Microsoft MFA

Frequently asked questions

February 2020

FAQ

Authentication options & troubleshooting

AUTHENTICATION OPTIONS & PROCESS

1. How do I enroll in MFA?

Information surrounding enrollment in MFA is available on ACaeronet; please visit the MFA overview page to access the detailed enrollment guides for mobile devices and corporate-issued iPads.

Note: Frontline employees that were not issued a corporate device may request an MFA token via ServiceNow. There is no cost for the initial token ordered. Any additional tokens requested would be at a cost of $25 (CAD) each.

2. How do I authenticate using MFA?

When attempting to access MFA-enabled applications from outside the Air Canada network, MFA confirms your identity using a combination of two different factors: your ACaeronet password and a code generated by either a mobile device (or received via SMS text message) or an MFA token (or "allowing" access via push notifications from your mobile device).

Once you successfully enter your username and password, you will receive a second prompt to further verify your identity through the preferred authentication method selected during the MFA enrollment process or by providing the code generated by your MFA token. Upon successful verification, you will be able to access the MFA-enabled application.*

**MFA-enabled applications are: ACaeronet, HR Connex portal, Employee Travel Site, Air Canada SharePoint sites, Microsoft Services (O365, Sharepoint, Teams etc.) and VPN.*

3. What authentication options do I have?

Employees who have enrolled in MFA using a mobile device have three (3) options to choose from:

Option	Details	Recommended to…
A – Verification code	*****Mandatory option for enrollment using corporate-issued iPad or phone***** • Requires a smart mobile device* • Requires downloading the Microsoft Authenticator app • Does not require connection to an internet or mobile network (i.e., will work in Airplane Mode) to use the app	• All users enrolling a corporate-issued iPad • Users who want uninterrupted access to MFA, regardless if they are connected to an internet or mobile network. Example: those who are often flying (pilots, service directors & flight attendants)
B – Notification	• Requires to have a smart mobile device* • Requires downloading the Microsoft Authenticator app. • Requires connection to an internet or mobile network (i.e., will **NOT** work in Airplane Mode) to use the app	• Users who are often connected to a Wi-Fi
C – SMS	• Does not require a smart mobile device* (i.e., you may use an older mobile phone without smart features).	• Users who do not have a smart mobile device

	• Requires connection to a mobile network (i.e., will **NOT** work in Airplane Mode)	

**A smart mobile device has internet access and can download applications.*

Employees who have an MFA token can authenticate by entering the code generated by their token.

4. Can I select back-up authentication methods?

Yes. Each employee can have up to five (5) devices (including an MFA token) and authenticate from any of them, anytime, anywhere. If you have an MFA token and would like to have the option to authenticate from other devices, follow the instructions on the MFA Token Overview Guide available on the MFA overview page.

During the MFA Profile setup for mobile devices, you are asked for a secondary authentication option if you choose to use the "Authenticator" app. If you skipped this step and would like to set up back-up authentication methods to prevent the likelihood of being locked out of MFA-enabled applications, go to the MFA overview page, then click on the "Change my settings" link and follow the user guide steps.

Please note that if you have registered for MFA using several different authentication options (i.e., SMS, and push notification), you will not always receive notifications via all options. The sign-in screen will allow you the option to receive a code or notification via another means if your default option is not available to you (i.e., your cell phone being outside of network coverage).

5. Am I required to authenticate each time I login to an MFA-enabled application from outside the Air Canada network?

As MFA is browser-based, if you login to an application with one browser and then switch to a different one to access the same or any other MFA-enabled application, you will be asked to provide second factor authentication again. Likewise, if you restart or shut down your computer you will be asked to provide second factor authentication as well.

6. How long do I have to authenticate using MFA?

When accessing MFA-enabled applications, the requestor has approximately 60 seconds to respond to the MFA prompt before timing out.

If you are unable to respond within this timeframe and would like to try again, please perform one of the following:

- **Web Browser**:
  1. Click the URL in the browser window and hit "Enter" or refresh the webpage, which will force MFA to resend an authentication request.
  2. If neither option works, you need to completely close your browser and retry access, which will create another authentication request.
  3. When presented with the "Approve sign in request" window, click 'Sign in another way' in order to use a different verification option.

Note: This option requires the user to have already configured a secondary authentication option (i.e., SMS). During your initial MFA Profile setup, you are asked for a secondary authentication option if you choose the Mobile App.

If you skipped this step and would like to setup back-up authentication methods to prevent the likelihood of being locked out of MFA-enabled applications, go to the MFA overview page, then click on the "Change my settings" link and follow the user guide steps.

- **Web Application**
  1. Close your application and restart, which will resend an authentication prompt.

MICROSOFT AUTHENTICATOR APP

7. What data does the Microsoft Authenticator app store on my behalf?

Microsoft Authenticator app stores the account information you create when you add an account. This information is confidential and is not shared with Air Canada. It is used solely for the authentication process. MFA does not allow Air Canada to see anything on your device, track your whereabouts or your device activity. Your own privacy is 100 per cent protected.

8. Does the Microsoft Authenticator app require data usage and/or additional fees?

It depends on the option you select during the enrollment process.

- Verification code option (through Microsoft Authenticator app) is always available and is free of charge, as it does not require data usage or Wi-Fi.
- Push notifications (through Microsoft Authenticator app) require minimal data usage, or a Wi-Fi connection.
- SMS messages could result in additional fees and charges depending on your your phone plan.

9. What are the codes in the Microsoft Authenticator app for? Why does the number keep counting down?

These codes are the second factor authentication you will be prompted to enter when accessing an MFA-enabled application. They change every 30 seconds so you never use the same code twice.

The codes do not require internet or data, so you do not have to worry about being connected to the Internet or having phone service to access them.

MFA Token

10. Does the MFA token require Wi-Fi or data to function?

No. Instead, your MFA token will generate single-use codes that provide you a second factor of authentication when logging-in to MFA-enabled applications from outside the Air Canada network. You simply press the button on your MFA token and a unique code will appear for you to enter into the MFA prompt screen.

11. Can I use someone else's MFA token to authenticate myself?

No. Each token is registered to an individual account. Codes generated on a different MFA token will therefore not allow you to authenticate if entered into an MFA prompt screen when trying to access your account.

12. Do I have to use the MFA token to authenticate myself?

If you have an MFA token, you can still enroll up to four (4) additional personal devices and authenticate from any of them (including the MFA token), anytime, anywhere. To add additional devices, please follow the instructions on the MFA Token Overview Guide available on the MFA overview page.

TROUBLESHOOTING

13. If I need assistance with MFA-related matters, who can I talk to?

If you are experiencing issues with MFA enrollment or authentication, try closing the browser and clearing your web browser's cookies and cache.

For all other issues, including questions surrounding your MFA token, or if you need immediate assistance, please contact the Help Desk at 1-866-274-5444 or at 1 (514) 422-4357 (within Montreal or outside of Canada and the United States).

14. How do I change my preferred MFA authentication method?

Start by accessing the MFA overview page, then click on the 'Change my settings' link and follow the user guide steps. If you currently only use an MFA token, then you will need to enroll an additional personal device (up to four others) in order to change your preferred MFA authentication method.

Note: We highly encourage you to select and keep the "Verification Code" option (A) as your preferred verification method. For users enrolling using a corporate-issued iPad, the Verification Code option (A) is mandatory.

15. What happens if my MFA token and/or mobile device(s) are unavailable and I need to access an MFA-enabled application?

If you do not have access to any of your enrolled mobile devices (including your MFA token), please call the Help Desk at 1-866 274-5444 (North America) or at 1 (514) 422-4357 (within Montreal or outside of Canada and the United States) for assistance

16. What do I need to do if I change my mobile device used for MFA authentication?

It depends on the MFA authentication type you have selected during enrollment:

- **If your MFA profile is configured to text a phone number** and the device has changed but the number remains the same, then no changes are required.
- **If your MFA profile is configured to the Mobile App option**, then your MFA Profile must be updated (please configure Authenticator App). To change your settings, start by accessing the MFA overview page, sign-in with your Air Canada credentials and follow the link in the change settings section to access the guide. Follow the steps in the change settings user guide.

17. What do I do if I only get notifications when I have the Microsoft Authenticator app open?

To get notifications, you need to enable the app to use sound or vibrate with its notifications.

If the app is enabled and you still do not get notifications, please check for the following:

- **Is your phone in 'Airplane Mode', 'Do Not Disturb' or 'Quiet' mode?** These modes can prevent apps from sending notifications.
- **Are you receiving notifications from other apps?** If not, there may be an issue with the network connection on your phone, or the notifications channel from Android or Apple. You can address the first scenario in your phone settings, but you may need to talk to your service provider for help with the second scenario.
- **Can you receive notifications for some accounts on the app, but not others?** If yes, remove the problematic account from your app and add it again to enable push notifications.

18. How do I remove an account from the app?

- **iOS:** From the menu button in the top left corner of the app (3 horizontal bars), select "Edit accounts" and swipe left on an account tile and tap "Delete".
- **Windows Phone:** From the main screen, select the menu button, then "Edit accounts". Tap the "X" next to the account name.
- **Android:** From the main screen, select the menu button, then "Edit accounts". Tap the "X" next to the account.

19. How do I authenticate if my mobile device is not connected to a network (for example, when in flight)?

If your mobile device does not have any connection to a mobile or Wi-Fi network you can still authenticate using the verification code option through the Microsoft Authenticator app. The same applies if the push notification or SMS option are not working. When presented with the "Approve sign in request" window, click "Sign in another way" in order to use a different verification option.

Note: This option requires the user to have already configured a secondary authentication option during your initial MFA Profile setup if you chose the Microsoft Authenticator app (options A & B).

If you skipped this step and would like to setup back-up authentication methods to prevent the likelihood of being locked out of MFA-enabled applications, go to the MFA overview page, then click on the 'Change my settings' link and follow the user guide steps.

20. What do I do if I receive a push notification to approve access even though I am not trying to access an MFA-enabled application?

This may happen if someone else is trying to access your account. You should deny the request and immediately call the Help Desk at 1-866 274-5444 or at 1 (514) 422-4357 (within Montreal or from outside Canada and the United States).

21. Why am I being inconsistently prompted for my second factor authentication?

There are four (4) situations that may explain why you are not consistently prompted for your second factor authentication:

1. You did not sign out from your ACaeronet account.
2. You did not close your browser.
3. You answered "Yes" to the question "Stay signed in?".
4. Artificial Intelligence (there are risk calculations that take into consideration multiple factors such as location and device. For example, if you log in frequently to MFA-enabled applications from the same network (i.e., your home Wi-Fi) the number of times you are required to authenticate will diminish.

If you have any further questions, please reach out to MFA_Program@aircanada.ca