Multi-Factor Authentication Instructions

Version 1.0

May 18, 2017

Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Description | Author |
| 1.0 | 05/17/2017 | Draft document created |  |
|  |  |  |  |
|  |  |  |  |

Table of Contents

[1 Introduction 1](#_Toc482868268)

[2 Requirements 1](#_Toc482868269)

[3 Initial Setup from Secondary Access Points 2](#_Toc482868270)

[3.1 Administrative Login 2](#_Toc482868271)

[3.2 Change Password Function 3](#_Toc482868272)

[3.3 Multi Factor Authentication Screen 4](#_Toc482868273)

[3.4 Restore Factory Defaults 6](#_Toc482868274)

[3.5 Additional Notes 7](#_Toc482868275)

# Introduction

Due to PCI requirements, Multi Factor Authentication will be introduced with the Sierra 1.76.1 software release.

Multi Factor Authentication (MFA) is a method of computer access control in which a user is only granted access after successfully presenting multiple separate pieces of authentication.

Sierra Management Interface will authenticate users with Administrative Access (User Management and/or Utilities) on every login by requiring not only the user ID and password, but also a 6-digit security code that will be sent to the user’s mobile phone. This code will differ every time and expire after 5 minutes.

# Requirements

The requirements for MFA are:

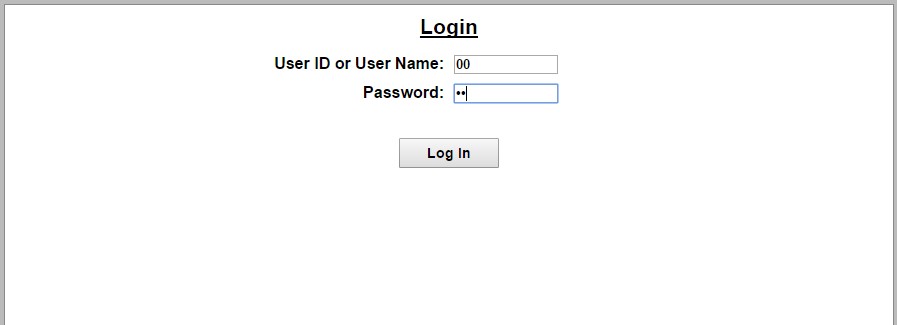
* A newly installed Unitec system running 1.76.1 software or higher
* Active Internet connection for Sierra
* Mobile phone with texting capabilities onsite

Note: MFA is only required for remote access points – for example, logging into Sierra through the router, logging in remotely through the Internet, or logging in from secondary units. Local access points do not require MFA. Local access points include logging directly into the Sierra application from the Primary kiosk with a keyboard and mouse, and logging directly into a Sierra Site Controller with a monitor, keyboard and mouse.

# Initial Setup from Secondary Access Points

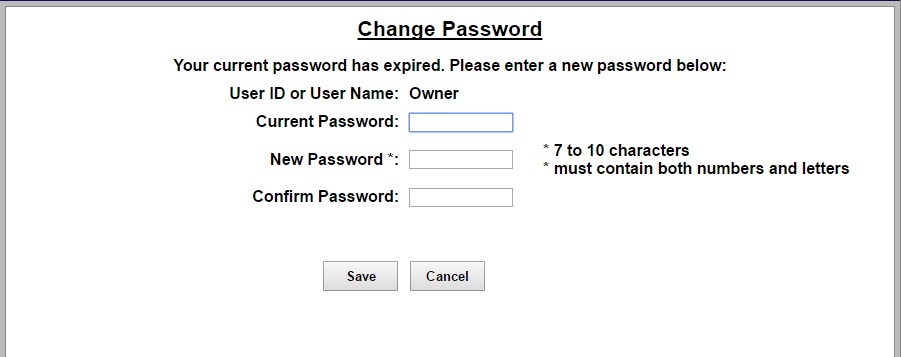
## Administrative Login

Upon logging into Sierra for the first time, the distributor technician will login as before, with user ID “00” and password “00.”



## Change Password Function

The Change Password Setup screen will then be displayed.

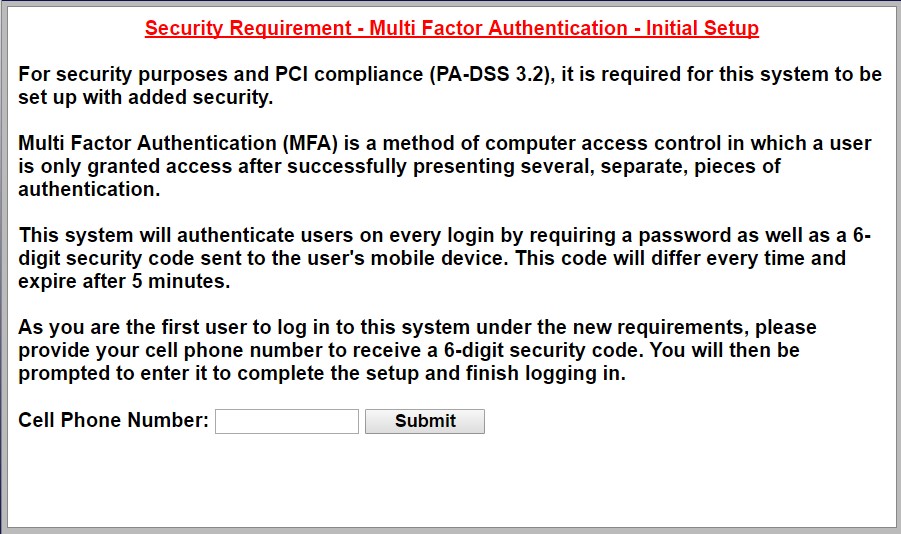


To change the password, the distributor tech will enter their old password (00), then enter the new password. Enter the new password again, then click Save. A new password will be required every 3 months. The last 5 passwords may not be used.

NOTE: If the password is entered incorrectly 6 times, the user will be locked out of the system for half an hour.

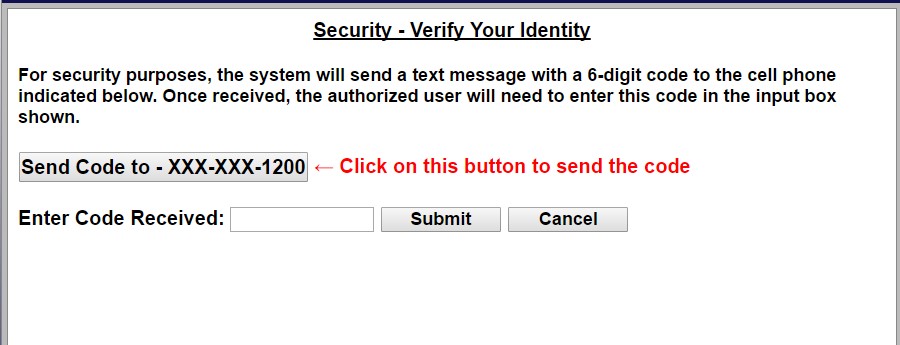
## Multi Factor Authentication Screen

Once the administrative password is changed, the MFA screen will be displayed. It explains the requirements.



The distributor tech must enter their mobile phone number and click Submit.

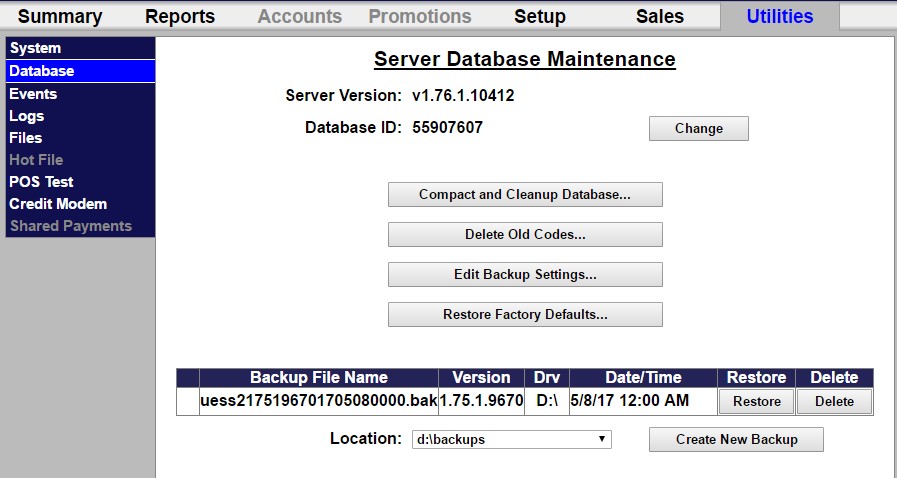
The next screen will be displayed. The tech must click the Send Code to… button to generate the security code and send it to their mobile device.



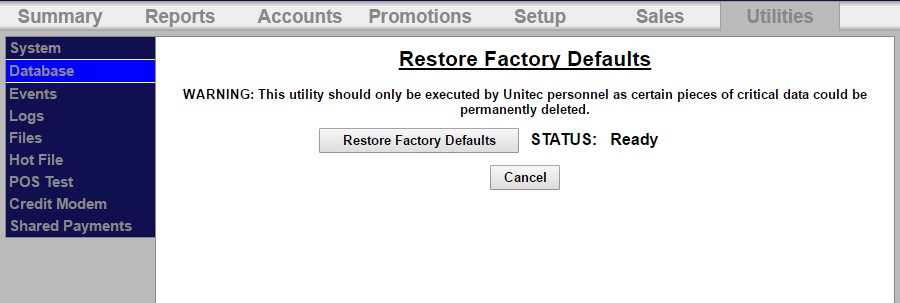
Once the tech receives the code, they must enter it into the field. When that 6-digit code is successfully entered, Sierra will display the Summary screen, as expected. The distributor tech will then proceed to setup the Sierra system as per usual.

## Restore Factory Defaults

When the initial setup is complete, the distributor tech MUST restore factory defaults to delete and reset the password and the MFA mobile phone number.



The tech must go to Utilities>Database then select Restore Factory Defaults.



The tech will select Restore Factory Defaults then OK to confirm.

## Additional Notes

The Multi Factor Authentication requirements apply to new kiosks in the field, only. Any units that are updated to 1.76.1 in the field do not have MFA automatically enabled, but it WILL enable if the Restore Factory Defaults function is performed.

A Manager level user (login 10/10) has been added as a default user for Sierra. The Manager user is assigned all access rights except User Management and Utilities. This will allow any service techs in the field to perform any subsequent setup and change programming without having to use multi factor authentication.