KYOCERA Document Solutions America, Inc.

Kyocera Microsoft® connector
Multi-Factor Authentication

Deployment Guide

Business Services Support
March 2019
Version 1.0

History of Revision(s)

Date	Version	Description	Author
03/2019	1.00	English Version	Richard Huelbig

Table of Contents

1. INTRODUCTION

The purpose of this document is to provide instructions on how to enable and use the Application Password for Microsoft Office 365®**,** with the Kyocera Microsoft connector. The use of an Application Password is a form of multi-factor authentication used with devices such as Kyocera's Multi-Function Products ("MFP").

Microsoft's "standard" multi-factor authentication can be enabled and used while Application Password is used.

Microsoft's "standard" multi-factor authentication includes methods such as having a special one-time code texted to a cell phone, having the code sent via voice call to a cell phone, or using a special application residing on a cell phone.

An Application Password can be created for every user who wants to access the MFP.

PREREQUISITES

Kyocera's Microsoft connector must be installed according to Kyocera Microsoft connector Setup And Operation Guide. This guide can be found on KDACentral.

Includes:

- Installation and configuration of the Kyocera Microsoft connector package file on the MFP.
- Proper licensing of the package file with either a full license or a 60 day trial license.
- Installation and configuration of the Kyocera Microsoft connector Settings Utility on a PC or server.

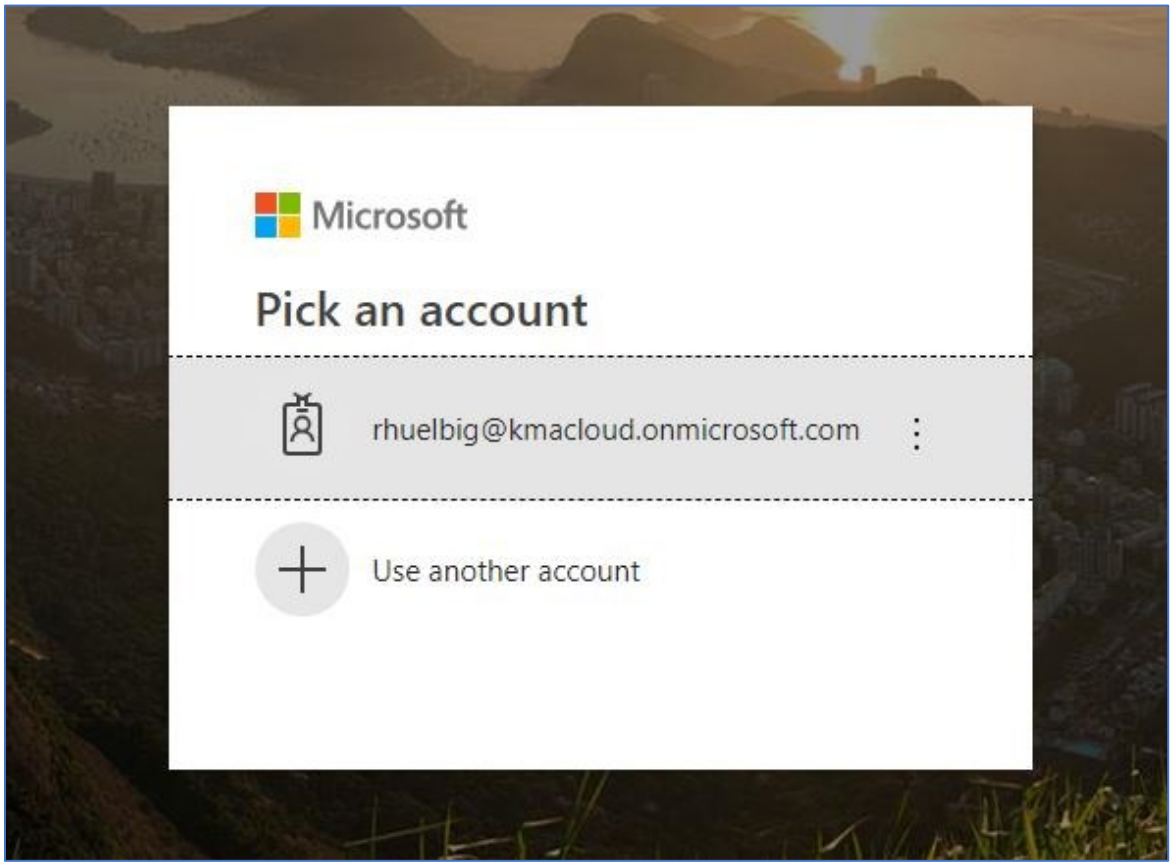
Multi-factor authentication must be configured by the Microsoft Office 365's administrator. The MFP should have Card Authentication Kit (B) installed and licensed in order to register user information to a supplied proximity card.

A "standard" password is the password, that, along with a user name or some other form of identification, allows access to an application. In some instances, two-step (two-factor) authentication may be enabled which requires the entry of a "secondary" password.

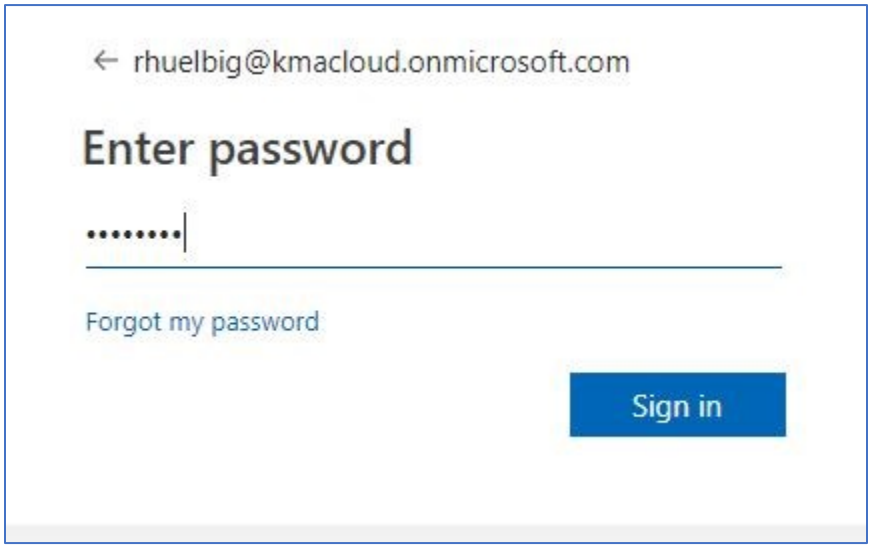
According to Microsoft's website (https://support.microsoft.com/en-us/help/12409/microsoft-account-app-passwords-and-two-step-verification) "An app password is a long, randomly generated password that you provide only once instead of your regular password when signing in to an app or device that doesn't support two-step verification. You only need to create an app password if you have two-step verification turned on and are using an app that doesn't support it."

2. CREATING AN OFFICE 365 APPLICATION PASSWORD

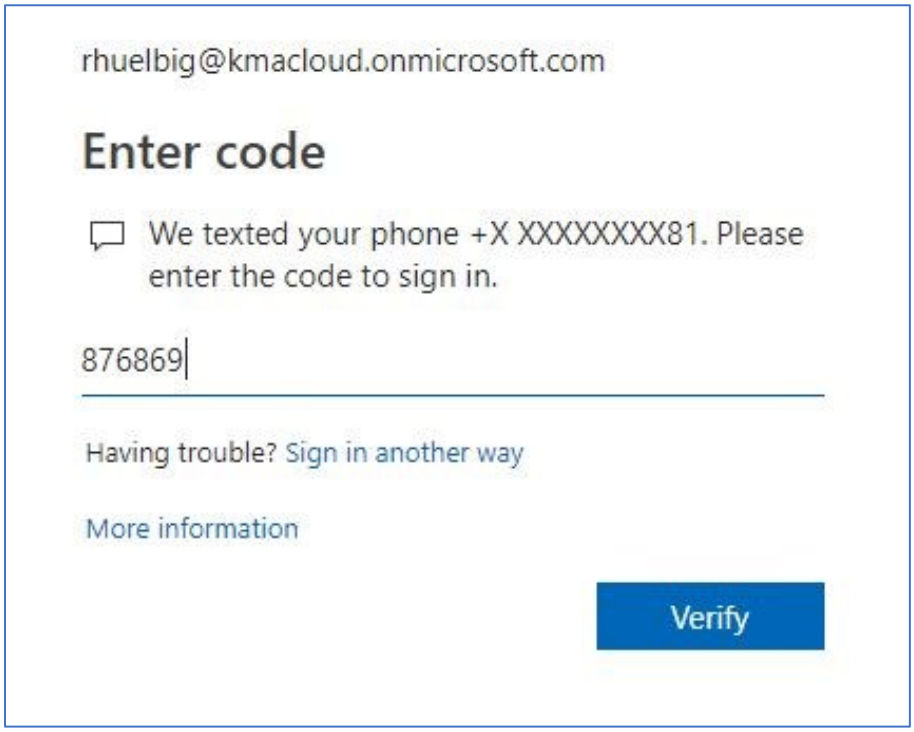
Log into your Microsoft Office 365 account. Either enter or click on your username.



Enter your password into the appropriate field.

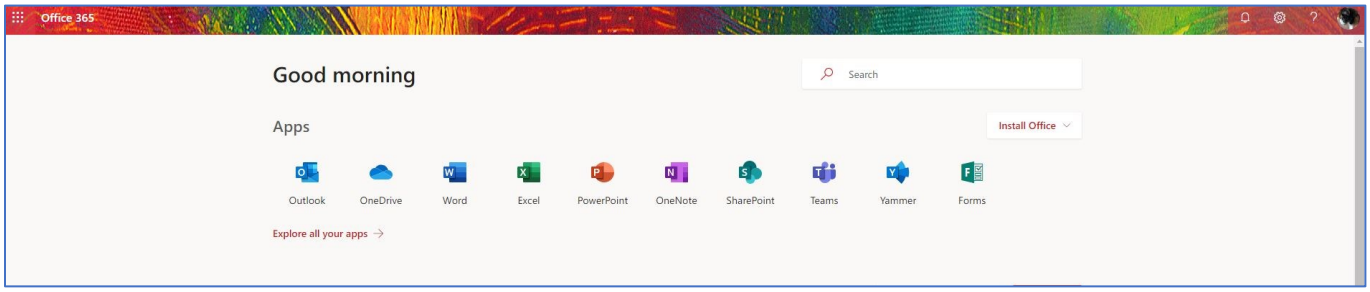


If the Office 365 administrator has enabled multi-factor authentication for your account, and it's configured to send a code to a phone via text message, a text and one-time code will appear on your phone. Enter that code (in this case it's 87869) into the appropriate field show here. Click "Verify".

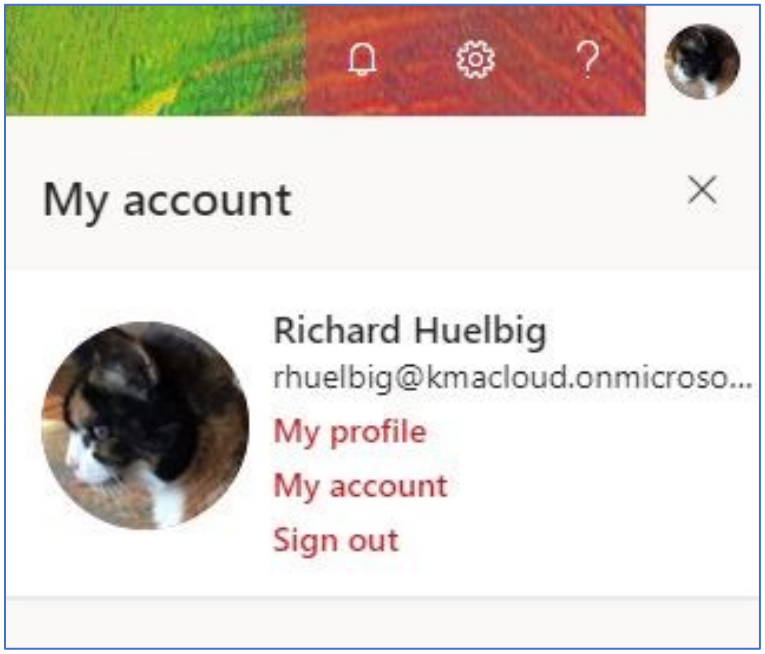


Select whether you would like to remain logged into your Office 365 account.

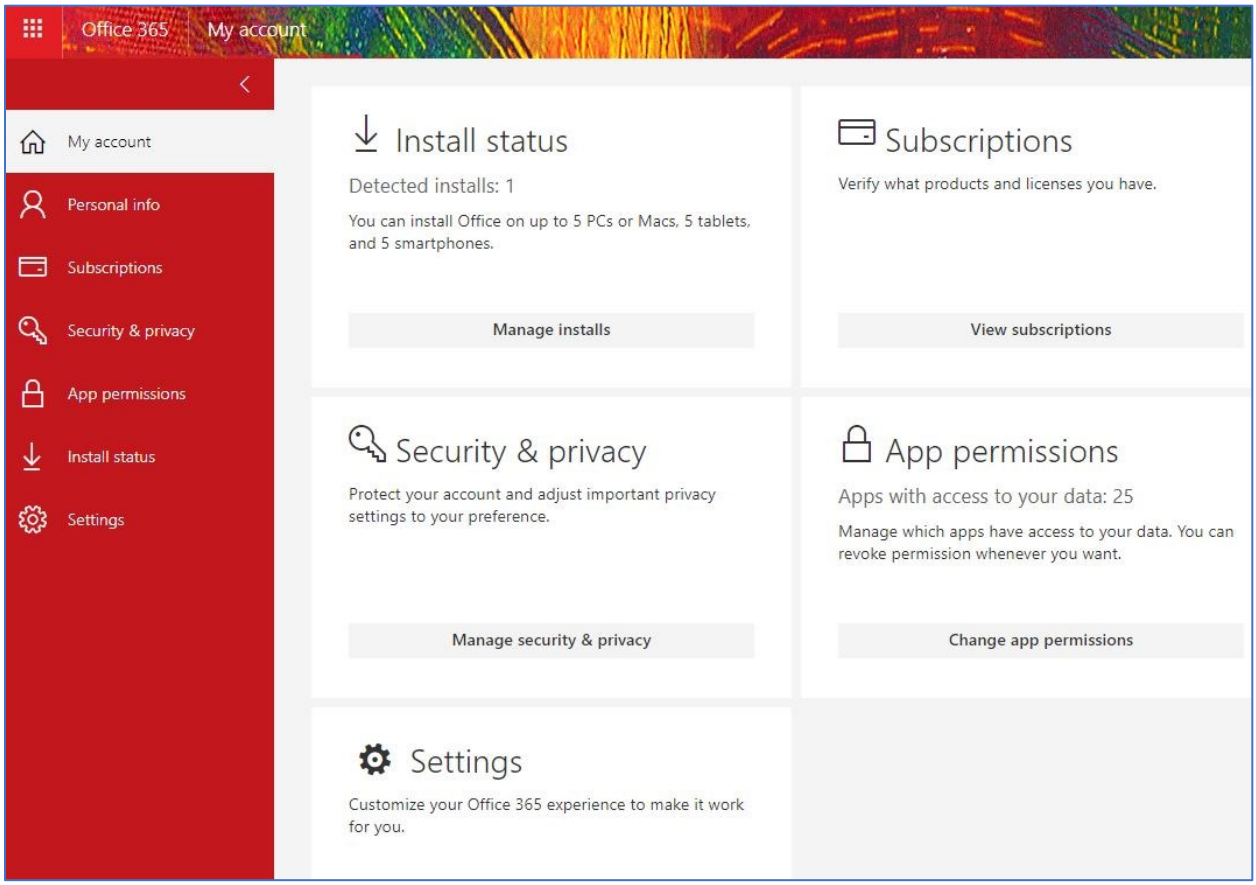
You will now be logged into your Microsoft Office 365 account. (Note that the screen layout shown here may differ from the one you are using.)



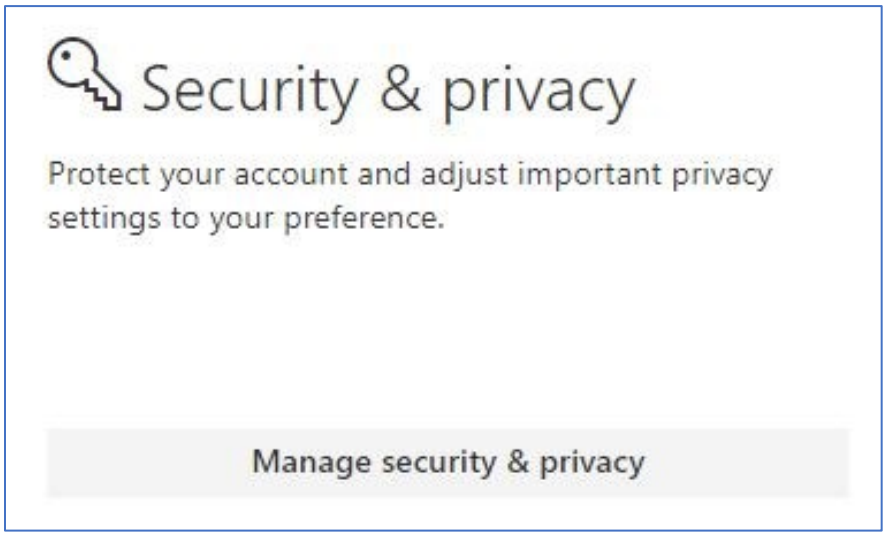
In the upper right-hand corner of the screen locate your account avatar and click on it. Select “My account".



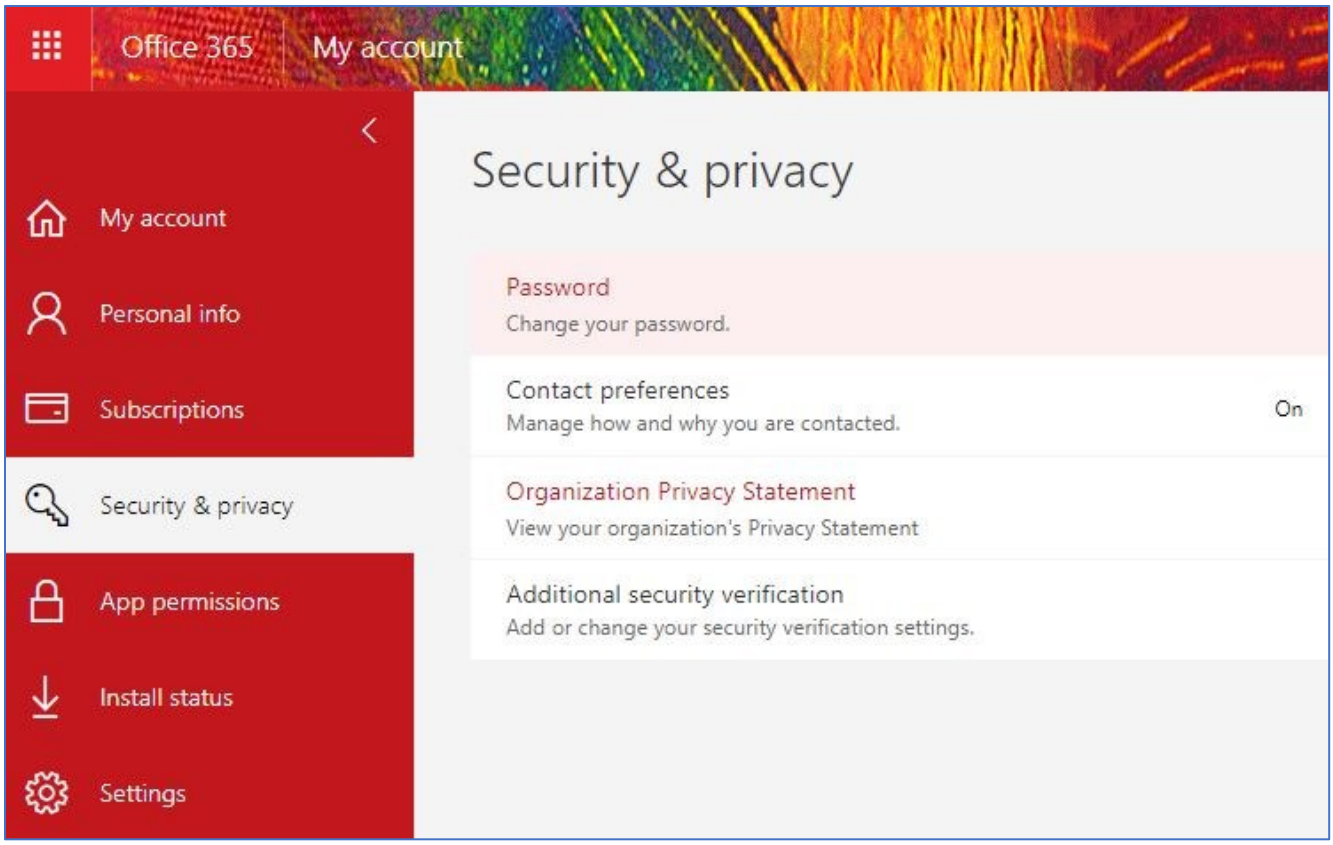
You will now be presented with a screen that provides various configuration options for your account.



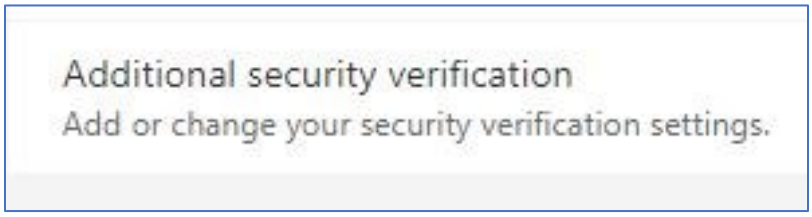
Click on the "Security & Privacy", "Manage security & privacy" button.



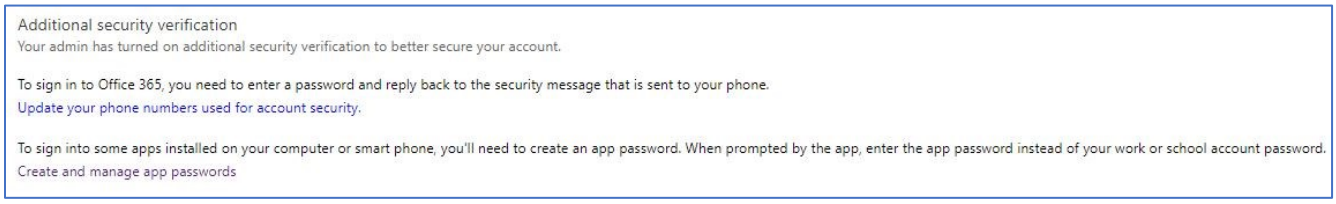
The following screen will appear.



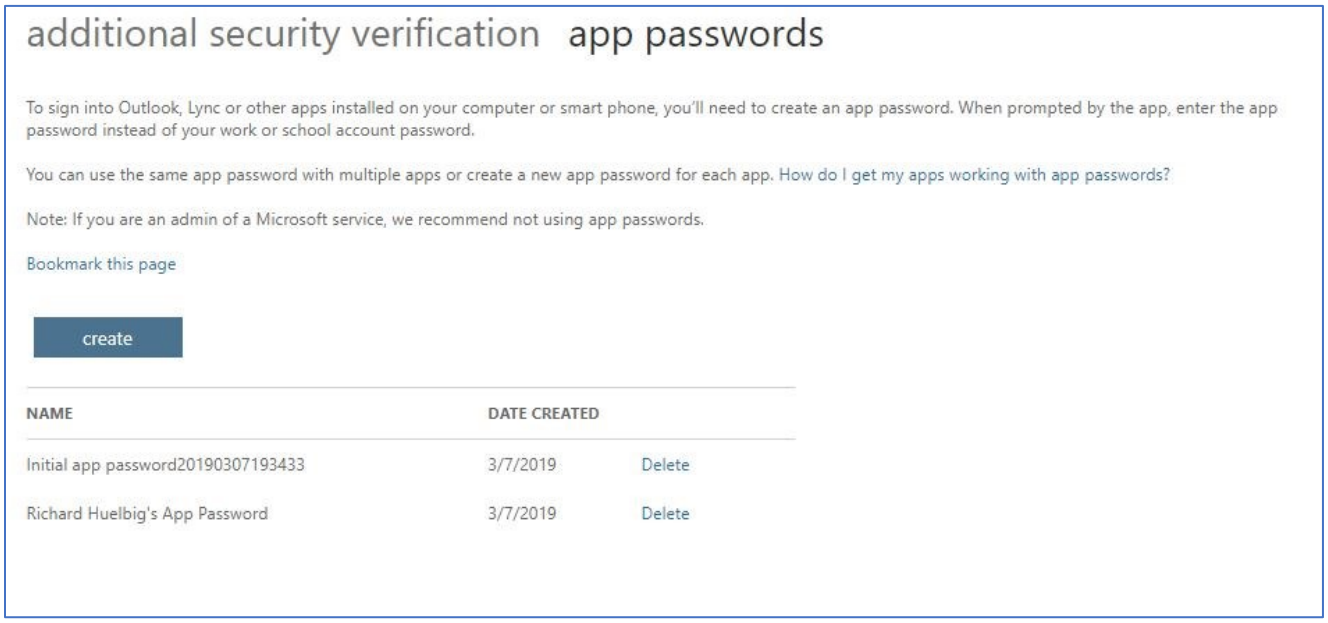
Select "Additional security verification".



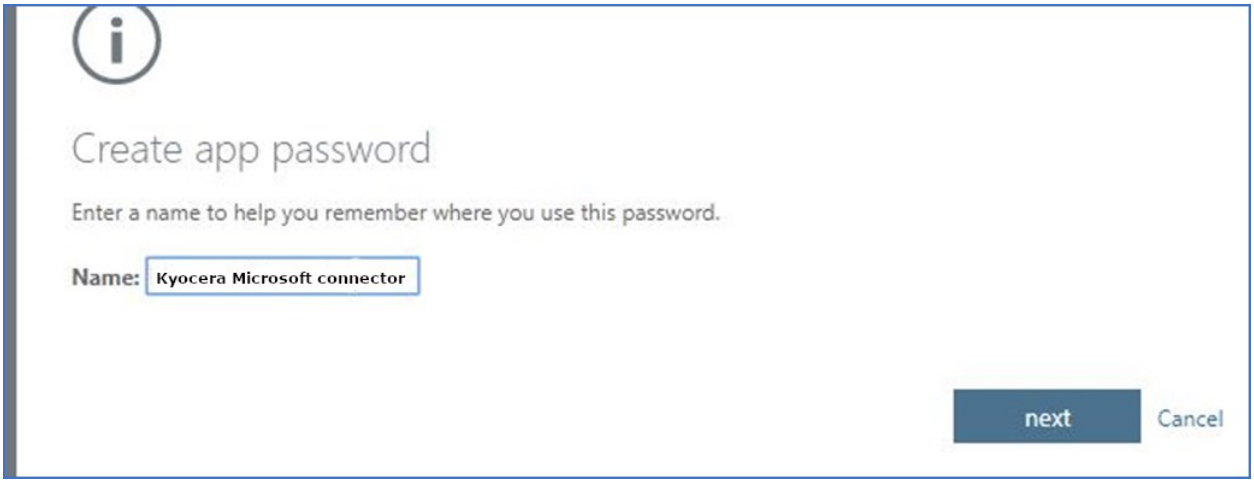
A new list of security selections will appear. Click on "Create and manage app passwords"—the third choice.



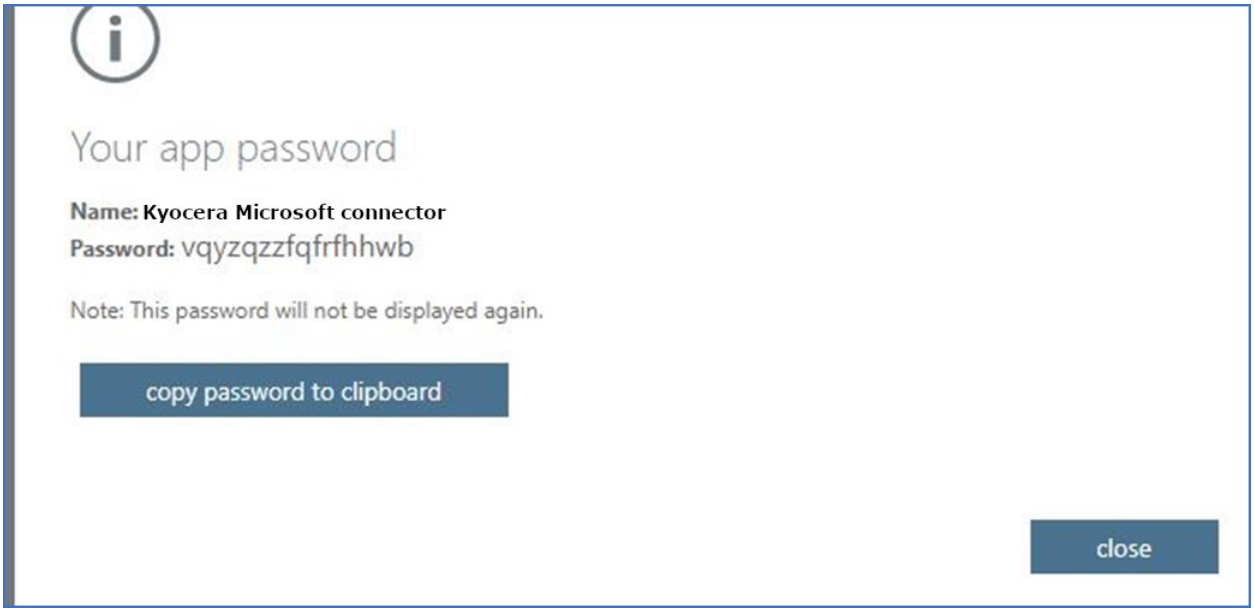
A new screen appears that allows you to create or delete Application Passwords. Note that on this screen, an "Initial app password" is displayed. Additional Application Passwords, such as "John Smith's App Password", once created and displayed to the user, will no longer appear (only the label "John Smith's App Password" will appear in the list). Click on the "Create" button.



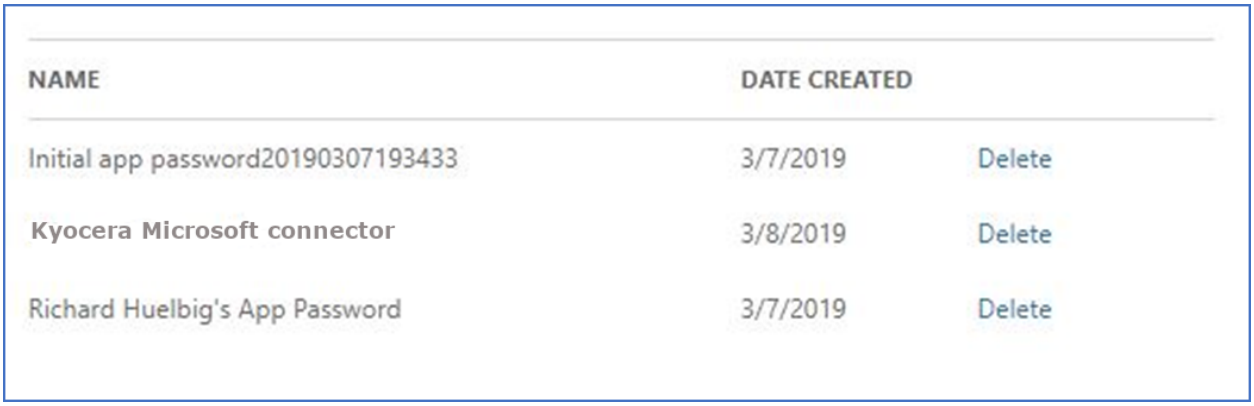
Enter a name for the new Application Password. Press the "Next" button.



A new Application Password will be displayed. Either copy the password to the clipboard, or temporarily write it down. This is the password that will now be used when you log into the Kyocera Microsoft connector. Click "close".



You will note that the label for the new Application Password appears in the list, but, as noted in the previous screen, the password itself will no longer be displayed.



You have successfully created an Application Password for use with the Kyocera Microsoft connector.

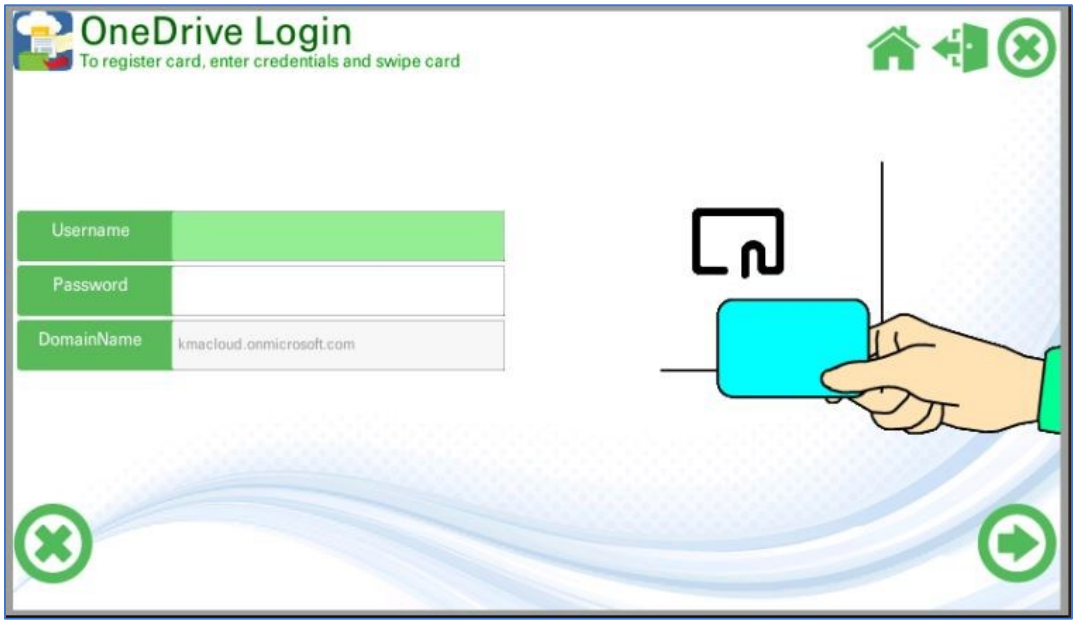
USING AN APPLICATION PASSWORD WITH KYOCERA'S MICROSOFT CONNECTOR

Locate the MFP with the Kyocera Microsoft connector.

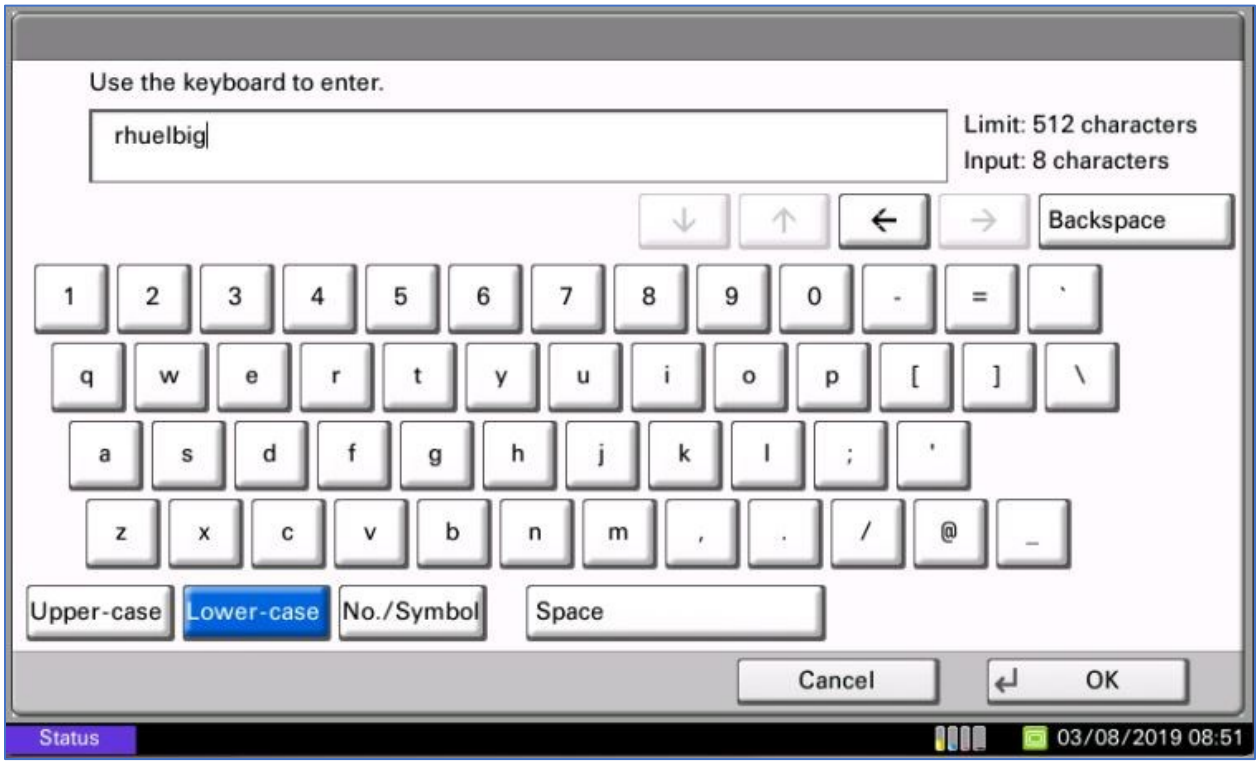
Click on the Kyocera Microsoft connector application icon.

The applications that have been configured into the Kyocera Microsoft connector will appear on the MFP panel. Here three buttons are displayed. One for SharePoint® On-Line, one for OneDrive®, and one for Exchange® On-Line. Select the button for the application you wish to use.

In this instance, the OneDrive button was selected. You will be asked to log in. Note that the Domain Name field is pre-populated—this is part of configuring the Kyocera Microsoft connector Settings utility on a PC or server. Select the "Username" button.

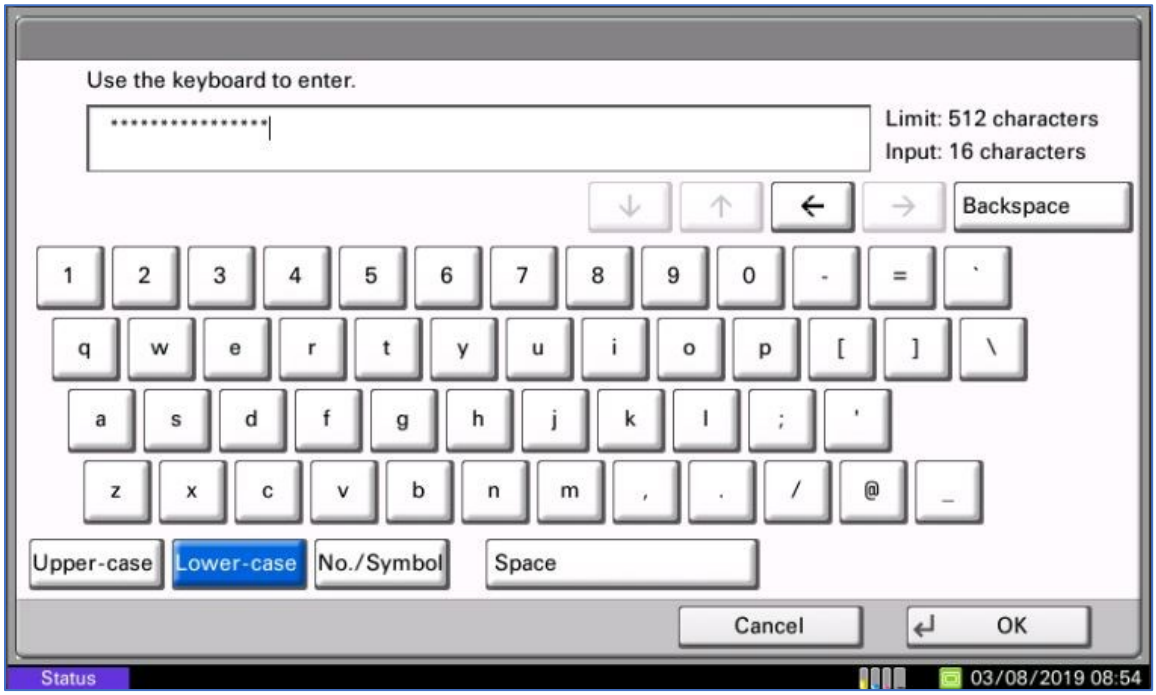


When the keyboard appears on the MFP display, type the username of the user for whom the Application Password was created. Press the "OK" button.

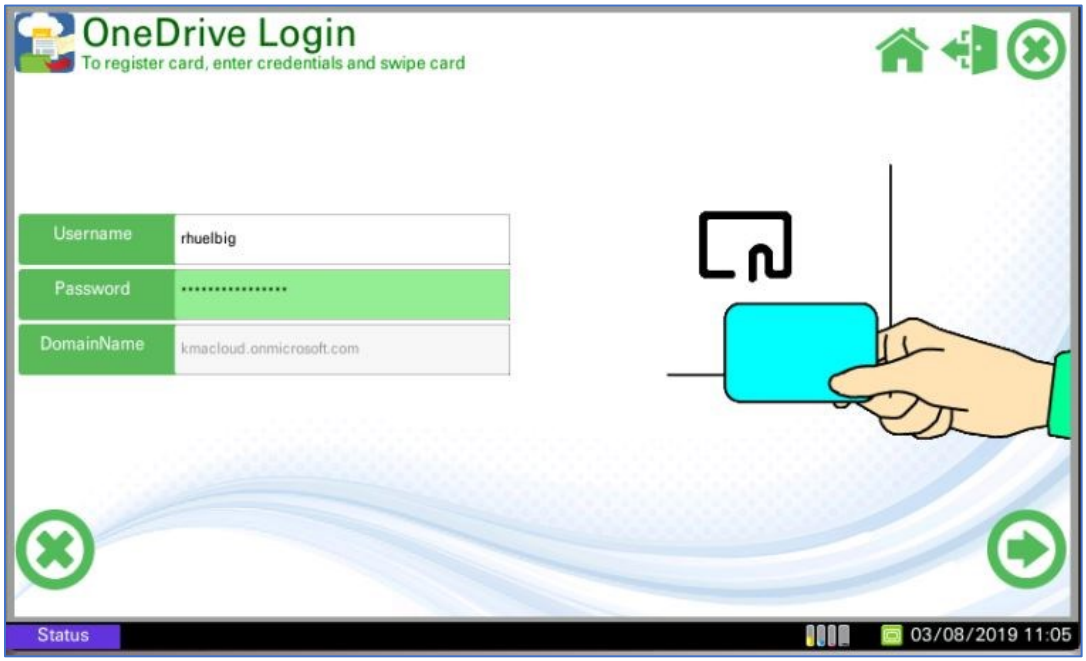


You will see that the user's name appears in the Username field. Press the "Password" button.

When the keyboard appears on the MFP display, type the Application Password created for the user account. <u>DO NOT</u> enter the user's "standard" Microsoft Office 365 password—an authentication error will occur. Press the "OK" button.



You will now be returned to the OneDrive Login screen and you will observe that the Username and Password fields contain entries. Of course the Password field will not show the password (which in this case, as a reminder is the Application Password created earlier).

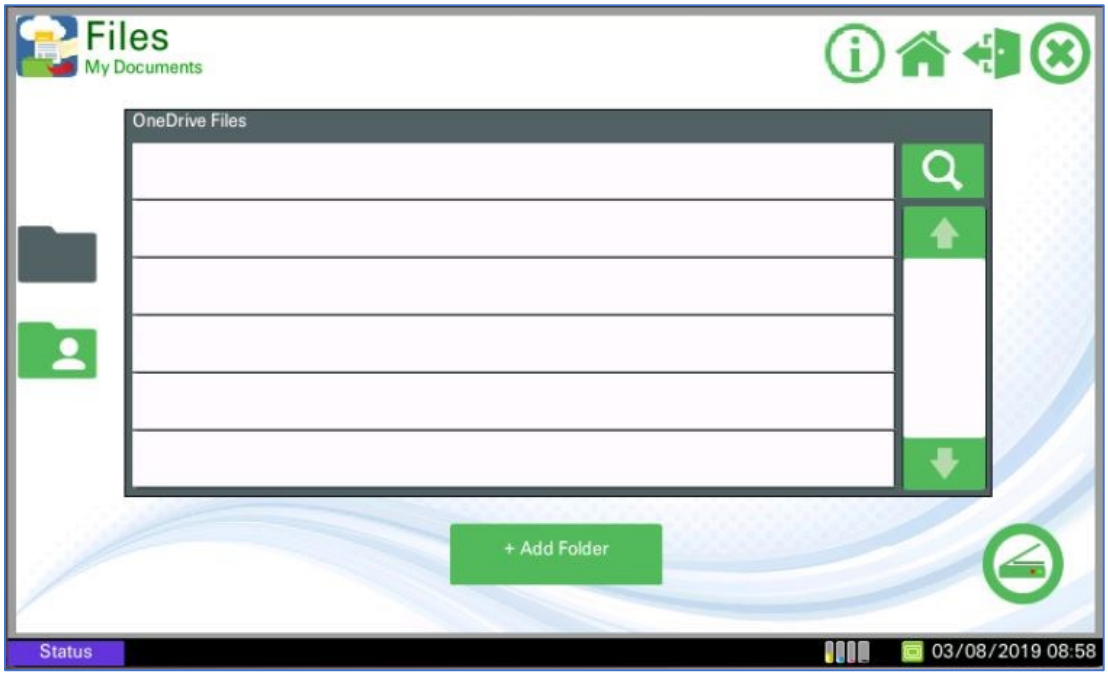


You now have two choices:

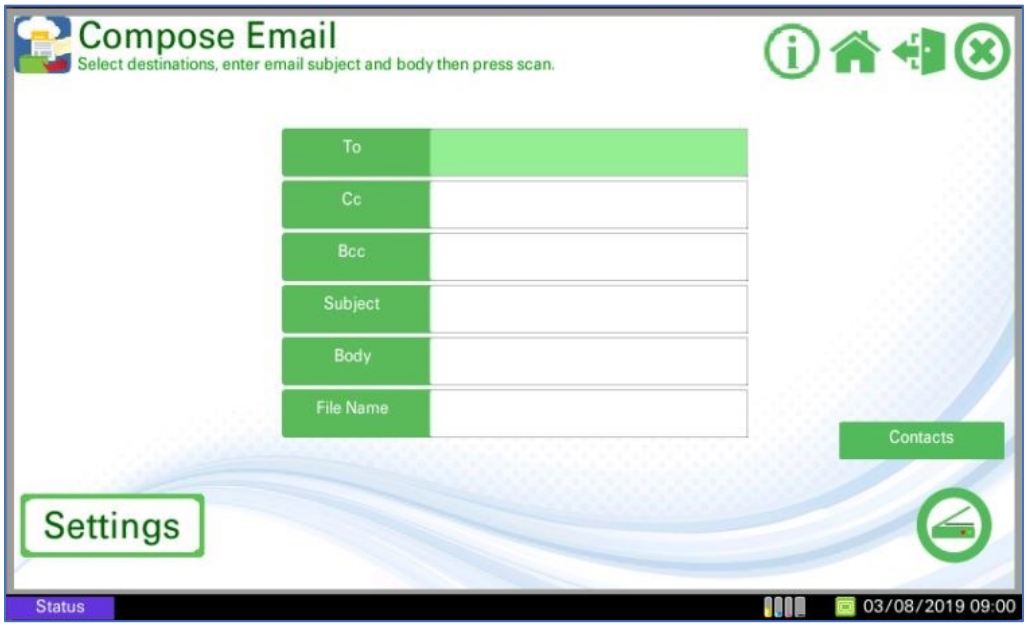
1) **If you do not wish to register the user name and Application Password to a proximity card you can simply press the right-arrow key in the lower-right corner and you will be logged into OneDrive.**

2) **If you do wish to register the user name and Application Password to a proximity card simply scan the card with the card reader. Depending on how the reader is configured you should hear a "beep" and you will be brought to the OneDrive screen. This selection is obviously the preferred method of automating the login. For future logins, you will only need to scan the proximity card with the card reader—it will not be necessary to manually enter either the user name or the Application Password.**

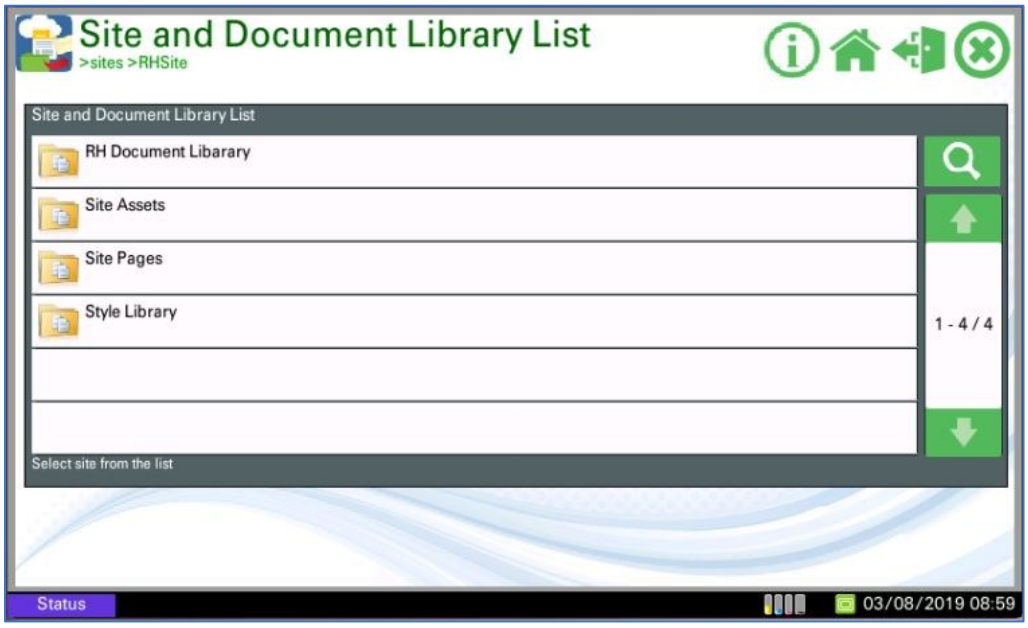
Had you chosen to access OneDrive On-Line, after logging in, you would be presented by a screen similar to this.



Had you chosen to access Exchange On-Line, after logging in, you would be presented by a screen similar to this.



Finally, had you chosen to access SharePoint On-Line, after logging in, you would be presented by a screen similar to this.



You have successfully implemented Kyocera Microsoft connector with Multi-Factor Authentication.

Specifications and design are subject to change without notice.

KYOCERA is a trademark of Kyocera Corporation in the United States and/or other countries.

Microsoft, Office 365, SharePoint, Exchange and OneDrive are trademarks of Microsoft Corporation in the United States and/or other countries.

Other trademarksin this Deployment Guide are the trademarks of their respective owners.

PLEASE NOTE: This document is provided for information purposes only. KYOCERA does not warrant or guarantee that the customer's Kyocera MFPs or printers have been equipped or have the proper security or specifications for their needs or requirements. Supported functions or specifications vary and may require optional equipment. For more information, please refer to the catalogs or user manuals for the detailed features of each product.