MAGICENDPOINT FAQ

SERVICES GUIDE

March 2024

WINMAGIC®

Authenticate. Encrypt. Achieve.

Table of Contents

Setup and Installation 1

Install the MagicEndpoint application on your phone 1

iOS 1

Android 1

Convert your key file protection to your phone using BLE (default) 2

Convert the password key file to the phone token: Bluetooth with Phone 2

Convert your key file protection to your phone using Network (optional) 4

Create the one-time password (OTP) on your phone for recoveries 8

Using the phone to log into applications 11

Phone token via Bluetooth 11

Logging into boot logon 11

Logging into Windows 12

Log into the SecureDoc control center 13

Network with a phone 14

Logging into boot logon 14

Log into Windows 14

Log into SecureDoc control center 15

Logging into online applications 16

Log in to online applications with MagicEndpoint 17

Log into online applications from a different, “unmanaged” device 18

Log into your device if BLE or Network push aren’t working 20

Use the OTP 20

How to use the OTP from the MagicEndpoint app on your phone 20

Logging in if the MagicEndpoint registered phone isn’t available 27

Challenge response 27

Self-help recovery 29

The MagicEndpoint registered phone is lost, damaged or stolen 31

Registering a new phone if the current MagicEndpoint phone is lost, damaged or stolen 31

Re-register another network phone 33

Contact 34

About WinMagic 35

MagicEndpoint 35

SecureDoc™ 35

Setup and Installation

Install the MagicEndpoint application on your phone

Scan the QR code below:

Scan to Download

Or see the next sections to download directly from the app store.

iOS

1. Open the Apple App Store application:
2. Search for and download the “WinMagic Authenticator” application.
3. Launch the application and allow all permissions.

Android

1. Open the “Play Store” application:
2. Search for and download the “WinMagic Authenticator” application.
3. Launch the application and allow all permissions.

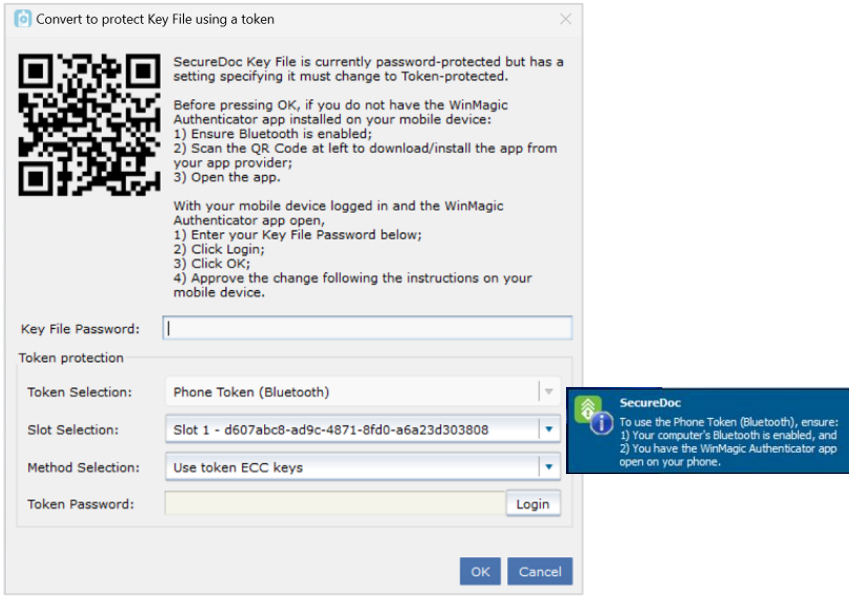
Convert your key file protection to your phone using BLE (default)

Preconditions

- ✓ Enabled “Allow Mobile Device-based Authentication using Phone Token (Bluetooth)” option in the SecureDoc profile.
- ✓ Installed the SecureDoc client software with BLE successfully enabled in the profile.
- ✓ Both the computer with SecureDoc and the phone have Bluetooth turned ON.
- ✓ The MagicEndpoint app on the phone is launched and open.

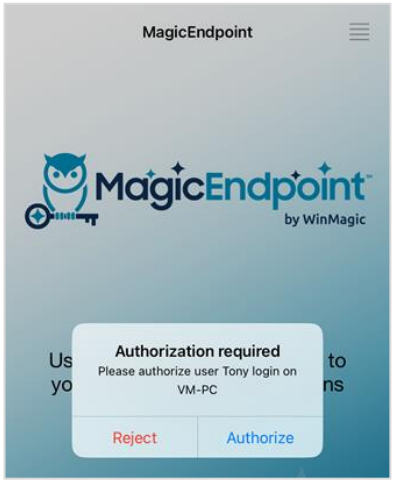
Convert the password key file to the phone token: Bluetooth with Phone

1. SecureDoc will prompt you to convert the key file.



2. Launch the WinMagic authenticator app on the phone.
   Make sure Bluetooth is enabled on both the SecureDoc computer and the phone.
3. On the SecureDoc computer with the “Convert to protect Key File using a token” window, configure the following:
   - Key File Password: *Enter key file’s valid password
   - Token Password: *Click **Login**
4. Click **OK**.

An authorization prompt will appear on the phone:



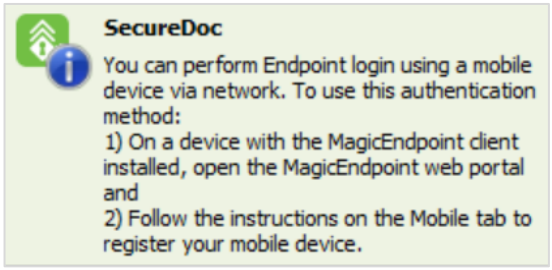
5. Tap **Authorize**.
   An authentication successful message should appear.

Convert your key file protection to your phone using Network (optional)

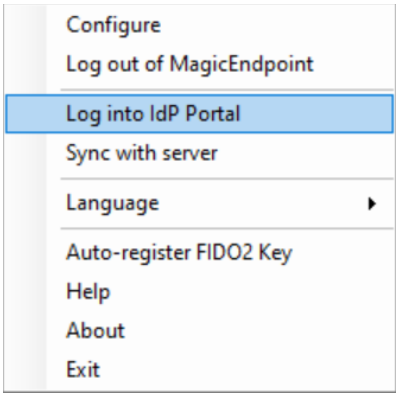
Preconditions

- ✓ Enabled option “Allow Mobile Device-based Authentication using network” in the SecureDoc profile.
- ✓ Installed the package with Network Phone on the computer successfully.
- ✓ Both the computer with SecureDoc and the phone are connected to the Internet.
- ✓ The MagicEndpoint app on the phone is launched and open.

At Windows startup, SecureDoc will prompt you to perform endpoint login using a mobile device via a network:

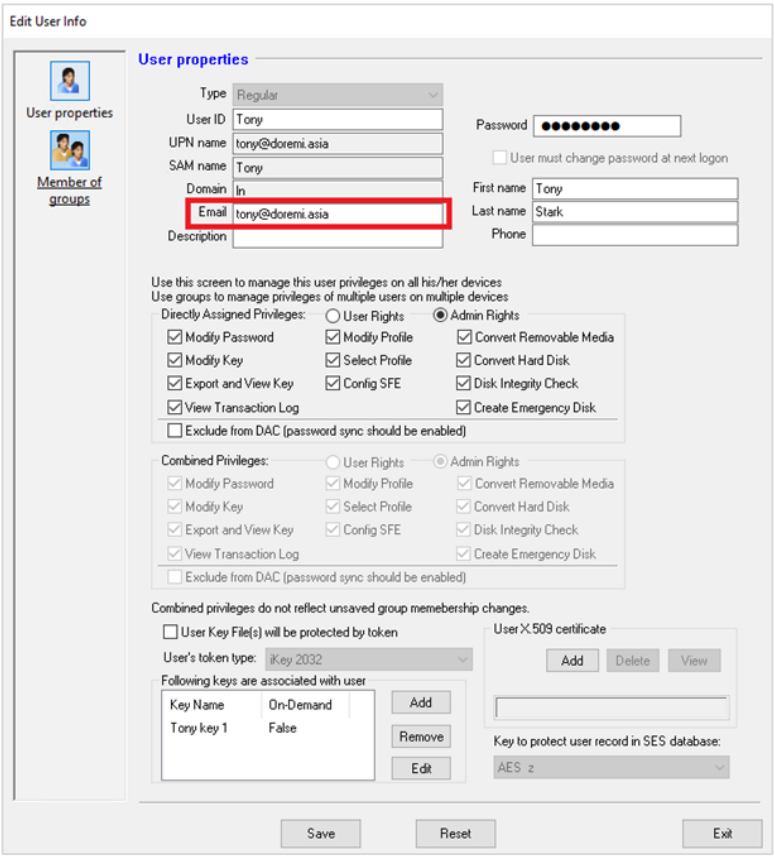


1. Install MagicEndpoint onto the phone.
2. Right-click on the MagicEndpoint icon in the Windows task bar and select **Log into IdP Portal**.

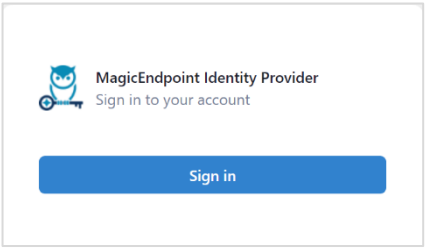


The IdP portal will launch in your Internet browser.

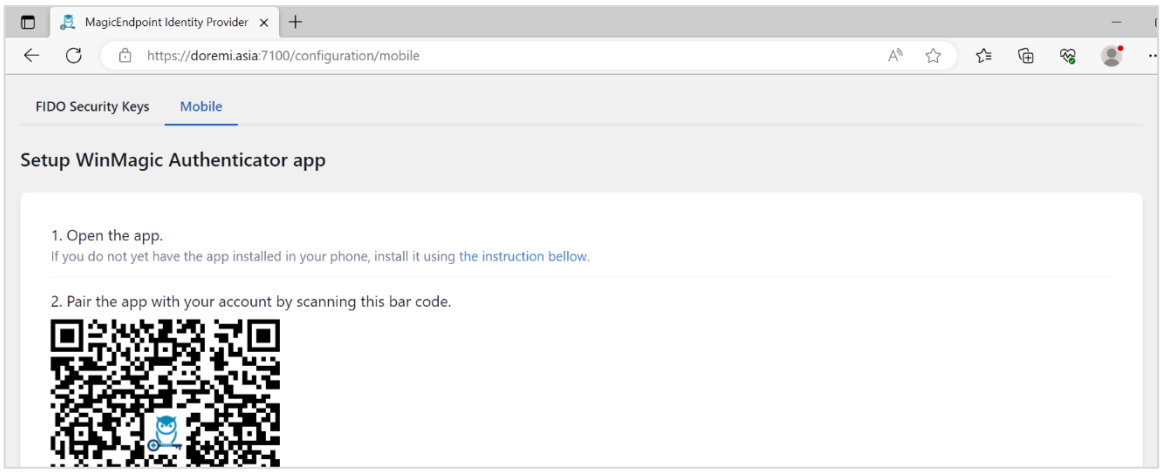
Note: The user's email must have been previously saved in the SecureDoc enterprise server database. If the email is not in the database, the system administrator must add this information on the user's behalf.



3. Click **Sign-in**.

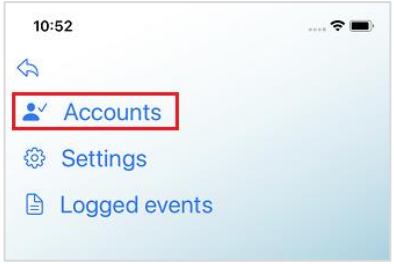


4. Go to the Configuration tab and select **Mobile**.

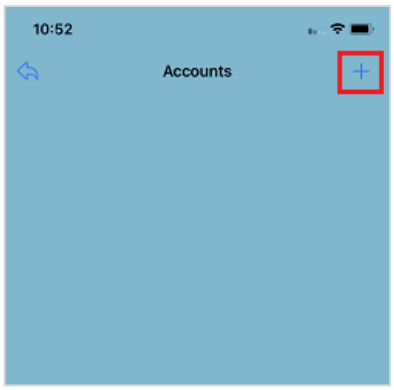


5. Launch the MagicEndpoint application on the phone.
6. Open the menu in the top right corner.

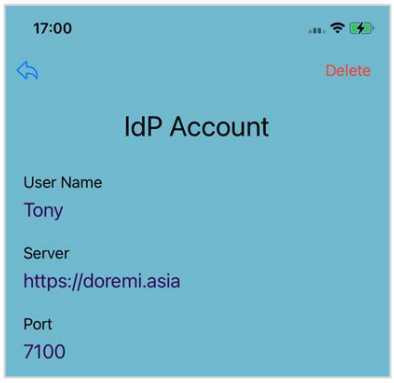
7. Select **Accounts**.



8. Click the **+** symbol.



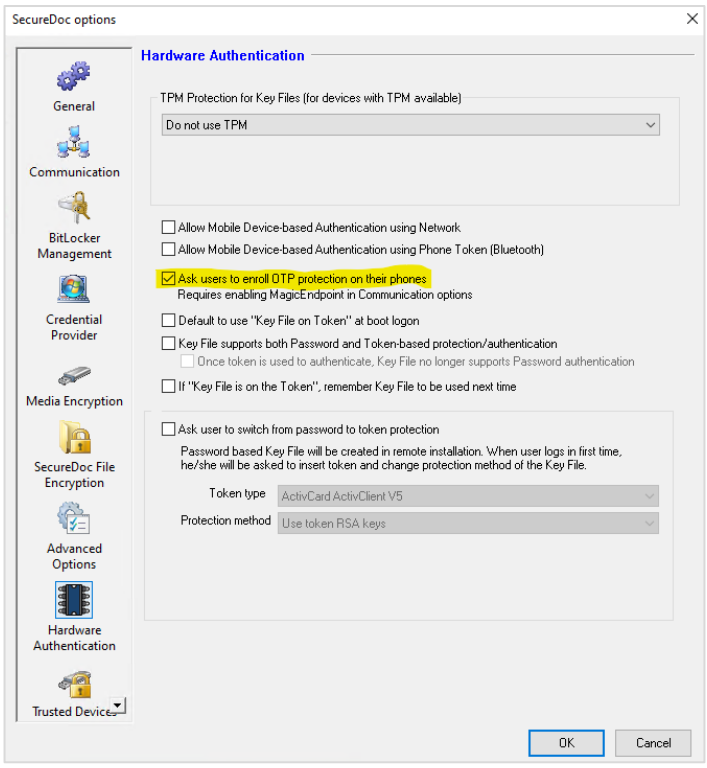
9. Scan the QR code from the “Mobile” tab in your internet browser.
   You should see a “Registration success!” message in the browser window.
10. Select the registered account on the mobile app to confirm configuration.



Create the one-time password (OTP) on your phone for recoveries

Preconditions

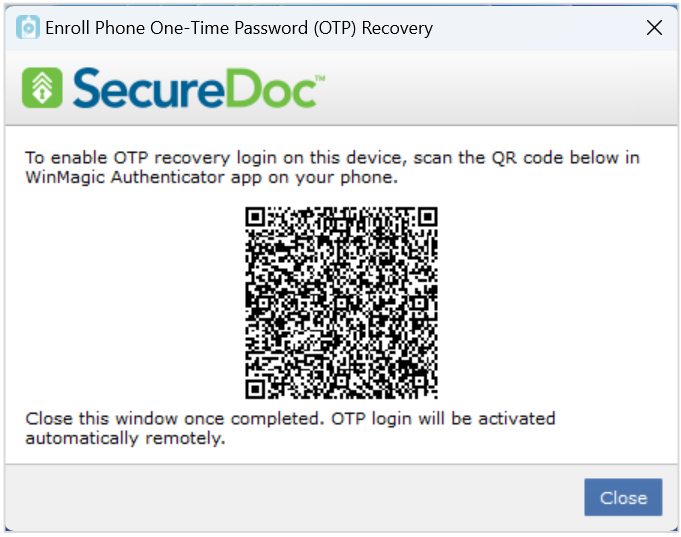
- ✓ Select the “Ask users to enroll OTP protection on their phones” checkbox in the SecureDoc options.



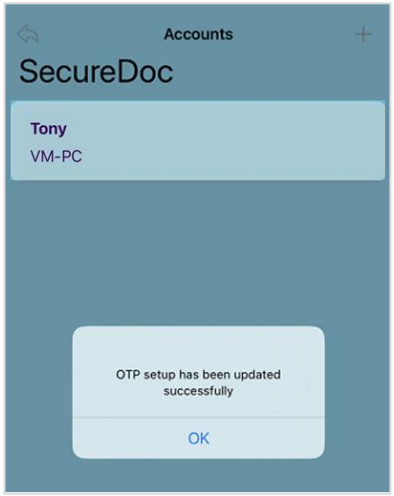
After the password key file has been converted to a phone token (Bluetooth or network phone), SecureDoc will warn you to set up an OTP:

1. Click **OK**.

SecureDoc will prompt you to enroll phone one-time password (OTP) recovery:



2. Launch the MagicEndpoint authenticator app on the phone.
3. In the mobile app, navigate to Menu > Accounts > **+**.
4. Scan the QR code.
   You should see an “OTP setup has been updated successfully” message on the phone.



5. Click **OK**.
6. Tap the account.

The OTP will be shown as asterisks:

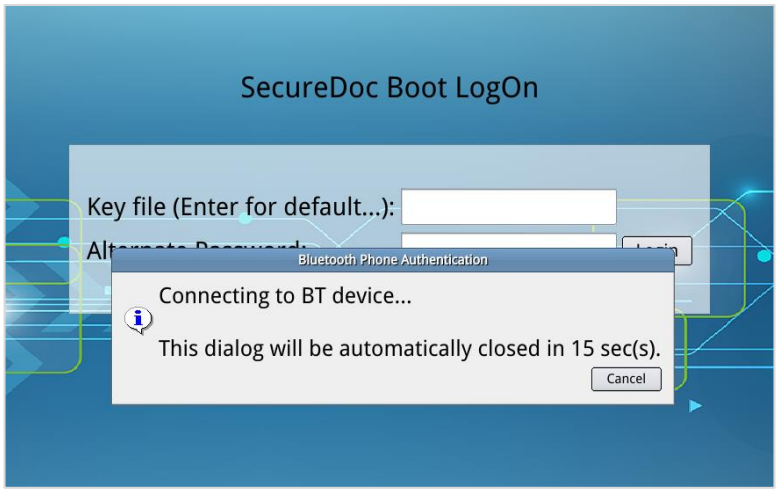
1. Tap “Blue Code”.
   The one-time password will appear:

Using the phone to log in

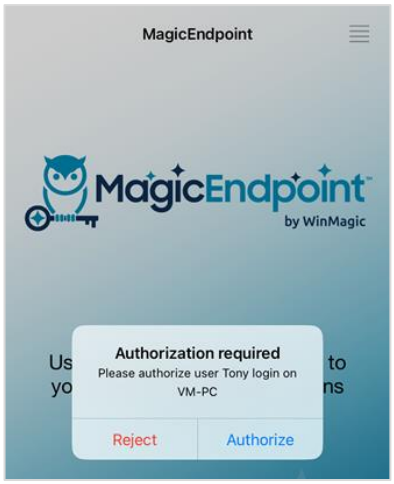
Phone token via Bluetooth

Logging into boot logon

1. At pre-boot, make sure the authenticator app is open on the phone.
   SecureDoc will scan for Bluetooth signals and connect to the phone.



   An authorization prompt will appear on the phone:

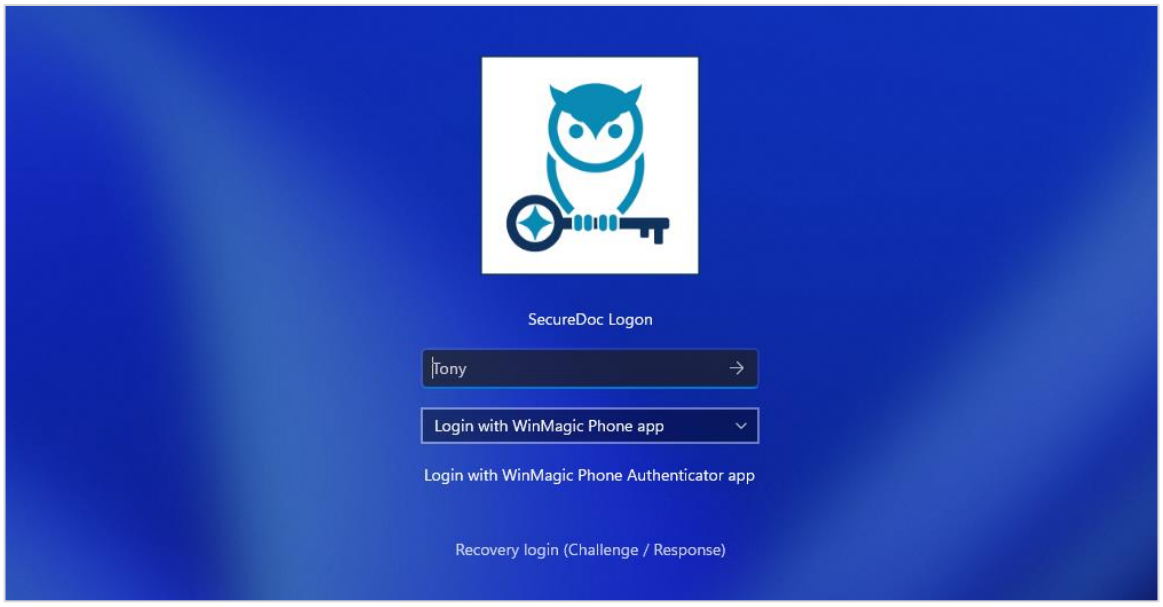


2. Tap **Authorize**.
   An authentication successful message should appear.

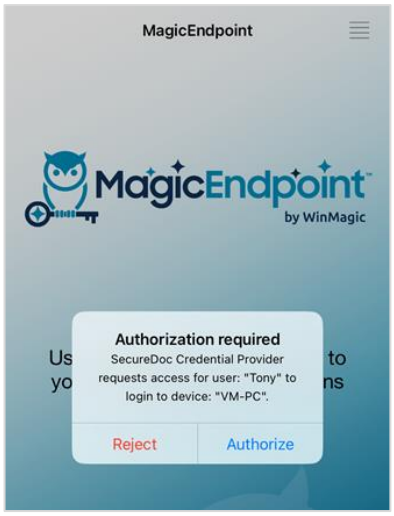
Logging into Windows

At the SecureDoc Windows logon screen…

1. Choose to “Login with the WinMagic Phone app” and click the login arrow →



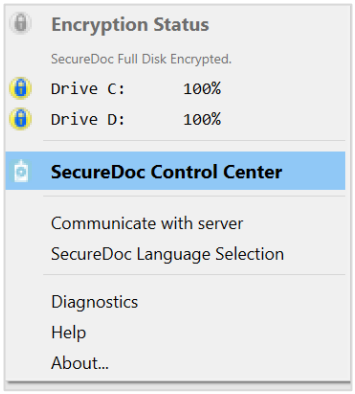
An authorization prompt will appear on the phone:



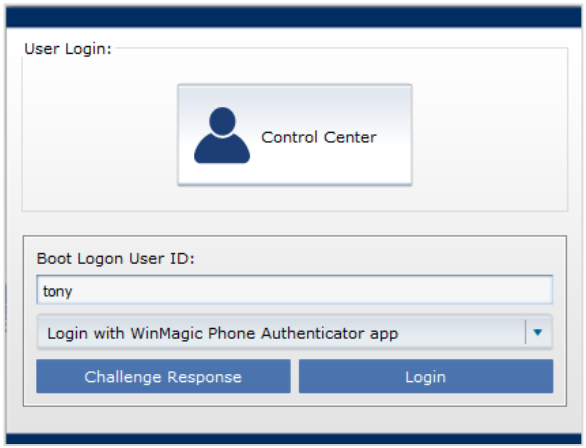
2. Tap **Authorize**.
   An authentication successful message should appear.

Log into the SecureDoc control center

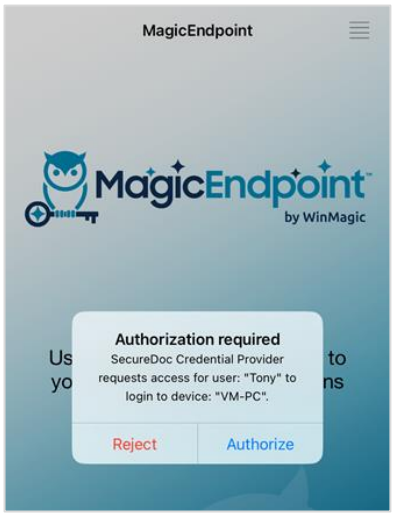
3. Launch the SecureDoc control center:
    a. Right-click the SecureDoc icon in the system tray
    b. Select **SecureDoc Control Center**:



4. Click **Login**.



An authorization prompt will appear on the phone:



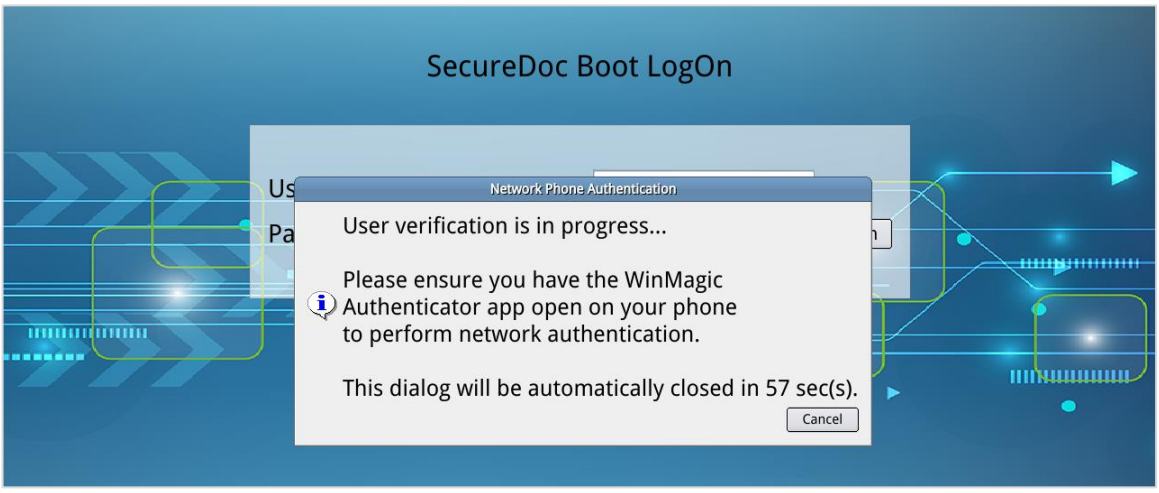
5. Tap **Authorize**.
An authentication successful message should appear.

Network with a phone

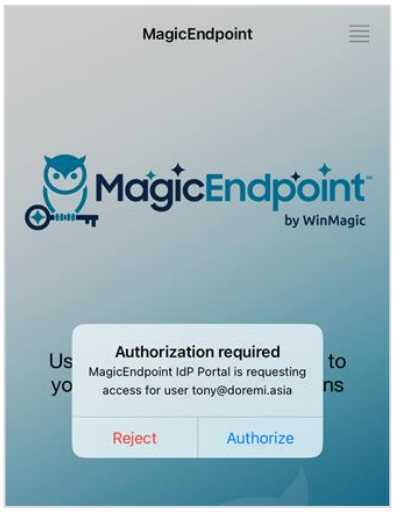
Logging into boot logon

At pre-boot, make sure the client and the phone are connected to the internet network.

1. Type in the valid username and click **Login**.



An authorization prompt will appear on the phone:



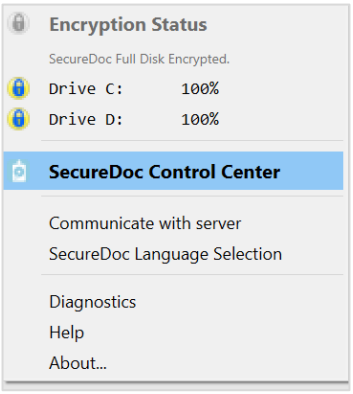
2. Tap **Authorize**.
   An authentication successful message should appear.

Log into Windows

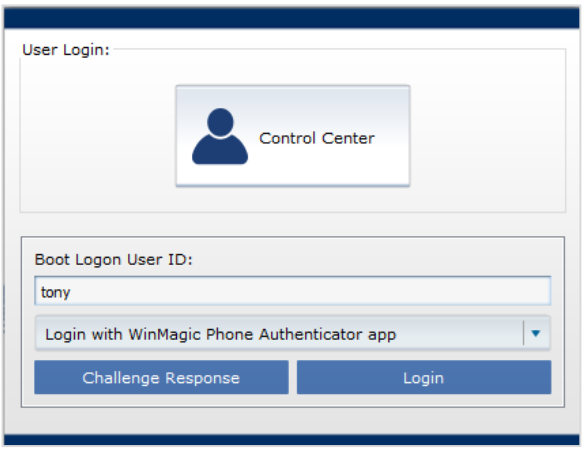
Logging into Windows using the network with a phone has the same user experience as logging in with phone via Bluetooth. See the previous Logging into Windows section.

Log into SecureDoc control center

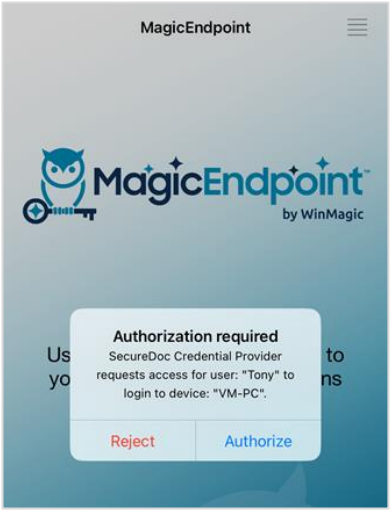
1. Launch the SecureDoc control center:
    a. Right-click the SecureDoc icon in the system tray
    b. Select **SecureDoc Control Center**:



2. Click **Login**.



An authorization prompt will appear on the phone:



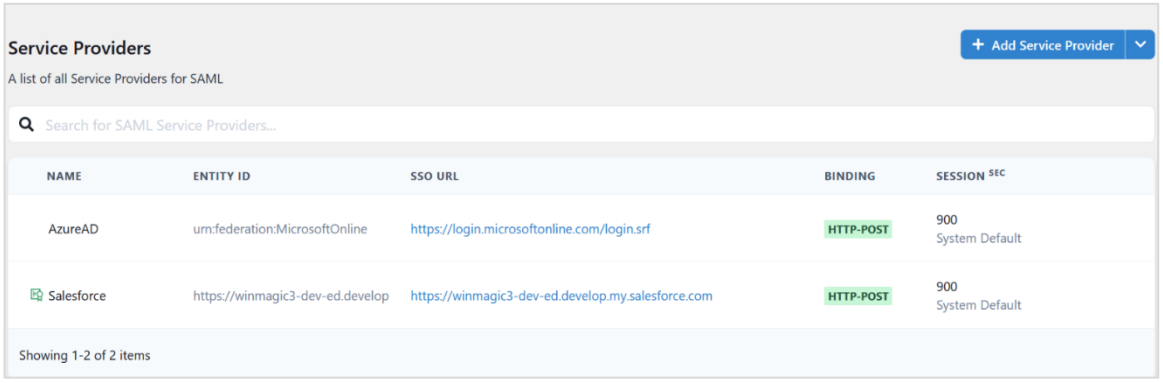
3. Tap **Authorize**.

    An authentication successful message should appear.

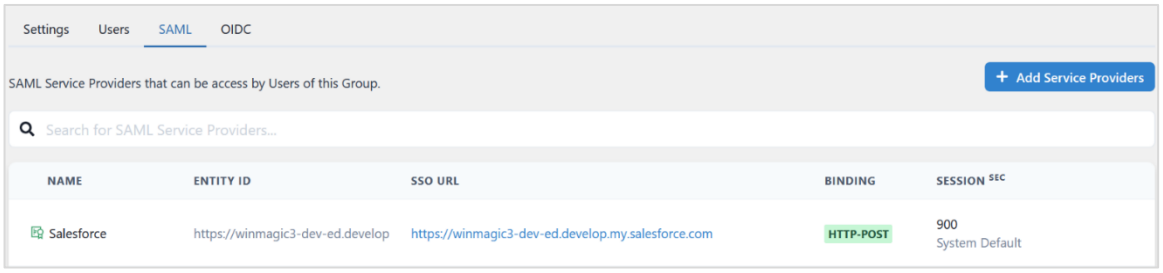
Logging into online applications

Preconditions

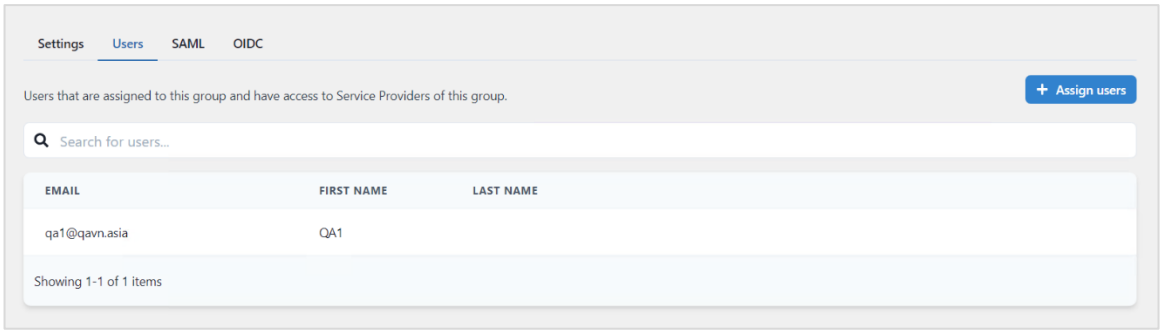
- ✓ The service provider (e.g., Salesforce) has been set up to log in using an IdP portal:



- ✓ The service provider has been assigned an IdP group:



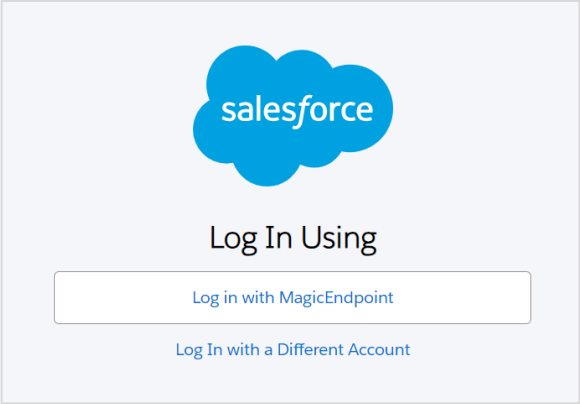
- ✓ The user has been assigned to IdP group:



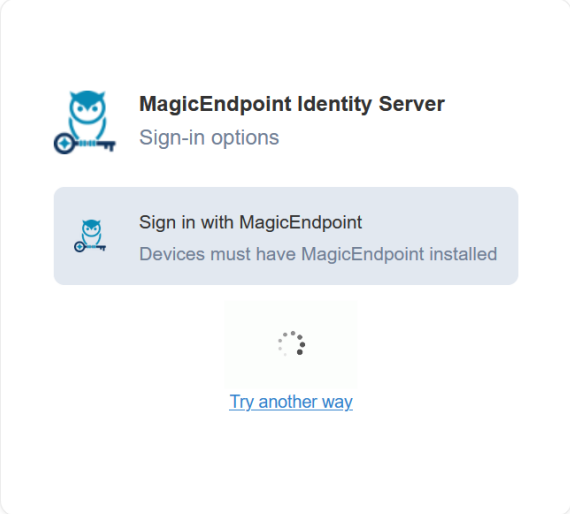
Log in to online applications with MagicEndpoint

With MagicEndpoint successfully configured in the SecureDoc platform…

1. Navigate to the service provider in an internet browser (e.g., Salesforce).



2. Select **Log in with MagicEndpoint**.
   MagicEndpoint will help log into the service provider with no user action — no username or password.



Log into online applications from a different, “unmanaged” device

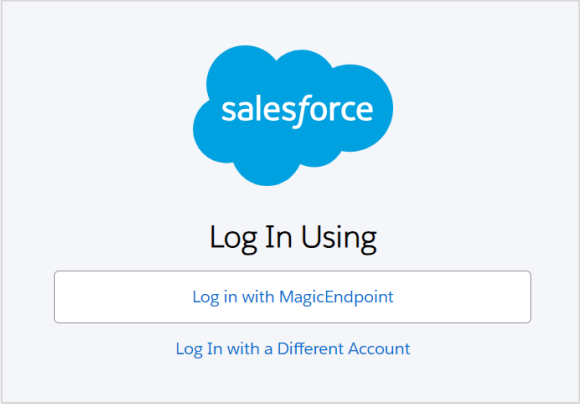
Preconditions

To log into an online application from a different “unmanaged” device, the end-user must register their phone with the IdP server:

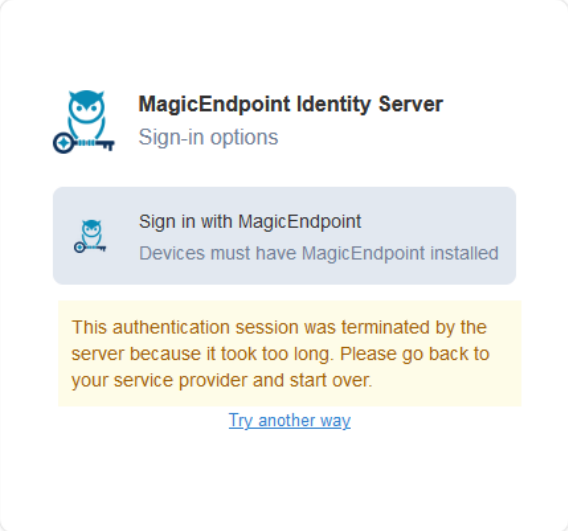
- ✓ Using Bluetooth and the phone
- ✓ Using the network and the phone (the user is a registered user)

On a different, unmanaged device…

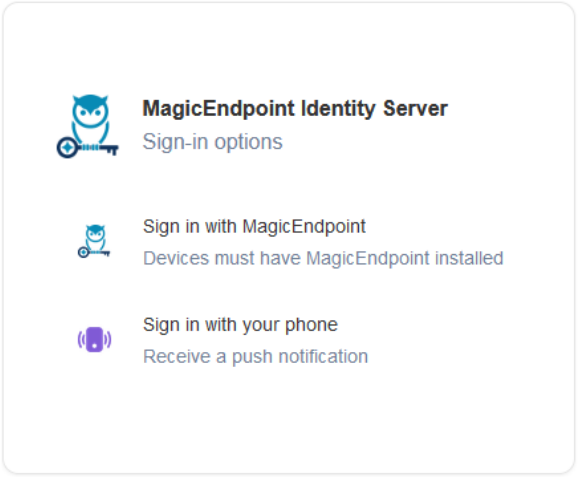
1. Navigate to a service provider in an Internet browser (e.g., Salesforce).
2. Click **Log in with MagicEndpoint**.



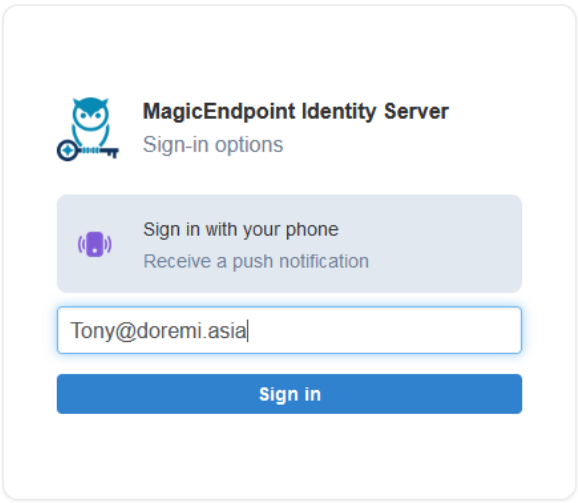
Authentication will fail because MagicEndpoint isn’t installed on the unmanaged device.



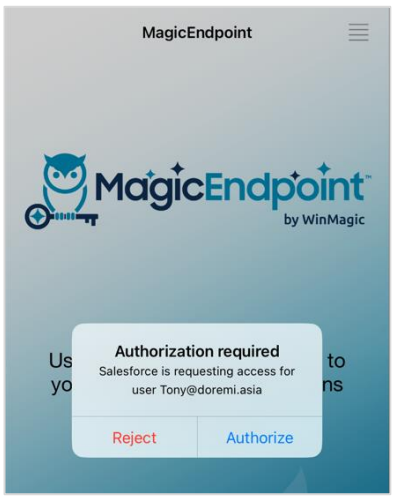
3. Click Try another way.
4. Choose **Sign in with your phone**.



5. Type in the email that is registered with the IdP portal.



6. Click **Sign in**.
   An authorization prompt will appear on the phone:



7. Tap **Authorize**.
   An authentication successful message should appear.

Log into your device if BLE or Network push aren't working

Use the OTP

You can use the OTP to log in at pre-boot, the SecureDoc customer portal, or the SecureDoc control center if

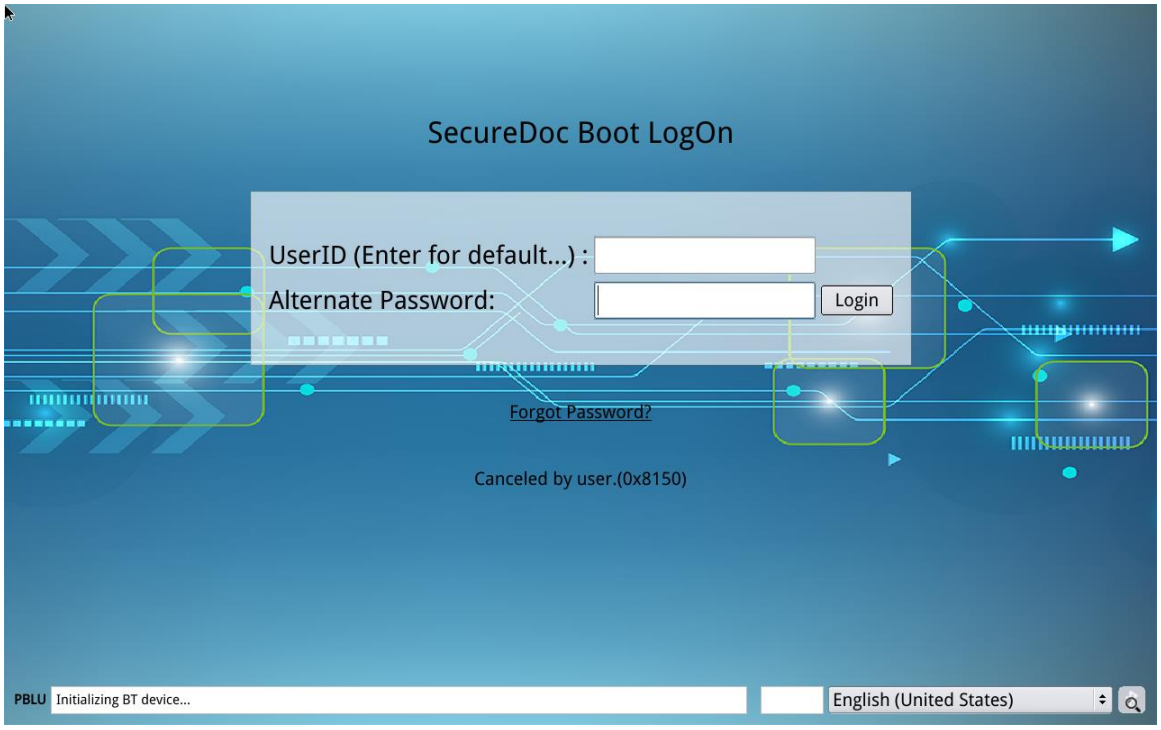
- The phone is lost or damaged — use an OTP on a backup phone
- Bluetooth is not working on the phone or computer with SecureDoc
- No network is available on the phone or computer with SecureDoc
- The IdP server has stopped working (phone network)

How to use the OTP from the MagicEndpoint app on your phone

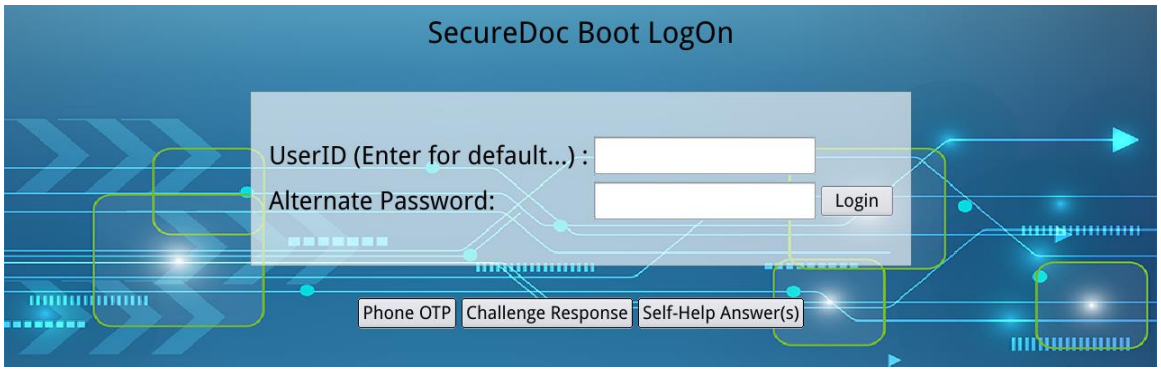
Note: SecureDoc will require you to change the password and re-convert to phone token (Bluetooth) or re-register the phone (network) after Windows loads successfully.

Recovery via OTP at pre-boot

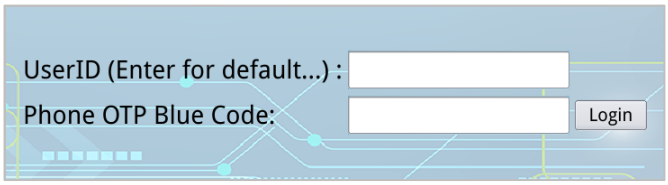
8. Restart the system.
9. Enter the username at Boot LogOn.
10. Cancel "Scanning for Bluetooth or network."
11. Select Forgot Password?



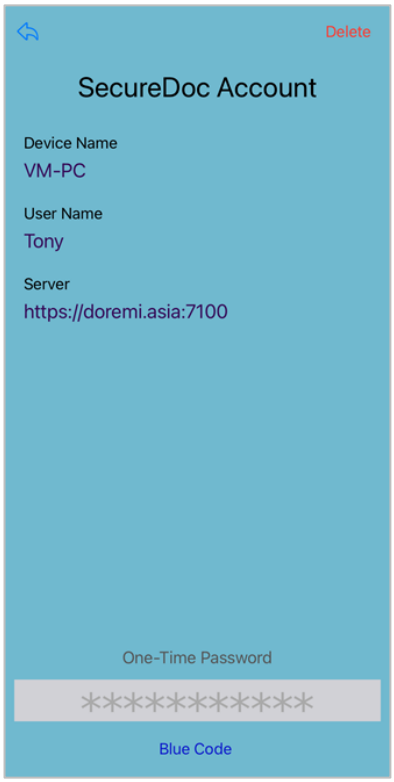
12. Click **Phone OTP**.



A “Phone OTB Blue Code” field will appear:

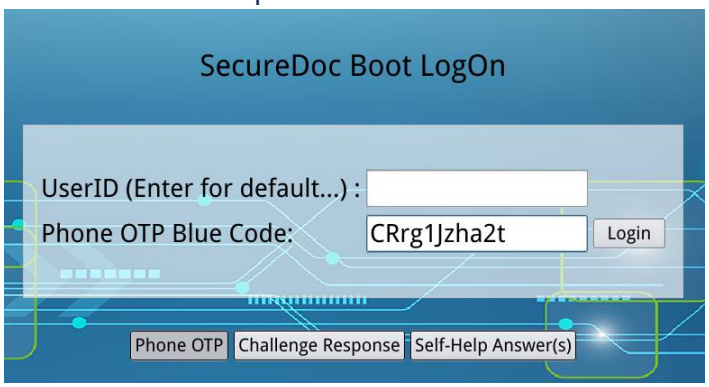


13. Launch the MagicEndpoint app on the backup phone.
14. Go to Menu > **Accounts**.
15. Select the same SecureDoc user ID.



16. Tap “Blue Code” and verify on the phone.
    The one-time password will appear:

17. Enter the one-time password into the OTP field.

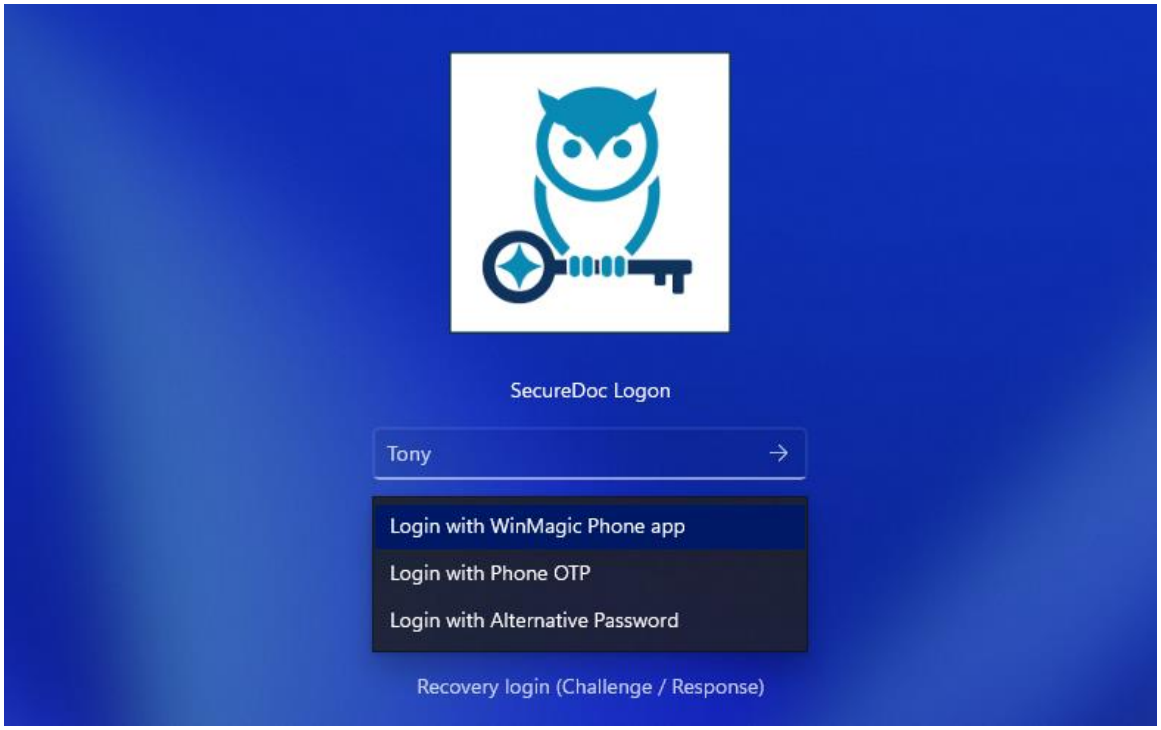


18. Click **Login**.
    You should be successfully logged in and Windows should load automatically without needing a Windows password.

Recovery via OTP at SecureDoc customer portal

At the SecureDoc Windows logon screen…

1. Choose “Login with Phone OTP” from the dropdown.



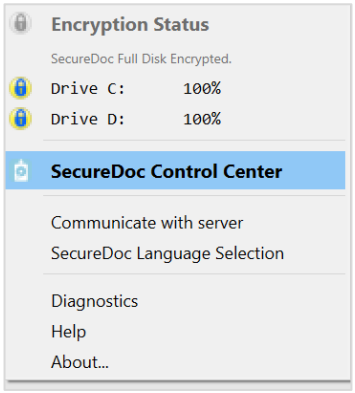
2. Launch the MagicEndpoint app on the backup phone.
3. Go to Menu > **Accounts**.
4. Select the same SecureDoc user ID.

5. Tap “Blue Code”.
   The one-time password will appear:

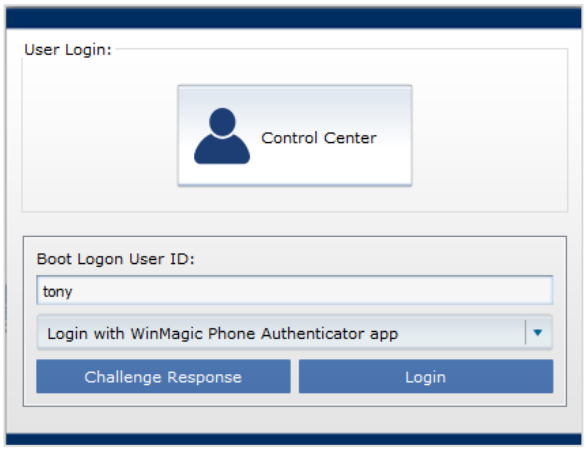
6. Enter the OTP in the SecureDoc customer portal.
7. Click the → button to log in.
   You should be logged in successfully.

Recovery via OTP at SecureDoc control center

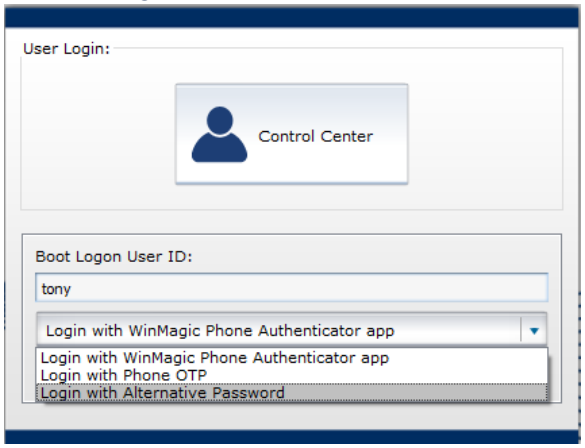
1. Launch the SecureDoc control center:
   a. Right-click the SecureDoc icon in the system tray
   b. Select **SecureDoc Control Center**:



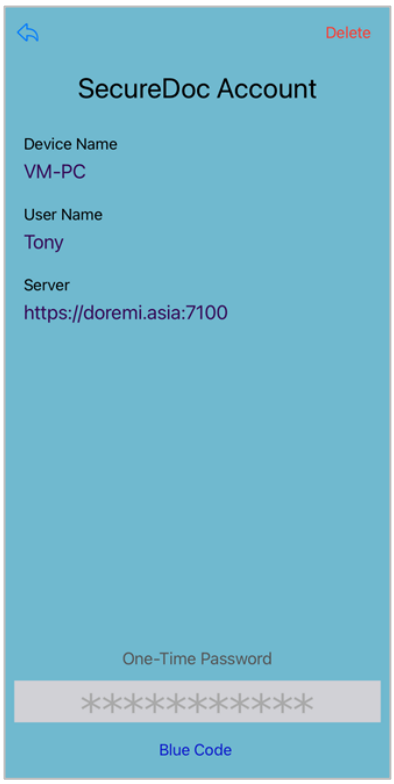
2. Click **Login**.



3. Select “Login with Phone OTP” from the dropdown menu.

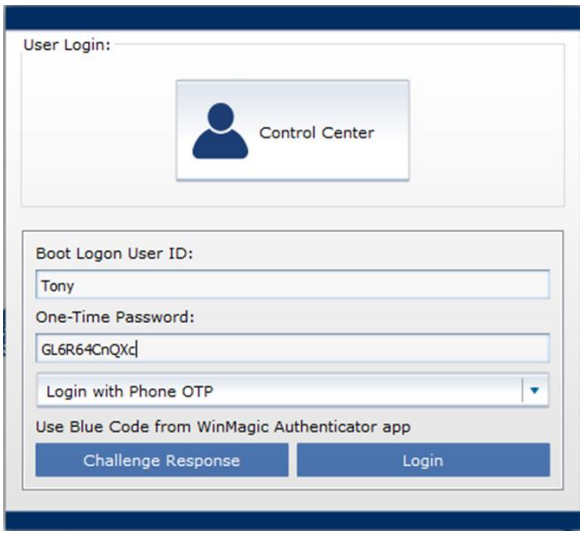


4. Launch the MagicEndpoint app on the backup phone.
5. Go to Menu > **Accounts**.
6. Select the same SecureDoc user ID.



7. Tap “Blue Code”.
   The one-time password will appear:

8. Enter the OTP into SecureDoc control center.



9. Click **Login**.
   You should be logged in successfully.

Logging in if the MagicEndpoint registered phone isn't available

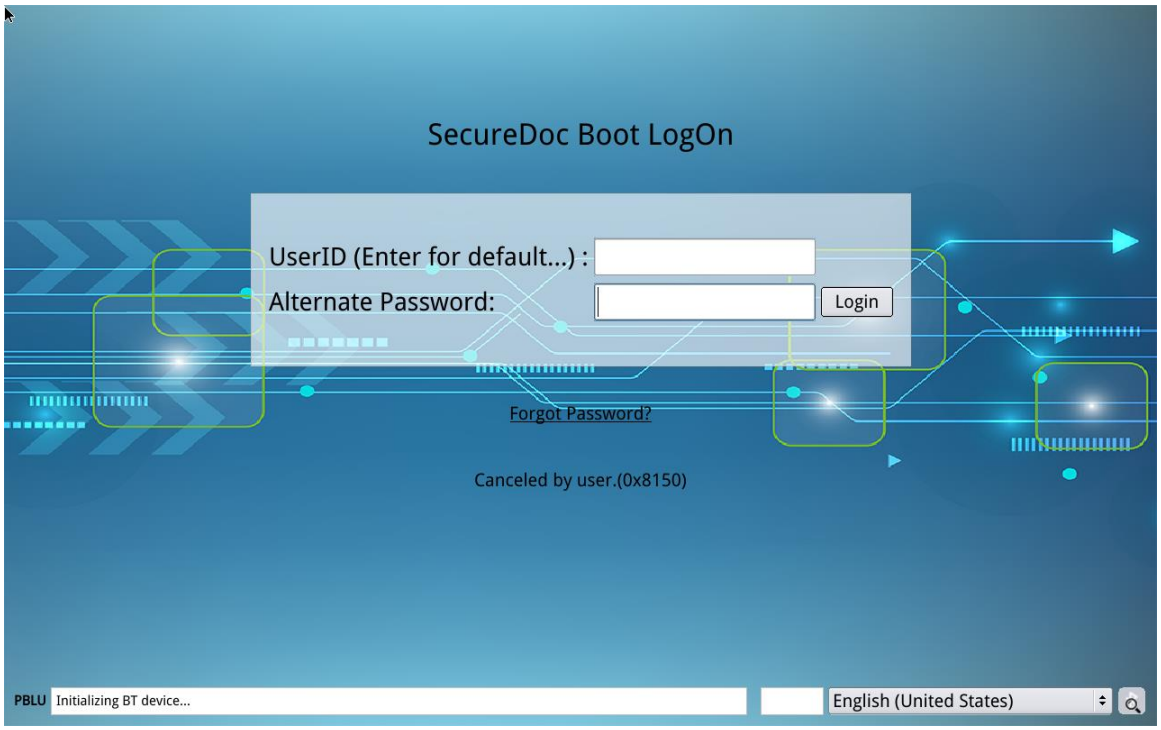
Note: SecureDoc will require you to change the password and re-convert to phone token (Bluetooth) or re-register the phone (network) after Windows loads successfully using "Challenge response" or "Self help" at pre-boot.

Available recovery methods:

- Challenge Response: contact the administrator.
- Self Help: Secret questions and answers.

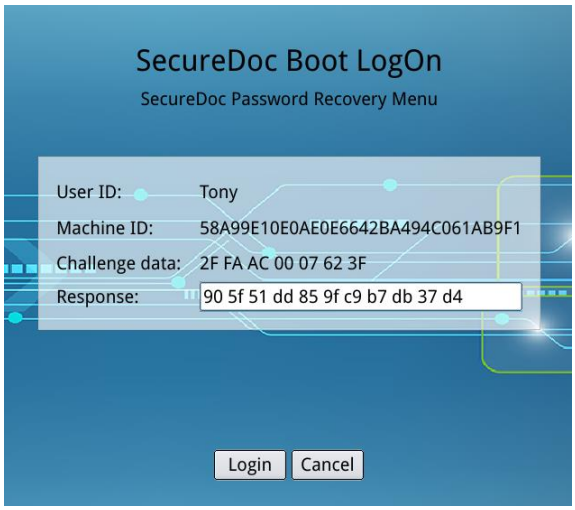
Challenge response

1. Restart the operating system.
2. Enter the username at Boot LogOn.
3. Cancel "Scanning for Bluetooth or network."
4. Select Forgot Password?



5. Select **Challenge Response**.

6. Contact the SecureDoc enterprise server administrator to get the response string.
7. Enter the response string.



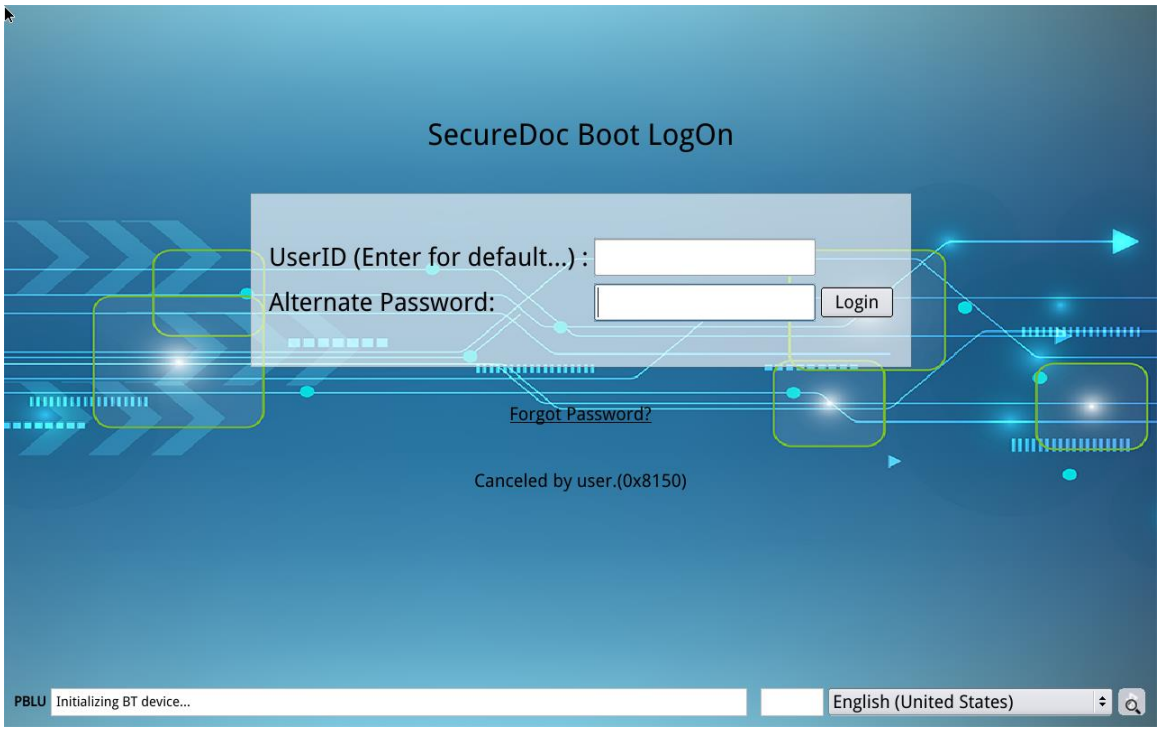
8. Click **Login**.
   You should be logged in successfully.

Self-help recovery

Precondition

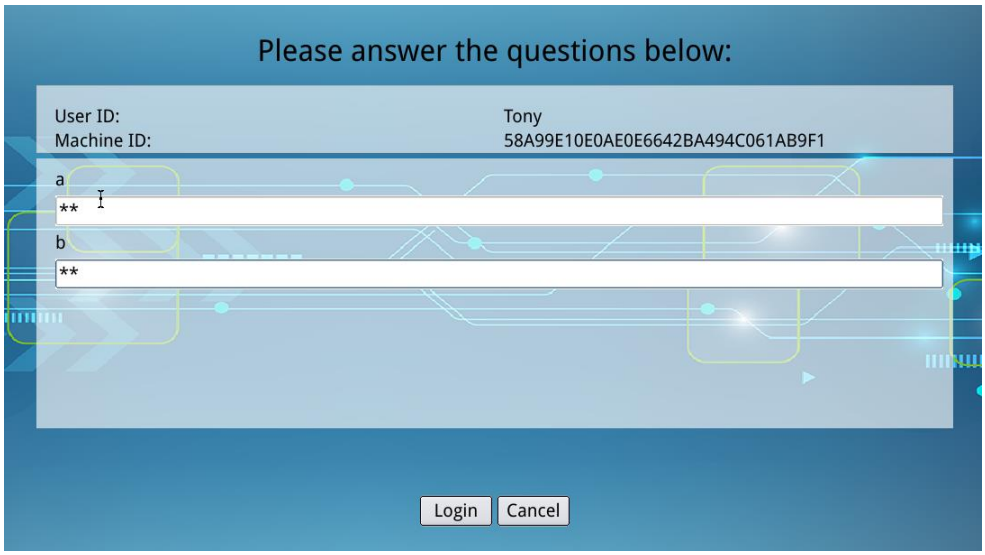
- Self-help questions have been configured in Global Operations. The end-user must have submitted answers to the SecureDoc enterprise server.

1. Restart the operating system.
2. Enter the username at Boot LogOn.
3. Cancel “Scanning for Bluetooth or network.”
4. Select Forgot Password?



5. Select **Self-Help Answer(s)**.

6. Type in the answers.



7. Click **Login**.
   You should be logged in successfully.

The MagicEndpoint registered phone is lost, damaged or stolen

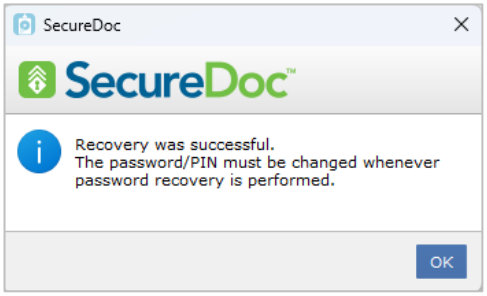
In case the registered phone has been lost, damaged, or stolen, the end user will use the recovery methods (OTP/Challenge Response or Self-Help) to log into Windows first and then register a new phone (keep using Phone Token – Bluetooth or Network).

Registering a new phone if the current MagicEndpoint phone is lost, damaged or stolen

Note: SecureDoc will require you to change the password and re-convert to phone token (Bluetooth) or re-register the phone (network) after Windows loads successfully.

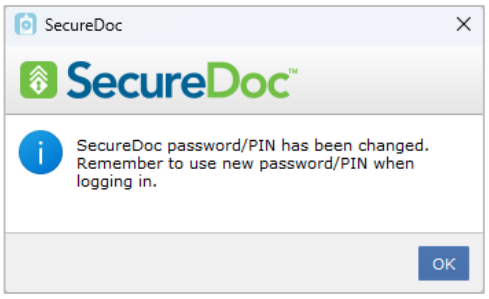
Reconvert phone token — Bluetooth

Upon successfully using a recovery method to log into Windows, SecureDoc will require the user to change their password/PIN.

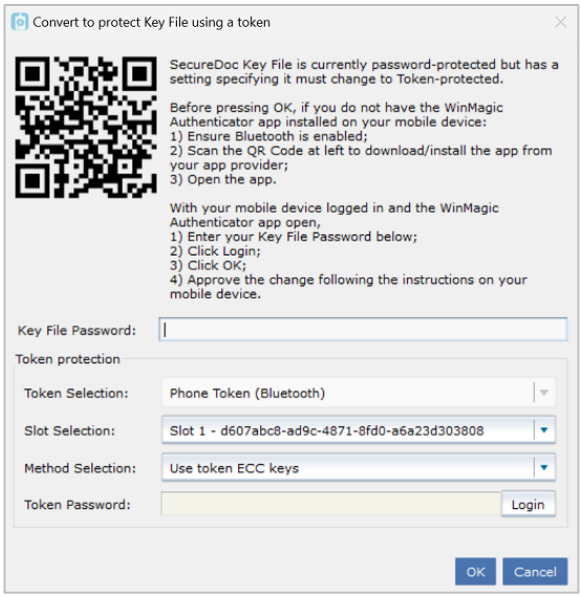


1. Click **OK**.
2. Enter a “New Password” and re-enter the new password in the “Confirm New Password” field.

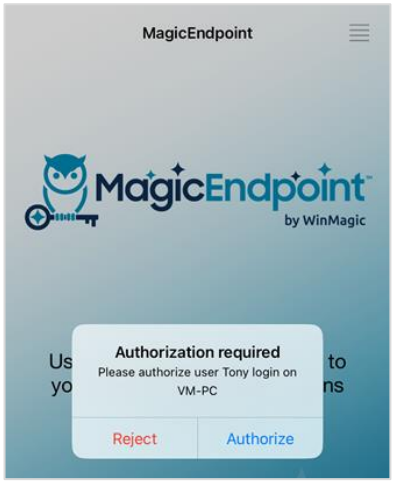
You’ll see a notification stating the password has been changed.



3. Click **OK**.
   SecureDoc will require you to “convert to protect Key File using a token.”



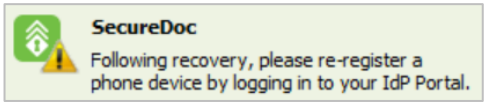
4. Enter the password for the key file.
5. Click **Login** beside the “Token Password” field.
6. Click **OK**.
7. Open the MagicEndpoint app on the phone.
   An authorization prompt will appear on the phone:



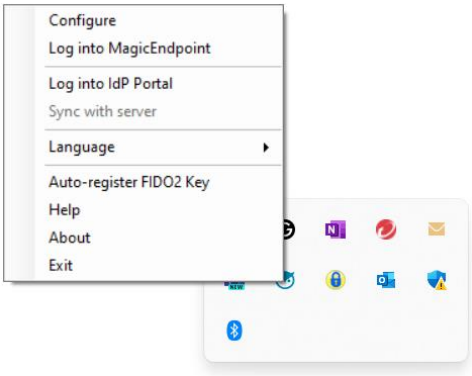
8. Tap **Authorize**.
   The password key file will re-convert to the phone token.

Re-register another network phone

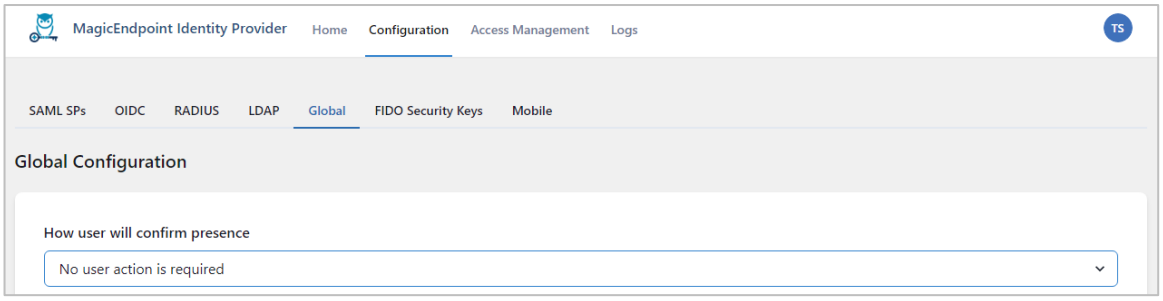
Upon logging into Windows, SecureDoc will prompt to re-register a network phone:



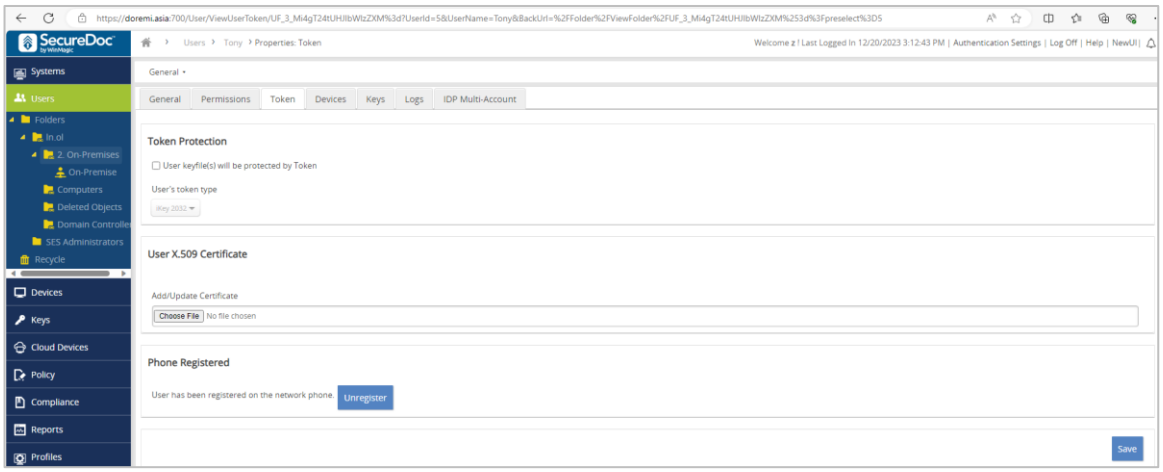
1. Right-click the MagicEndpoint icon in the Windows task bar.
2. Select **Log into IdP portal**.



Usually, the IdP has been previously configured as “No user action is required”:



If the IdP is configured as “User must authenticate” instead, the system administrator must log into the SecureDoc enterprise server to “Unregister” the network phone:



3. Click **Sign-in** to log into the IdP portal.
4. Go to **Configuration** and open the **Mobile** tab.
5. Click **Proceed** if the end-user wants to register a new phone.

6. Proceed to scan the QR code and follow the registration prompts.

Note: If the old phone is recovered, the user will not need to register a new phone. However, as soon as a new phone is registered with MagicEndpoint, the old phone will no longer work for MagicEndpoint authentication.

Contact

If these steps above didn't solve your issue or you're looking for further instruction, contact mesupport@winmagic.com.

About WinMagic

With over 25 years of continuous innovation, WinMagic is a leading authority in endpoint encryption and authentication solutions.

WinMagic's passwordless authentication solution, MagicEndpoint, uses MFA to authorize endpoint access via a smartcard, USB token, phone, TPM, PIN, password or combinations for Windows and pre-boot sign-on. Users are then granted secure, passwordless authentication to online applications and services without requiring any user action. The solution supports zero-trust security frameworks by continuously verifying the endpoint's security posture plus the user's presence and intent.

Founded on public-key-based FIDO standards, MagicEndpoint offers the most secure online authentication while delivering the best user experience with no user action.

MagicEndpoint

MagicEndpoint offers the most secure user authentication with the best possible user experience. Once the user has unlocked the endpoint, the endpoint gives access to everything else — no user action required. Based on cutting-edge FIDO2 security, MagicEndpoint actively verifies a "user + device" entity. The endpoint provides the IdP server real-time intelligence to monitor the user, device and even the user's intent. This continuous verification supports zero-trust frameworks without burdening the user. Free your users from all remote authentication steps today and step up your security with MagicEndpoint passwordless authentication.

SecureDoc™

SecureDoc ensures your personal information and intellectual property is secure while withstanding the most rigorous compliance demands. The software is easy to install and offers comprehensive encryption for hard drives, PDAs and removable media.

Enable secure access through various authentication methods in the pre-boot environment, including MFA via Bluetooth low energy, hardware keys and more. SecureDoc seamlessly integrates with existing infrastructure while managing profiles, interacting with Active Directory and providing tools for password recovery and encryption key management.