MasterCard Worldwide

MasterCard smartdata.gen2™

May 2014

Job Aid:
Security User Migration Supplement

Releases 14.1-14.3

Updates to February 2014 Communication

As previously communicated, MasterCard is undertaking a security infrastructure project to help enhance security controls employed by multiple Commercial products, including Smart Data.

As part of this effort, after release 14.2, Smart Data User Information will be migrated from the independent smartdata.gen2 database to a centralized Information Security database. This process is expected to begin on July 19, 2014. (*Please contact your Smart Data regional representative for the timeline.*)

Update to Previously Communicated User Experience Changes

In February 2014, we communicated certain changes to the user experience related to security. Following additional customer feedback and internal review, we have revised the planned changes for the 2014 user migration. These changes are listed in the table below.

Notes on the Table:

NEW: A functional change that was not communicated in February, but which is now planned.

RETAINED: The change will take place as described in February (and as described again herein).

REVISED: Communicated in February as a change, but the functionality has been altered from the February communication. New description is provided.

Please note that release content, timelines and final functionality remain subject to change.

Feature and Description	Status, New Description & Timing
Temporary Password expiration Currently, the temporary password (forgot password and manual reset) expires in 60 days. Note: Currently, the password set when creating a new user ID never expires and will continue to function the same way.	**Status: NEW** This one-time use temporary password will never expire. Note: The user ID will continue to become inactive after 90 days of non-use. **Timing:** Effective with migration

Feature and Description	Status, New Description & Timing
Password: 30 minute lock and auto unlock Currently, when a user tries to log in with an incorrect password more than 6 times, the user ID is locked. The user has to contact the help desk or the program administrator and the ID has to be manually unlocked. We proposed a change. Note: If the users are uncertain of the password, they can use the Forgot Password feature any time prior to the 6th attempt.	**Status: NEW** The user ID will be locked for 30 minutes after 6 invalid attempts and unlock automatically thereafter. The user status will continue to display as Active and cannot be manually unlocked. No emails will be sent. The error message on the Login page will be changed to "Invalid login. After too many attempts you will need to wait 30 minutes." **Timing:** Effective with migration
Password Duration Currently, duration is configurable between 20 and 90 days. Password duration was proposed to be fixed at 60 days.	**Status: REVISED** **With migration:** Configuration will be removed; password duration will be a fixed 60 days. The 60 days will start on the day of migration. **With 14.3 release:** Configuration restored; password duration will be between 20 and 60 days
Password changes; spaces and repeating characters Currently, the password field does not allow spaces, and a user may create a Smart Data password with repeating characters. We proposed a stronger password specification. Note: Users with more than two repeating characters in their passwords are not required to change it with 14.2. The rule is applicable when the password is changed.	**Status: NEW** The password field will allow spaces, which will be treated as a special character. Further, passwords will not be able to contain more than 2 repeating characters. Example: Tweet123 will be allowed but not Tweeet123. **Timing:** This change will take effect with release 14.2 and has been covered in the 14.2 documentation.
Change Password in My Profile Currently, a user can change the password from within My Profile screen. A new process was proposed.	**Status: RETAINED** A "Change Password" button will display on My Profile; when clicked it will open a separate Change Password screen. (See prospective design, last page.) **Timing**: Effective with migration
User Information Screen Changes proposed to the user information screen to enable/disable the user for/from 2FA.	**Status: RETAINED** **No change for current users.** This functionality will be communicated in the User Guide for two-factor authentication users. **Timing:** Effective with 14.3 release

Feature and Description	Status, New Description & Timing
Help Files Currently, various product support documentation can be accessed without logging in; we proposed to limit access to only registered users.	**Status: RETAINED** Access to help files, user guides and online tutorials (typically linked from the Resource Center) will require a valid smartdata.gen2 user ID and password. **Timing:** Effective with migration
Inactive User IDs After migration, User IDs will continue to become inactive 90 days after last successful login or from the date of creation.	**FYI; no changes**

Security Update: Change Password in My Profile

Beginning in July 2014, security updates for smartdata.gen2 will result in a change to the Change Password function. Currently, users can change their password on the My Profile page. After the security changes, a Change Password button will appear instead, which will launch a window where users can update their passwords. (Please note that the following prospective screen designs are subject to change.)