Multi-Factor Authentication (MFA) FAQs

What does MFA cover?

MFA is designed to secure access to the Horizon user and Admin portals and Collaborate apps, additional portals, such as Business and Complaint Call recording,
Akixxi, and the client bolt- ons apps such as Receptionist, Call Centre clients, and Integrator which operate alongside these, are presently not within the current scope
of MFA.

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.

How does MFA integrate?

Our MFA solution seamlessly integrates with our platform to enhance the security of customers’ logins. Users can opt to enable MFA for an additional layer of
protection.

Is there a recommended authenticator for users?

We do not favour any authenticator app and are open to supporting any app that is Time-based One-Time Password (TOTP) compatible.

Has MFA an additional cost?

No, Multi-Factor Authentication (MFA) is provided as a complimentary layer of security to Horizon and Collaborate. We believe in enhancing the security of your communications without adding extra financial burden.

Is MFA mandatory for users, or is it optional?

MFA is entirely optional for UCaaS customers. While we highly recommend its use for increased security, organizations can choose whether or not to enable MFA based on their specific security policies and preferences.

How can our customers activate MFA for their UCaaS accounts?

Activating MFA is a straightforward process that can initiated from account settings. We provide step-by-step guides and support resources to assist users in setting up MFA on Gamma Academy.

What benefits does MFA bring to users?

MFA adds an extra layer of security to your logins, reducing the risk of unauthorised access. This is particularly crucial for protecting sensitive communication data, ensuring the privacy and confidentiality of our customers' conversations.

Can MFA be applied to only part of the users?

Yes, our MFA solution provides flexible options to accommodate different user preferences and security requirements. Organizations can choose from the following MFA settings based on their needs:

o MFA Disabled (Previous default setting): This is the default option where MFA is not enforced, and users can continue with their existing authentication method.

o MFA Enabled (User opt-in): Individuals have the choice to enable MFA for their accounts. Users can opt for an extra layer of security if they desire.

o MFA Enabled (Forced for admins): All administrator-level users are required to validate via MFA. MFA remains optional for non-admin users, providing an added layer of protection for critical accounts.

o MFA Enabled (Forced for all users): In this setting, all users, including administrators and non-

administrators, are required to validate using MFA. This option
ensures a uniform and elevated level of security across the entire user base.

Do clients need to be updated to the latest version of Collaborate?

Yes, users will need to have the latest version of Collaborate to take advantage of the multi-factor authentication (MFA) feature. This ensures optimal compatibility
and access to the enhanced security features provided by MFA.

Can we provide training or support for customers adopting MFA?

Absolutely. We encourage channel partners to offer guidance and support to customers during the MFA adoption process. Our customer service operations team is
also available to assist with any questions you may have.

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 Gamma Academy Knowledge Base, accessible via the Gamma Academy.

Where can I find support regarding the setup process?

Support for the setup process is available on the Gamma Academy.