INSTRUCTIVO PARA INSTALACIÓN Y CONFIGURACIÓN DE CLIENTE ZEROTRUST

(IT-59015 versión 02)

Appgate SDP

Industry-Leading Zero Trust Network Access

INDICE

Toda copia impresa se considera no controlada, salvo en los casos en los que sea explícitamente autorizada por un distribuidor designado, quien deberá entregar la copia numerada y firmada al final del documento. Tratar confidencialmente.

1. OBJETIVO

El objetivo de este documento es describir los pasos a seguir para la instalación y configuración del cliente ZeroTrust.

2. ALCANCE

Desde la instalación hasta la configuración del aplicativo.

3. REQUERIMIENTOS

Para proceder con la instalación y configuración del cliente ZeroTrust para el acceso seguro en las aplicaciones de BYMA, se requiere:

- Usuario y Clave (provista por BYMA)
- Link de Profile de Cliente (provista por BYMA)
- Celular con la aplicación Autenticator de Google para el uso del segundo factor de autenticación, o IMPORTANTE: el celular debe tener la fecha y hora sincronizada, de lo contrario no funcionará el OTP.
- La estación (PC/notebook) donde se ejecuta el cliente ZeroTrust de acceso seguro a aplicaciones de BYMA debe tener acceso a Internet para los puertos tcp/443, udp/443, udp/53
- El cliente ZeroTrust no puede ejecutarse a través de una conexión VPN SSL, porque el Windows dará prioridad de conexión a la VPN y no al cliente ZeroTrust.

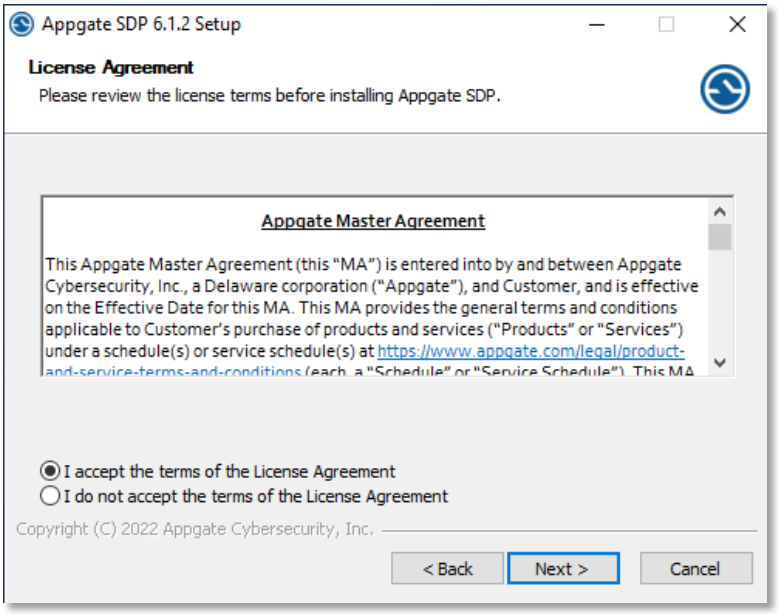
4. INSTALACIÓN

Para la instalación se deberán seguir los siguientes pasos:

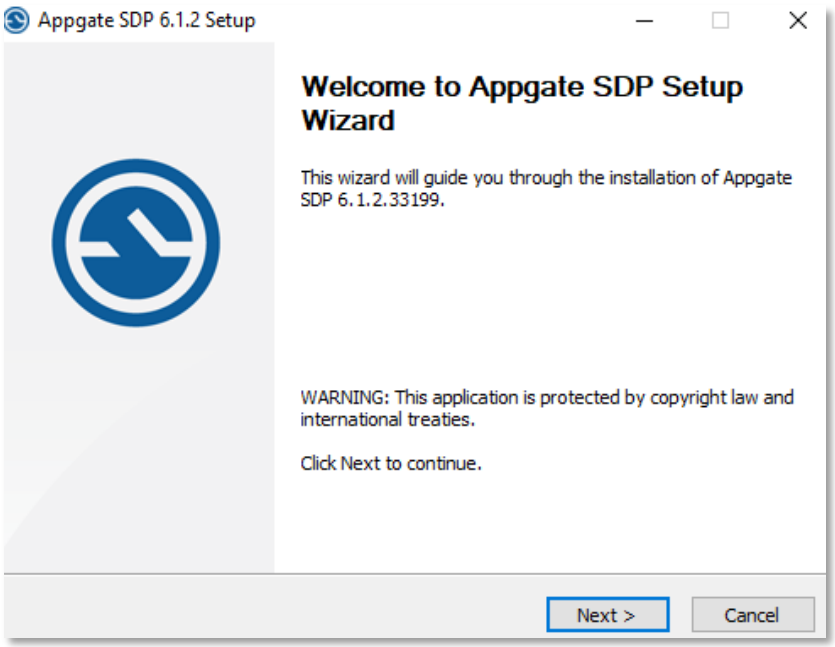
1) Bajar el cliente para la instalación de la web https://home.byma.com.ar/sba/links.html. Descarga de Aplicaciones
2) Seleccionar la opción Cliente AppGate (ZeroTrust)
3) Ejecutar el archivo bajado

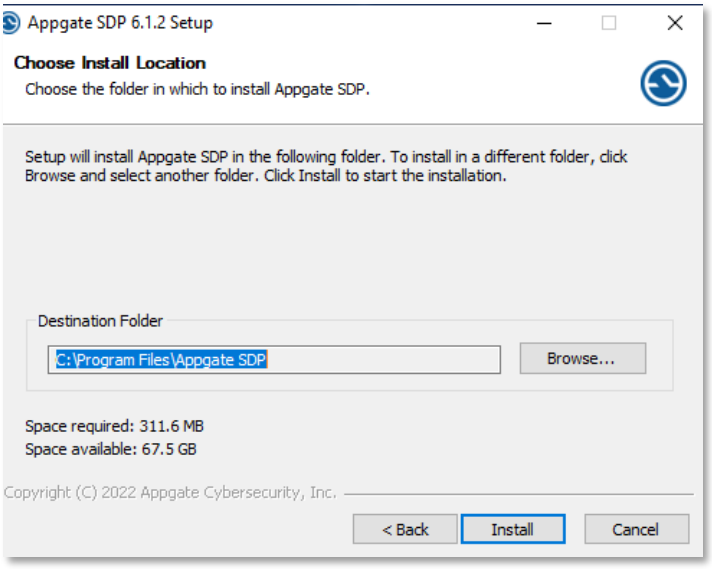
El usuario que instale la aplicación debe tener los permisos necesarios en el equipo para poder realizar una instalación de software.

4) Presione el botón Next en la siguiente pantalla:

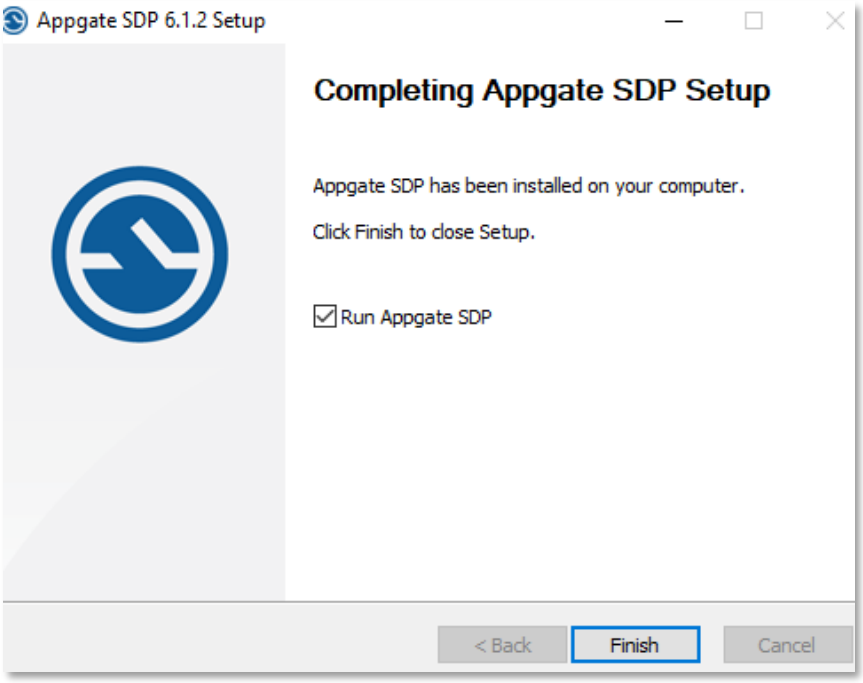


5) Aceptar el bullet "I accept the terms of the License Agreement" para que se habilite el botón Next. Luego presione el botón Next.
6) Seleccione la ubicación en el disco de la máquina donde se instalará el software. Por default es C:\Program Files\Appgate SDP\. El disco debe tener al menos 330MB de espacio disponible. Luego presione el botón Install.





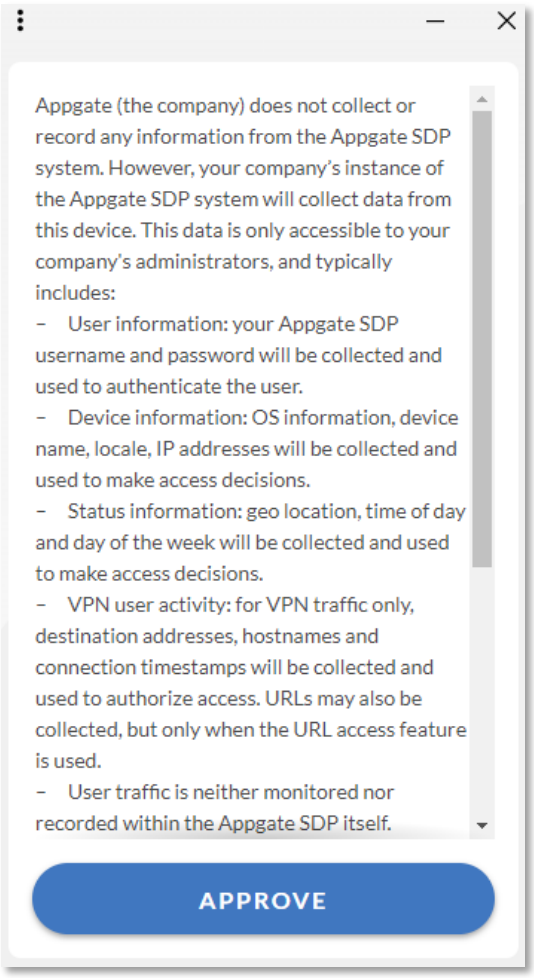
Al finalizar mostrará la siguiente pantalla, a la que se debe dar Finish para terminar.



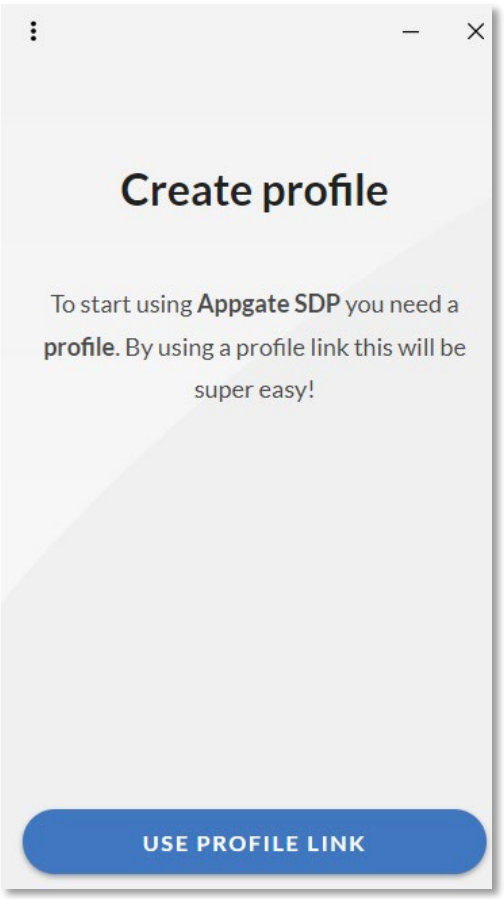
5. CONFIGURACIÓN

Para la configuración deberán seguir los siguientes pasos:

- Abrir la aplicación



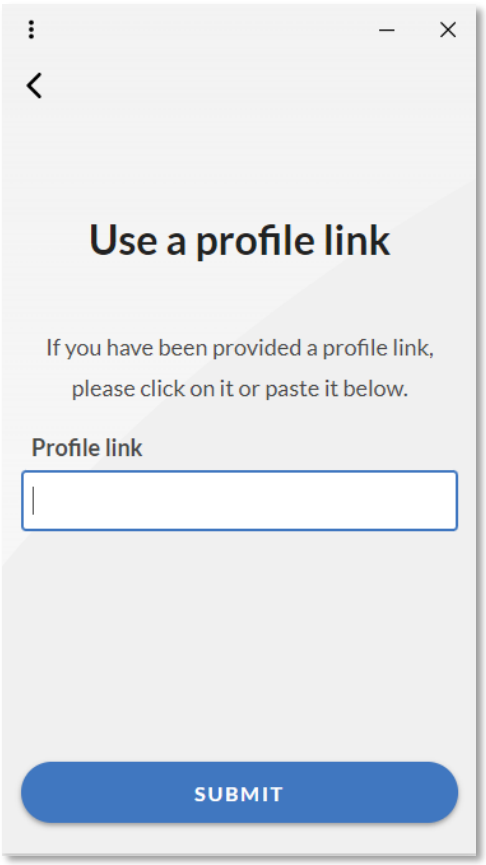
- Para continuar deberan aceptar presionando el botón APPROVE.
- Una vez aprobado aparecerá la primera vez la pantalla para crear un Profile de usuario.



- Para poder continuar se debe disponer del Link de Profile de Cliente, como se indicó en la sección Requerimientos. Formato del Link de Profile de Cliente

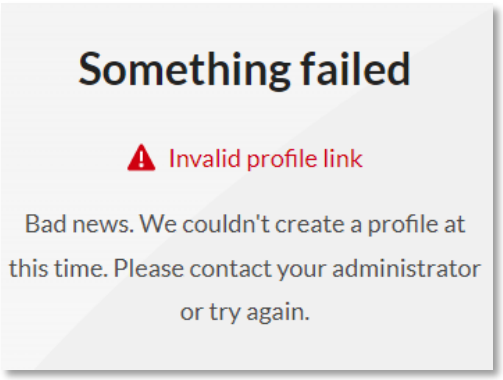
appgate://ctrl-ltm-zt.tecval.com.ar/
eyJwcm9maWxlTmFtZSI6Ik9rdGEgUHJvZHVjY2lvbiIsInNwYSI6eyJuYW1lIjoiT2t0YV9Qcm9kdWNjaW9uIiwia2V5IjoiZDM1NzVhMTJlMWYzYzQyYTRhMzYyMzc4YWQ2NjQ4NTcwMmE0MDhkNDgyNDEzMDVmYTBmZjJiZWIzMDA3MzgxYyJ9LCJjYUZpbmdlcnByaW50IjoiY2VkZDU1NTk0YmNlNDM3MjY2N2VkMWExNzM3Yzg5NTZhNzc5Y2U3ZGIzN2ZhNzhhMTYwZWFkM2ZjNmQxYTMwNiIsImlkZW50aXR5UHJvdmlkZXJOYW1lIjoiT2t0YSBQcm9kdWNjaW9uIn0=

- Proseguir presionando el botón USE PROFILE LINK para configurar el perfil de usuario. Se presentará la siguiente pantalla:

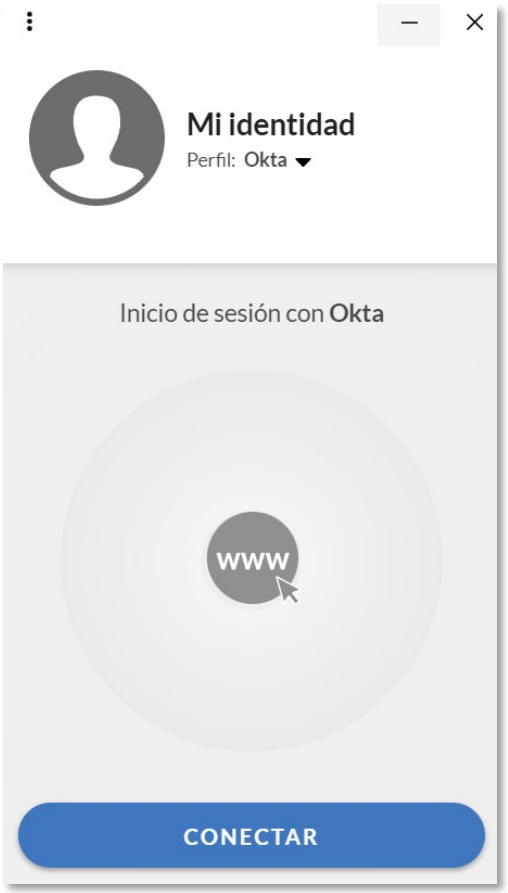


- Copiar el texto del Link de Profile de Cliente recibido y colocarlo en Profile link. A continuación, presionar el botón SUBMIT.

- Si se presenta el siguiente error implica que el string del Link de Profile de Cliente es incorrecto, no se copió completo o ya no está vigente.

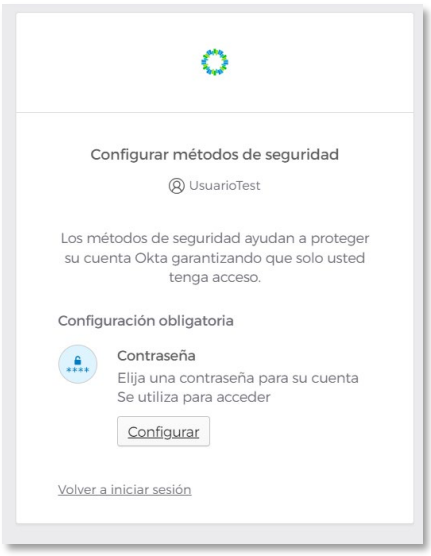


- Si el Link fue copiado correctamente y la aplicación tiene acceso a Internet según los puertos que figuran en Requerimientos, a continuación, quedar configurado el usuario.



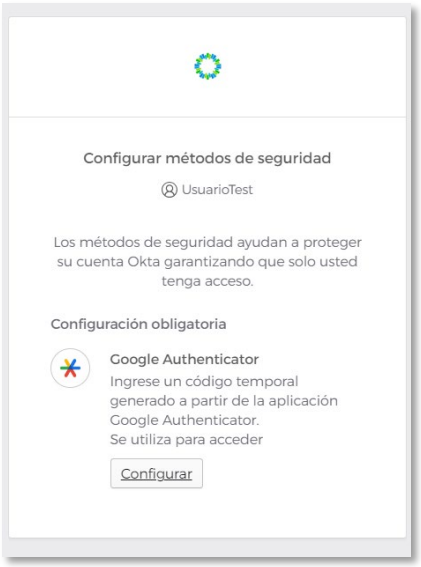
- A continuación, presionar el botón CONECTAR para realizar la autenticación de usuario y clave para conectarse al servicio de acceso.

- El cliente lo redireccionara hacia la web de OKTA para autogestionar su usuario y contraseña por primera vez. donde configurar su pass a través del botón configuración

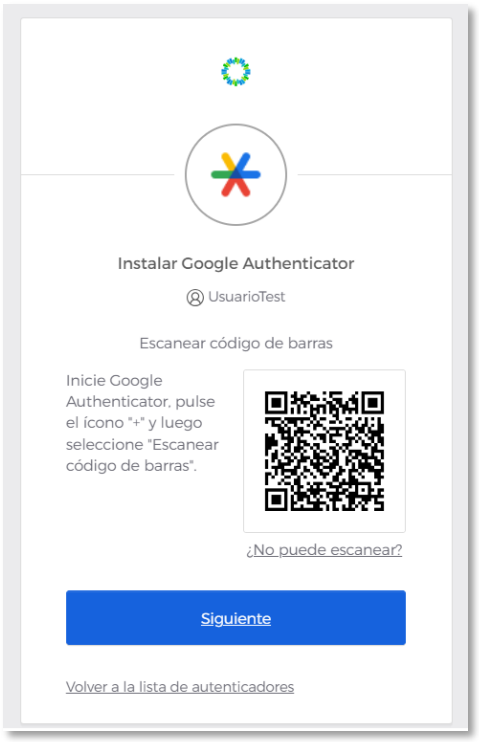


- El sistema le indicara los parámetros de contraseñas necesarios para la creación de una pass segura

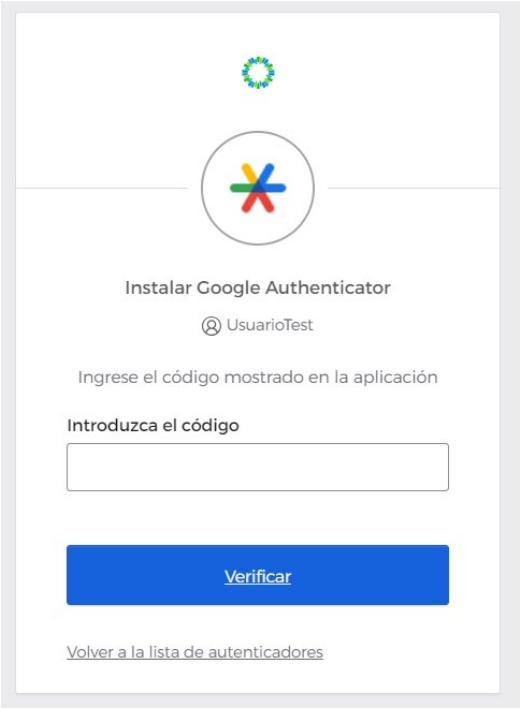
- Luego de colocar su pass y confirmar el mismo deberá apretar el botón siguiente el cual lo redirigirá a la configuración del doble factor de autenticación



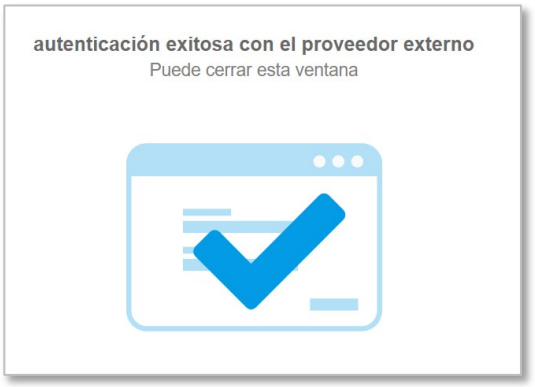
- Al ir al botón de configuración se desplegará el código QR para realizar el enrolamiento de Google Autenticator



- Una vez escaneado el QR desde su celular con la app de Google Autenticator el mismo quedara configurado y le generara un código de 6 dígitos (Los cuales serán solicitados en cada login de forma aleatoria). Estos deberán ser ingresados una vez de haber apretado en el botón siguiente



- A continuación, la web mostrara un cartel de autenticación exitosa lo cual indicara que la app esta lista para ser utilizada



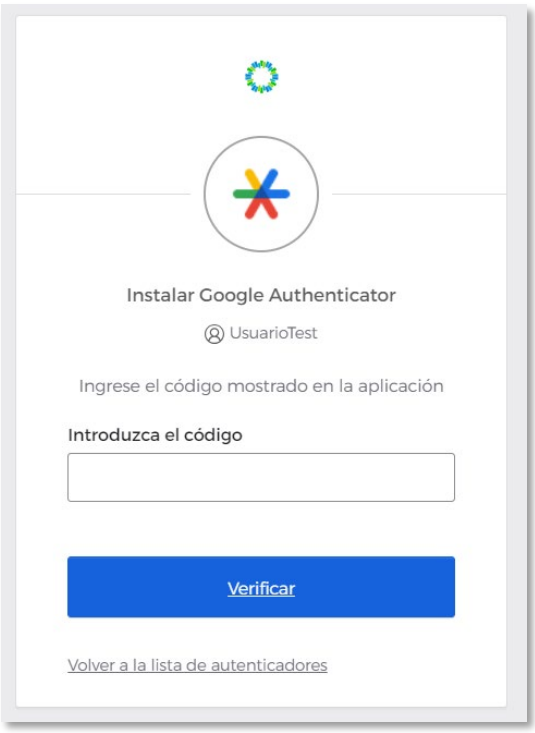
Como se menciona en Requerimientos

Debe estar instalada en el celular previamente y para setear la clave de Segundo Factor para este acceso, desde la aplicación Google Autenticator en el celular, se debe presionar el símbolo más de colores que hay en la esquina derecha inferior de la pantalla.

A continuación, seleccionar Escanear un código QR y con el cuadrante en pantalla de la cámara apuntar al código QR de a aplicación.

Al escanearlo se generará en la aplicación una nueva entrada que tendrá como título Appgate SDP (<nombre de usuario>@AD+...) y debajo los 6 dígitos de la clave de segundo factor de autenticación. Esta clave es única para este usuario, y cambia cada 60 segundos.

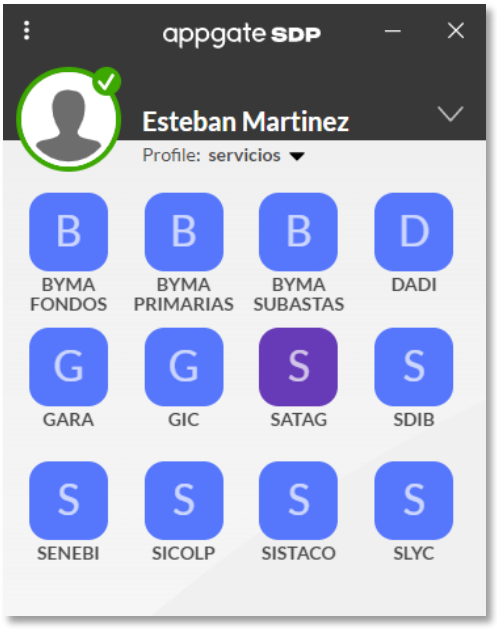
A partir de ese momento la aplicación pedirá esta clave de única vez (Two Factor Authentication) luego de introducir el usuario y contraseña en cada login que se realice. Sin esta clave de única vez NO se podrá acceder a los servicios de BYMA por más que cuente con el usuario y clave válidos.



Una vez ingresado el código de única vez y que sea validado, se ingresará al portal de la aplicación.

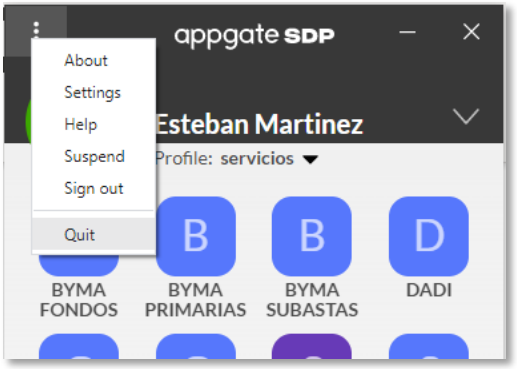
Los íconos de acceso a las aplicaciones web que figuran en el portal variarán dependiendo del Profile del Usuario, según se trate de un Depositante, ALYC, etc.

Las aplicaciones cliente como el Emulador para acceso a la custodia, estación EOMM+ para la negociación, etc. no figurarán en el portal del usuario, ya que no son webs. En esos casos ejecutar el cliente correspondiente y teniendo el cliente ZeroTrust de acceso seguro corriendo y conectado (con su usuario), tendrá habilitado el acceso para dichas aplicaciones también, siempre que corresponda a su perfil de usuario.



El cliente ZeroTrust de acceso seguro a BYMA, no debe cerrarse mientras se utilicen aplicaciones de BYMA/CVSA, porque de lo contrario dejarán de funcionar.

Si se quiere desconectar porque ya no accederá a aplicaciones de BYMA/CVSA, ir a los 3 puntitos que se encuentra en la parte superior del cliente, y seleccionar Sign out si se quiere desconectar, pero no cerrar el cliente o Quit si se quiere desconectar y cerrar el cliente.



N/A

7. DOCUMENTACIÓN REFERIDA

N/A

CONTROL DE CAMBIOS

FECHA	CAMBIO-MOTIVO
Agosto 2023	Creación del documento

Importante: completar los siguientes datos sólo en el caso de tratarse de una copia impresa controlada. Las copias controladas sólo pueden ser generadas por un distribuidor designado en el sistema y distribuidas a los destinatarios preestablecidos.
Copia controlada N°
Distribuidor: _____ ***Destinatario:*** _____ ***Ubicación de la copia:*** _____ ***Fecha de impresión:*** _____
_____ ***Firma del distribuidor***