MFA SETUP INSTRUCTIONS

Overview

This document covers the steps necessary to setup your multi-factor authentication (MFA) account. Multi-factor authentication (MFA) is a method of authentication that requires the use of more than one verification method and adds a critical second layer of security to user sign-ins. Off-premise access to on-premise applications, such as the Outlook Web App, Office365 and HR related application will require this additional identity verification. Any user that will access these applications will need to set up an MFA account.

Section 1: New User Login and Setup

- Associates that DO manually enter or swipe a badge at the time clock (Non-Exempt), use this site.
  - https://mfapa.dcsg.com/portal
- Associates that DO NOT manually enter or swipe a badge at the time clock (Exempt), use this site.
  - https://mfa.dcsg.com/portal

IMPORTANT NOTE:
If you receive a login failed message, verify you have entered the appropriate username and password.

For help, please contact the Dick’s Sporting Goods, Inc. IT Service Desk at 866-418-3456 or ITServiceDesk@dcsq.com

1. Log In to the portal using your network credentials.

2. If this is your first time logging in to the portal, you will be prompted to set up your profile. Select the authentication method you would like to use. The following table describes the authentication methods:
MFA SETUP INSTRUCTIONS

Authentication Methods

<table>
<thead>
<tr>
<th>Method Type</th>
<th>Description</th>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phone Call</td>
<td>Places an automated voice call to the Authentication phone. The user answers the call and presses # in the phone keypad to authenticate.</td>
<td>Section 2: Application Setup – Phone Call</td>
</tr>
<tr>
<td>Mobile Phone Text</td>
<td>Sends a text message containing a verification code to the user. The user is prompted to reply to the text message with the verification code.</td>
<td>Section 3: Application Setup – Mobile Phone Text</td>
</tr>
<tr>
<td>Mobile App</td>
<td>Pushes a notification to the Multi-Factor mobile app on the user’s smartphone or tablet. The user taps “Verify” in the app to authenticate. Alternately, the app can be setup to prompt the user for a user defined PIN that will be used to authorize the authentication.</td>
<td>Section 4: Application Setup – Mobile App</td>
</tr>
</tbody>
</table>

3. Once the process is completed you can Log Out. You can make changes as needed any time by logging back in to the portal. This includes changing the security questions or authentication method.

Section 2: Application Setup – Phone Call
This authentication method places an automated voice call to the Authentication (Primary) phone. To authenticate, answer the call and press # on the phone keypad. Phone calls are generated from 855.330.8653

1. Select Method (Phone Call) and enter the primary phone number that will be used for the authentication processes.
MFA SETUP INSTRUCTIONS

2. Press the **Call Me Now to Authenticate** button to verify the new settings. You will receive a phone call from 855.330.8653 that will prompt you to press # to verify the authentication. This will complete the method setup and will direct you to the security questions page so you can finish configuring your profile.

   **IMPORTANT**: Once the phone call method is completed, all applications that will need the additional identity verification will use this method.

---

**Section 3: Application Setup – Mobile Phone Text**

This authentication method sends a text message containing a verification code. You will then be prompted to reply to the text message with the verification code.

1. Select **Method** (Text Message) and enter the mobile number that you will use to reply to the authentication requests.
2. Press the **Text Me Now to Authenticate** button. You will receive a text message with a verification code.

![Text Me Now to Authenticate](image1)

3. Send a reply with the verification code. This will complete the method setup and will direct you to the security questions page so you can finish configuring your profile.

![Verification Code](image2)

**IMPORTANT**: Once the text message method is completed, all applications that will need the additional identity verification will use this method.

Section 4: Application Setup – Mobile App

This authentication method pushes a notification to the Multi-Factor mobile app on your smartphone or tablet. You then tap “Verify” in the app to authenticate.

1. Before proceeding, you must install the Microsoft Authenticator app on your mobile device. On your mobile device, access the App Store (Apple devices) or Play Store (Android devices) and search for “Microsoft Authenticator”.

![Microsoft Authenticator](image3)

**NOTE**: You can install and configure your account on two devices.
2. Install the application to your device.

4. This will then take you to a separate page where you can add the configuration to your device app.

5. Open the app on your device and select the + located in the upper right. This will allow you to scan the **QR code** from the web page or enter the **Activation Code** and **URL** manually.

6. Once the account is added to your device, select the **Authenticate Me Now** button at the bottom of the portal page. Your mobile device will receive a notification prompting you to verify the authentication request by pressing “Verify”. This will complete the method setup and will direct you to the security questions page so you can finish configuring your profile.

**IMPORTANT**: Once the mobile app method is set up, all applications that will need the additional identity verification will use this method.