Shelter Management Information System (SMIS) Privacy Protocol: Multifactor Authentication

Effective June 9, 2022

Introduction

The Shelter Management Information System (SMIS) is a web-based information management system that is administered by the City of Toronto's Shelter, Support and Housing Administration (SSHA) Division. It is used by both City of Toronto staff and Purchase-of-Service (POS - external agencies funded by the City of Toronto) staff to provide services to individuals and families experiencing homelessness.

This protocol is only applicable to POS staff (as City staff use an alternative security process).

As of June 9, 2022, all POS users are required to conduct "Multifactor Authentication" (MFA) to access SMIS. MFA requires users to confirm their identity using two methods (SMIS Login/Password + Access Code via email).

MFA **replaces** the previous Endpoint Security (EPS) process, whereby a SMIS Security Key was installed on every unique piece of POS hardware (e.g. laptop) before that specific device could access SMIS. SSHA replaced EPS, as EPS is only supported by Internet Explorer, which is being phased out by Microsoft on June 15, 2022.

MFA allows POS programs to now use any work-issued Windows desktop or laptop to access SMIS and **does not require** an EPS Access Code to be installed. Further, MFA allows SMIS to now be compatible with Microsoft Edge and Google Chrome (note that SMIS is no longer compatible with Internet Explorer, as it is being phased out).

Workflow for Users

To access SMIS, **POS users** will now complete the following steps:

1. The User will enter their username and password into SMIS, per usual;
2. SMIS will then direct the User to a MFA page and send them an email containing a SMIS Access Code. This page will provide on-screen instructions; and,
3. The User will (1) retrieve the Access Code and enter it into SMIS and (2) indicate whether they would like to trust the current device (meaning that they will not be required to enter an Access Code for this device/browser for the next 3 months.
    a. If the Access Code is correct, the User is granted access to SMIS.
    b. If an incorrect Access Code is entered 3 times, the User's account is locked, and they will need to connect with smishelp@toronto.ca to unlock their account.

The User will only be required to conduct the above steps 2-3 if at least one of the following conditions is applicable.

1. The User is logging into SMIS for the **first time on the current device**;
2. The User is logging into SMIS for the **first time on the current browser**;

3. The User is logging into SMIS on a **device/browser that they have not 'trusted'**; or,
4. The User is logging into SMIS on a **device/browser with an expired trust** (e.g., the User trusted the device/browser 91+ days prior and therefore must update their trust).

If none of the above conditions are met, the user will not be required to complete the MFA and can log into SMIS directly after entering their username/password, without the need to enter a Access Code.

Guidelines for Users

1. Only access SMIS for **authorized reasons**, as directed by your Supervisor/Manager**.**
2. Only access SMIS using **devices that are password-protected** (e.g., do not access SMIS through a public library computer).
3. Only access SMIS using **work-issued devices** (e.g., do not use your personal device).
4. Only access SMIS when connected to **networks that are private and password-protected**. In other words, never access SMIS through networks that are public or are not password-protected (e.g., do not access SMIS through your home Wi-Fi without a VPN, or the public Wi-Fi offered by your local coffee shop).
5. When working remotely, only access SMIS from a **secure remote office** and ensure that your computer is set to automatically **lock the screen** after 10 minutes of inactivity.
6. MFA uses your existing **email address**, as linked to your SMIS profile. If this email is out-of-date, you must connect with your Access Manager to request an update.
7. **Do not save your SMIS password** on any devices (e.g. do not use a password manager tool to save your username and password in your browser). Note that SMIS will prevent users from doing so, however, do not attempt a workaround.
8. Follow the **SMIS privacy guidelines** at all times when using SMIS (available **here).**

Please direct any questions regarding these guidelines to the SMIS Privacy Contact at 416-392-8741 and/or smishelp@toronto.ca.

Frequently Asked Questions

Q1. Where can I find my SMIS Access Code?

SMIS will send you an Access Code via email **after** you have logged in. Please ensure that you are looking in the correct email mailbox, as listed on the MFA SMIS page. Also please ensure to check your spam/junk folder. If you still cannot find the email, please connect with your Access Manager or email smishelp@toronto.ca.

Q2. Why did my Access Code fail?

Please ensure that your Access Code is not expired (Access Codes expire seven minutes after they were generated, as indicated by the on-screen timer). Also please ensure that you accurately copied the Access Code from the SMIS email. If it is still not working, please connect with your Access Manager or email smishelp@toronto.ca.

Q3. How do I unlock my account if my password/Access Code fails?

Please connect with smishelp@toronto.ca.

Q4. Who do I contact to learn more about MFA?

Please connect with your Access Manager or email smishelp@toronto.ca.