear all FIDO2 registrations of all gateway users.

```
root@gateway ~]# php /usr/local/ezlogin/ez_queryrunner.php "truncate table prefix_user_fido2"
```

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'"
```

Common errors while setting up and authenticating with FIDO2 authenticator.

1. Error: HTTPS is required



Error: HTTPS is required

Ezeelogin needs to be accessed with a valid certificate to enable FIDO2 authentication, and self-signed

certificates will not work.

2. Error: This is an invalid domain.

A red error message box with a white 'X' icon in the top right corner. The text inside reads: "Error: This is an invalid domain." data-bbox="109 182 374 197"/>

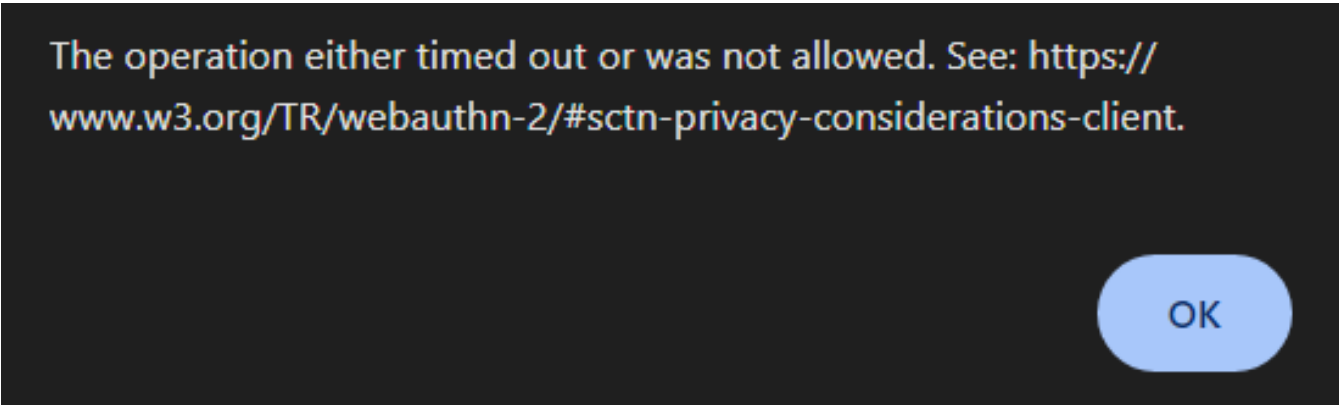
Ezeelogin needs to be accessed with a domain name to enable FIDO2 authentication, and accessing it via an IP address will not work.

3. Error: The operation either timed out or was not allowed. See: <https://www.w3.org/TR/webauthn-2/#sctn-privacy-considerations-client>.

A red error message box with a white 'X' icon in the top right corner. The text inside reads: "Error: The operation either timed out or was not allowed. See: https://www.w3.org/TR/webauthn-2/#sctn-privacy-considerations-client." data-bbox="102 341 870 355"/>

This error usually occurs when you cancel the setup of FIDO2 authentication. Try to re-setup and complete the FIDO2 authentication setup.

4. The operation either timed out or was not allowed. See: <https://www.w3.org/TR/webauthn-2/#sctn-privacy-considerations-client>.

A dark grey dialog box with white text. The text reads: "The operation either timed out or was not allowed. See: https://www.w3.org/TR/webauthn-2/#sctn-privacy-considerations-client." In the bottom right corner, there is a blue rounded button with the text "OK" in white. data-bbox="107 492 831 541"/>

This error usually occurs when you cancel the authentication prompt while trying to log in to the GUI. Refresh the browser tab or access Ezeelogin within a new tab to resolve the issue.

Related Articles:

[Disable two factor authentication from backend](#)

[Clear two factor authentication](#)

Online URL: <https://www.ezeelogin.com/kb/article/configure-fido2-with-ezeelogin-651.html>