



SUMMIT
ONLINE / 2021

TWO FACTOR AUTHENTICATION FOR ZABBIX

(THE POWER OF OPEN SOURCE)

■ **EVGENY YURCHENKO**

Co-Founder, BGmot Inc., Canada



Two factor authentication (2FA)

Why 2FA for Zabbix?

- increased security
- complying with corporate policies
- if Zabbix UI exposed to Internet it's a must

Two factor authentication (2FA)

- How does it work?

Two 2FA methods implemented:

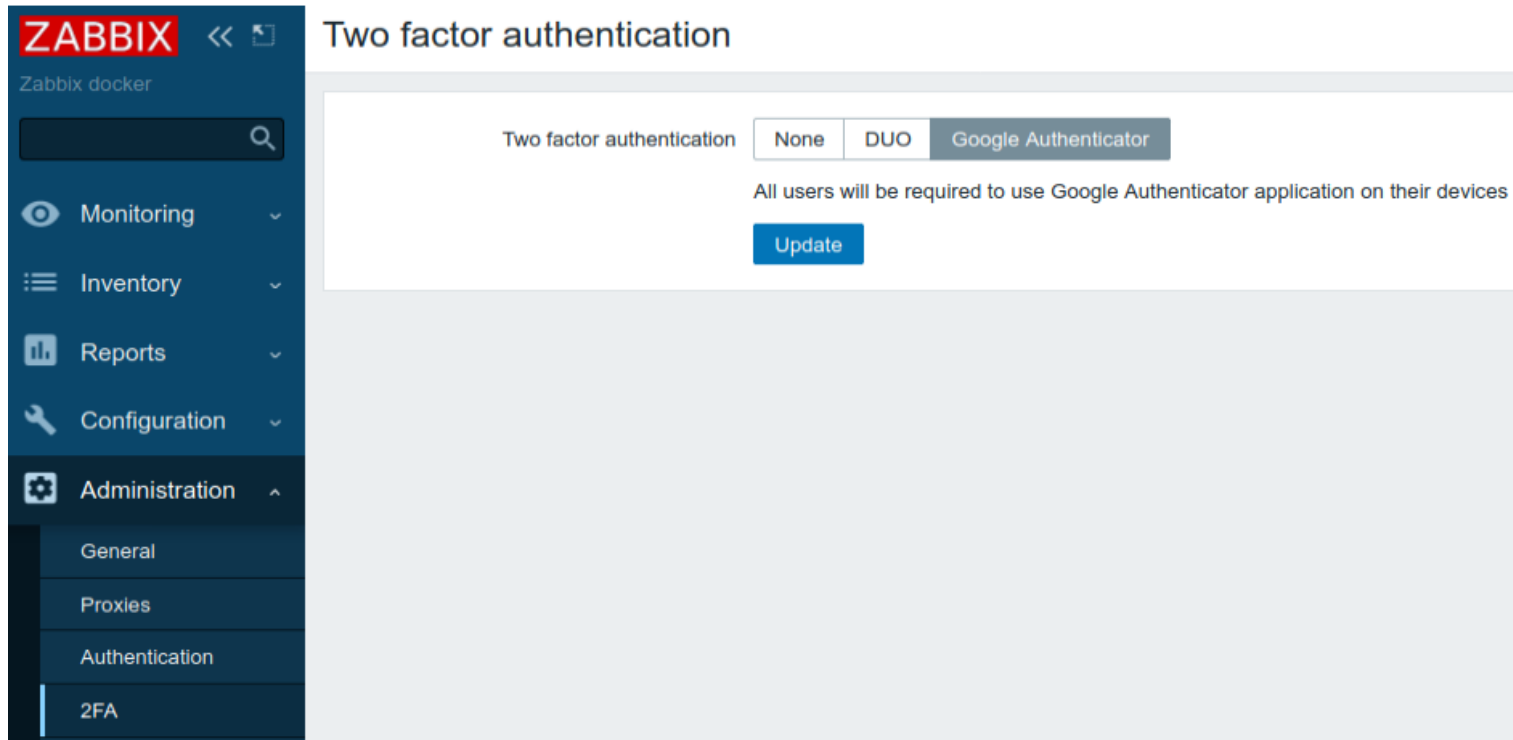
- using Google Authenticated application (simple)
- using DUO 2FA provider (sophisticated)

Regardless of method the workflow is the same:

- a user is authenticated using configured Zabbix logic (internal, LDAP etc)
- if previous step succeeds then the user is required to confirm his identity using registered device

2FA – Google Authenticator

- Enable 2FA in Zabbix UI. This is global setting, i.e. affecting all the users.



The screenshot displays the Zabbix web interface. On the left is a dark blue sidebar with the Zabbix logo and navigation menu items: Monitoring, Inventory, Reports, Configuration, Administration (expanded), General, Proxies, Authentication, and 2FA. The main content area is titled "Two factor authentication" and features three radio buttons: "None", "DUO", and "Google Authenticator". The "Google Authenticator" option is selected. Below the buttons, a message states: "All users will be required to use Google Authenticator application on their devices". An "Update" button is positioned below the message.

2FA – Google Authenticator

- When a user logs in for the first time

The diagram illustrates the process of enabling 2FA for a user logging in for the first time. It consists of two panels connected by a large blue arrow pointing from left to right.

Left Panel (Standard Login):

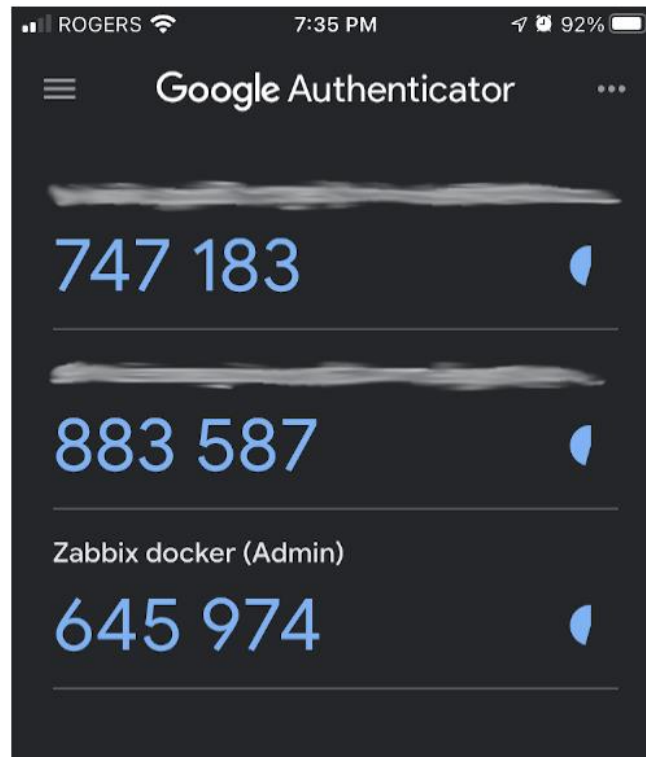
- Logo: **ZABBIX**
- Username field: Admin
- Password field: [Redacted]
- Remember me for 30 days:
- Sign in button
- or sign in as guest link

Right Panel (2FA Enrollment):

- Logo: **ZABBIX**
- Text: Scan this QR code in Google Authenticator app on your device to enroll in 2FA:
- QR code
- Text: Enter 6-digit code generated by Google Authenticator app on your device to complete authentication:
- Input field for 6-digit code
- Sign in button

2FA – Google Authenticator

- User scans QR code and his device gets “enrolled”



2FA – Google Authenticator

- From now on this user will have to enter only the one-time code generated by Google Authenticator application

The diagram illustrates the transition from a standard login form to a two-factor authentication (2FA) step. On the left, the ZABBIX login form includes fields for Username (Admin) and Password (masked with dots), a checked checkbox for 'Remember me for 30 days', and a 'Sign in' button. Below the button is a link for 'or sign in as guest'. A large blue arrow points to the right, where the 2FA step is shown. This step features the ZABBIX logo, the instruction 'Enter 6-digit code generated by Google Authenticator app on your device to complete authentication:', a small input field for the code, and a 'Sign in' button.

ZABBIX

Username
Admin

Password
.....

Remember me for 30 days

Sign in

[or sign in as guest](#)

ZABBIX

Enter 6-digit code generated by Google Authenticator app on your device to complete authentication:

Sign in

2FA - DUO

- Another method of performing 2FA is using third party service – DUO
- Benefits:
- DUO is widely used in many companies -> natural integration/adoption
- Users management/audit at DUO web site
- DUO application on your device provides much more flexibility in providing security confirmation: push-acknowledgement, voice call, SMS
- Up to 10 users for free
- More details at <https://duo.com/product/multi-factor-authentication-mfa/two-factor-authentication-2fa>

Two factor authentication (2FA)

- See demos and detailed instructions at:
- https://bgmot.com/zabbix_twofa_gglauth
- https://bgmot.com/zabbix_twofa_duo

Source code (available for 5.0 and 5.2 at this moment):
<https://github.com/BGmot/zabbix>

The code DOES NOT affect default Zabbix server behaviour!