Multi factor Authentication (MFA)

Introduction

The Multi-Factor Authentication (MFA) service for Horizon adds an important extra layer of security to access your services. The MFA service is optional but can be made mandatory for all users or configured by admins on a user-by-user basis.

Why is MFA more secure?

Multi-factor authentication requires users to enter more login information than just a username and password. The Gamma MFA service adds an extra layer of security by requiring the user both to ‘know something’ (their regular password) and ‘have something’ (their mobile phone). Their mobile phone is identified through the use of the Time-Based One-Time Password (TOTP). This extra check makes it significantly more difficult for anybody to impersonate a given user.

For users who use biometrics (e.g. fingerprint or face recognition) to secure their mobile phones, a third factor of authentication is also added on the addition of TOTP, offering an even higher level of protection.

How does TOTP MFA work?

Time-based one-time password MFA is a method of verifying that the user who is attempting to log in has in their possession a particular mobile device that has been registered at set-up.

To identify the device, a unique, secret code is shared between the user’s Horizon account and an app on the user’s mobile device known as an authenticator app.

When the user logs in after registration, the MFA service must check that the user’s device ‘knows’ the same shared code as stored in the account at registration. The MFA system makes the comparison by using a secondary 6-digit MFA Code – created by combining the secret code with the current time and date. Both the registered mobile device and the Horizon account will generate the same MFA Code at any given time.

At log-in, the user must enter this MFA Code from their phone authenticator app. If the MFA Code from the authenticator app and the code generated in the Horizon account match at log in, the MFA service will authenticate the user.

For extra security, the MFA code is regenerated in both the Horizon account and the authenticator app, every 30 seconds.

Who can enable MFA and how is it turned on?

MFA is configured in the Horizon Portal at the company level, and only Company Administrators can amend the global settings. (Note that MFA is not currently configurable at Site level).

Company Administrators can enforce MFA for all users or make MFA optional for users, with a further option to make MFA mandatory for Administrators only. Where end-user MFA usage is set as optional, Company Administrators can then configure whether MFA is enabled for each user, as well as configure whether that individual can enable and disable their MFA for themselves.

Company Administrators (and end users with the relevant permissions) can also reset MFA. Whenever MFA is reset or disabled and then re-enabled, the end user will need to re-register.

Note that Channel Partners and Gamma Support will still be able to access the Horizon Portal via the existing SSO route without an MFA challenge.

How do end users configure MFA?

If MFA is enabled for a given user, they must register their MFA on their next login, using their mobile phone.

This will involve the user first downloading and launching an authenticator app. Microsoft Authenticator, Google Authenticator or most other common authenticator apps will all be suitable.

The user will be asked to scan a QR code which will be displayed on the Horizon portal. Once successfully scanned, a 6-digit password (MFA Code) will be generated in the authenticator app which the user must key into the Horizon portal. This will complete the setup process.

Thereafter, at login, after entering their regular username and password, the user will be asked to key in the 6-digit MFA Code generated by their authenticator app.

Please note that Collaborate of Softphone users must be on the latest version of the Collaborate apps to use MFA.

What emails will the MFA service send to end users?

When a Company MFA setting is changed by a Company Administrator, all Company Administrators will receive an email to notify them of the new setting.

Please note that end users will NOT receive an email when Company level settings are changed. For example, if MFA is made mandatory for all users, an email will not automatically be sent by Horizon to each user. You may wish to prepare users with tailored communications before any mass enablement as, in the case of full company switch-on, users will not be able to bypass the registration process and will be unable to log in to Horizon / Collaborate until registration has been completed.

Individual users will only receive automatic emails from Horizon when MFA settings for their account have been changed by an Administrator. This will only occur when MFA has been set to Optional at Company Level – which permits MFA configuration to be adjusted for individual users.

What services are available to assist?

Within both the Horizon and Collaborate user interfaces are ‘help’ prompts that will launch assistance information about the current screen when pressed. These will assist your users in registration for MFA.

More information can be found in the MFA section of the Knowledgebase, accessible via the Gamma Academy.