

GAJSHIELD-DC SERIES

TWO FACTOR AUTHENTICATION GUIDE

Table of Contents

Manage Two Factor Authentication	1
Two-Factor Authentication on GajShield Firewall	1
How to Configure Two-Factor Authentication	2
Frequently Qsked Quentions (FAQ).....	3
Why two-factor authentication?	3
Why GajShield web management requires 2FA?	3
What if I forget my mobile at home?	3
What if I loose my mobile phone?	3
Can I setup 2FA for all the accounts used to manage the firewall? .	3
Can I change the timeout value used for email OTP?	4

Manage Two Factor Authentication

Enhance your security by enabling Two-Factor Authentication to manage GajShield Firewalls.

Two-factor authentication, or 2FA as it's commonly abbreviated, adds an extra step to your basic log-in procedure. Without 2FA, you enter in your username and password to log into your firewall. The password is your single factor of authentication. Second factor makes your account more secure. In our modern connect world, password is now the weakest link as passwords are easily stolen, either electronically or by social engineering techniques. Passwords are also easily guessable. Most often passwords are shared with colleagues and when they leave the organisation, these are not changed leading to compromising your network security.

Two-Factor Authentication on GajShield Firewall

You can use two-factor authentication to manage your firewall. Along with your password, One-Time-Password is used to login into your system. This can be enabled for all administrators who manage the firewall. For OTP (One Time Password) you can use 'Google Authenticator', a mobile app from Google. This app is available on major mobile platforms like iOS, Android etc.

SUPPORTED APPS	
Google Play	Google Authenticator , FreeOTP Authenticator , Authy 2 Factor Authentication .
Apple Store	Google Authenticator , Free OTP Authenticator , Authy 2 Factor Authentication .
Windows Store	Authenticator

Note

By default Two-factor authentication is not enabled on any administrative accounts on GajShield.

It is recommended that 2FA (Two Factor Authentication) is enabled for all Administrative accounts.

How to Configure Two-Factor Authentication

To enable Two-factor authentication, login into your firewall using your regular username and password. If you have not setup 2FA, you can ignore the OTP option. 2FA can be setup by 'superuser' for all administrators or for an individual administrator.

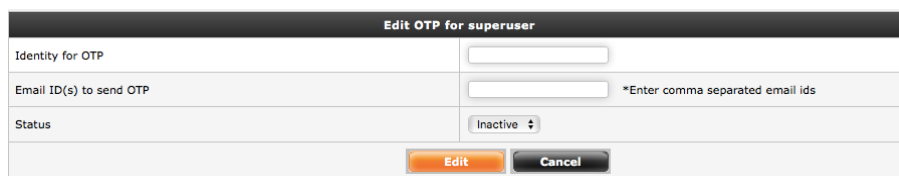
Prerequisite

GajShield firmware
version 2.6 and later

Note

You need to enable ntp services on your firewall for 2FA to work. Please look at GajShield Administrative Manual for further details to configure ntp.

1. **Click on Management – Administration – OTP Configure.** Edit the configuration of the administrator for whom you would like to configure OTP.



2. **Provide the identity for your OTP.** This can be any value which will help you to identify your OTP on the APP of your mobile phone.
3. **Email ID(s) to send OTP.** Provide the email address to which a one-time-password will be sent, incase the administrator does not have the 2FA app hdy.
4. **Status:** Activate your OTP configuration by selecting 'Active' option and click on 'Edit' to save the configuration. Click on 'Back' which will take you to the main screen as show below

OTP Type		Time Out	Tasks
OTP		30 Seconds	-
OTP on Email		300 Seconds	⚙️

Admin Name	OTP Identifier	Admin Email ID(s)	QR Code	OTP Authentication	Tasks
superuser	labfirewall	john@mycompany.com	Click to View the QR Code	Enabled	⚙️ ↺ 📧

5. Click on '**Click to View the QR Code**' to view the QR code generated. This QR code can then be used with your OTP app.



6. Configured administrator will require setup of 2FA app on their smart phone using the generated QR-code. For all future log on to firewall will require OTP.

Frequently Asked Questions (FAQ)

Why two-factor authentication?

Two-factor authentication is one of the best ways to protect against remote attacks such as phishing, credential exploitation and other attempts to takeover your accounts. Without your physical device, remote attackers can't pretend to be you in order to gain unauthorized access to corporate networks, cloud storage, financial information, etc. By leveraging something the user already has, allows a seamless and cost effective solution for Two Factor authentication to be implemented.

Why GajShield web management requires 2FA?

Responsibility of your firewall is to ensure the safety of your organisation. It protects your data not only from outsiders, but also prevents data leaks from inside your network. Password makes this device very vulnerable to attack. Most often it has been found that administrators do not change the default password or the password that was originally set. Also, times, it is easy to guess the password. The added layer of two-factor authentication prevents unauthorised access to your firewall. It is easy to setup and implement for every account that is used to manage the firewall

What if I forget my mobile at home?

If you forget your mobile, GajShield firewall can send you a one-time-password on email. This can be used only once to log into your firewall. This password is valid for timeout parameter, which is configurable through OTP-on-Email Timeout. By default, this is set to 300 seconds.

What if I loose my mobile phone?

If you loose your mobile phone, you can send a one-time-password on email. You can reconfigure 2FA on your new mobile. The OTP provided by the old firewall will no longer work.

Can I setup 2FA for all the accounts used to manage the firewall?

Yes, you can setup 2FA for each account separately. Each account will provide a different password on any given time and no account can use the password generated from 2FA setup for another account.

Can I change the timeout value used for email OTP?

The default timeout for an email OTP is 5 minutes. This can be changed to a timeout preferred by your organization with maximum limited to 30 minutes.