SMIS Release Notes Version 3.8

The Shelter Management Information System (SMIS) a web-based information management system used by many programs across the City that provide services to individuals and families experiencing homelessness. SMIS is administered by the City's Shelter, Support and Housing Administration (SSHA) division. SMIS is primarily used by City-funded shelters, 24-hour respites, and COVID-19 temporary shelter programs to conduct client intake, admission, case management, and discharge. It is also used by some service programs (e.g., eviction prevention, drop-in programs).

This set of Release Notes describes the enhancements that are included in the June 2022 SMIS enhancement, release version 3.8. All changes included in this SMIS enhancement were prioritized by the City of Toronto SMIS Steering Committee and Director Group. Combined, these changes address the highest current priority change requests in SMIS.

Please note that this document will also be available online at Shelter Management Information System (SMIS) – City of Toronto.

Contents

1) SMIS Is Now Compatible with Other Browsers

SMIS is **now compatible** with Microsoft Edge and Google Chrome. SMIS is **no longer compatible** with Internet Explorer.

What this means for users: Moving forward, please use the existing SMIS URL (website) in either of these two browsers (Edge and Chrome). If you attempt to access SMIS using Internet Explorer, you will receive an error message and be directed to use one of the compatible browsers.

2) Signature Pads Are Now Compatible with Other Browsers

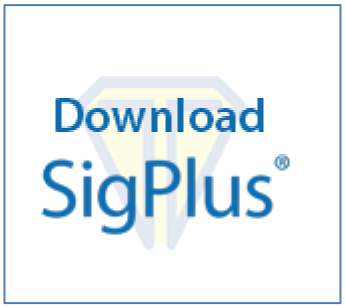
The Signature Pads are now compatible with Microsoft Edge and Google Chrome. The Signature Pads are no longer compatible with Internet Explorer.

Access managers must complete the following 3 steps for every computer that uses Signature Pads, in order for the Pads to function on Edge and Chrome. You **do not need** to complete these steps for devices that do not use the Signature Pads.

Specific instructions are provided below. For full details on these Add-Ons, please see the Full Installation Guide by Topaz.

Step 1: Download and install the "SigPlus" software

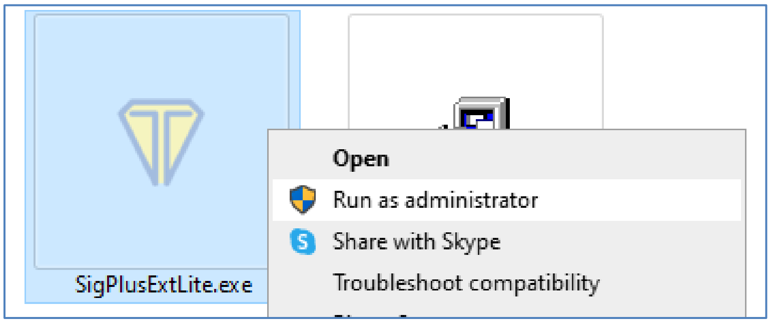
1) This step is only applicable to **new** devices. If your device is already using signature pads, please skip this step and go to Step 2.
2) Go to the SigPlus Website (model number T-L462-HSB-R).
3) Click "Download SigPlus". Depending on your browser, you may need to right-click and then click "Save as".



4) Save the File to your desktop.
5) Open the File to start the installer.
6) Follow the on-screen prompts to complete the installation in the setup wizard.

Step 2: Download and Install the "Topaz SigPlusExtLite" File to your desktop

1) Go to the Topaz SigPlusExtLite website.
2) Save the File to your desktop. Depending on your browser, it may automatically save for you, simply by going to the website.
3) Right-click the file on your Desktop and select "Run As Administrator".



4) Follow the on-screen prompts to complete the installation in the setup wizard.

Step 3: Install the Add-Ons for Edge and Chrome

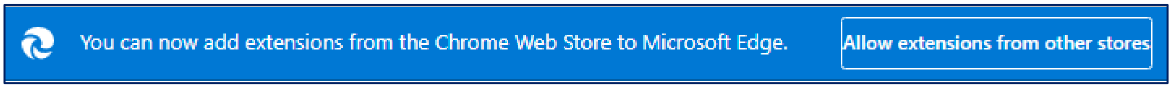
Browser "Add-Ons" must be installed:

1) On every **unique device** that uses Signature Pads;
2) For **every unique user profile** for that device;
3) For **Edge** and **Chrome** separately.

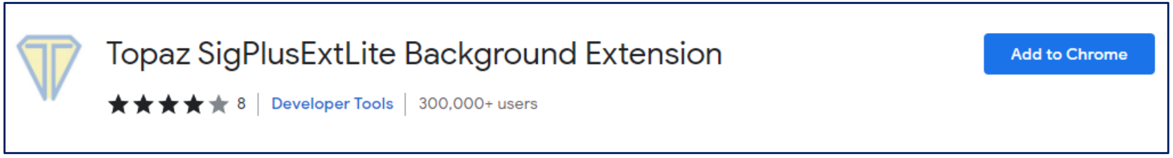
For example, if your agency uses Signature Pads on two distinct computers, and those computers are accessed via three distinct user profiles, you will need to install the Add-Ons up to a total of 12 times (for each device, for each user profile, for each browser).

To Install the Add-On on Microsoft Edge

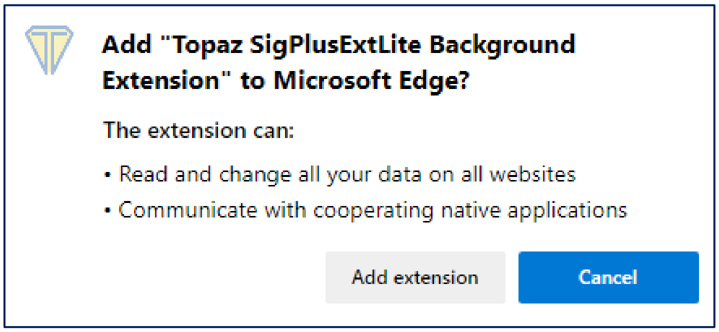
1) Open the Microsoft Edge browser
2) Copy the following link and paste it in your Edge Browser: https://chrome.google.com/webstore/detail/topaz-sigplusextlite-back/dhcpobccjkdnmibckgpejmbpmpembgco
3) Click the "Allow Extensions from Other Stores" Button at the top of the page, in the blue banner


You can now add extensions from the Chrome Web Store to Microsoft Edge.

4) Click the "Add to Chrome" Button. Note that this will add the extension to Microsoft Edge, despite the fact that it indicates that it is adding it to Chrome


Topaz SigPlusExtLite Background Extension

5) Click the "Add Extension" Button



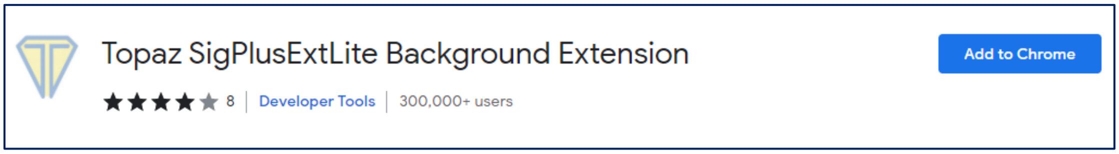
Add "Topaz SigPlusExtLite Background Extension" to Microsoft Edge?

The extension can:

- Read and change all your data on all websites
- Communicate with cooperating native applications

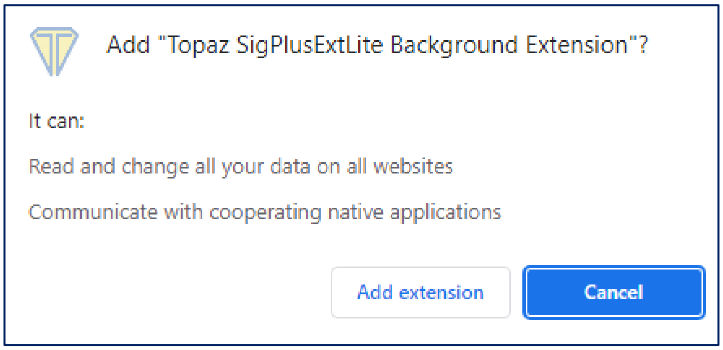
To Install the Add-On on Google Chrome

1) Open the Google Chrome browser
2) Copy the following link and paste it in your Chrome Browser: https://chrome.google.com/webstore/detail/topaz-sigplusextlite-back/dhcpobccjkdnmibckgpejmbpmpembgco
3) Click the "Add to Chrome" Button



Topaz SigPlusExtLite Background Extension

4) Click the "Add Extension" Button



Add "Topaz SigPlusExtLite Background Extension"?

It can:

Read and change all your data on all websites

Communicate with cooperating native applications

3) Eliminating Endpoint Security (EPS) in SMIS

Purchase-of-Service (POS) agencies **no longer require Endpoint Security (EPS)** to access SMIS. EPS was a 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 is replacing EPS, as EPS is only supported by Internet Explorer, which is being phased out by Microsoft on June 15, 2022.

What this means for users: Moving forward, POS users can now access SMIS **on any work-issued Windows laptop/desktop** and do not require EPS to be installed. SMIS will also continue to work on devices that previously had EPS installed.

Users do not need to uninstall EPS.

For more information on acceptable uses of SMIS, please see the (1) SMIS Privacy Guidelines and (2) SMIS Privacy Protocol-Multifactor Authentication", available on the City of Toronto's web site.

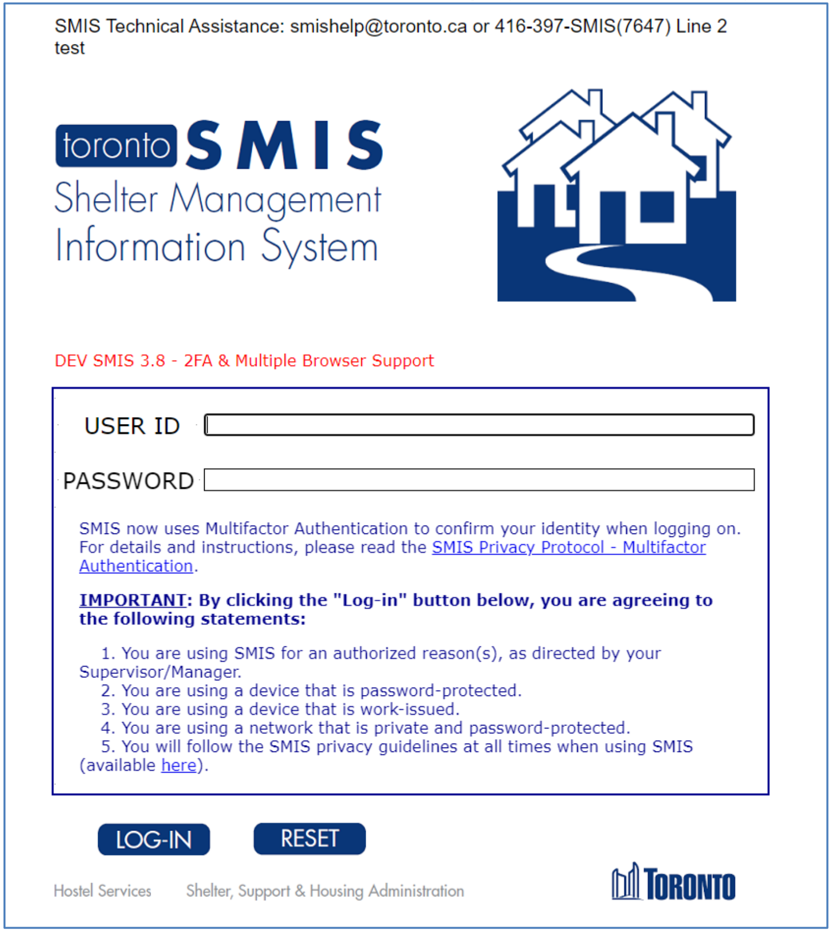
4) Adding Multifactor Authentication for POS Users

SSHA is introducing "Multifactor Authentication" (MFA) to replace EPS. MFA requires POS users to confirm their identity using two methods (SMIS Login/Password + Access Code via email).

MFA is only applicable to POS users. This change is **not applicable to City of Toronto staff**, as City staff already use the City's server as the secondary verification.

What this means for users: POS users will now complete the following steps to access SMIS:

1. The User will access the SMIS webpage in Microsoft Edge or Google Chrome.



SMIS Technical Assistance: smishelp@toronto.ca or 416-397-SMIS(7647) Line 2
test

DEV SMIS 3.8 - 2FA & Multiple Browser Support

USER ID

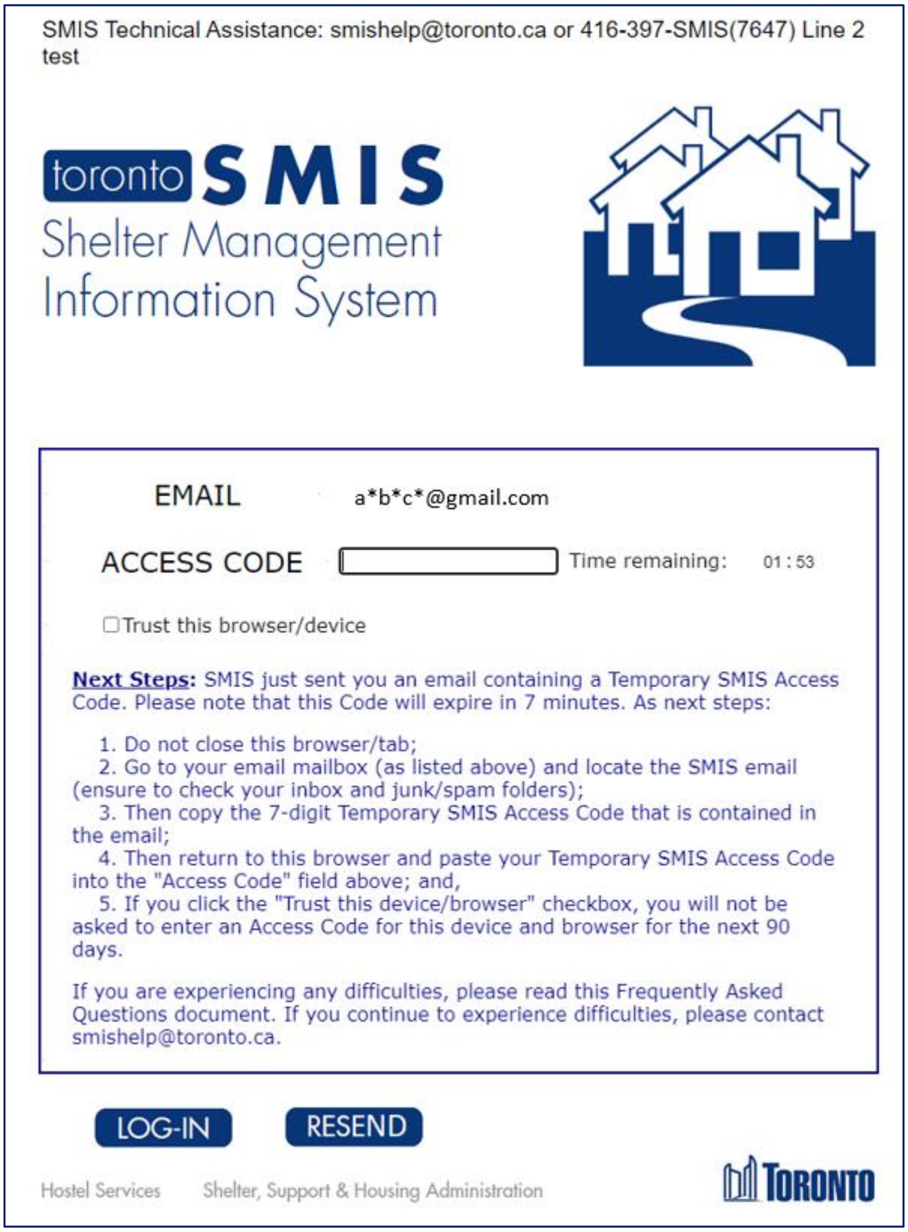
PASSWORD

SMIS now uses Multifactor Authentication to confirm your identity when logging on. For details and instructions, please read the SMIS Privacy Protocol - Multifactor Authentication.

IMPORTANT: By clicking the "Log-in" button below, you are agreeing to the following statements:

1. You are using SMIS for an authorized reason(s), as directed by your Supervisor/Manager.
2. You are using a device that is password-protected.
3. You are using a device that is work-issued.
4. You are using a network that is private and password-protected.
5. You will follow the SMIS privacy guidelines at all times when using SMIS (available here).

2. The User will enter their User ID and Password into SMIS, per usual.
    - **a.** Note that the User's account will be locked if they enter an incorrect password three times in a row. If the User locks their account, they must request a reset by contacting smishelp@toronto.ca.
    - b. SSHA has also added additional help text (in blue) to the login page, requiring the User to agree to the listed statements prior to logging in. These statements are further detailed in the "SMIS Privacy Protocol-Multifactor Authentication", available on the City of Toronto's web site;
3. If the User ID and Password are correct, SMIS will then direct the User to a new MFA page, which displays the following fields:
    - a. **Email:** The User's email address that is associated with their SMIS profile. Note that this information is partially redacted to protect user confidentiality;
    - b. **Access Code:** Allows the User to enter their Access Code, which is sent to them via email to the email address listed above;
        - **i.** Note that the User's account will be locked if they enter an incorrect Access Code three times in a row. If the User locks their account, they must request a reset by contacting smishelp@toronto.ca.
    - **c.** **Time Remaining:** Indicates the amount of time that the current Access Code will remain active for. Once this counter hits 0:00, the current Access Code is expired and the User will be required to click "Resend" to generate a new code.
    - d. **Trust This Browser/Device:** Allows the User to indicate whether they would like to 'trust' the current browser/device. This mean that the User will not be required to complete MFA (e.g. enter an Access Code) for this device and this browser for the next 3 months (90 days). On the 91st day, they will then be required to complete MFA once again. At that time, they can choose to re-trust the device and reset the 90 day clock.
        - i. Note that if the User's account becomes locked (enters an incorrect password or Access Code 3 times in a row) SMIS will automatically reset any active 'Trusts' for this User.
        - ii. Note that 'Trusts' are browser **and** device-specific, meaning that the User must Trust each unique browser (Edge, Chrome) on each unique device (e.g. computer, laptop) that they intend to use to access SMIS.
    - **e.** **Log-in:** Allows the User to enter the SMIS main page, provided they have entered a correct and active Access Code.
    - **f.** **Resend:** Allows the User to have a SMIS send them a new Access Code via email. Note that this field is hidden until the current Access Code expires order to prevent the user from generating multiple Access Codes simultaneously.



SMIS Technical Assistance: smishelp@toronto.ca or 416-397-SMIS(7647) Line 2
test

EMAIL a*b*c*@gmail.com

ACCESS CODE Time remaining: 01 : 53

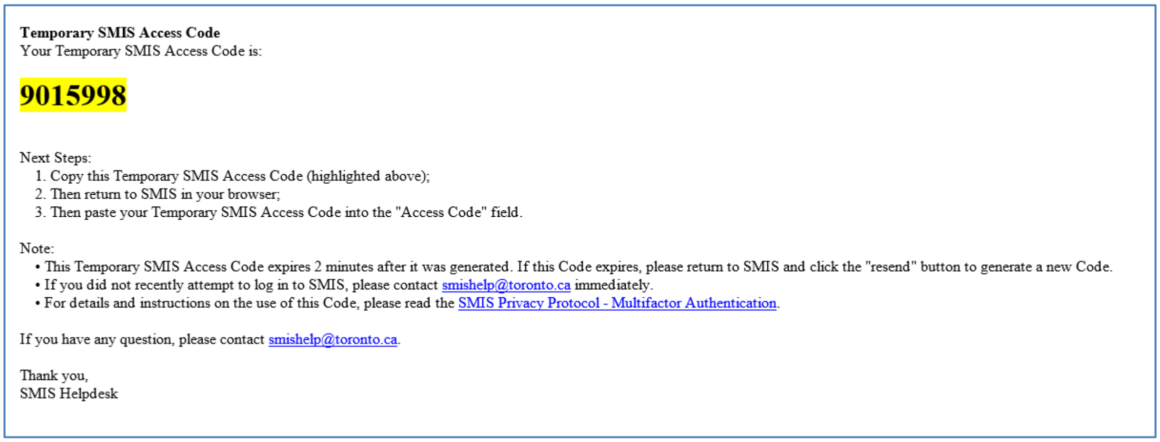
□Trust this browser/device

Next Steps: SMIS just sent you an email containing a Temporary SMIS Access Code. Please note that this Code will expire in 7 minutes. As next steps:

1. Do not close this browser/tab;
2. Go to your email mailbox (as listed above) and locate the SMIS email (ensure to check your inbox and junk/spam folders);
3. Then copy the 7-digit Temporary SMIS Access Code that is contained in the email;
4. Then return to this browser and paste your Temporary SMIS Access Code into the "Access Code" field above; and,
5. If you click the "Trust this device/browser" checkbox, you will not be asked to enter an Access Code for this device and browser for the next 90 days.

If you are experiencing any difficulties, please read this Frequently Asked Questions document. If you continue to experience difficulties, please contact smishelp@toronto.ca.

4. As soon as the MFA page loads, SMIS will send the User send them an email containing a **SMIS Access Code**.



Temporary SMIS Access Code
Your Temporary SMIS Access Code is:

9015998

Next Steps:
1. Copy this Temporary SMIS Access Code (highlighted above);
2. Then return to SMIS in your browser;
3. Then paste your Temporary SMIS Access Code into the "Access Code" field.

Note:
- This Temporary SMIS Access Code expires 2 minutes after it was generated. If this Code expires, please return to SMIS and click the "resend" button to generate a new Code.
- If you did not recently attempt to log in to SMIS, please contact smishelp@toronto.ca immediately.
- For details and instructions on the use of this Code, please read the SMIS Privacy Protocol - Multifactor Authentication.

If you have any question, please contact smishelp@toronto.ca.

Thank you,
SMIS Helpdesk

5. The User will then go to their email and retrieve the Access Code. Please note that it may take a few minutes for the email to arrive, depending on the email protections that are in place by the User's Agency. **Please ensure to check your junk/spam folders for the email as well.**
6. The User will copy the code and enter it into the "Access Code" field.
   a. Note that if the "Time Remaining" counter reaches 0:00, the current Access Code is expired. The user must click "Resend" to generate a new Code.
7. The User can also choose to 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 and this browser for the next 3 months).
8. If the Access Code is correct, the User is granted access to SMIS.