Improved Cybersecurity Controls

January 2025

Key Messages

- The cybersecurity of Government of Saskatchewan accounts will be getting stronger. You may experience the need to use multifactor authentication in more situations than before.
- Restrictions will be based on your location and whether you are using a Government of Saskatchewan device.
- Multifactor authentication requires users to identify themselves in more than one way. It usually includes a password and a code sent to a trusted device like your cellphone or a fingerprint. Soon, text and phone call authentication will not be a multifactor authentication option.
- If you have not already done so, please download the Authenticator app on your mobile device so your access to government systems, information and files is not interrupted. The Authenticator app is the primary method for multifactor authentication.
- If you are unable to use the Authenticator app, contact your supervisor or ministry Security Officer to determine if you are eligible to receive a FIDO2 security key.
- Please complete the ServiceNow password reset verification enrolment if you have not done so already. The Information Technology Division Service Desk will use those questions to verify your identity if you have issues with multi-factor authentication.
- You can confirm if you have downloaded the Authenticator app and are enrolled in the ServiceNow password reset verification system by following the instructions in the How to Check Your Multifactor Authentication Readiness document.
- For additional information, please visit Taskroom's new Multifactor Authentication page or contact your security officer.

QUESTIONS AND ANSWERS:

- Required actions – Updated INSERT DATE
- Impact of multifactor authentication (MFA)
- Phasing out of text message and phone MFA – UPDATED INSERT DATE
- Microsoft Authenticator App
- Security of information
- FIDO2 security key
- ServiceNow password reset verification – UPDATED INSERT DATE
- Questions

Saskatchewan

Improved Cybersecurity Controls

January 2025

REQUIRED ACTIONS

What is multifactor authentication (MFA)?

MFA is a modern practice of proving you are who you say you are in more than one way online. In today's information technology world, a password is no longer enough to protect government systems and data, as hacking techniques become more advanced and sophisticated.

MFA asks you to verify your identity in many ways, typically in this format:

a) Something you know (like a password)
b) Something you have (like a trusted mobile device)
c) Something you are (like a fingerprint)

Even if an attacker knows your password, they cannot gain access to government systems and data without the other two factors as well.

What is the Microsoft Authenticator app?

The Microsoft Authenticator app is a modern, secure and free app for your Apple iOS or Android mobile devices that is the Government of Saskatchewan's (GOS) preferred tool for employees to use to perform MFA.

What is a FIDO2 security key?

FIDO2 security key is a modern device with a fingerprint reader that you can use to perform MFA. You register a PIN and your fingerprint on the FIDO2 security key, then link the FIDO2 security key to your user account and plug it into your computer. When you are prompted for MFA, you provide your PIN and touch the fingerprint reader on the FIDO2 security key. The FIDO2 security key is an alternative MFA tool if Authenticator cannot be used.

I have already installed the Authenticator app or FIDO2 and have been using it for a while. How will I be impacted by these changes?

Staff who do not have the Authenticator app correctly installed or a FIDO2 security key/token will need to take **additional action**. All staff will still need to ensure the ServiceNow password reset verification enrolment is complete.

How do I know if I need to take further action with the Authenticator app?

Please follow the instructions in the How to Check Your Multifactor Authentication Readiness. By following a few easy steps, you'll know whether further action is needed.

Improved Cybersecurity Controls

January 2025

Why is it important to complete the ServiceNow password reset verification enrolment?

If there are issues with MFA or if a user loses their mobile device or FIDO2 security key, they will need to call the Information Technology Division (ITD) Service Desk at 306-787-5000 to gain access to the requested system or files. The ITD Service Desk will only be able to confirm your identity by asking you the password reset questions. If you have not enrolled, they won't be able to confirm your identity, and you won't be able to access the files or systems you need until your identity is verified. This rule applies to everyone with no exceptions.

How do I know if I need to complete the ServiceNow password reset verification enrolment?

Please follow the instructions on the second page of the How to Check Your Multifactor Authentication Readiness document.

How do I enroll in the ServiceNow password reset verification system?

Follow the instructions in Password Reset Enrollment document.

When would I have to set up MFA or complete the ServiceNow password reset verification again?

If you receive a new GOS username (for example, you got a job in a new ministry). Both MFA and ServiceNow password reset verification are associated with your username.

Note: if you change jobs within one ministry, you will have the same GOS username, so no action is required.

IMPACT OF MULTI-FACTOR AUTHORIZATION (MFA)

Is the hassle of MFA worth it?

Yes! Modern MFA is the most effective way to protect user accounts. Extensive cybersecurity research has shown that user accounts protected by MFA are over 99 per cent less likely to be compromised.

I already get prompted for MFA on occasion, so what is changing?

MFA prompts will happen more often. Still, if you are in a government office on a government computer, you should not expect to see an MFA prompt in most cases. Situations requiring MFA will vary and evolve. Generally, if you are in the office using a GOS device, you will not receive an MFA unless you are working on a critical app.

Will this transition affect all my devices?

This change is happening to your account, which can be used on multiple devices. The Authenticator app will go on your phone only but can be used when you access data from any computer.

Am I going to be kicked off important files if I'm not using a trusted device?

No, you will be prompted by MFA to access the files.

How often will I need to use MFA?

The frequency of MFA prompts depends on several factors.

If you only work in a GOS location on a GOS computer, you will not be prompted for MFA unless there is a security risk detected for your user account (for example, impossible travel between two locations that your user account logged in from).

If you work on a GOS device in a non-GOS location (for example, working from home), the baseline for MFA frequency is once every 90 days. You will receive MFA prompts more regularly if there is a change in the general status of your network security, like if your password changes, there is a security risk on your account as described above or there is a change to the network at the non-GOS location you work from.

If you work in many different non-GOS locations (for example, you travel to different sites), you will generally experience an MFA prompt each time you connect from a new non-GOS network or access the GOS system from a new non-GOS computer.

PHASING OUT OF TEXT MESSAGE AND PHONE MFA

Why can't I continue to use text messaging or phone calls for MFA?

Text messages and phone calls will be phased out because the systems these methods are built on were never designed for cybersecurity. It is easy for attackers to bypass text message and phone MFA methods. GOS will eventually only allow modern MFA methods such as the Microsoft Authenticator app and FIDO2 security keys.

How will text message and phone MFA be phased out?

If you are prompted for MFA and have not yet set up the Authenticator app or a FIDO2 security key, you will see a window asking you to set up the Authenticator app. You can snooze this window up to three times for 14 days each time, after which you must set up modern MFA.

Once you set up a new MFA method, it becomes your default MFA method, and you will not be able to change your default method back to text or phone messaging.

As we transition to our new MFA standard, eventually the text message and phone MFA will be turned off. This will be clearly communicated ahead of time, but we encourage all GOS users to begin this transition immediately.

Improved Cybersecurity Controls

January 2025

When will text message and phone MFA be turned off?

This date will be communicated well in advance, but the tentative date is September 2025.

MICROSOFT AUTHENTICATOR APP

I have already installed the Authenticator app on my mobile phone. Is there anything else I must do to be ready for MFA?

In addition to installing the Authenticator app, you need to follow the Enrolling in the Microsoft Authenticator App document's instructions to register your work account in the Authenticator app before you are ready to perform MFA.

I enrolled in the ServiceNow password reset verification system with the Microsoft Authenticator option. Am I ready for MFA?

No. Enrolling in the ServiceNow password reset verification system with the Authenticator app is separate from enrolling in the Authenticator app for MFA.

Is there anything else I should know about setting up the Authenticator app?

If you are setting up the Authenticator app (or any other MFA method) while not on a GOS device, you will be prompted for MFA.

If you are a new user, you will be issued a one-time code you can use for this MFA prompt to set up your MFA.

Otherwise, if you don't already have an MFA method set up, you'll need to contact the ITD Service Desk at 306-787-5000 for assistance.

I don't have a government-issued mobile phone. Can I still use the Microsoft Authenticator app?

Yes. The Microsoft Authenticator app can be installed on any mobile device, including personal ones. It can also be used for personal accounts in addition to your government work account to make your personal accounts more secure.

How will the Authenticator app and MFA be impacted if I change to a new work cell phone?

A: If you receive a new cell phone, you will need to set up the Authenticator app on the new phone.

You may be prompted for MFA when you attempt to do so. If you have access to your old phone with the Authenticator app installed, you can use it to complete MFA.

Otherwise please contact the ITD Service Desk for assistance at 306-787-5000 with setting up the Authenticator app on your new phone.

Can I still use the Authenticator app when my cell phone does not have data or internet access?

A: Yes. Please see the How to Use the Authenticator App Offline document.

SECURITY OF INFORMATION

What level of control or visibility will the government have over my personal phone if I install the Authenticator app?

None. The Authenticator app doesn't give the government any control over or visibility into your personal phone.

Are there any other apps I need to install on my personal phone to use Authenticator for MFA?

A: No. Other apps, such as the Trellix or Microsoft Defender security apps, are not required to install the Authenticator app on a personal phone before it can be used for MFA.

However, if you also want to access GOS files or data such as your work email directly from your personal phone, you will then need to also install any required cybersecurity apps on your personal phone.

I don't want to use my personal phone for this. How else can I access files I need?

Depending on your job role, your ministry, agency, or government organization may decide to procure a FIDO2 key. Otherwise, you will be required to contact the ITD Service Desk when you are prompted for MFA.

FIDO2 SECURITY KEY

I can't use a mobile device during work hours. How will I perform MFA?

A: Your ministry can order a FIDO2 security key if you will be regularly prompted for MFA. If you work in a government office, you won't be regularly prompted. If you are prompted and don't have a FIDO2 key, you must contact the ITD Service Desk at 306-787-5000.

Should I be concerned about the privacy of my biometric data, like my fingerprint, if I'm using the FIDO2 key?

No. You don't need to worry about the privacy of your biometrics data, such as facial recognition or fingerprint. FIDO2 security keys don't store actual biometric data in their raw form. When you set up a device for MFA (e.g., the Authenticator app on a mobile phone or a FIDO2 security key), the device stores a representation of your biometrics. This representation is encrypted and cannot be exported or stolen from the device.

When you perform MFA, the device compares the biometric you present (e.g., the finger you touch) with the representation it has stored to determine if the two match. It then sends a binary yes/no to the system. The representation of your biometric never leaves the device.

This biometric data is not collected or stored by the government. The government can never access or disclose this biometric data in any way. Government mobile devices are securely wiped before being redeployed or donated. If the device is not being redeployed or donated, it is destroyed.

FIDO2 security keys can only be set up for MFA by one user. Only that user can reset the FIDO2 security key to factory settings so it can be used by another user. No one, including ITD, Microsoft or the vendor, can access the biometric information stored on the key.

SERVICENOW PASSWORD RESET VERIFICATION

If I lose my mobile phone or FIDO2 security key, or don't have access to it and get prompted for MFA, what should I do?

Until you obtain a new mobile phone, the ITD Service Desk can assist you if you are prompted for MFA. The Service Desk must verify your identity the same way they would if you called for a password reset, so your ServiceNow password reset verification must be complete.

Once your identity is verified, the ITD Service Desk will issue you a one-time code called a Temporary Access Pass that you can use in the MFA prompt.

What happens if I can't complete an MFA prompt, and I'm not enrolled for ServiceNow password reset verification system?

You would follow the same process as if you called in for a password reset and couldn't verify your identity. You won't be able to access the files or app that caused the MFA prompt until your identity can be verified. There are no exceptions to this policy.

QUESTIONS

Who do I contact if I have questions about any of these initiatives?

Please reach out to your security officer, the Cyber Security and Risk Management branch or the ITD Service Desk at 306-787-5000.

Improved Cybersecurity Controls

January 2025

FOR MANAGERS ONLY

How do I know if an employee needs a FIDO2 key?

Please contact your security officer to reference your organization's approved process for when to procure FIDO2 security keys.