

Horizon

Multi-Factor Authentication



Contents

Setting Up Multi-Factor Authentication	3
<i>Note On Automatic Emails</i>	4
Managing User Multi-Factor Authentication	4
Logging Into The Horizon Portal Using Multi-Factor Authentication	6
Logging Into Collaborate Using Multi-Factor Authentication.....	8
<i>First Time Login</i>	8
<i>Subsequent Logins</i>	9

Setting Up Multi-Factor Authentication

1: Log in to Horizon using your Horizon credentials:

Horizon Uat Login

Username:

Password:

☒ Remember Me

[Forgot Password](#)

Please note that only individuals who have a Horizon account and authorised access to the Horizon Portal should proceed beyond this point. For the security of customers, any unauthorised attempt to access Horizon information will be monitored and may be subject to legal action. Customers are reminded to keep their customer login information confidential and secure and to contact their Reseller immediately if they are aware someone else knows their login details.

2: Provided the user has the correct credentials, select 'Administration' and select the 'Manage MFA' option from the drop-down.

3: In the 'Company MFA Settings' section, select from the drop-down the option relevant to your organisation:

Dashboard / Administration / Manage MFA

Manage MFA

The multi-factor authentication (MFA) used by Horizon is compatible with most smartphone authenticator apps. Please ensure users have an appropriate device and authenticator app before enabling.

Company MFA Settings

Company MFA: MFA Disabled

Manage Voice

To enable MFA for end users please search for their account on the [user search](#). MFA options are within the 'permission' tab when editing a user.

Manage Admin MFA

Username	Admin Type	First Name	Last Name	Email Address	Enabled	Status
ITAdmin1597299921811	Company Admin	firstName	lastName	admin@email.com	✖	Disabled <input type="button" value="Enable MFA"/>

- MFA Disabled
- MFA Available (optional for all users)
- MFA Administrator (mandatory for Admin users)
- MFA Enabled (mandatory for all users).

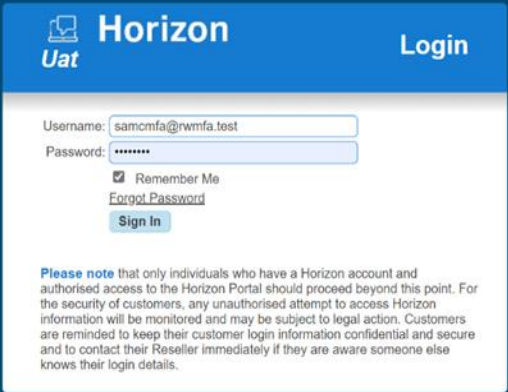
4: Click 'Save'.

Note On Automatic Emails

When the 'Global Settings' above are changed, notification emails will only be sent to company administrators. No emails will be sent to individual users or site administrators.

Managing User Multi-Factor Authentication

1: Log in to Horizon using your Horizon credentials:



Horizon Uat Login

Username: samcmfa@rwmfa.test

Password: *****

☒ Remember Me

[Forgot Password](#)

[Sign In](#)

Please note that only individuals who have a Horizon account and authorised access to the Horizon Portal should proceed beyond this point. For the security of customers, any unauthorised attempt to access Horizon information will be monitored and may be subject to legal action. Customers are reminded to keep their customer login information confidential and secure and to contact their Reseller immediately if they are aware someone else knows their login details.

2: Provided the user has the correct credentials, select 'Users' and then select 'List Users' from the drop-down.

3: Select the relevant name on the list of users, and select 'Edit':

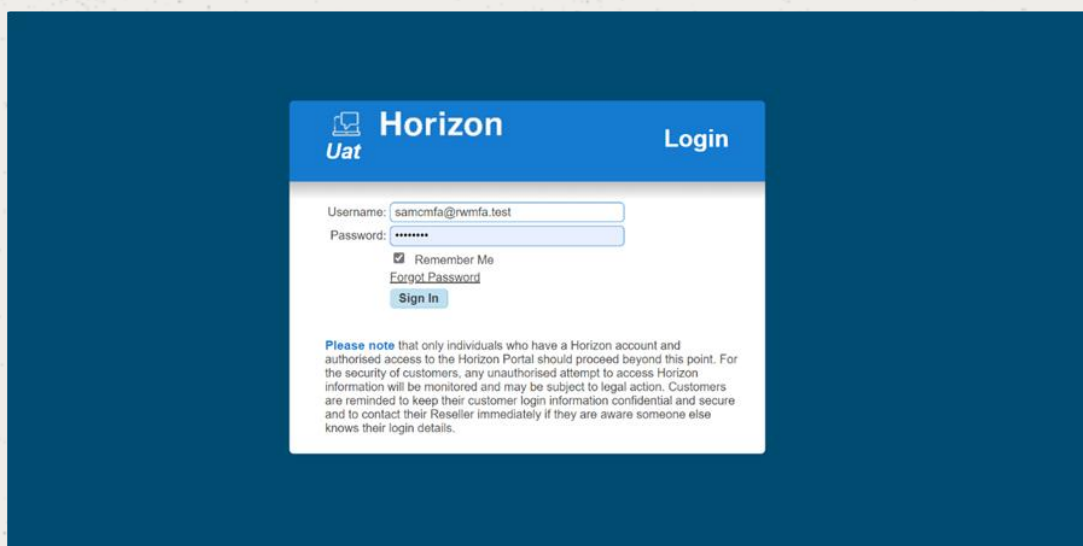
The screenshot shows the 'User Management' page in a web application. The top navigation bar includes 'Dashboard', 'Users', 'Site Management', 'Call Groups', 'Device Management', 'Administration', 'Recorded Calls', and 'Statistics'. The 'Users' tab is active. Below the navigation bar, the page title is 'Dashboard / User Management'. The main section is titled 'User Management' and contains a form for adding or editing a user. The form has fields for 'First Name', 'Last Name', 'Username', 'Number', 'Extension', 'Department', 'Site', and 'Mac Address'. The 'Username' field is pre-filled with 'itdomain1597299921811.com'. The 'Department' dropdown is set to 'All'. Below the form is a 'Search' button. Under the 'Users' section, there is a table with columns: 'First Name', 'Last Name', 'Phone Number', 'Extension', 'Email Address', and 'Site'. The table contains one row with the user 'test' and email 'user@email.co.uk'. An 'Edit' button is next to the user entry. At the bottom of the table, there are buttons for 'Delete Selected', 'Add', and 'Download'.

4: Select 'Permissions' on the user's profile, then toggle the 'This user login requires MFA' on or off, depending on the requirements. If you want to allow a user to enable, disable or reset their own MFA via their Horizon User Portal, then toggle the 'This user can enable, disable, and reset their own MFA' on. Click 'Save'.

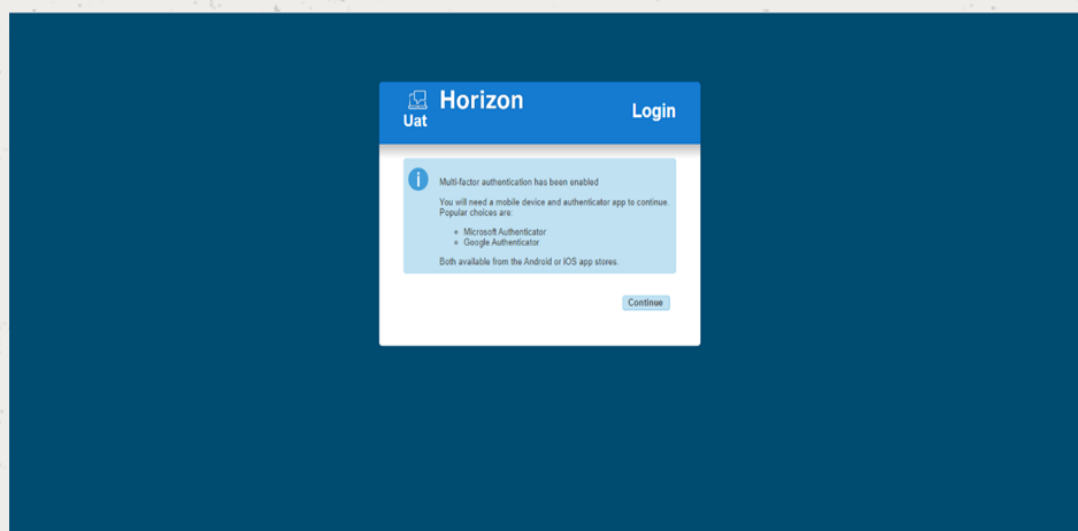
The screenshot shows the 'Edit User' page for a user named 'test'. The top navigation bar is the same as in the previous screenshot. The page title is 'Dashboard / User Management / Edit User'. The main section is titled 'Edit test test'. Below the title is a tabbed interface with tabs: 'Profile', 'DDI', 'Services', 'Call Setup', 'Permissions', 'Phone', 'Barring', and 'Call Centre'. The 'Permissions' tab is active. The 'Access and Permissions' section contains five toggle switches, all currently set to 'off': 'This User can enable Call Forwarding', 'This User can use Advanced Call Setup', 'This User can use CLI presentation', 'This User can use Profiles', and 'This User can use Remote Office'. The 'MFA Settings' section contains two toggle switches: 'This user login requires MFA' (set to 'off' with a note '(Status: Disabled)') and 'This user can enable, disable, and reset their own MFA' (set to 'off'). A 'Save' button is at the bottom right of the page.

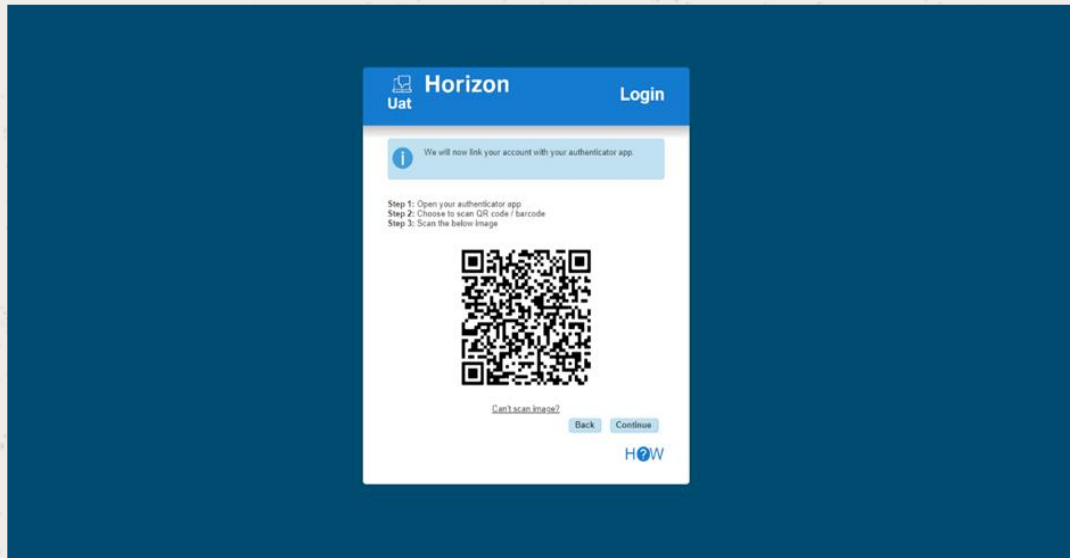
Logging Into The Horizon Portal Using Multi-Factor Authentication

1: Log in to Horizon using your Horizon credentials. To log in using MFA, you will need to download an authenticator application to complete the log in:

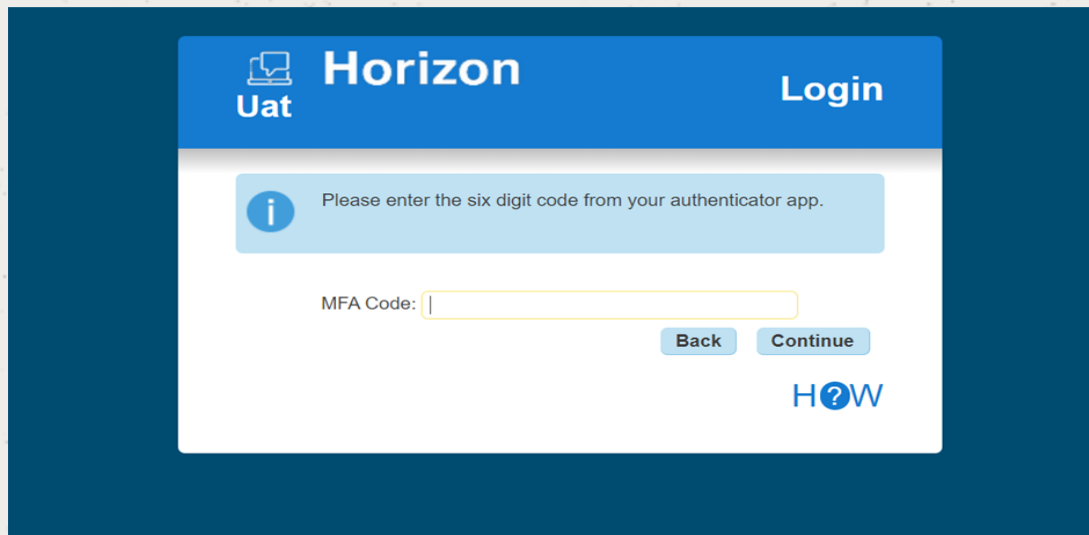


2: You will be prompted to use your mobile device to complete log in if MFA has been enabled. Follow the directions from the following screenshots to ensure you can access the secure passcode:





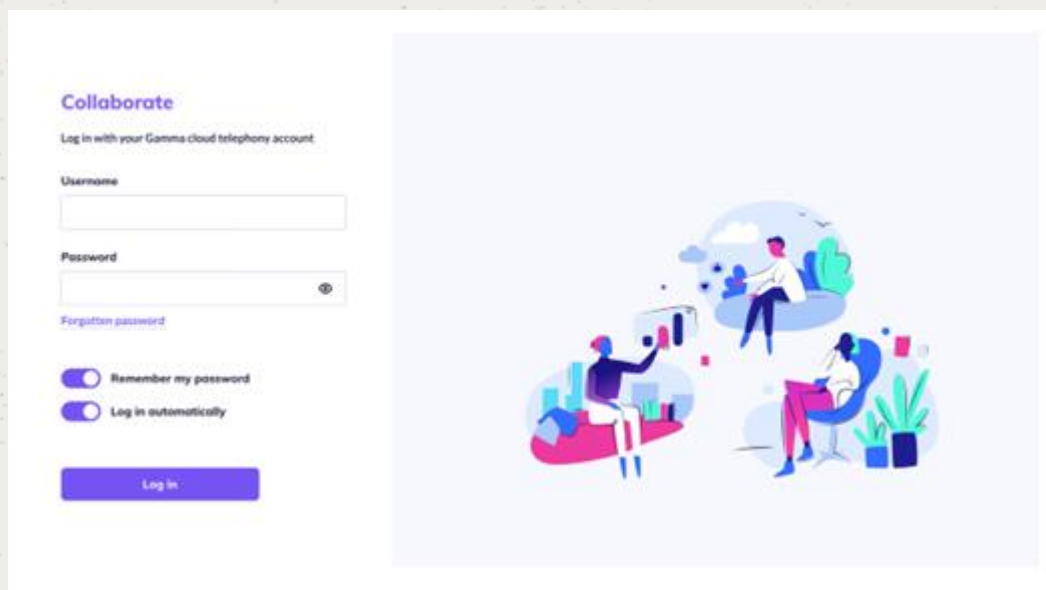
3: Enter your secure passcode from your Authenticator app, and click 'Continue':



Logging Into Collaborate Using Multi-Factor Authentication

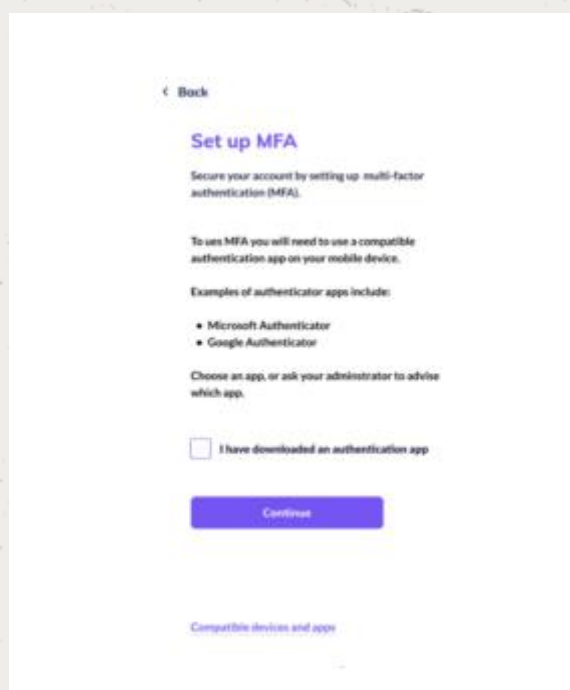
First Time Login

1: Log in to Collaborate using your existing credentials:

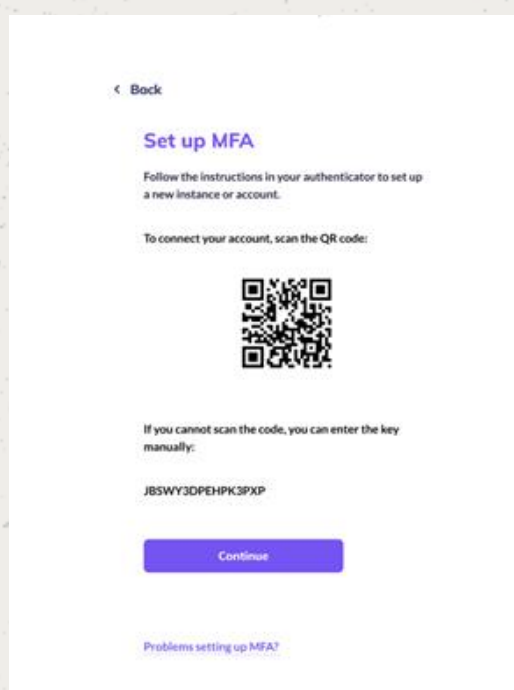


The image shows the Collaborate login interface. On the left, there is a login form with the following elements: the 'Collaborate' logo, the text 'Log in with your Gamma cloud telephony account', a 'Username' input field, a 'Password' input field with an eye icon for toggling visibility, a 'Forgotten password' link, two toggle switches for 'Remember my password' and 'Log in automatically', and a 'Log in' button. On the right, there is a large illustration of three people in a modern office setting, one standing and pointing at a screen, another sitting at a desk, and a third sitting in a chair, all engaged in collaborative work.

2: For first time log in to Collaborate – Users will be prompted to download an authenticator app and follow the instructions for set up:

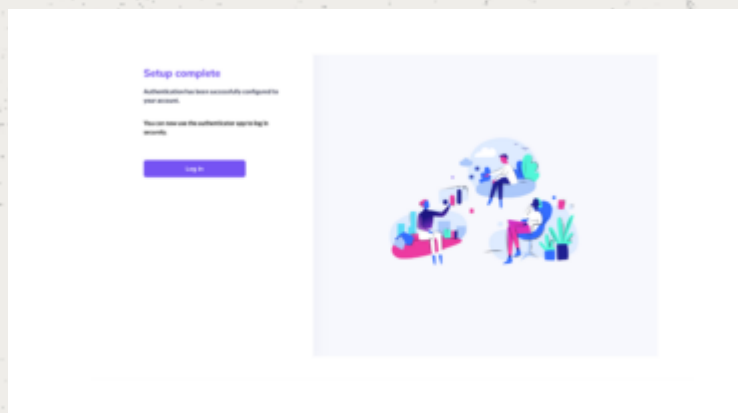


The image shows the 'Set up MFA' screen on the left. It includes a 'Back' link, the title 'Set up MFA', and instructions to secure the account by setting up multi-factor authentication (MFA). It states that a compatible authentication app is needed and lists examples: Microsoft Authenticator and Google Authenticator. A checkbox labeled 'I have downloaded an authentication app' is present, followed by a 'Continue' button. A link for 'Compatible devices and apps' is at the bottom.



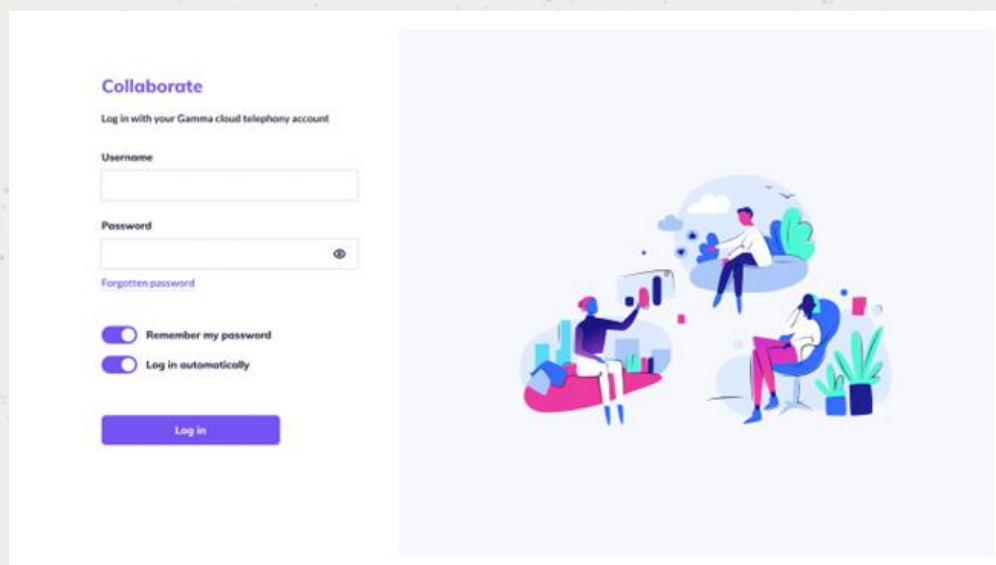
The image shows the 'Set up MFA' screen on the right. It includes a 'Back' link, the title 'Set up MFA', and instructions to follow the authenticator's instructions. It prompts the user to scan a QR code to connect their account. A QR code is displayed in the center. Below it, a manual entry option is provided with the text 'If you cannot scan the code, you can enter the key manually:' followed by the key 'JBSWY3DPEHPK3PXP' and a 'Continue' button. A link for 'Problems setting up MFA?' is at the bottom.

3: Once your authenticator has been set up you will be able to log into Collaborate using MFA:

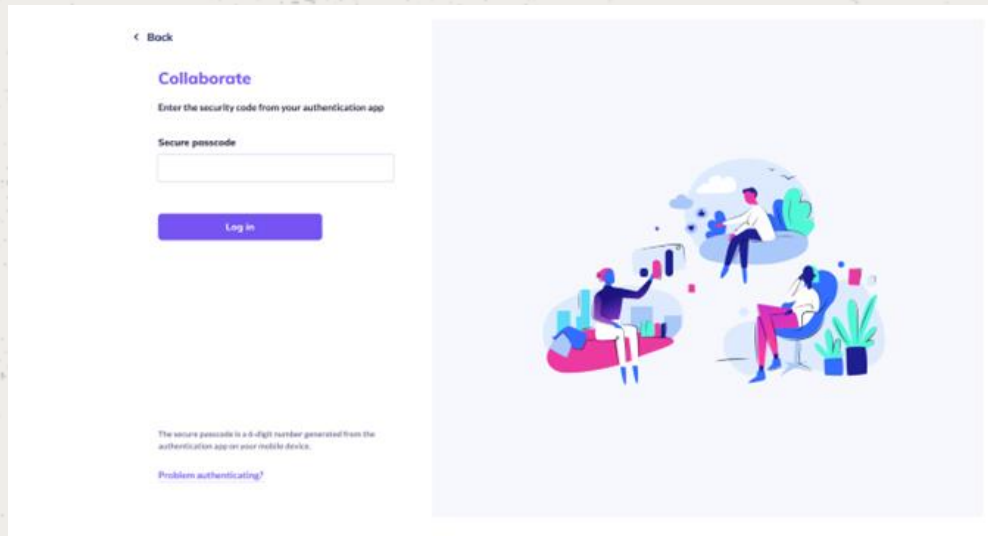


Subsequent Logins

1: Log in to Collaborate using your Collaborate credentials:



2: Enter your secure passcode from the authenticator app and access Collaborate:



The screenshot displays the 'Collaborate' login interface. On the left, there is a white card with a 'Back' link at the top. Below it, the word 'Collaborate' is written in purple. The instruction 'Enter the security code from your authentication app' is followed by a 'Secure passcode' label and a text input field. A purple 'Log in' button is positioned below the input field. At the bottom of the card, a small note explains that the secure passcode is a 6-digit number generated from an authentication app, and a link for 'Problem authenticating?' is provided. To the right of the card is a large, light blue illustration depicting three stylized figures in a collaborative work environment, with one person standing and pointing at a screen while others sit and observe.