Heartland

Restaurant

Multi-Factor Authentication FAQ

Table of Contents

Date	Product Version	Author	Summary
03/12/2024	9.25	JWD	Original article introduced.

Multi-Factor Authentication (MFA) FAQ

Will MFA apply to the Essentials and Complete products? Mobilebytes?

Yes, we have enabled multi-factor authentication in both the Essential and Complete editions of Heartland Restaurant, as well as Mobilebytes.

Will MFA apply to Global Payments Restaurant (Canada)?

Yes, we have also enabled multi-factor authentication in Global Payments Restaurant.

Is there an "opt out" option?

No, all users are required to use multi-factor authentication when logging into the Admin Console, POS, KDS, and Kiosk.

What apps now require multi-factor authentication?

Anyone who logs into the Admin Console must now acquire and enter an MFA authentication code.

The POS, KDS, and Kiosk apps also now require MFA authentication codes to log in.

Does MFA impact Online Ordering or the Guest App?

As of the current version, Online Ordering and the Guest app do not use or require multi-factor authentication.

Will restaurant staff be required to use authentication codes to access the POS?

No. Once a dealer or manager logs into the POS, restaurant staff will access the PIN screen and enter their PIN numbers as they always have. When clocking in, they will experience no difference in the process.

However, any restaurant staff that uses the Admin Console will be required to use authentication codes to log in, just like any dealer.

Will this impact both new and existing Heartland Restaurant merchants?

Yes, both new and existing merchants are required to use multi-factor authentication to log into the Admin Console, POS, KDS, and Kiosk.

How do we sign up for MFA if we are not already enrolled?

Manual enrollment is not required. Any user who logs into the Admin Console will be automatically enrolled into the MFA service.

Will our login passwords expire? If so, how often will we need to reset them?

Login passwords will not expire. We have made no changes to login password expiration. Multi-factor authentication just requires you to enter an additional code after logging in.

How often will the Admin Console request an authorization code?

When you first enter a new authorization code, you can ask the program to “remember” it for up to 45 days. Afterwards, when logging in with the usual email and password credentials, the Admin Console will not request an authorization code again until the first code’s 45-day time period has elapsed.

How do I receive authorization codes from the Admin Console?

The first time you use multi-factor authentication, the program will email the authorization code to you. Afterwards, the program will let you choose to receive each new code by text message, email, or from a third-party authenticator app (Authy, Microsoft Authenticator, or Google Authenticator).

How long will POS/KDS/Kiosk authorization codes be valid?

For merchants, new authorization codes remain valid for one (1) hour.

For dealers and Support staff, new authorization codes remain valid for twelve (12) hours.

Can an authorization code be used more than once?

While it is valid, you can use the same authentication code to log into multiple authorized tablets and apps.

Is there a login timeout period on POS, KDS, or Kiosk?

We have added no automatic timeout durations for permanent logins to POS, KDS, or Kiosk. They will remain logged in until a user forces a log out, clears the app's data, or uninstalls the app.

What if I reset an existing registered device to its factory settings and reinstall the POS?

To log into a newly installed POS on a reset device, you will need a valid authentication code.

What if a device gets logged out and none of the staff can access the Admin Console?

If restaurant staff need to log back into an instance of the POS, KDS, or Kiosk app, but they cannot access the Admin Console to acquire a new authorization code, they can request a temporary login code for that location from either the dealer or the Heartland Support department.

Can I use the same authorization code for multiple device logins?

Yes. While valid, you can use one authorization code to log into multiple devices and apps.

If I delete a device from authorized tablets to add a new one, will I need a new code to add the device?

Authorization codes are associated with locations, not specific apps or devices. So long as the code is valid, you can use it to add one or more new devices. Once a code expires (one hour after it was generated), you will need to acquire a new code to add more devices.

Do we need to add any URLs to the network's whitelisting document?

As of now, no new URLs have been identified.

At what point will MFA be required?

Once MFA is enabled, you will be prompted for an authentication code the next time you log into a POS. For devices, we are trying to preserve the connection. Devices will not be disconnected unless they force their iPads to log out.

Do I need separate codes for each product (POS, KDS, and Kiosk)?

No, you do not need separate codes. Multi-factor authentication is not tied to a merchant’s license, but to a location’s data. Therefore, you can use a single authorization code to log into the POS, KDS, and Kiosk apps.

What is the format of Device Licensing Codes?

Device Licensing Codes consist of six alpha-numeric characters.