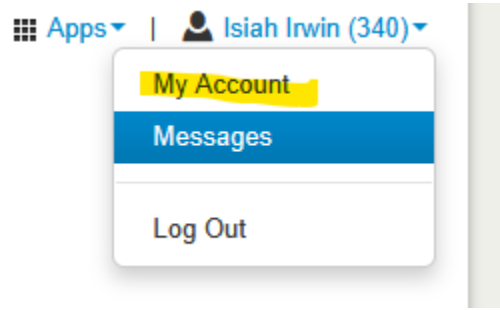


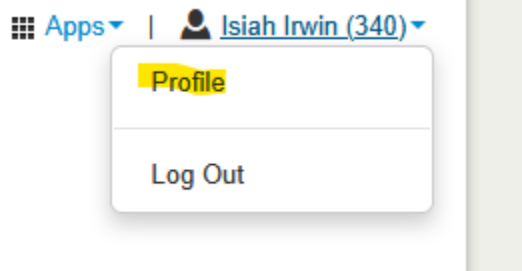
Multi-Factor Authentication (MFA) on the Manager Portal

PROCESS

- Log into the Production HPBX Manager Portal.
- Click on the down arrow next to your name in the top right corner of the screen & click on “My Account”.



- Click on the down arrow in the top right corner of the screen again & click on “Profile”.



Multi-Factor Authentication (MFA) on the Manager Portal

- On the “Profile” Screen click on “Set Up Google Authenticator”.

(Please note, any Time-based One Time Password (TOTP) authenticator should work; for example, Authy, Google Authenticator, LastPass Authenticator, etc. ITC has successfully tested with Google Authenticator and DUO,

Change Account Security

Email Address(es)

placeholder@hpbx.com



Multi-Factor Authentication

 Set Up Google Authenticator

MFA only applies to the user/password login method and will be bypassed by SSO. You will need to download the Google Authenticator app to use this feature.

New Password

Confirm New Password

Minimum length of 8 characters, minimum of 1 capital letter(s), minimum of 1 number(s), minimum of 1 special characters(s), Your extension cannot be part of your password.

Current Password

Your current password is required to update your email address or security information.

Change Voicemail PIN

Multi-Factor Authentication (MFA) on the Manager Portal

- After clicking on “Set Up Google Authenticator” a QR code should be displayed. Scan the QR code with the Authenticator app on your phone. This should add the entry “HPBX_Manager_Portal” in your Authenticator app. Type in your “Current Password” (i.e. Manger Portal Password) & type in the “Passcode” from your Authenticator app for the new entry. Click save.

Multi-Factor Authentication



Scan this QR code with the Google Authenticator app.

WARNING: This code will not be accessible after finishing set up!

Passcode

Enter the passcode generated in Google Authenticator.

New Password

Confirm New Password

Minimum length of 8 characters, minimum of 1 capital letter(s), minimum of 1 number(s), minimum of 1 special characters(s), Your extension cannot be part of your password.

Current Password

Your current password is required to update your email address or security information.

Change Voicemail PIN

Multi-Factor Authentication (MFA) on the Manager Portal

If the Authenticator App was set up successfully, you should see a “Google Authenticator enabled” button appear.

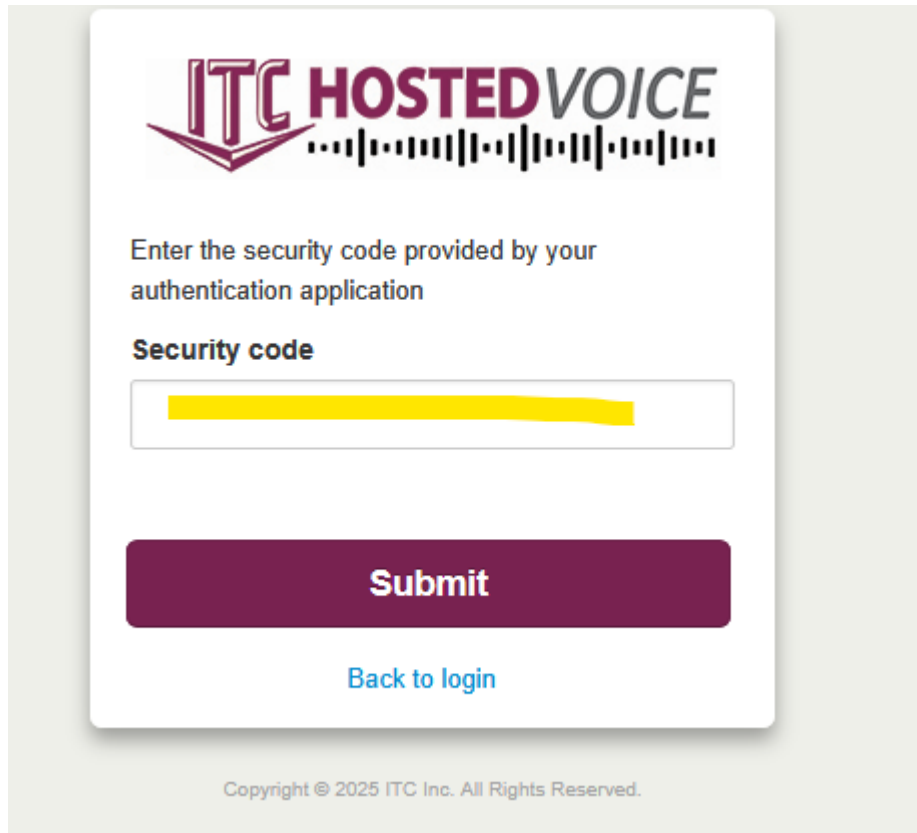
Multi-Factor Authentication	 Google Authenticator enabled 
New Password	
Confirm New Password	 Minimum length of 10 characters, minimum of 1 capital letter(s), minimum of 1 number(s), minimum of 1 special characters(s), Your extension cannot be part of your password.
Current Password	 Your current password is required to update your email address or security information.

Change Voicemail PIN

New PIN	
	Minimum length of 4 characters, your extension cannot be part of your password.

Multi-Factor Authentication (MFA) on the Manager Portal

- This can be tested by logging out of the Manager Portal. When attempting to log back in, you should be met with prompt requiring a code from your authenticator app.



The screenshot shows a login interface for ITC Hosted Voice. At the top is the logo, which consists of the letters 'ITC' in a stylized font next to the words 'HOSTED VOICE'. Below the logo is a prompt: 'Enter the security code provided by your authentication application'. Underneath this is a label 'Security code' followed by a text input field containing a yellow bar. Below the input field is a large purple button labeled 'Submit'. At the bottom of the form is a blue link that says 'Back to login'. At the very bottom of the page, there is a small copyright notice: 'Copyright © 2025 ITC Inc. All Rights Reserved.'

ITC HOSTED VOICE

Enter the security code provided by your authentication application

Security code

Submit

[Back to login](#)

Copyright © 2025 ITC Inc. All Rights Reserved.