

GM Envolve - Azure Multi Factor Authentication (MFA) Guide

Table of Contents

- Overview2
- MFA First Time Login Experience4
 - First Time Login Experience and MFA Setup4
- MFA Login Experience8
 - Login Experience for Azure migrated Applications8
- Verify and Update MFA Methods10
 - How to manage Multi-Factor Authentication (MFA) preferences.....10
- MFA Reset Process.....16
- Frequently Asked Questions (FAQs)16

Overview

What is happening?

GM is making changes to enhance security and will begin leveraging **Microsoft Multi-Factor Authentication (MFA)** for all GM applications.

What is MFA?

MFA is a security method that requires you to provide more than one form of identification at the time of login to ensure you are who you claim to be.

Why is GM launching MFA?

MFA provides a higher level of security for GM and reduces the risk of certain types of cyber-attacks. Passwords can easily be compromised – either by phishing, guessing or other techniques cybercriminals use.

What is changing?

Employees that utilize GM applications will be prompted to authenticate using MFA before they can access the application.

Who is impacted?

Employees that access GM applications will be impacted by this change. Each user will be required to have their own MFA account with Microsoft to complete the sign-in authentication with GM. Also, each user is required to have their own GM VSP Azure account to sign into GM applications. (Example: **gbrown@vsp.autopartners.net**)

What do I need to do to prepare?

You need to set up MFA preferences within Microsoft for the GM environment in order to complete the sign-in authentication with GM.

Refer to the section **Verify and Update MFA Methods** for detailed instructions on how to set up a Multi-Factor Authentication (MFA) preference.

What happens if I do not prepare?

If you do not have an MFA configured, you cannot access any GM applications that MFA has been enabled. You will be prompted to setup MFA preferences on first-time login. However, you can continue to access any GM applications that have not yet been activated for MFA. It is recommended to set up MFA now so you can readily access the applications without any disruption once MFA is enabled for all GM applications.

What MFA authentication methods are approved for usage with GM?

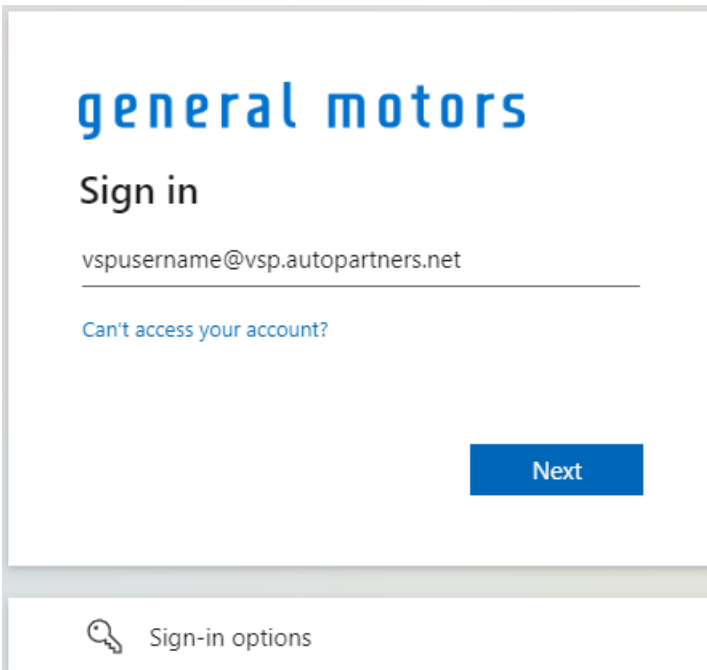
1. Text message to a cell phone.
2. Phone call to a cell or landline phone.
3. Installation of Microsoft Authenticator on a mobile device.

Note: Email is not available as a verification method because many users share email accounts. However, email will be available for account recovery purposes only.

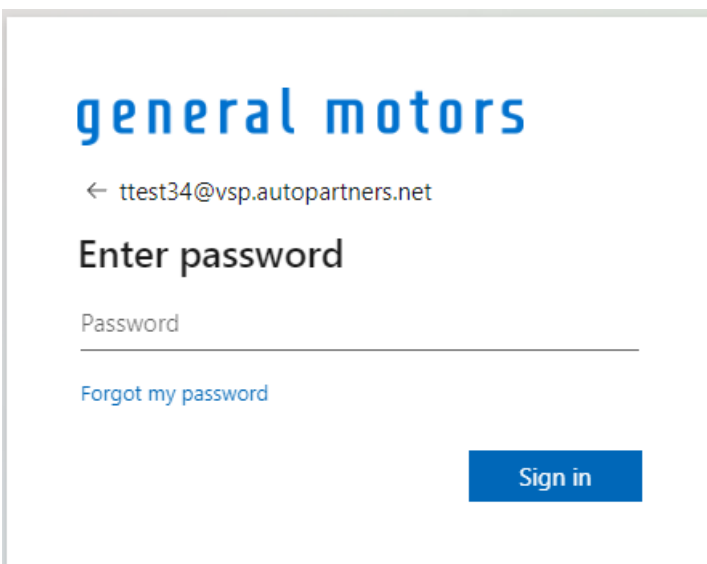
MFA First Time Login Experience

First Time Login Experience and MFA Setup

Follow these steps to sign in to Azure for accessing an application for the first time. If MFA has not been setup, it will prompt you and guide you through configuring an MFA method.



1. Sign in by replacing **vspusername** with your username.



2. Input your VSP password.

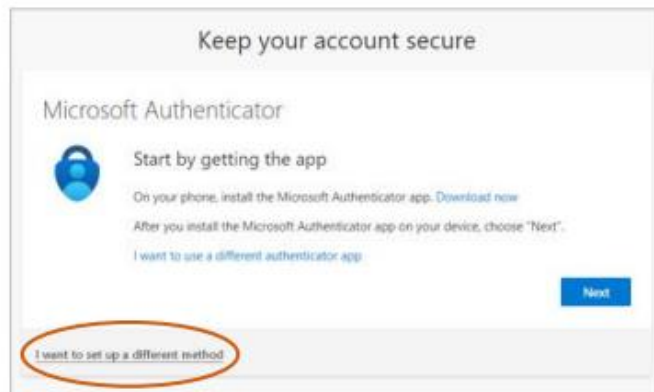
Note: If unable to access the site due to incorrect password, reset your VSP password in [Global Connect](#) and try again. Do **NOT** update your password via Azure.

3. Click **Next**.



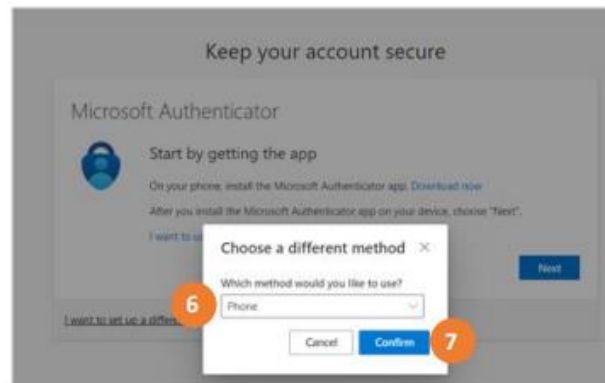
4. Read and understand the on-screen instructions.

5. It is recommended that you set up a phone number first. Click **I want to set up a different method** if you would like to register one or more phone numbers for your 2-Step Verification.



6. In the drop-down menu, select **Phone**.

7. Click **Confirm**.



8. Select your country code from the drop-down menu.

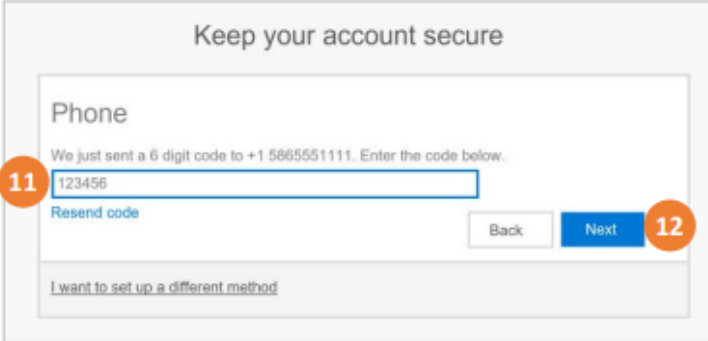
9. Enter your phone number.

10. Click **Next**.



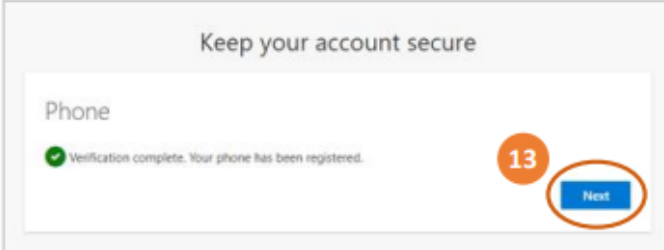
11. Enter the verification code.

12. Click **Next**.



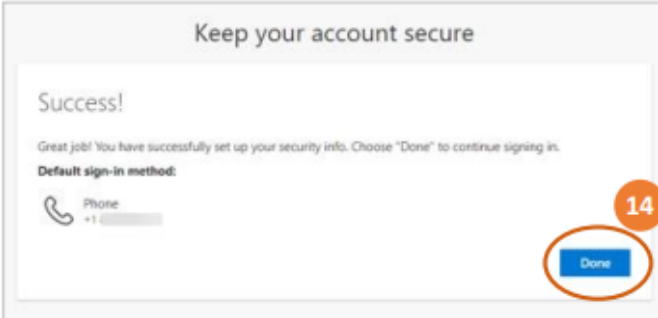
The screenshot shows a web page titled "Keep your account secure". Under the heading "Phone", it says "We just sent a 6 digit code to +1 5865551111. Enter the code below." There is a text input field containing "123456". To the left of the input field is an orange circle with the number "11". Below the input field is a link "Resend code". To the right of the input field are two buttons: "Back" and "Next". The "Next" button is highlighted with an orange circle and the number "12". At the bottom, there is a link "I want to set up a different method".

13. Click **Next**.



The screenshot shows the same "Keep your account secure" page. The "Phone" section now displays a green checkmark icon and the text "Verification complete. Your phone has been registered." To the right of this message is an orange circle with the number "13". Below the message is a blue button labeled "Next", which is circled in orange with the number "13" next to it.

14. Click **Done**.



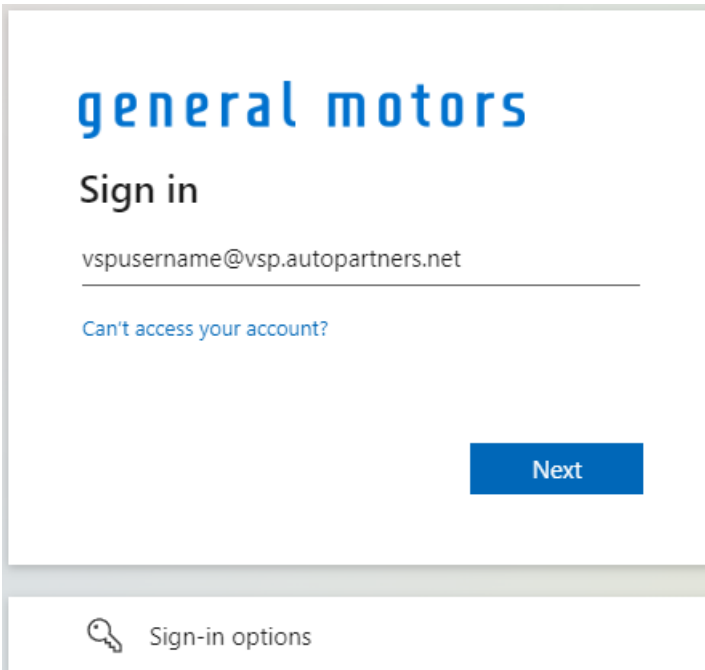
The screenshot shows the "Keep your account secure" page with a "Success!" heading. Below it, it says "Great job! You have successfully set up your security info. Choose 'Done' to continue signing in." Under the heading "Default sign-in method:", there is a phone icon and the text "Phone +1 5865551111". To the right of this information is an orange circle with the number "14". Below the information is a blue button labeled "Done", which is circled in orange with the number "14" next to it.

Note: You may not be redirected to the Azure VSP application screen. To proceed with accessing your application, close and reopen your browser.

MFA Login Experience

Login Experience for Azure migrated Applications

Follow these steps to sign in to Azure for accessing an Azure application. If MFA is configured, you will be requested to verify and complete MFA.




general motors

Sign in

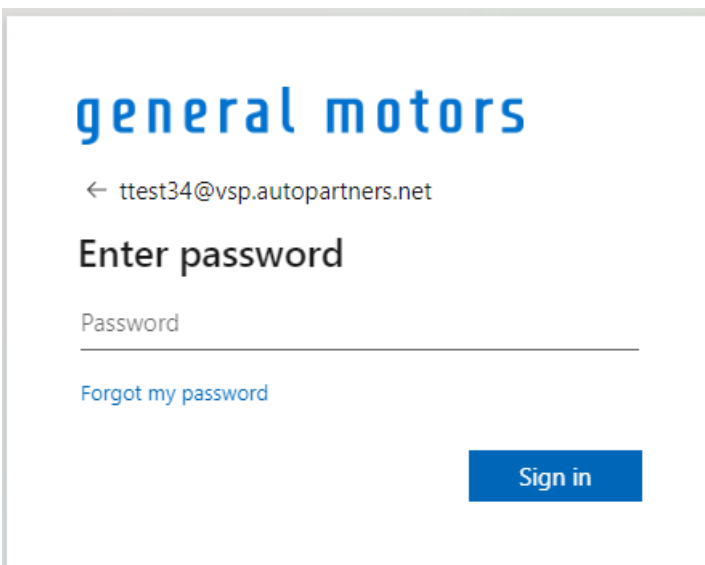
vspusername@vsp.autopartners.net

[Can't access your account?](#)

Next

 [Sign-in options](#)

1. Sign in by replacing **vspusername** with your username.



general motors

← ttest34@vsp.autopartners.net

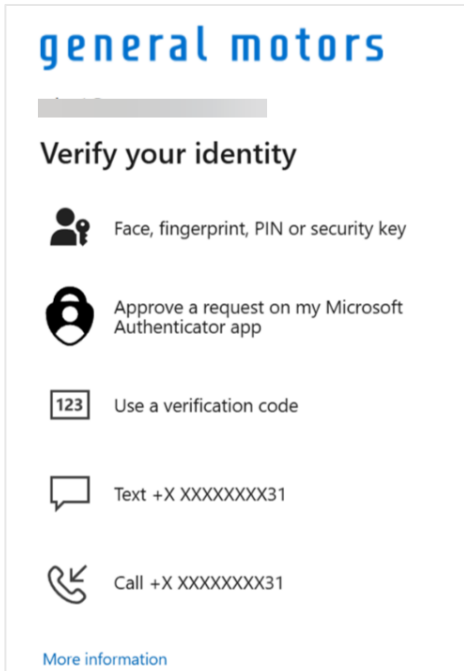
Enter password

Password

[Forgot my password](#)

Sign in

2. Input your VSP password.



3. If prompted, complete Multi-Factor Authentication (MFA).

Note: If unable to access the site due to incorrect password, reset your VSP password in **Global Connect** and try again.

Verify and Update MFA Methods

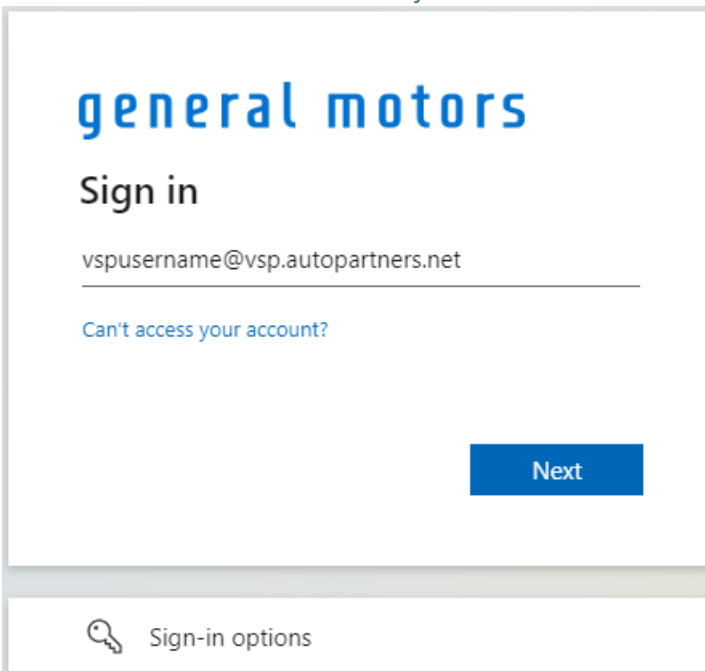
How to manage Multi-Factor Authentication (MFA) preferences

Ensuring your MFA preferences are up to date is important to keeping your account secure and ensuring you can access applications.

Follow these instructions to manage your MFA preferences. You can verify, update, or configure MFA methods, as well as setup a recovery email.

Azure Sign In

1. Visit the [Microsoft Azure Security Info website](#) and follow these steps.

A screenshot of the General Motors Azure Sign In page. The page features the 'general motors' logo in blue at the top left. Below the logo, the text 'Sign in' is displayed in a bold, dark font. Underneath, there is a text input field containing the placeholder 'vspusername@vsp.autopartners.net'. To the left of the input field, there is a link that says 'Can't access your account?'. At the bottom right of the main content area, there is a blue button labeled 'Next'. At the very bottom of the page, there is a light gray bar containing a key icon and the text 'Sign-in options'.

Sign in by replacing **vspusername** with your username.

Input your VSP password.

If unable to access the site due to incorrect password, reset your VSP password in [Global Connect](#) and try again. Do **NOT** update your password via Azure.

2. Review your phone number and email address to ensure they are accurate. If your information is correct, no further action is required. You can close the window. If either your phone number or email address are not correct or you would like to set up additional phone numbers or the Microsoft Authenticator App follow these steps to update them.

Update Multi-Factor Authentication Settings

1. Click **Change**
2. Enter the correct phone number or email address
3. Select the desired verification method
4. Click **Next**
5. Enter the verification code
6. Click **Next**
7. Click **Done**

Security info
These are the methods you use to sign into your account or reset your password.

Default sign-in method: Phone - text +1 5865551111 [Change](#)

+ Add sign-in method

Phone +1 5865551111 [Change](#) [Delete](#)

Phone

You can prove who you are by answering a call on your phone or texting a code to your phone.

What phone number would you like to use?

United States (+1) 5865551111

☒ Text me a code
☐ Call me

Message and data rates may apply. Choosing Next means that you agree to the [Terms of service](#) and [Privacy and cookies statement](#).

[Cancel](#) [Next](#)

Phone

We just sent a 6 digit code to +1 5865551111. Enter the code below.

475549

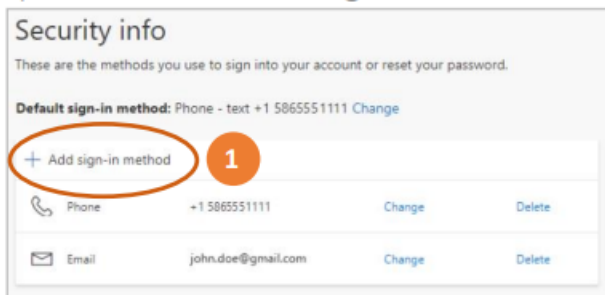
[Resend code](#)

[Back](#) [Next](#)

Add Authenticator as a Sign-in Method

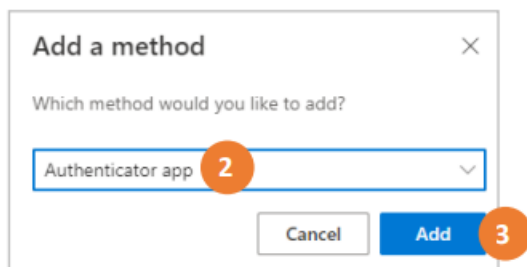
If you want to add an authenticator app as a sign-in method on your mobile device, follow the steps below.

1. Using a desktop browser, click **Add sign-in method**.



2. Select **Authenticator app** from the drop-down.

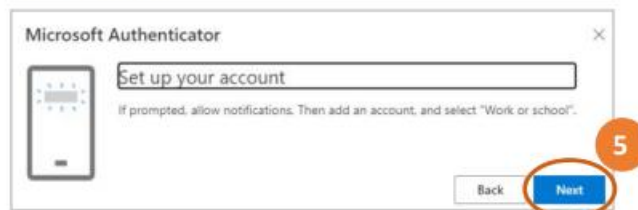
3. Click **Add**.



4. Open the **Microsoft Authenticator** application on your mobile device. If you do not have the latest version of the app currently installed, scan the QR code below for your device type or search for the Microsoft Authenticator app in the Google Play Store or the App Store and follow on-screen instructions to install.

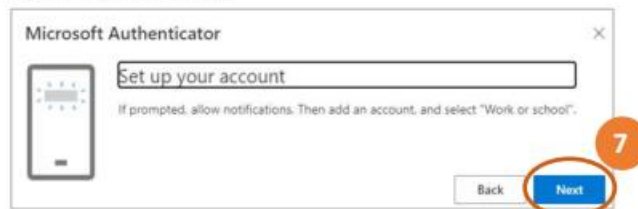


5. Click **Next** on your computer.



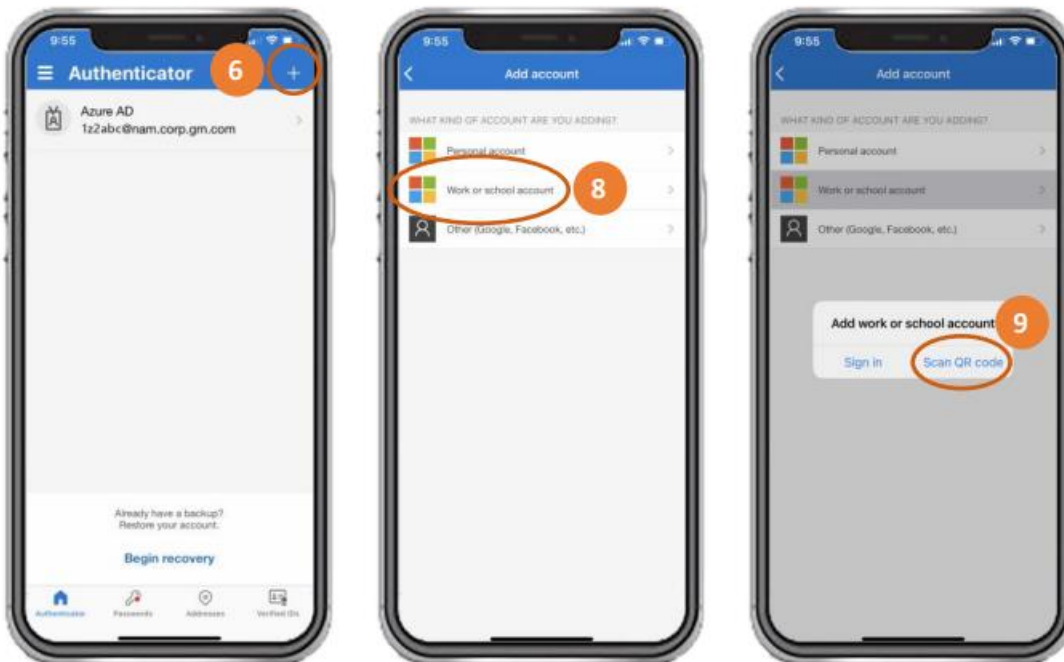
6. With the Microsoft Authenticator app open on your mobile device, tap the + plus sign in the upper-right corner.

7. On your computer, click **Next**.



8. On your mobile device, tap **Work or school account**.

9. On your mobile device, tap **Scan QR code**.



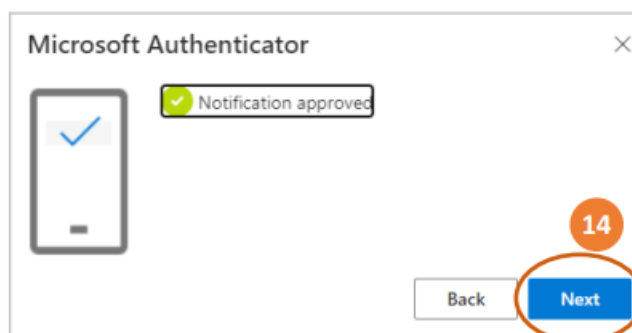
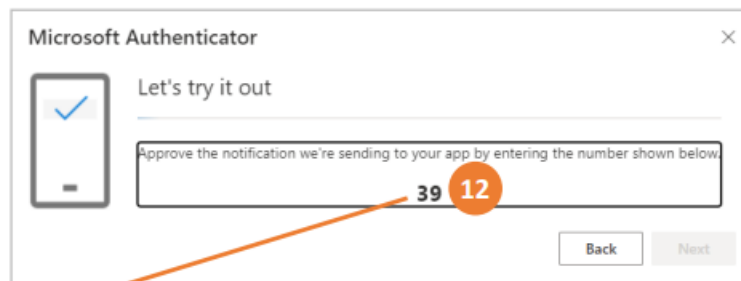
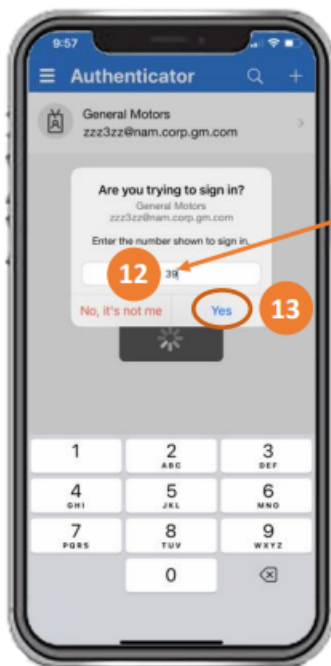
10. Scan the generated QR code on your computer screen using the camera on your mobile device.

11. On your computer, click **Next**.

12. Enter the code displayed on your computer screen into the field on the app.

13. On your mobile device, tap **Yes**.

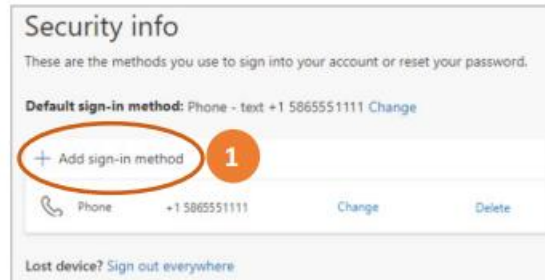
14. Click **Next** on your computer.



Add Email as a Recovery Method

In the future version of MFA, email cannot be used as a verification method, but it will be used for account recovery. To add your email to your profile, follow the steps below.

1. Click **Add sign-in method**.
2. Select **Email** from the drop-down.
3. Click **Add**.
4. Enter a non-GM email address.
5. Click **Next**.
6. Enter the security code sent to that email address.
7. Click **Next**.
8. You will see a confirmation message in the upper-right corner and email will be added to your list of methods.



Security info

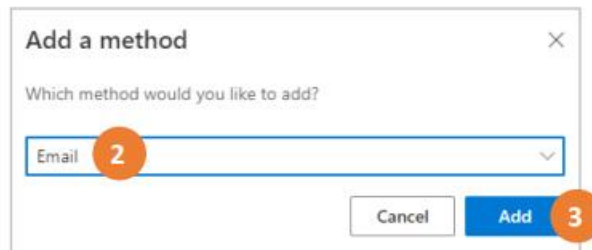
These are the methods you use to sign into your account or reset your password.

Default sign-in method: Phone - text +1 5865551111 [Change](#)

+ Add sign-in method 1

Phone +1 5865551111 [Change](#) [Delete](#)

[Lost device? Sign out everywhere](#)

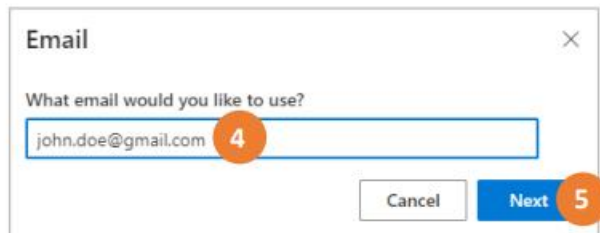


Add a method

Which method would you like to add?

Email 2

[Cancel](#) [Add](#) 3

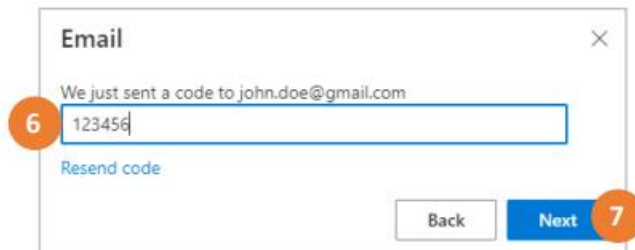


Email

What email would you like to use?

john.doe@gmail.com 4

[Cancel](#) [Next](#) 5



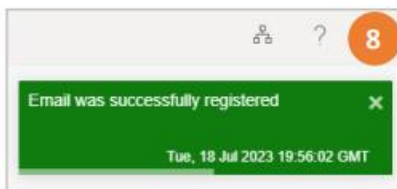
Email

We just sent a code to john.doe@gmail.com

123456 6

[Resend code](#)

[Back](#) [Next](#) 7



MFA Reset Process

Azure MFA Reset is typically requested when a user has no usable Azure MFA method, for example, user only has one MFA phone registered and the phone is lost.

A reset is the last resort and must be requested only when a user is unable to manage their Azure MFA methods via self-service in the Microsoft Azure [Security info](#) site.

Who do I contact if I require assistance?

If you require assistance, please contact the US [GM Envolv Solutions Center](#)

USA Support Center:

Phone: [1-800-353-3867](tel:1-800-353-3867)

Email: gmenvolvesolutionscenter.service@gm.com

What to Expect After MFA Reset

When the user accesses an Azure MFA protected, they will be prompted to set up their MFA methods.

The process to set up Azure MFA is the same as described in the **MFA First Time Login – Setting Up MFA** section of the document.

Frequently Asked Questions (FAQs)

Do I need to complete MFA authentication every time I access a different GM application?

No, once you complete MFA authentication with one GM application you are authenticated to access all GM applications utilizing MFA. The authentication remains valid as long as your internet browser window is active and has not timed out. If you time-out or logout, you need to re-authenticate using MFA.

What if I already have an MFA account with my organization or a personal account?

You must have a separate MFA account with Microsoft for the GM environment in order to complete the sign-in authentication with GM and access GM applications.

Important Reminder:

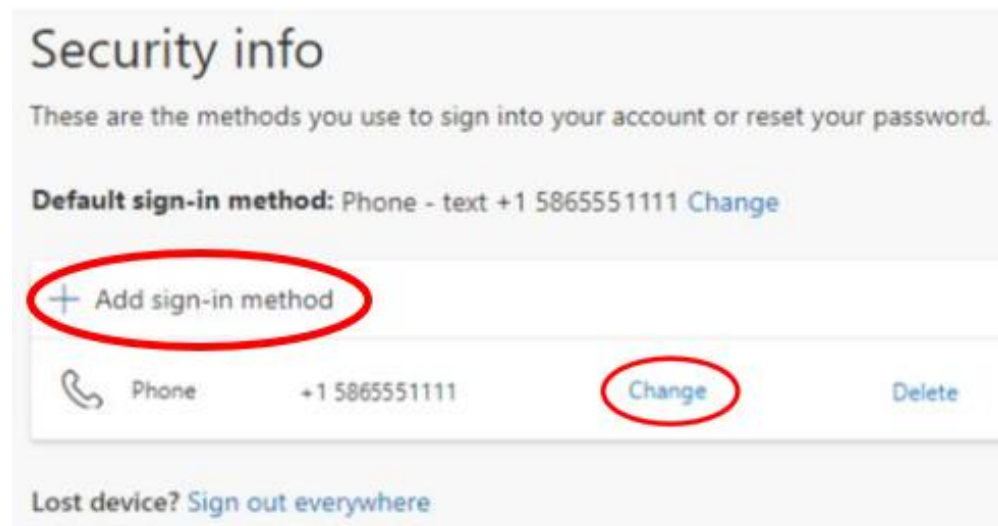
Keeping your MFA contact information up to date is important since it is used to gain and maintain access into the GM environment for GM applications. Ensure you update your MFA contact information whenever it changes. Go to the Microsoft MFA site to update your account.

<https://aka.ms/mfasetup>

Sign into Microsoft with your account or if you are prompted with a list of different accounts, select the account you want to adjust the MFA settings for. Ensure you select your GM account.

To modify your phone number, click “**Change**” and follow the prompts to complete the change.

To add a new sign-in method, click on “**Add Sign-in method**” and follow the prompts to complete the set up.

**Who do I contact if I require assistance?**

If you require assistance, please contact the US GM Envolv Solutions Center

USA Support Center:

Phone: [1-800-353-3867](tel:1-800-353-3867)

Email: gmenvolvesolutionscenter.service@gm.com

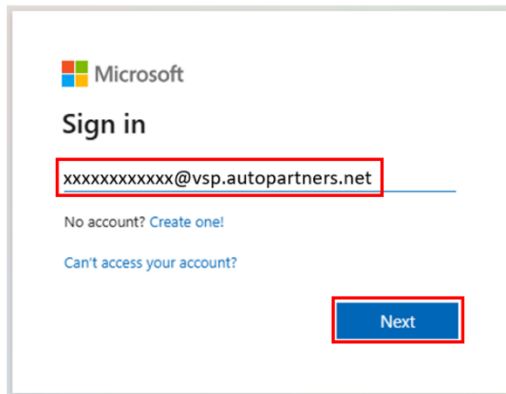
How do I set up a Multi-Factor Authentication (MFA) account with GM?

1. Go to the Microsoft site.

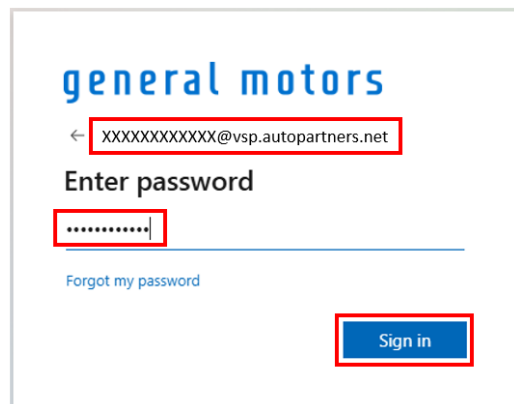
<https://aka.ms/mfasetup>

2. You will be presented with the following sign-in screen. Enter your existing GM user ID that you use to log into GM applications with followed by the GM domain address. Click **“Next”**.

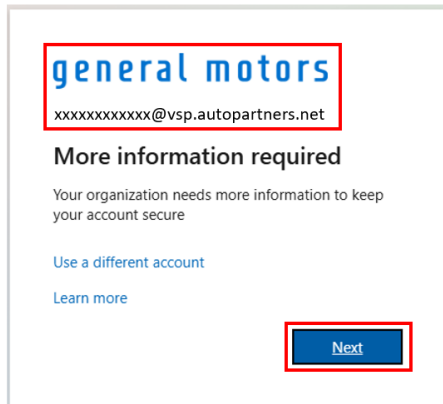
Example: **XXXXXXXXXX@vsp.autopartners.net** (XXXXXXXXXX = gbrown)

A screenshot of the Microsoft sign-in page. At the top is the Microsoft logo. Below it is the text "Sign in". There is a text input field containing "xxxxxxxxxx@vsp.autopartners.net", which is highlighted with a red rectangle. Below the input field are two links: "No account? Create one!" and "Can't access your account?". At the bottom right is a blue button labeled "Next", also highlighted with a red rectangle.

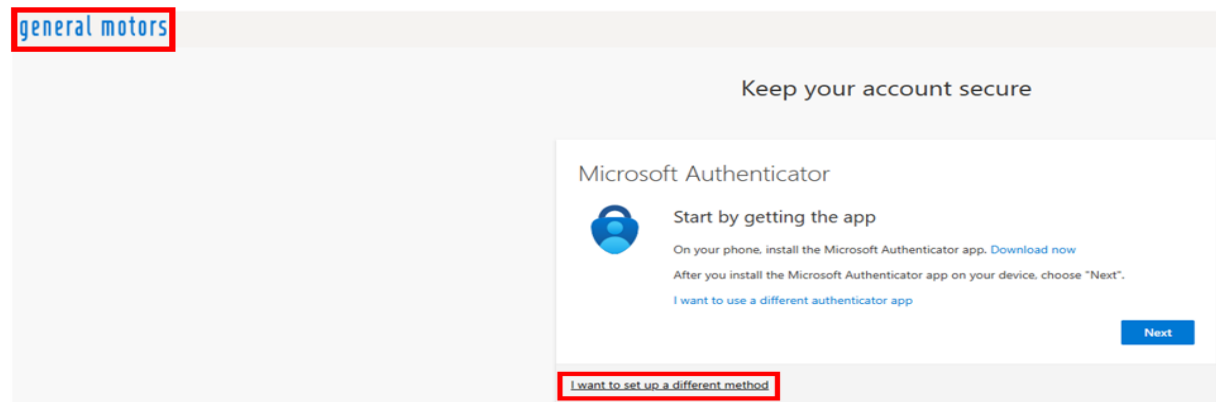
3. You will be prompted to enter your password. Enter the existing password that you use for your GM user ID. Click **“Sign in”**.

A screenshot of the General Motors sign-in page. At the top is the "general motors" logo. Below it is a back arrow icon followed by the text "xxxxxxxxxx@vsp.autopartners.net", which is highlighted with a red rectangle. Below this is the text "Enter password". There is a password input field containing "*****", which is highlighted with a red rectangle. Below the input field is a link: "Forgot my password". At the bottom right is a blue button labeled "Sign in", also highlighted with a red rectangle.

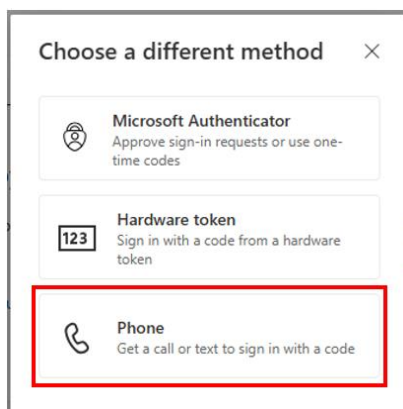
4. You will be presented with the following screen. Click **“Next”**.



5. You will be prompted with the following screen. Click on **“I want to set up a different method”**. The easiest method to use is a text message to a cell phone.



6. You will be presented with the following screen. Click **“Phone”**.



7. Enter your phone number and select **“Receive a code”**. Click **“Next”**. A code will be sent to your cell phone via text message.

Phone

You can prove who you are by answering a call on your phone or receiving a code on your phone.

What phone number would you like to use?

Canada (+1) 416-123-4567

☒ Receive a code

☐ Call me

Message and data rates may apply. Choosing Next means that you agree to the [Terms of service](#) and [Privacy and cookies statement](#).

Next

[I want to set up a different method](#)

8. Enter the 6-digit code in the appropriate field and click “Next”.

Keep your account secure

Your organization requires you to set up the following methods of proving who you are.

Phone

We just sent a 6 digit code to +1 416-123-4567. Enter the code below.

123456

[Resend code](#)

Back Next

[I want to set up a different method](#)

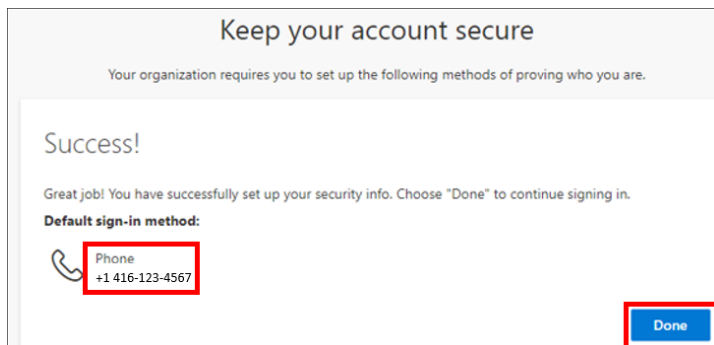
9. You will receive a confirmation that your phone is registered. Click “Next”.

Phone

✓ Verification complete. Your phone has been registered.

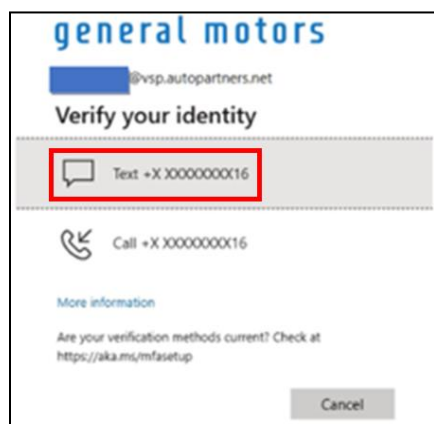
Next

10. You will receive another confirmation indicating you have successfully set up your security information. Click “Done”.

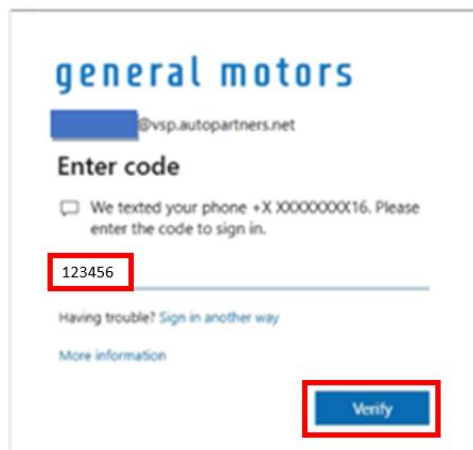


11. This completes the initial MFA setup.

12. When you access GM applications you will be presented with the following MFA screen. Select “**Text**”.



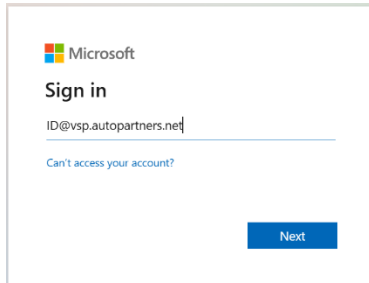
13. Enter the code you received from the text message. Click “**Verify**”.



14. The GM application will be opened.

How do I log in with a VSP Account?

1. Once your MFA (Multi Factor Account) preferences are set up, you will be prompted to sign in using your credentials.
2. Login via VSP users ID and password ID@vsp.autopartners.net



3. After logging in with your credentials, you will see a list of available verification options. Select your preferred method and verify your identity

