

Okta User Guide

Version: 2.3

Date: 08/25/21

Prepared by:

Stephen Sales
Program Analyst

Table of Contents

1.	Virginia DMV	1
2.	Introduction.....	4
3.	Points of Contact.....	4
3.1	Support.....	4
3.2	General Links	4
4.	Establishing your Okta account.....	5
4.1	Activating your account	5
4.2	Creating your account	5
5.	Multifactor authentication	6
5.1	Setting up multifactor authentication	6
5.2	Okta Verify.....	8
5.3	SMS Authentication.....	12
5.4	Email Authentication	13
6.	Signing In	15
6.1	Web Address.....	15
6.2	Selecting a multifactor authentication option	16
6.3	Authenticating with Okta Verify	17
6.4	Authenticating with SMS	18
6.5	Authenticating with Email	19
7.	Updating User Profile	21
7.1	User Profile Modification	21

2. Introduction

This document is a snapshot of the Virginia DMV Okta Authentication application. The configuration may change at any time. Some information in this document may no longer be accurate following handoff. All interested parties should refer to the Okta Help Center at the following address:

https://support.okta.com/help/s/?language=en_US for the most accurate, and up-to-date information.

Note: Please keep your RSA tokens/fobs till notified and given the information needed to mail back your RSA tokens/fobs back to the DMV.

As DMV moves to transition away from RSA, Extranet Users will need to establish their Okta credentials prior to being able to access their DMV Extranet Applications in the Okta environment. Users can proactively establish their Okta accounts prior to the given migration/cut-over dates, however, users will not be able to actively use those Okta credentials till those Extranet Applications are transitioned over and as a result will continue to using their RSA credentials and link until then.

3. Points of Contact

3.1 Support

In the event a user needs technical assistance and/or basic troubleshooting logging in, the **DMV IT Helpdesk** can be contacted at the following: 804-497-7124 between Monday-Friday 7AM-6:30PM and Saturday between 7AM-2PM.

In the event a user needs assistance with account management **User Agreement Services** can be contacted at the following: 804-474-2294 and/or useagreement@dmv.virginia.gov.

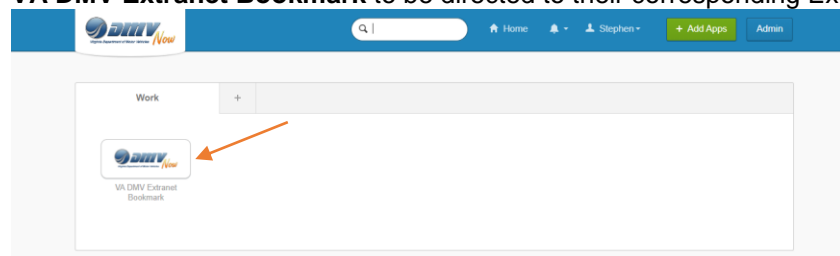
3.2 General Links

Note: The starting URL/ Hyperlink for the DMV Extranet is changing as DMV transitions away from using RSA credentials and migrates Extranet application security to OKTA.

Users that only access Extranet applications secured by OKTA and that no longer have or need their RSA credentials, should use the following link to access the DMV Extranet:

<https://virginiadmvmv.okta.com/login/login.htm>

Once signed in users should be able to access the following webpage. Users then need to **click** on the **VA DMV Extranet Bookmark** to be directed to their corresponding Extranet application.



Note: <https://business.dmv.virginia.gov> URL will continue to default to RSA secured Extranet starting page until all DMV Extranet applications are secured with OKTA.

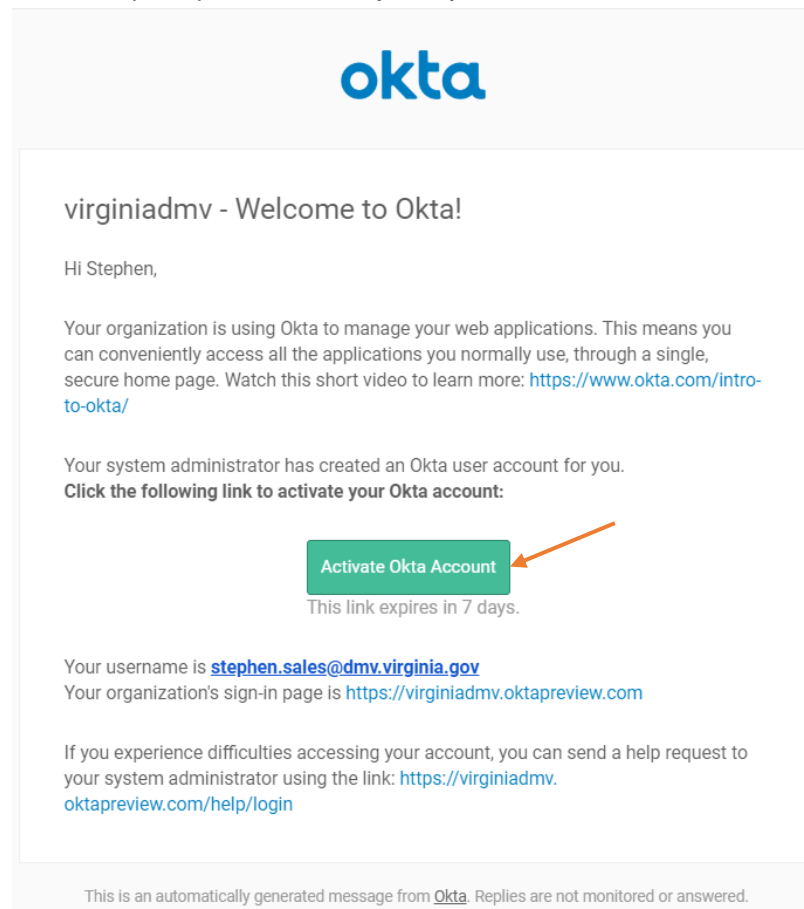
4. Establishing your Okta account

Note: Users will first need to receive their activation email from DMV. If you are a user who has yet to receive your activation email please contact Use Agreement Services to have your email validated and an activation email will then be sent out. However, if you have already verified your email address with Use Agreement Services, please contact the DMV IT Helpdesk.

When establishing your account, you can setup multiple authentication factors (Email, SMS, and/or Okta Verify). However, while one multifactor is necessary, we recommend at least two.

4.1 Activating your account

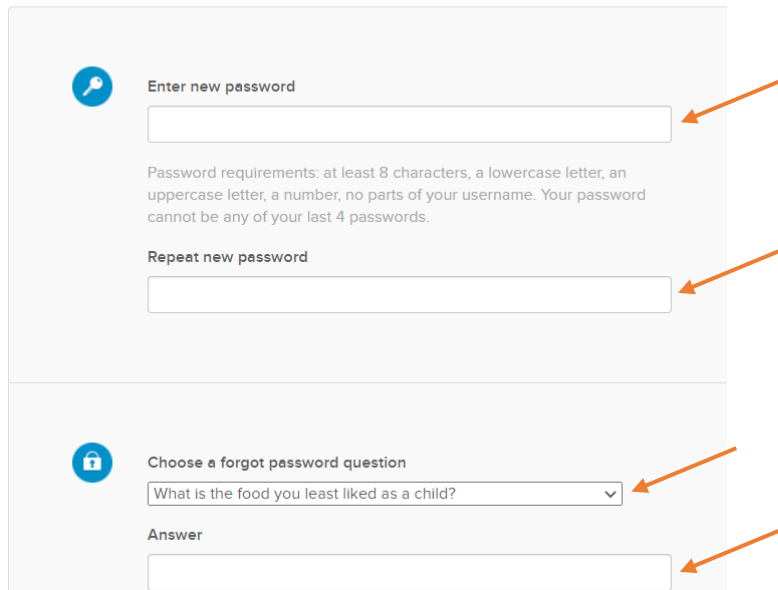
A DMV administrator will need setup your account. Once the account is established, the user will receive a "Welcome to Okta" email sent from Okta. Following the opening of the email, the user will notice the **Activate Okta Account** link within the email (**green box**). The user must click on **Activate Okta Account** in order to establish their account. Lastly, the link for account activation expires after 7 days if the link expires please contact your system administrator.



4.2 Creating your account

1. Create a new password unique to you, and follow the password requirements listed.
2. Choose a security question from the drop down menu, and provide an answer.

Welcome to virginiamv, Stephen!
Create your virginiamv account



Enter new password

Password requirements: at least 8 characters, a lowercase letter, an uppercase letter, a number, no parts of your username. Your password cannot be any of your last 4 passwords.

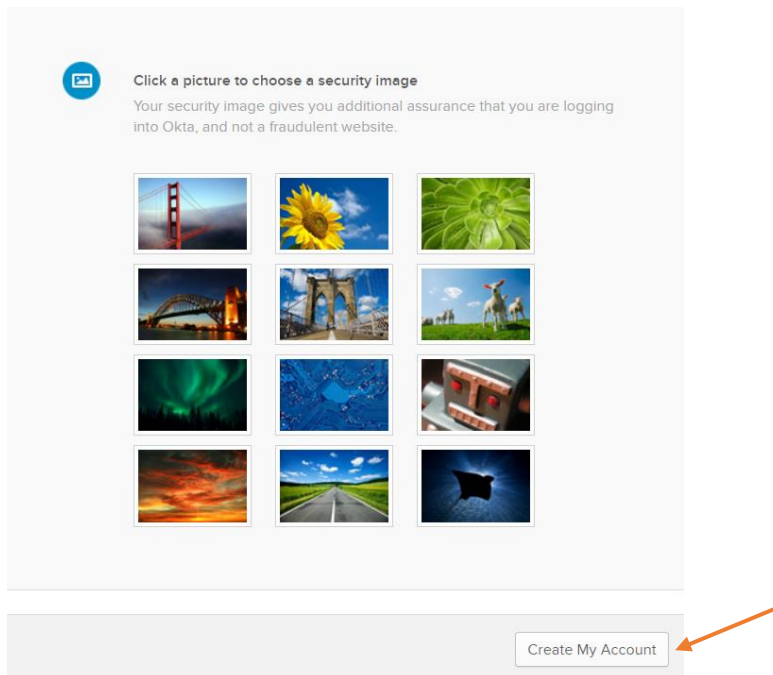
Repeat new password

Choose a forgot password question

What is the food you least liked as a child? ▼













Answer

3. Select your security image, and click **Create My Account**.



Click a picture to choose a security image

Your security image gives you additional assurance that you are logging into Okta, and not a fraudulent website.

Create My Account

5. Multifactor authentication

5.1 Setting up multifactor authentication

In setting up your multifactor authentication you can select Okta Verify (application on phone), SMS authentication, and/or email authentication by clicking **Setup** below each option. Each user needs to

establish **at least one form of multifactor authentication** before they are permitted to click on **Finish** to proceed to the Admin Console.



Set up multifactor authentication

Your company requires multifactor authentication to add an additional layer of security when signing in to your Okta account



Okta Verify

Enter single-use code from the mobile app.

Setup



SMS Authentication

Enter a single-use code sent to your mobile phone.

Setup



Email Authentication

Enter a verification code sent to your email.

Setup



Notice that after setting up at least one form of multifactor authentication the **Finish** tab appears. The **green check mark** beside multifactor option indicates a successful multifactor setup.

Note: This is where you can setup multiple authenticators at one time.


Set up multifactor authentication


You can configure any additional optional factor or click finish

Enrolled factors

 Email Authentication 

Additional optional factors

 Okta Verify
Enter single-use code from the mobile app.

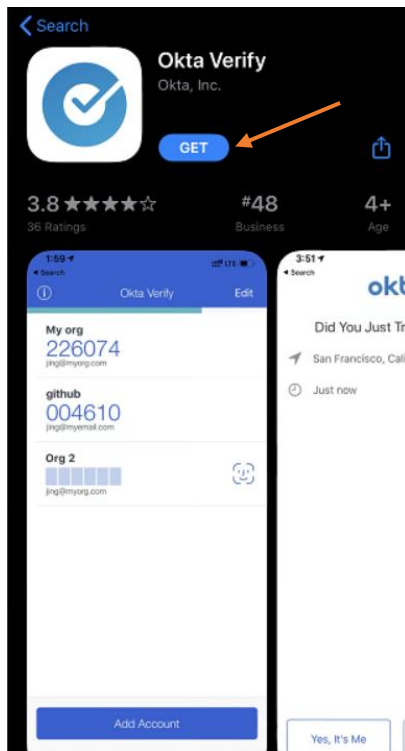
 SMS Authentication
Enter a single-use code sent to your mobile phone.

5.2 Okta Verify

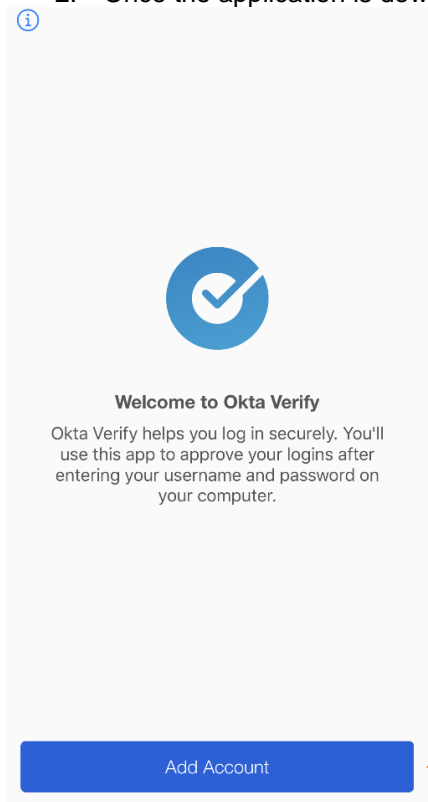
To sign in, users must start the Okta Verify app on their mobile device to generate a six-digit code they use to sign into their org. The numbers are generated using the industry standard time-based one-time password algorithm.

Setting up Okta Verify

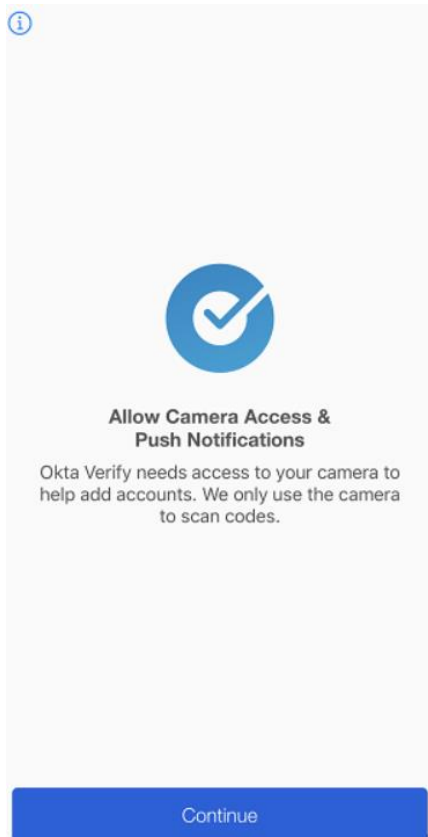
1. Download the Okta Verify app for iOS from the Apple App Store or Google Play for Android devices.



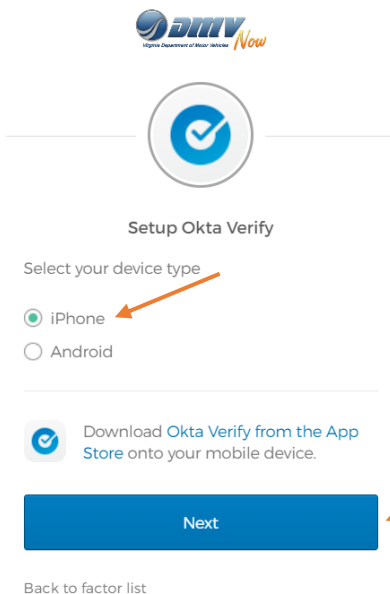
2. Once the application is downloaded, open the application, and click **Add Account**.



3. Enable camera access (this is necessary in order to scan the QR code), and click **Continue**.

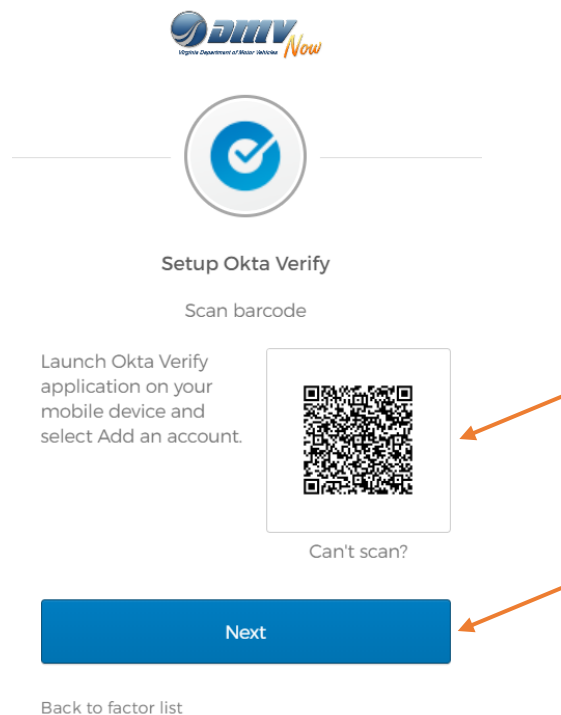


4. Now that the application is downloaded, open the application, click setup on **Okta Verify**, select your device, and click **Next**.

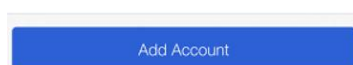
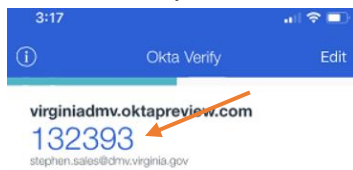


5. Use your device to scan the QR code, and click **Next**.

NOTE: Do not scan the QR code in the below screenshot, this is only a screenshot of what it should look like on your own PC.



6. Once you scan the QR code you will receive a six-digit code within the Okta Verify application.



7. Enter the six-digit code provide by the Okta Verify application, and click **Verify**.



Setup Okta Verify

Enter code displayed from the application

Enter Code

Verify

[Back to factor list](#)

5.3 SMS Authentication

End users sign in to their org and authenticate by entering a security token that is sent to their mobile device.

If your org uses a single phone number to authenticate multiple end users:

- All users will enroll in this factor with the same phone number.
- Due to a high level of user activity, the number may be blacklisted. If this occurs, contact Okta Support immediately to confirm that the number is trusted by your org.

Setting up SMS Authentication

1. Input your cellphone number.
2. Click **Send code**.



Receive a code via SMS to authenticate

United States ▼

Phone number

+1 234-567-8910

Send code

[Back to factor list](#)

3. Enter the six-digit code, and click **Verify** to complete SMS Authentication.



Receive a code via SMS to authenticate

United States ▼

Phone number

+1 8049381696

Sent

Enter Code

337898

Verify

[Back to factor list](#)

5.4 Email Authentication

The email account displayed is established by the user's org admin. Users receive a code in an email message to enter during Okta sign in. The one-time verification code in the email is valid for 5 minutes. This time frame cannot be adjusted.

Setting up Email Authentication

1. Click **Send me the code**.



Set up Email Authentication

Send a verification code to your registered email.

Send me the code

[Back to factor list](#)

2. The six-digit code will be sent to your registered email account.



virginiadmv - Action Required: Confirm your email address

Hi Stephen,

You are receiving this email so we can confirm this email address for your account.


Please use the following one-time code to complete verifying your email address:


072092

If you believe you have received this email in error, please reach out to your system administrator.

This is an automatically generated message from [Okta](#). Replies are not monitored or answered.


3. Enter the six-digit code, and click **Verify** to complete Email Authentication.


Virginia Department of Motor Vehicles



Set up Email Authentication

A verification code was sent to s...v@gmail.com. Check your email and enter the code below.

 Haven't received an email? [Send again](#)

Verification code

1 2 3 4 5 6

Verify

[Back to factor list](#)

6. Signing In

6.1 Web Address

In order to sign into Okta, the user needs to be directed to the following web address:

<https://virginiadmv.okta.com/login/login.htm>. Once at the login screen, the user will need to enter their **Username** (DMV email account), their password that they previously established, and click **Sign In**. In the event they need assistance signing in (for example, forgot password) please click on **Need help signing in?** and follow the prompts.



Sign In

Username

stephen.sales@dmv.virginia.gov

Password

☐ Remember me

Sign In

Need help signing in?

6.2 Selecting a multifactor authentication option

After completing the initial sign in, the user will be directed to the following webpage, in which they need to select an Okta multifactor for authentication. In the example below, SMS Authentication was selected, however, the user can click on the drop down menu and select another means of multifactor authentication.

Note – Users will only be given the multifactor authentication options that they have previously setup.



SMS Authentication

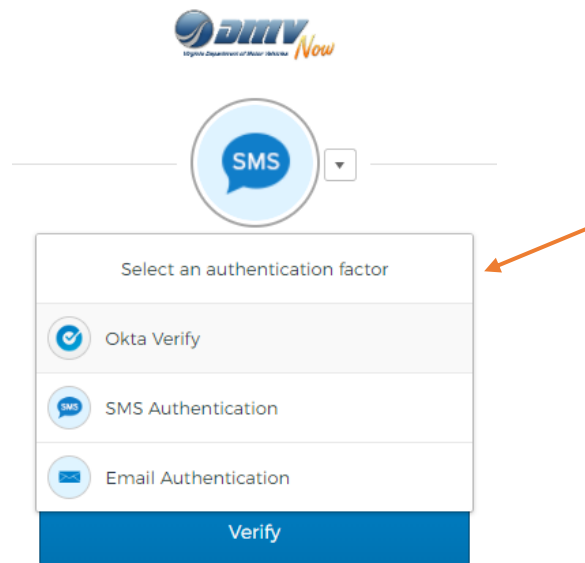
(+1 XXX-XXX-1696)

Enter Code

Send code

Verify

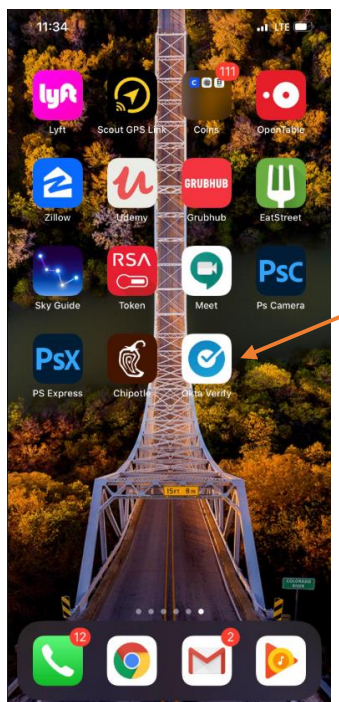
The drop down menu will give the user the ability to select other multifactor authentication options.



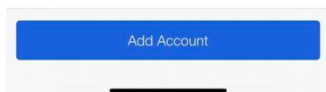
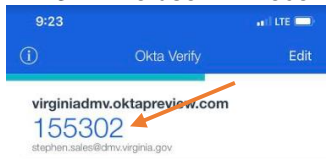
6.3 Authenticating with Okta Verify

Using Okta Verify Authentication

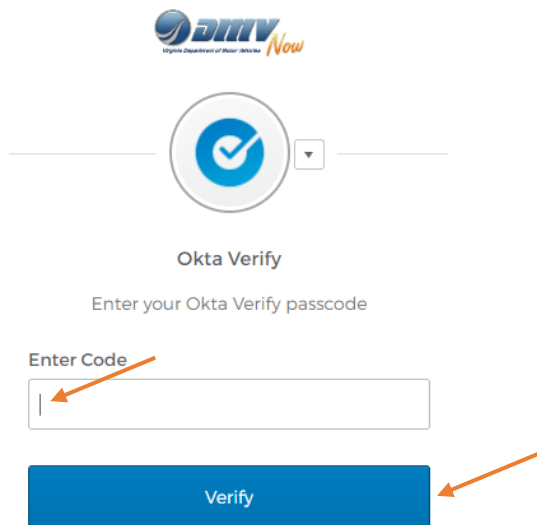
1. Click **Okta Verify**.
2. Open application on mobile device.



3. The user will receive a six-digit code within the application.





4. Enter the six-digit code into the **Enter Code** field, and click **Verify** to successfully authenticate with Okta Verify.



6.4 Authenticating with SMS

Using SMS Authentication

1. Click **SMS Authentication**.
2. Click **Send code**.

SMS Authentication



(+1 XXX-XXX-1696)

Enter Code

Send code

Verify

3. Enter the security token that was sent to your device, and click **Verify**.

SMS Authentication

(+1 XXX-XXX-1696)

Enter Code

123456

Send code

Verify

To reset and configure your settings if you lose your phone or get a new phone number, select the **Account** tab on your homepage and then click the **Setup** button in the **Extra Verification** section.

Note about SMS Messaging

By design, enabling SMS factor authentication requires that end users receive an SMS text message on their mobile devices. When this factor is enabled by an admin, end users will receive an SMS text message with an authentication code when they sign in to Okta, even if they have sent an SMS opt out request on their device. If SMS messaging is of concern to your users, you may enable another factor of your choice as an alternative.

6.5 Authenticating with Email

Using Email Authentication

1. Click **Email Authentication**
2. Click **Send me the code**

- The one-time verification code in the email is valid for 5 minutes. This time frame cannot be adjusted.



Verify with Email Authentication

Send a verification code to
s...s@dmv.virginia.gov.

Send me the code

3. Check your email for the security token.



virginiadm - Action Required: One-time verification code

Hi Stephen,

You are receiving this email because a request was made for a one-time code that can be used for authentication.

Please enter the following code for verification:

771177

If you believe you have received this email in error, please reach out to your system administrator.

This is an automatically generated message from [Okta](#). Replies are not monitored or answered.

4. Enter the security token that was sent to your email, and click **Verify**.



Verify with Email Authentication

A verification code was sent to s...s@dmv.virginia.gov. Check your email and enter the code below.

Verification code

123456

Verify

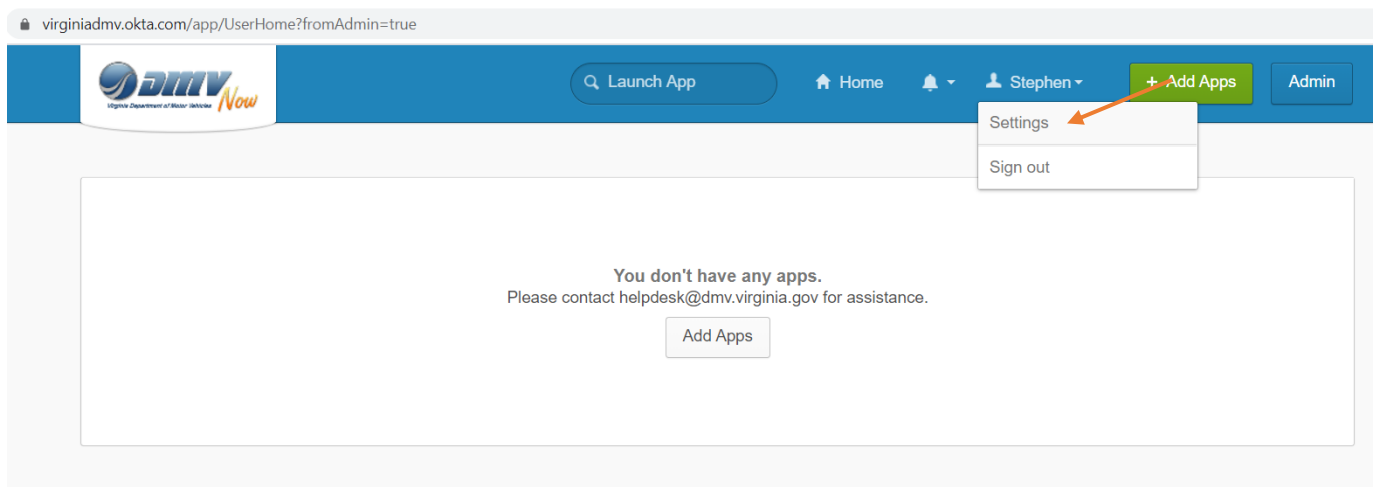
7. Updating User Profile

7.1 User Profile Modification

Note: If you reach this page during the account setup phase you are now done setting up your account, however, you can still access your profile (directions below) if you would like to access your profile features.

Accessing User Profile


1. Go to the following link: <https://virginiadmvmv.okta.com/login/login.htm> and sign in with your Okta credentials.
2. Click on **Your Name** and click **Settings** from the drop down menu.



3. Click **Edit Profile** and edit as necessary. This section will allow you to modify your personal

information, change password, add/remove other means of Okta Authentication (for example, Email, Okta Verify, and/or SMS through the **Extra Verification** option.

virginiadm.okta.com/enduser/settings?fromAdmin=true

HomeStephen+ Add AppsAdmin

Account

Edit Profile

Personal Information

First name	Stephen
Last name	Sales
Okta username	stephen.sales@dmvvirginia.gov
Primary email	stephen.sales@dmvvirginia.gov
Secondary email	
Mobile phone	
Mother maiden name	Powell

Change Password

Password requirements:

- At least 12 characters
- A lowercase letter
- An uppercase letter
- A number
- A symbol
- No parts of your username
- Your password cannot be any of your last 24 passwords
- At least 2 hour(s) must have elapsed since you last changed your password

Forgotten Password Question

Select a forgotten password question so you can reset your password in case you have trouble signing in to your Okta account.

Security Image

Your security image gives you additional assurance that you are

Extra Verification