

Horizon

Multi-Factor Authentication

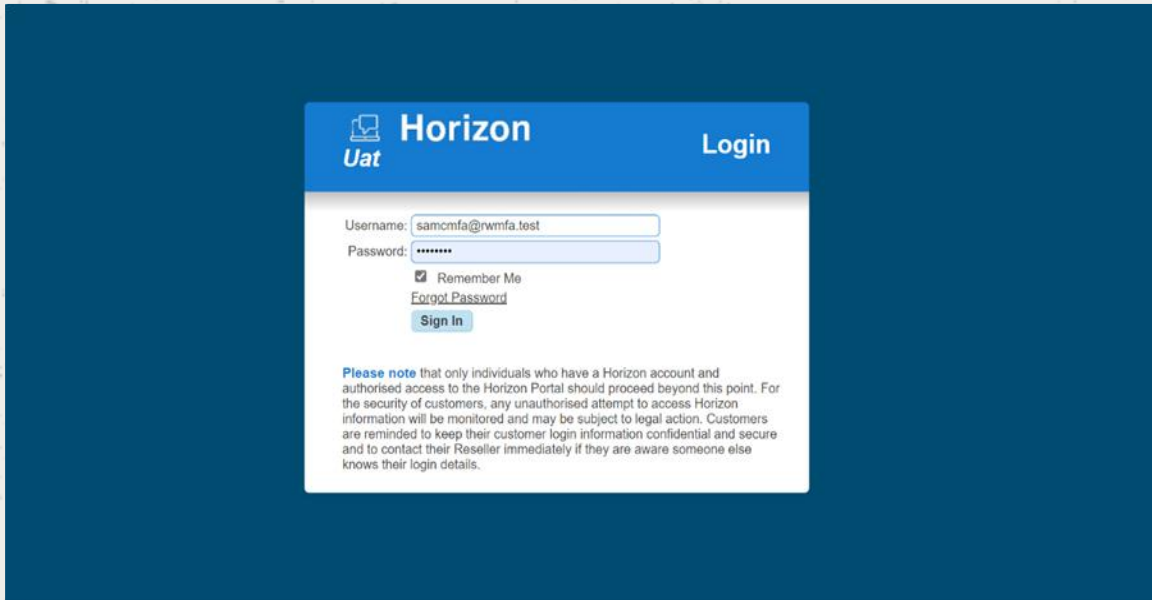


Contents

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

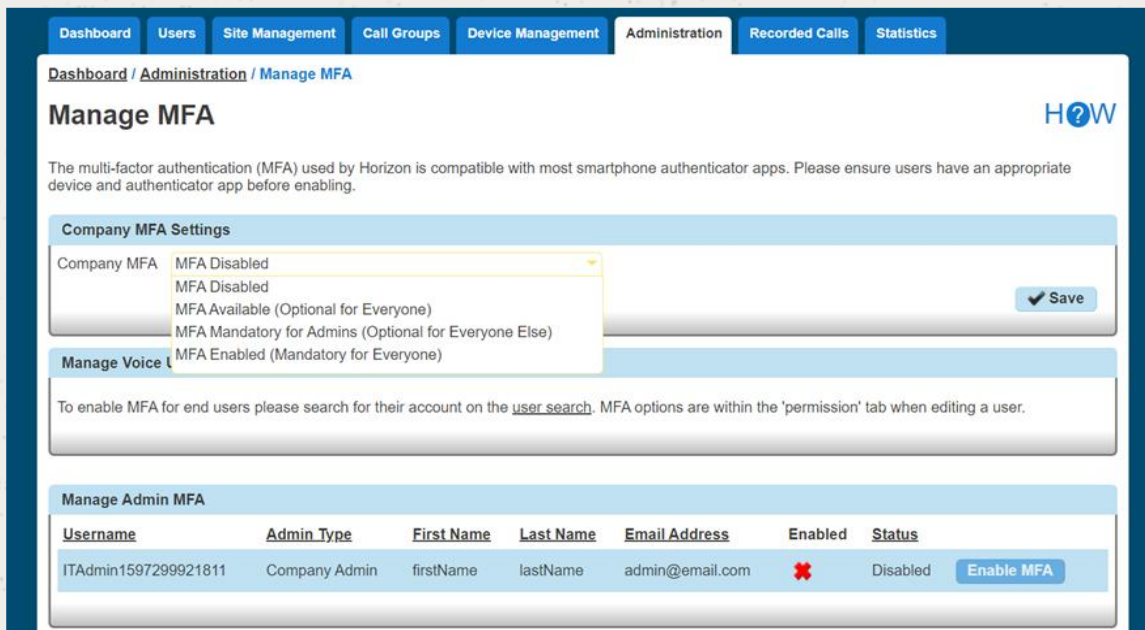
Setting Up Multi-Factor Authentication

1: Log in to Horizon using your Horizon credentials:



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:



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

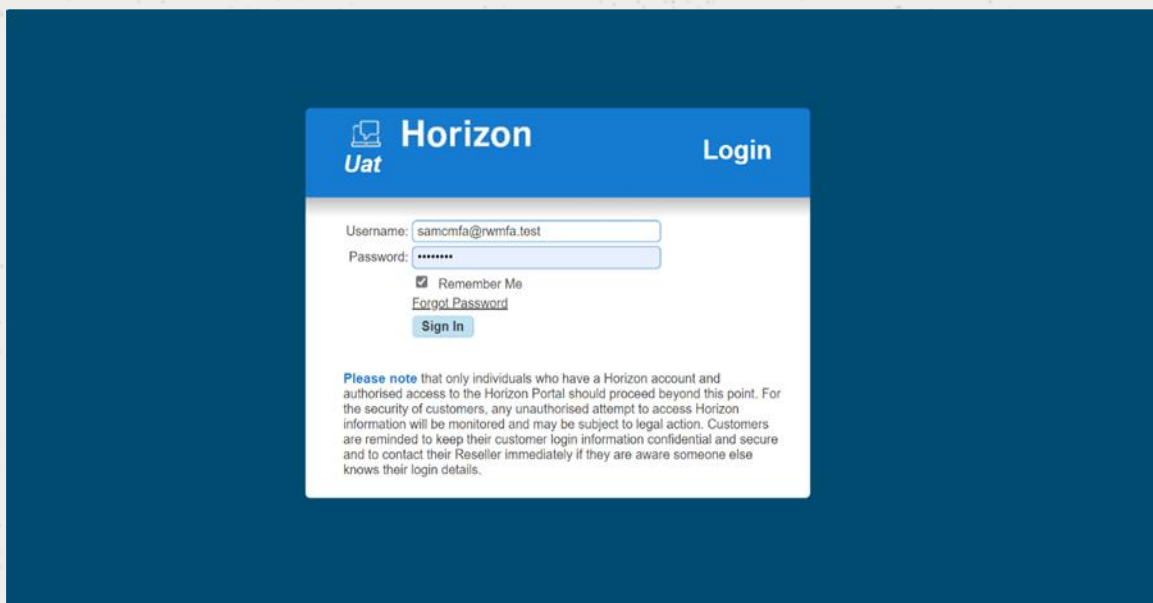
4: Click 'Save'.

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:



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':

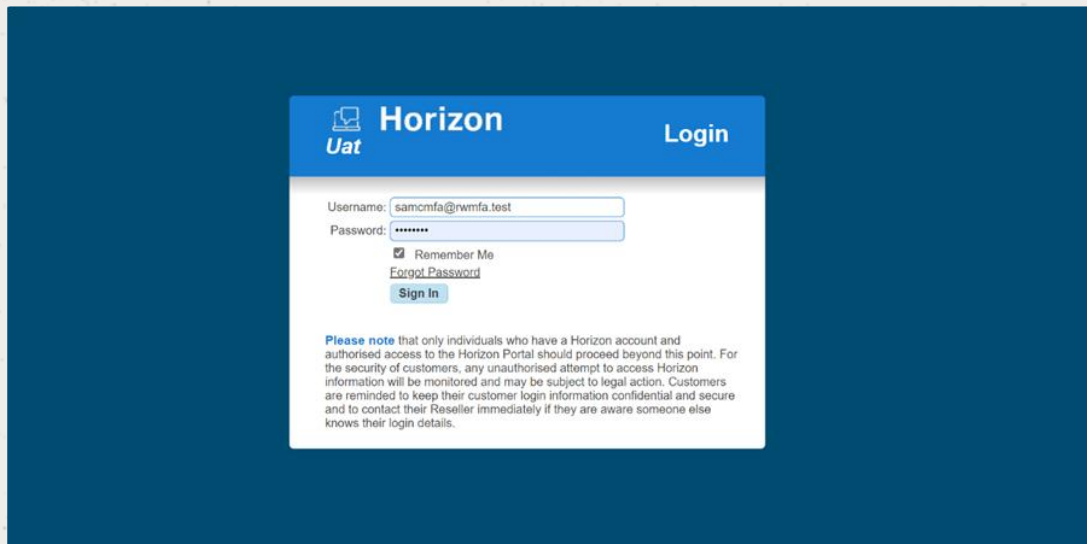
The screenshot shows the 'User Management' page in a web application. At the top, there is a navigation bar with tabs: Dashboard, Users, Site Management, Call Groups, Device Management, Administration, Recorded Calls, and Statistics. Below the navigation bar, the page title is 'Dashboard / User Management' and the main heading is 'User Management'. There are several input fields for user details: First Name, Last Name, Username (with a domain suffix 'itdomain1597299921811.com'), Extension, Site (dropdown menu), Number, Department (dropdown menu), and Mac Address. A 'Search' button is located below the input fields. Below the search section, there is a table of users with columns: First Name, Last Name, Phone Number, Extension, Email Address, and Site. The table contains one user entry: 'test' with email 'user@email.co.uk' and site 'ITSite1597299921811'. 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'.

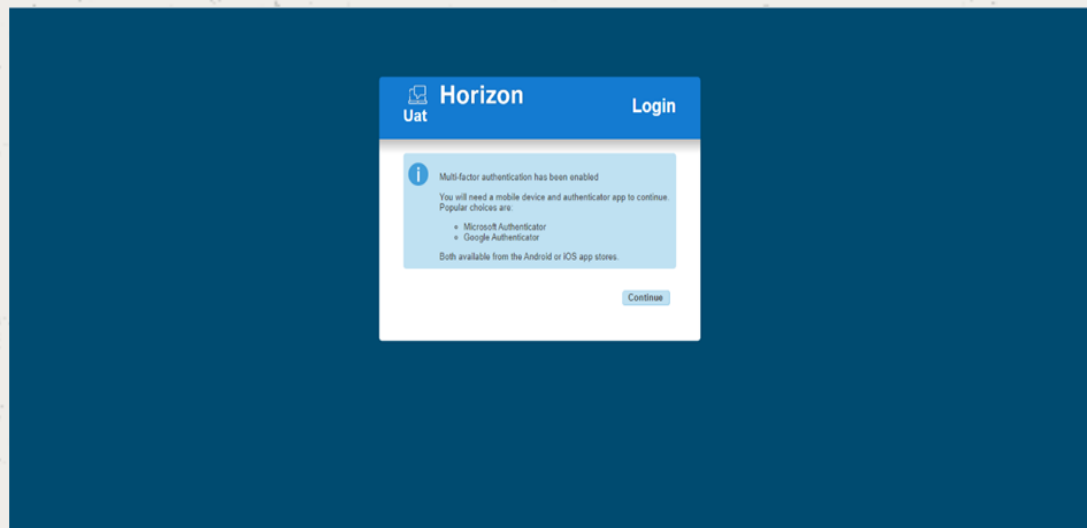
The screenshot shows the 'Edit User' page in a web application. At the top, there is a navigation bar with tabs: Dashboard, Users, Site Management, Call Groups, Device Management, Administration, Recorded Calls, and Statistics. Below the navigation bar, the page title is 'Dashboard / User Management / Edit User' and the main heading is 'Edit test test'. There are several tabs for user profile: Profile, DDI, Services, Call Setup, Permissions, Phone, Barring, and Call Centre. The 'Permissions' tab is selected. Below the tabs, there is a section titled 'Access and Permissions' with five toggle switches: 'This User can enable Call Forwarding' (off), 'This User can use Advanced Call Setup' (off), 'This User can use CLI presentation' (off), 'This User can use Profiles' (on), and 'This User can use Remote Office' (on). Below this section, there is a section titled 'MFA Settings' with two toggle switches: 'This user login requires MFA' (on, Status: Disabled) and 'This user can enable, disable, and reset their own MFA' (off). A 'Save' button is located at the bottom right of the page.

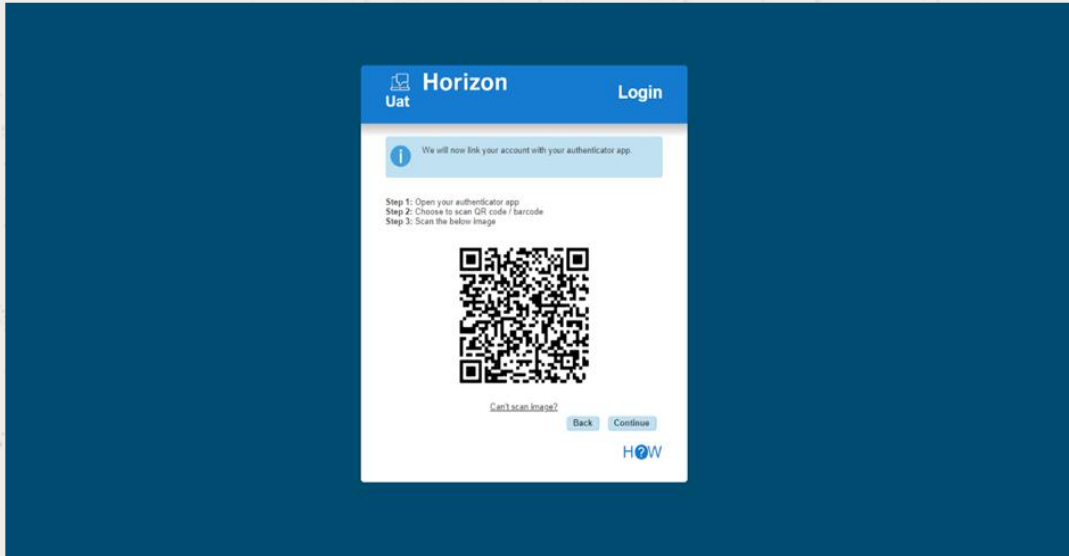
Logging Into The Horizon Portal Using Multi-Factor Authentication

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':

