Delinea

Secret Server Mobile

Administrator Guide

Version: 1.8.x

Publication Date: 12/11/2024

Secret Server Mobile Administrator Guide

Version: 1.8.x, Publication Date: 12/11/2024

Warranty Disclaimer

DELINEA AND ITS AFFILIATES, AND/OR ITS AND THEIR RESPECTIVE SUPPLIERS, MAKE NO REPRESENTATIONS ABOUT THE SUITABILITY OF THE INFORMATION CONTAINED IN THE DOCUMENTS AND RELATED GRAPHICS, THE SOFTWARE AND SERVICES, AND OTHER MATERIAL PUBLISHED ON OR ACCESSIBLE THROUGH THIS SITE FOR ANY PURPOSE. ALL SUCH MATERIAL IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. DELINEA AND ITS AFFILIATES, AND/OR ITS AND THEIR RESPECTIVE SUPPLIERS, HEREBY DISCLAIM ALL WARRANTIES AND CONDITIONS WITH REGARD TO SUCH MATERIAL, INCLUDING ALL IMPLIED WARRANTIES AND CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT.

THE MATERIAL PUBLISHED ON THIS SITE COULD INCLUDE TECHNICAL INACCURACIES OR TYPOGRAPHICAL ERRORS. CHANGES ARE PERIODICALLY ADDED TO THE INFORMATION HEREIN. DELINEA AND ITS AFFILIATES, AND/OR ITS AND THEIR RESPECTIVE SUPPLIERS, MAY MAKE IMPROVEMENTS AND/OR CHANGES IN THE MATERIAL DESCRIBED HEREIN AT ANY TIME.

Disclaimer of Liability

IN NO EVENT SHALL DELINEA AND ITS AFFILIATES, AND/OR ITS AND THEIR RESPECTIVE SUPPLIERS, BE LIABLE FOR ANY SPECIAL, INDIRECT, OR CONSEQUENTIAL DAMAGES (INCLUDING LOSS OF USE, DATA, PROFITS OR OTHER ECONOMIC ADVANTAGE) OR ANY DAMAGES WHATSOEVER, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE, OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF SOFTWARE, DOCUMENTS, PROVISION OF OR FAILURE TO PROVIDE SERVICES, OR MATERIAL AVAILABLE FROM THIS SITE.

Table of Contents

Introduction to the Secret Server Mobile Application

Through the Secret Server Mobile application, users can connect from a mobile device to a Secret Server instance to view, manage, and use secrets stored there. The mobile application interface is similar to the Secret Server interface, which makes it easy for users to navigate to find secrets and secret folders. The mobile application offers useful functionality including multi-factor authentication, biometric authentication, autofill, online and offline caching, and advanced secret workflows, all summarized below.

Multi-factor Authentication

The mobile application supports the same MFA mechanisms as used by Secret Server:

- DUO - Push
- DUO - Phone call
- Pin Code
- TOTP authenticators

Biometric Authentication

The mobile application supports using biometric authentication in place of usernames and passwords.

- Fingerprint (Android and iOS)
- Facial recognition (iOS only, not all phone/iOS combinations)

The application will auto-reconnect to Secret Server if the connection is temporarily dropped due to network issues.

Autofill

When a user enables their mobile device's autofill service and then registers Secret Server Mobile with that service, users can launch a web session from a secret on the mobile device and automatically populate username and password login credentials on specified web sites or other mobile applications.

When you select the mobile application or web page and click on the username field you should see a prompt from Secret Server Mobile to use the autofill service. Click this option to open the mobile app and log in if necessary, and the app runs a search of your secrets for:

- Browser web site - to search for any secret that has the same Domain value in the URL
- Other mobile application - to search for any secret that has the same name or URL value as the name of the mobile application that is being filled.

Users can also choose to manually modify the search value and run it again. Once the list of Secret Server Secrets has been returned, you can select which one you want to use and the autofill service will fill those credentials in the related username and password fields.

> **Note**: Currently the autofill service supports only the username and password fields.

Online Caching

Secure storage handles most of the security:

- on **iOS**, Secure Keychain is used. Keychain items are encrypted using two different AES-256-GCM keys.
- on **Android**, an AES key is obtained from the android key store. This is then used with an AES/GCM/NoPadding cipher to encrypt the value.
- Following login, the online cache displays the user's list of Secrets, without secret details
- The online cache is updated every 5-10 minutes.
- The cache is cleared out on user logout and user switch.
- No credential values are cached, except for the Secret Server login, which is used by Biometrics.

Offline Caching

An organization can permit its Secret Server Mobile users to save secrets to an offline cache. When a network connection to Secret Server is unavailable, users can access secrets they previously cached offline for a specified Time-To-Live (TTL) period. An organization’s Secret Server administrator controls TTL and access to offline caching globally, for all mobile devices in the organization. If an organization does not allow offline caching, the administrator sets the TTL to zero. To use offline caching, biometric authentication must be enabled.

Offline caching:

- Stores information in a secured encrypted database.
- Stores secrets tagged for offline caching along with their secret details
- Updates automatically by default, unless the auto-update feature is turned off
- The cache is cleared on user logout and user switch.
- Offline mode login is secured by biometric authentication (fingerprint or face ID).

Secret Workflows

From **Autofill**, **Home**, **Favorites**, **Recents**, and **Shared** screens, Secret workflows provide users with screens, confirmations, notices, prompts, indications, and controls related to:

- checking out and checking in a secret
- submitting, resubmitting, and canceling a request for access to a secret
- submitting a Double Lock password or a Ticket Comment, Reason, or Number to access a secret
- confirmation of submission, approval, denial, or cancellation of an access request
- notification of a duplicate request for access to a Secret
- notification of login failure with the reason for failure
- provision of access to a secret, including details and options, upon approval
- setting a duration and a beginning and end time for accessing a secret, now or at a later date

- visual indication of each secret you have checked out, from both Secret Server Mobile and the Secret Server web interface
- visual indication that a secret is checked out by another user
- entering a Comment and checking out a Secret at the same time

Onboarding and Prerequisites

Configure Secret Server

Before you can use Secret Server Mobile, an administrator must enable webservices on Secret Server and set time limits for offline caching.

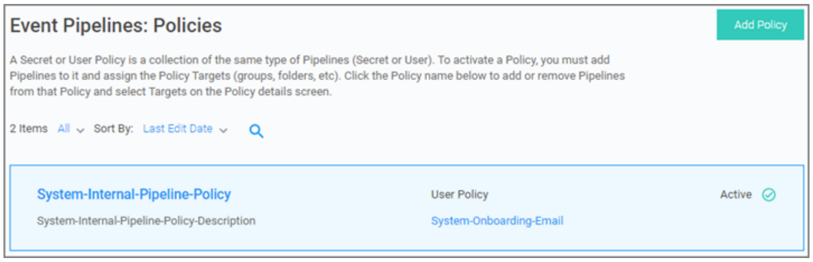
Enable Web Services with Time Limits in Secret Server

To allow communication via RestAPI between the mobile application and Secret Server, Webservices must be enabled in Secret Server. For maximum security, do not set session timeout to "Unlimited." See Enabling Web Services in the Secret Server documentation for more information.

Set Time Limits for Offline Caching in Secret Server

To use offline caching in the mobile application, an administrator must configure offline caching Time to Live (TTL) in Secret Server. Administrators can disable offline caching globally by setting the TTL to zero. For maximum security, restrict offline access to no more than a few days. See Setting Maximum Time for Offline Caching in the Secret Server documentation for more information.

In Secret Server 10.9 and newer, an administrator can send an email directly from the Secret Server UI to new Secret Server Mobile users, inviting them to connect to Secret Server and providing detailed instructions to help the user with initial setup and onboarding tasks. Secret Server administrators can check the mobile application onboarding progress in Event Pipelines. See Event Pipelines in the Secret Server documentation for more information.



Event Pipelines: Policies

A Secret or User Policy is a collection of the same type of Pipelines (Secret or User). To activate a Policy, you must add Pipelines to it and assign the Policy Targets (groups, folders, etc). Click the Policy name below to add or remove Pipelines from that Policy and select Targets on the Policy details screen.

2 Items All Sort By: Last Edit Date

System-Internal-Pipeline-Policy — User Policy — Active ✓

System-Internal-Pipeline-Policy-Description — System-Onboarding-Email

Operating System Requirements

The following Operating Systems are supported:

- iOS 12 and up
- Android 8 and up

Minimum Hardware Requirements

Mobile devices not more than four years old running operating systems as described above.

Compatibility Requirements

The Secret Server Mobile Application works with Secret Server on-premises and cloud instances starting with Version 10.8 and up. To utilize Secret Server's **onboarding feature**, Secret Server 10.9 is a minimum requirement.

Offline Caching requires Secret Server 10.9.000064 or higher.

The mobile application integrates via Secret Server's RESTApi.

Configuring the Application

Note: Before you download or install the Secret Server Mobile application, be sure to check the system Prerequisites.

Download, Install, and Launch the Application

Secret Server 10.9 and newer sends an email to newly-registered Secret Server Mobile users inviting them to connect to Secret Server and walking them through the download, installation, initial setup, and onboarding processes. You can follow the steps in the email but for your convenience we also provide much of the same information below.

You can download the Secret Server Mobile application from the following sources:

- Google Play Store
- Apple App Store

Once you download and launch Secret Server Mobile, log in by following the instructions at Login Methods.

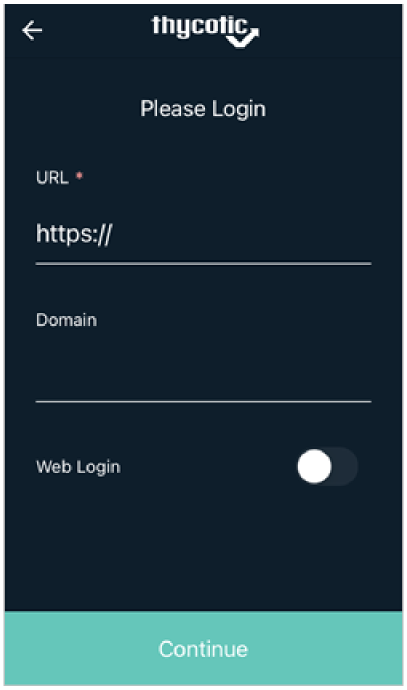
After you log into the application, choose the configurations that work best for you, including custom configurations for Web login, multi-factor and biometric authentication, and autofill, which are described below.

Configuring Web (SAML) Login

SAML support allows users to login via Web Login.

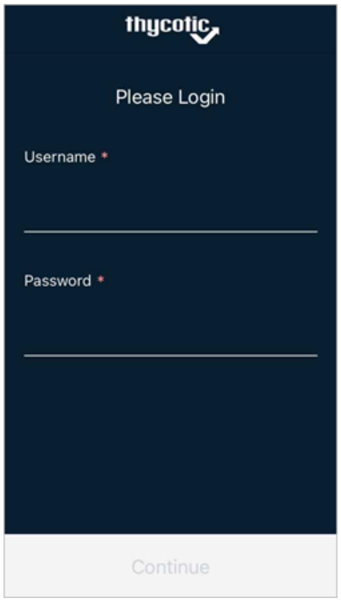
To use the Web Login option

1. Navigate to your Secret Server Mobile apps login screen.
2. Enable the **Web Login** switch.



3. Click **Continue**. You will see a quick page flash when the app reaches out to the server for the token generation.

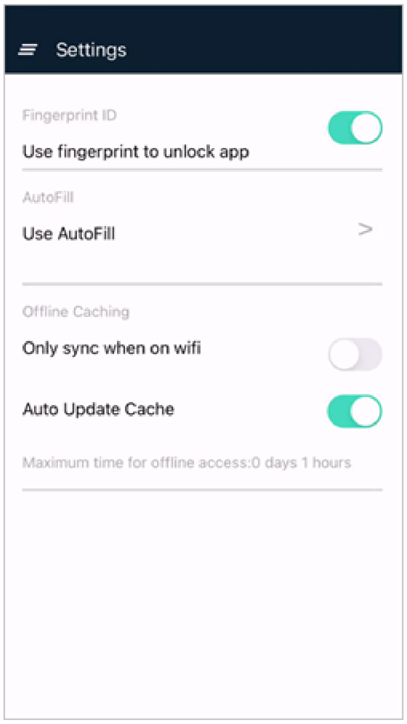
   Your Login page now looks like this:



Configuring Biometric Authentication

Delinea recommends using biometric authentication: either facial recognition (iOS only) or fingerprint ID (Android and iOS) in place of username and password credentials. You must enable biometric authentication to use offline caching features.

1. Navigate to the **Settings** page and select either fingerprint identification or facial recognition.



Settings

Fingerprint ID

Use fingerprint to unlock app: on

AutoFill

Use AutoFill >

Offline Caching

Only sync when on wifi: off

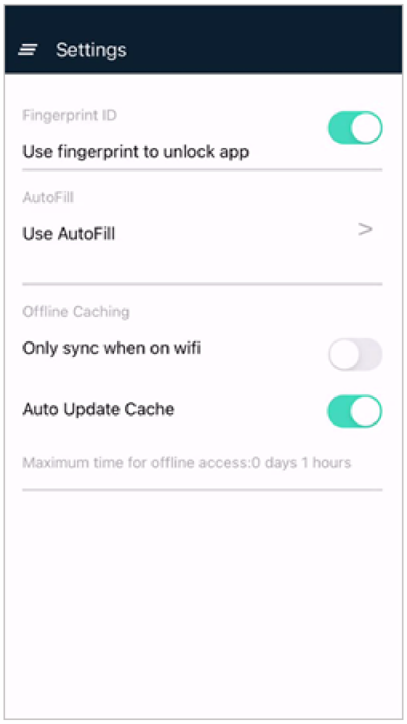
Auto Update Cache: on

Maximum time for offline access:0 days 1 hours

2. Click **OK** at the trust prompt and follow the directions to enter your fingerprint.

Configuring Autofill

1. On the **Settings** page you can choose automation settings including **Use AutoFill** for usernames and passwords.



Settings

Fingerprint ID

Use fingerprint to unlock app ●

AutoFill

Use AutoFill >

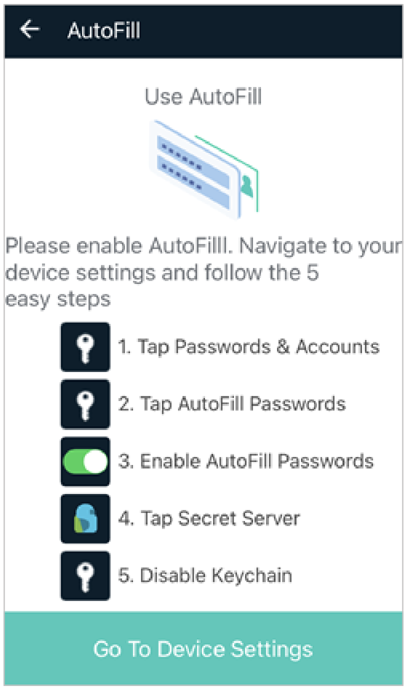
Offline Caching

Only sync when on wifi ○

Auto Update Cache ●

Maximum time for offline access:0 days 1 hours

2. On the **Use Autofill** page, follow the directions and click **Go To Device Settings**.



AutoFill

Use AutoFill

Please enable AutoFilll. Navigate to your device settings and follow the 5 easy steps

1. Tap Passwords & Accounts
2. Tap AutoFill Passwords
3. Enable AutoFill Passwords
4. Tap Secret Server
5. Disable Keychain

Supported MFA

The application supports the same MFA mechanisms as used by Secret Server:

- DUO – Push
- DUO – Phone call
- Pin Code
- TOTP authenticators

If available via device, the application supports biometric authentication instead of a Secret Server password:

- Fingerprint (Android and iOS)
- Facial recognition (iOS only)

The application will auto-reconnect to Secret Server if the connection is temporarily dropped due to network issues.

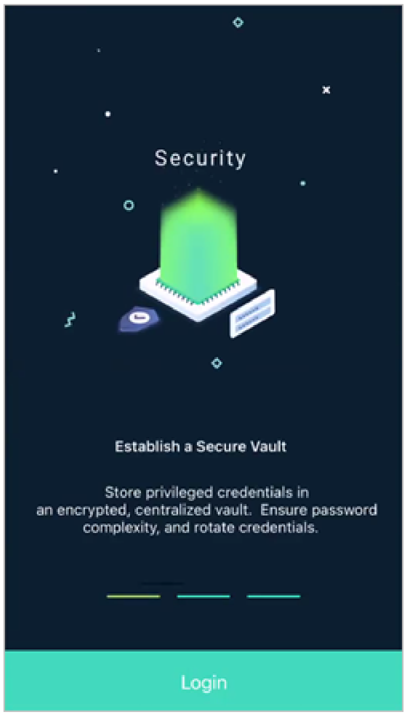
Mobile Setup

Once the user receives the invitation email from the onboarding process to install and use the Secret Server Mobile application, they use the provided app store links to download and install the product. The Secret Server Mobile application is available at

- Google Play
- Apple App Store

Following a successful installation users can manually enter the connection URL and user credentials or use the links in the onboarding email to run through the initial setup steps:

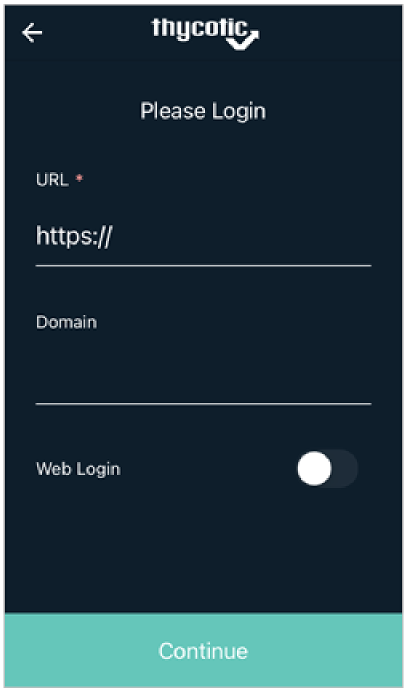
1. Open the Secret Server Mobile application.
2. Click **Login**.



Establish a Secure Vault

Store privileged credentials in an encrypted, centralized vault. Ensure password complexity, and rotate credentials.

3. Enter you Secret Server instance URL, for example `websitename.domain.com/secretserver`.



Please Login

URL *

https://

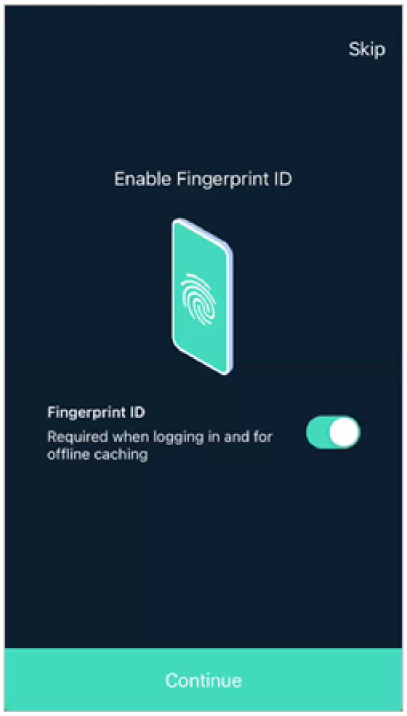
Domain

Web Login ○

The Domain value is optional.

4. Click **Continue**.

5. Enter your **Username** and click **Continue**.
6. Enter your **Password** and click **Continue**.
7. Delinea recommends using biometrics if supported by your mobile device. Set the biometrics switch to on, in this case Fingerprint.

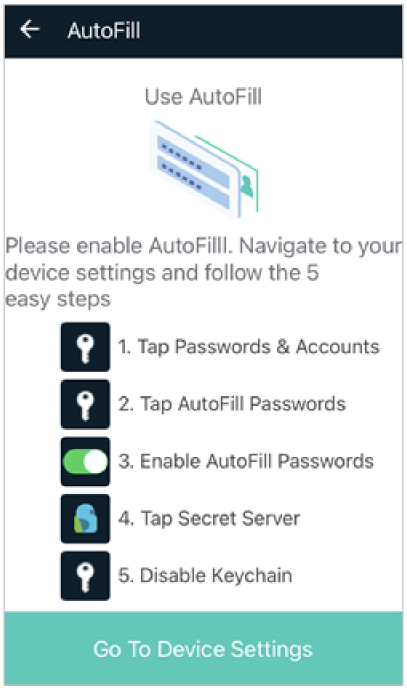


Enable Fingerprint ID

Fingerprint ID

Required when logging in and for offline caching

8. Click **Continue**.
9. During the initial login sequence, the application will also prompt if you prefer to enable auto-filling usernames and passwords.



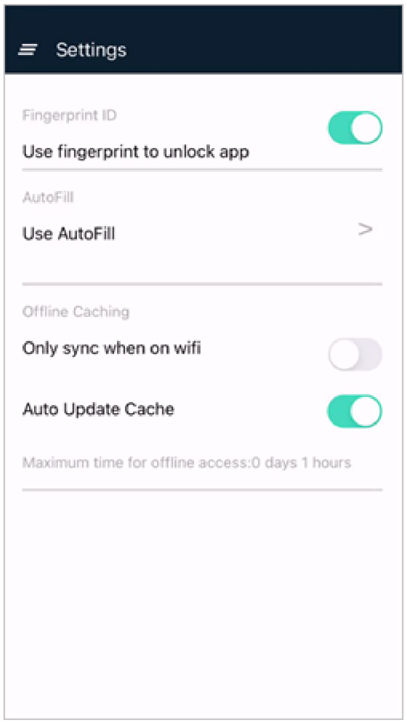
AutoFill

Use AutoFill

Please enable AutoFilll. Navigate to your device settings and follow the 5 easy steps

1. Tap Passwords & Accounts
2. Tap AutoFill Passwords
3. Enable AutoFill Passwords
4. Tap Secret Server
5. Disable Keychain

If you choose to enable autofill functionality, you navigate to the Settings page:



Settings

Fingerprint ID

Use fingerprint to unlock app

AutoFill

Use AutoFill

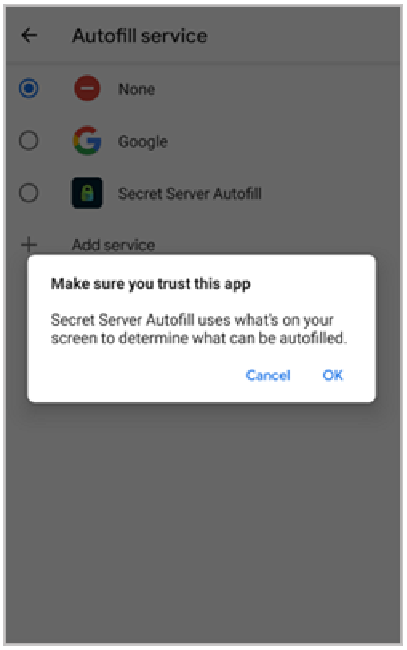
Offline Caching

Only sync when on wifi

Auto Update Cache

Maximum time for offline access:0 days 1 hours

a. Set the **Use AutoFill** switch to on.



Autofill service

● None

○ Google

○ Secret Server Autofill

+ Add service

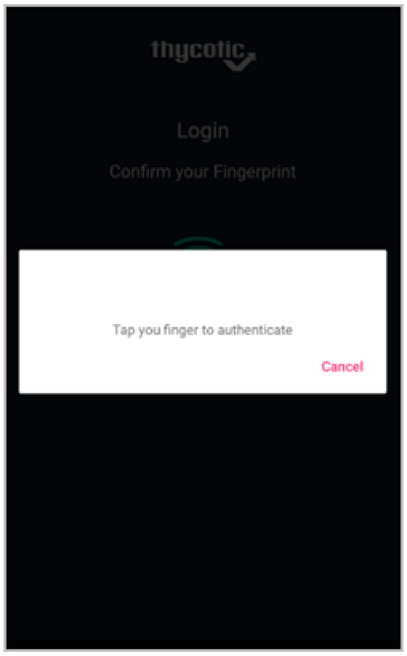
Make sure you trust this app

Secret Server Autofill uses what's on your screen to determine what can be autofilled.

b. Click **OK** to the trust prompt and select the **Secret Server Autofill** radio button.

The Secret Server Mobile is now ready for use on your mobile device.

If biometrics are enabled, the user will be prompted to authenticate via the enable biometrics functions on the next login:



Login

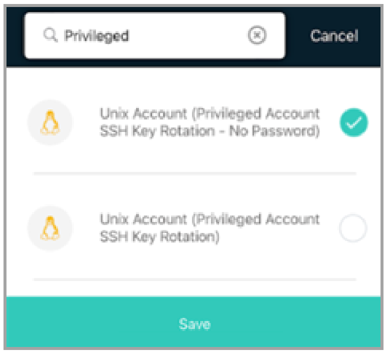
Confirm your Fingerprint

Tap you finger to authenticate

Using the Application

The Secret Server Mobile application interface has been designed to be similar to the Secret Server interface to make it easy for users to search and browse through folders and secret collections to quickly find specific folders and secrets. Clicking on a Secret will expand it and show the Secret information. You can click a secret to open, view, and edit it in a browser. You can also add and delete folders and secrets, mark them as Favorites, and designate them for availability offline.

You can find secrets by browsing through **Favorites** and **Recent** secrets. You can also search for a secret by name or by type (by the template it is based on). In the image below, the user has searched for *Privileged* and the application returned two secrets based on a Privileged Account template.


Privileged
Cancel
Unix Account (Privileged Account SSH Key Rotation - No Password)
Unix Account (Privileged Account SSH Key Rotation)
Save

The application allows users to automatically fill credentials from Secrets into other mobile apps or Web browser sites on the mobile device. For this to work correctly, the application needs to be registered with the device's autofill service.

The application allows users to launch a web session from a Secret on the mobile device and have the credentials auto-populate in the mobile devices default browser.

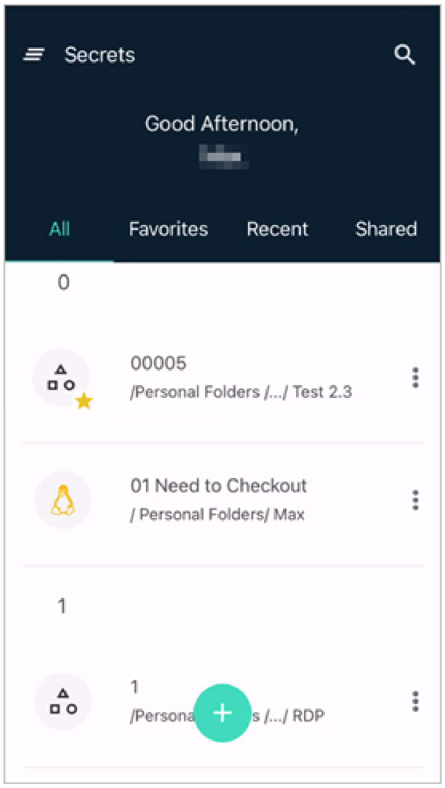
The interface also makes functionality readily accessible, such as multi-factor authentication, biometric authentication, autofill, online and offline caching, and advanced secret workflows.

After the user opens and logs into the mobile application, the Home screen appears.

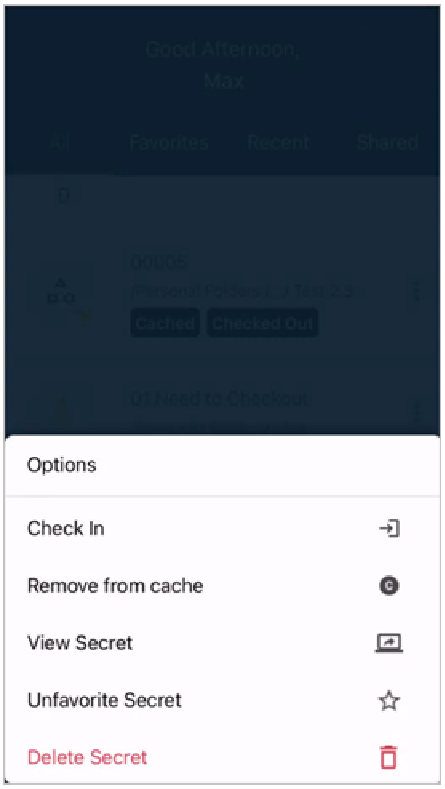
Home Screen

The Home screen offers several options enabling users to view secrets. The Search feature (magnifying glass icon) enables users to search for secrets by name. Four tabs on the Home page enable users to view their secrets four different ways:

- **All**: all secrets the user has view access to
- **Favorites**: secrets the user has designated as "Favorite"
- **Recent**: the 15 secrets accessed most recently by the user
- **Shared**: secrets shared between the user and other users

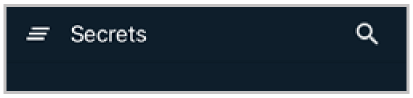


The Home screen displays a prominent Add icon + near the bottom enabling users to quickly add folders and secrets. Secrets and folders on the Home screen and elsewhere display a vertical ellipses ⋮ along one side. Clicking an ellipses opens access to options that are generated dynamically, meaning that the options presented match the actions the user is likely to want to make at that moment. These actions can include view, delete, edit, cache, refresh cache, remove from cache, check in or check out, favorite or unfavorite, request access. etc.

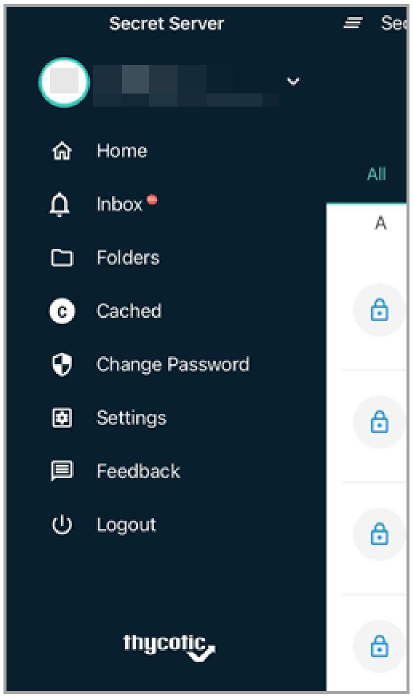


Side Navigation

In the top left corner of the Home screen is an icon composed of three horizontal lines stacked atop one another, sometimes in a straight stack and sometimes slightly askew. This icon is popularly known as a "hamburger." ☰ ☰



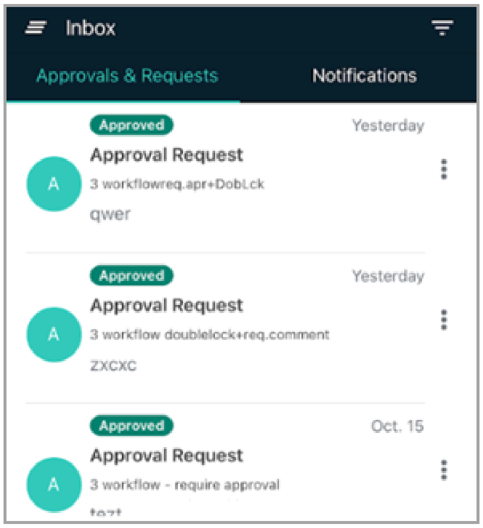
Clicking the hamburger icon opens up a side navigation panel with clickable components including options for Home, Inbox, Folders, Cached, Change Password, Settings, Feedback, and Logout.



Home takes the user directly back to the Home screen.

Inbox serves as a central repository for all notifications and all inbound and outbound access requests. Without opening the Inbox, the user can see the number of unopened messages waiting displayed in a red circle icon next to the inbox label.

When a user clicks the Inbox to open it, two tabs appear. The left-hand tab labeled "Approvals and Requests" displays all access requests the user has sent and all access requests from others that the user can approve. All unread requests are marked with a red circle icon. The user can also manually mark requests as read or unread.

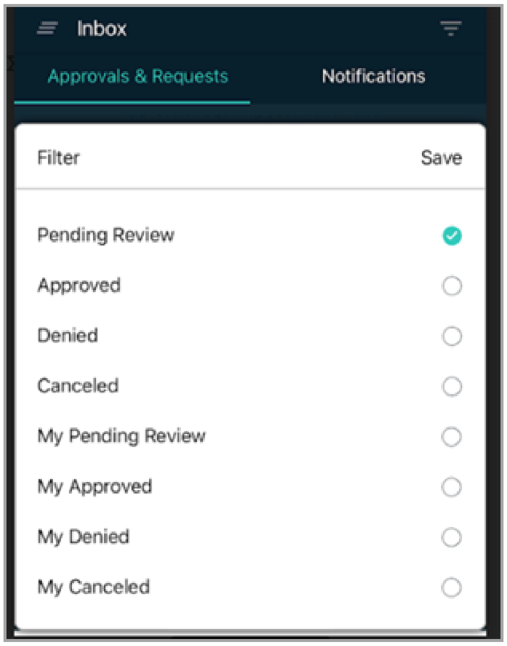


Approved
Yesterday
Approval Request
3 workflowreq.apr+DobLck
qwer

Approved
Yesterday
Approval Request
3 workflow doublelock+req.comment
ZXCXC

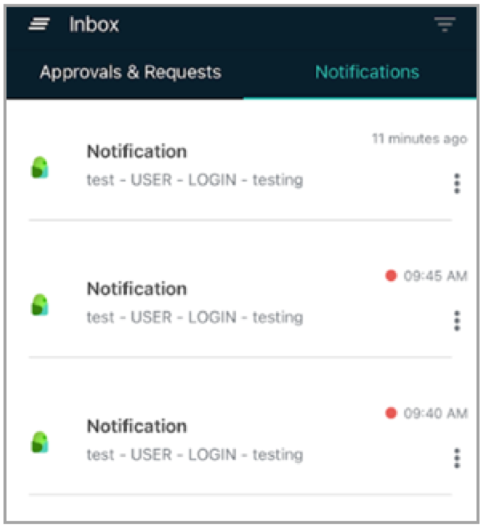
Approved
Oct. 15
Approval Request
3 workflow - require approval
tezt

The user can click the filter icon to filter the requests by state (approved, denied, canceled, or pending review) to see only the types of requests they are interested in. Filters include Pending Review, My Pending Review, Approved, My Approved, Denied, My Denied, Canceled, and My Canceled.



- Pending Review ✓
- Approved ○
- Denied ○
- Canceled ○
- My Pending Review ○
- My Approved ○
- My Denied ○
- My Canceled ○

The right-hand tab labeled **Notifications** displays notifications for events you are subscribed to receive. Unread notifications are indicated by a small red circle. The user can also manually mark requests as read or unread.

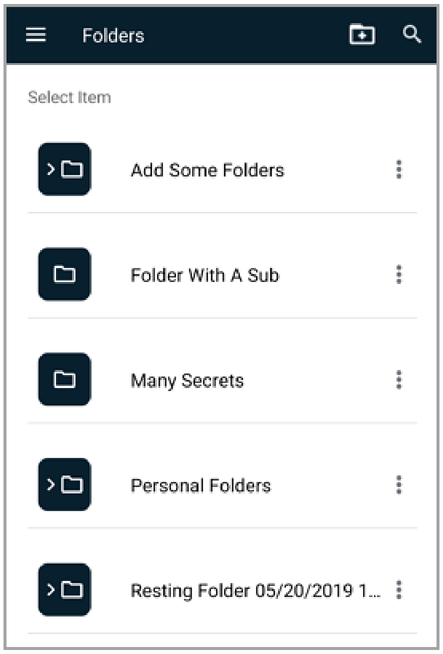


Notification — 11 minutes ago
test - USER - LOGIN - testing

Notification — ● 09:45 AM
test - USER - LOGIN - testing

Notification — ● 09:40 AM
test - USER - LOGIN - testing

Folders displays the tree full structure of the user's folders and secrets.



Folders

Select Item

Add Some Folders

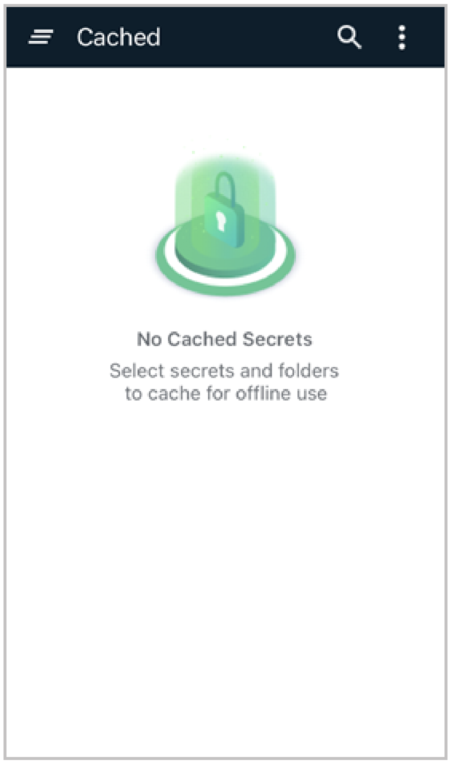
Folder With A Sub

Many Secrets

Personal Folders

Resting Folder 05/20/2019 1...

Cached displays any folders and secrets the user has designated to be cached for offline use.

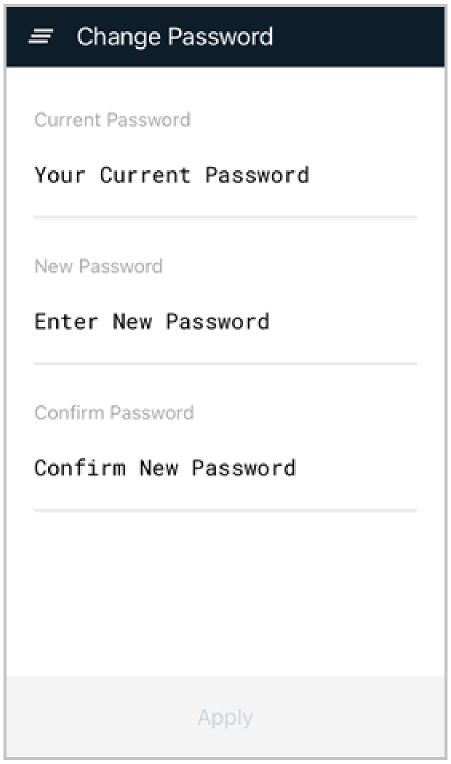


Cached

No Cached Secrets

Select secrets and folders to cache for offline use

Change Password displays standard options for confirming your current password and quickly changing to a new one.



Current Password

Your Current Password

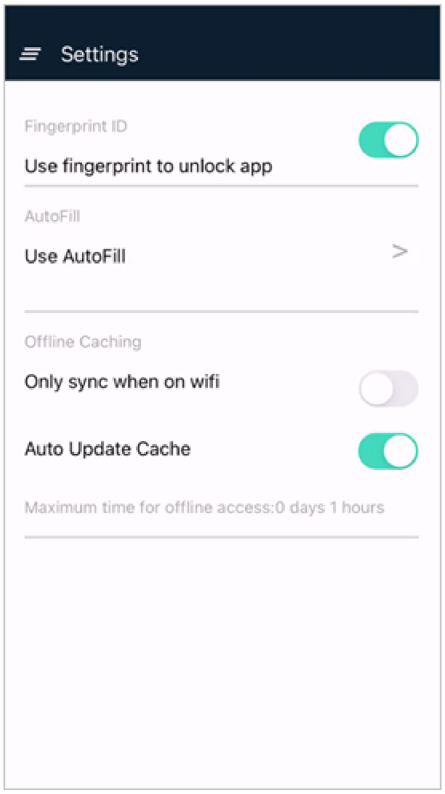
New Password

Enter New Password

Confirm Password

Confirm New Password

Settings displays options for the user to activate or deactivate functions like biometric authentication, autofill, only synching when on wifi, and automatically updating the cache.



Fingerprint ID

Use fingerprint to unlock app

AutoFill

Use AutoFill

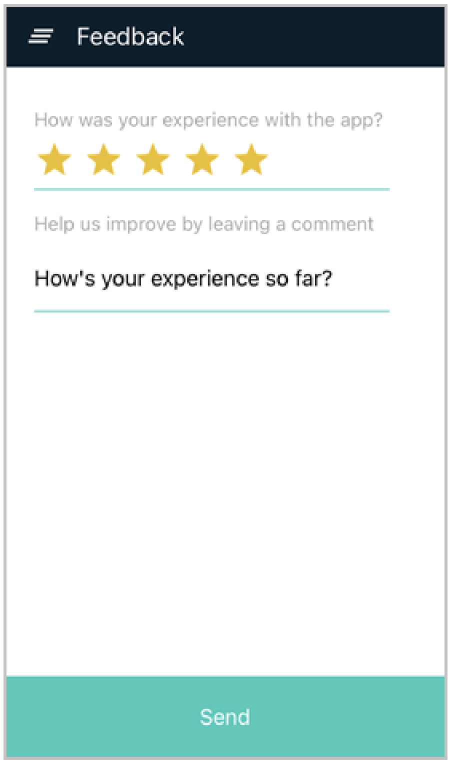
Offline Caching

Only sync when on wifi

Auto Update Cache

Maximum time for offline access:0 days 1 hours

Feedback allows users to provide a review of their experience with the Secret Server Mobile application.


Feedback

How was your experience with the app?

★ ★ ★ ★ ★

Help us improve by leaving a comment

How's your experience so far?

Logout immediately logs the user out when it is clicked, and shows the login screen.

Login Methods

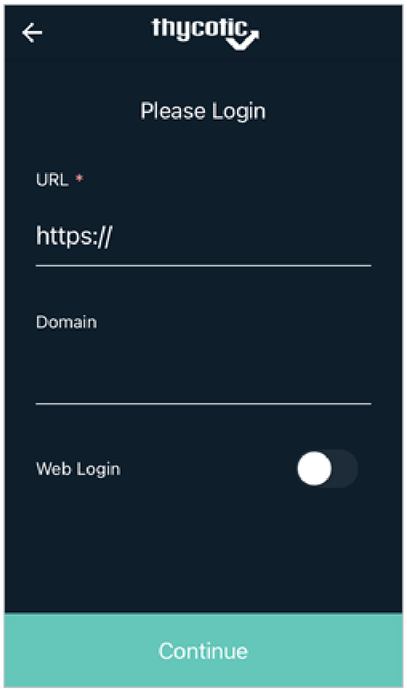
After you download and install Secret Server Mobile, you must launch (open) the application on your mobile device and log in.

Using Standard Login

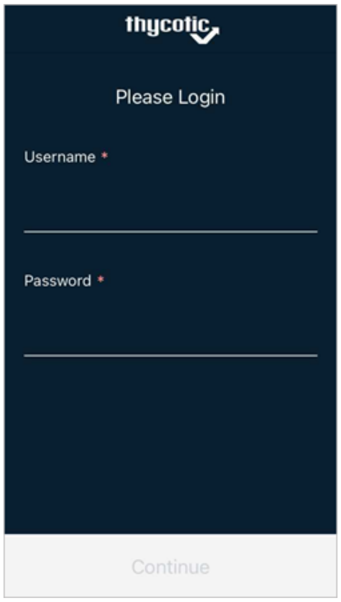
1. Open the mobile application on your mobile device. The first Please Login screen appears.
2. In the URL field, enter the URL to connect to Secret Server. For example:

   `https://websitename.domain.com` or `https://websitename.domain.com/secretserver`
3. In the Domain field, enter the domain name.

   If you are using your active directory (AD) credentials then you must enter the fully-qualified domain name (FQDN). If you are using a local Secret Server account, you can leave the Domain field empty.



4. Click **Continue** to open the second **Please Login** screen.

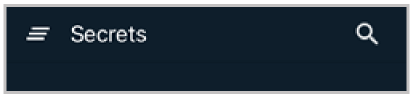


5. Enter your **Username** and **Password**.
6. Click **Continue**.

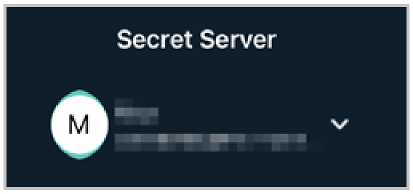
Switching User Login

The mobile application supports switching the user.

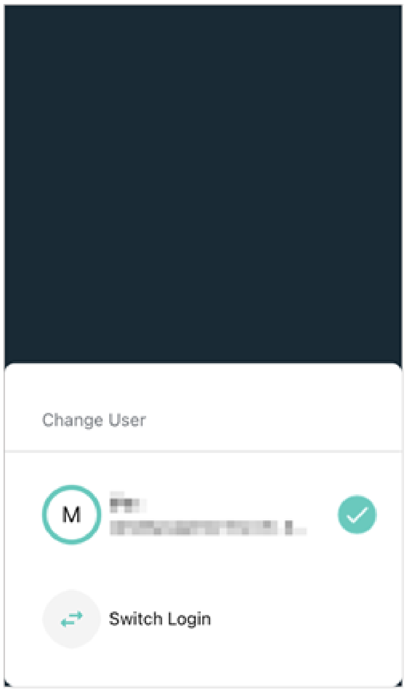
1. Select the Hamburger menu on the top left.



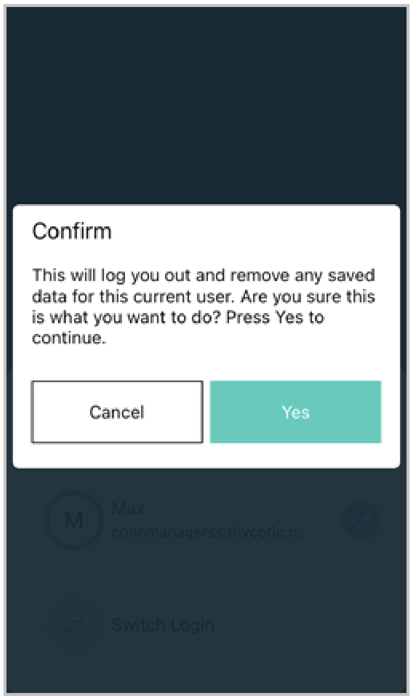
2. Click the currently logged in user.



3. On the **Change User** page, select **Switch Login**.



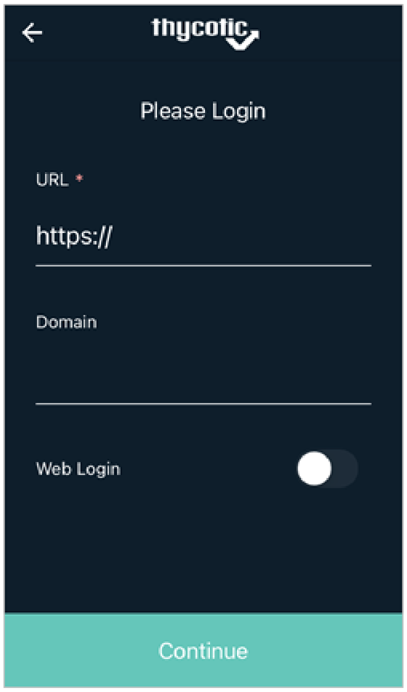
A prompt appears with information about switching users.



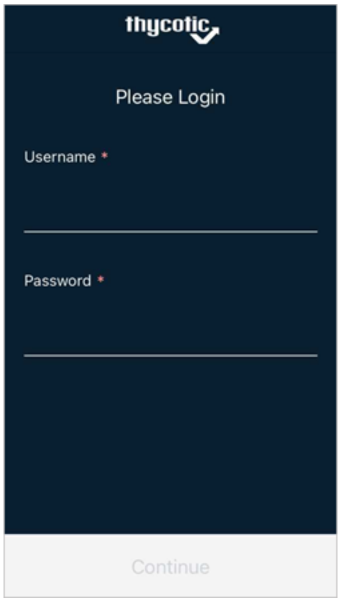
Confirm

This will log you out and remove any saved data for this current user. Are you sure this is what you want to do? Press Yes to continue.

4. Click **Yes**.
5. On the first **Please Login** screen, enter your **URL** and **Domain**. In some cases you will use the same URL and Domain you used for this first user.



6. Click **Continue** to open the second **Please Login** screen.

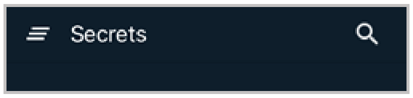


7. Enter your **Username** and **Password**.
8. Click **Continue**.
9. Enter your two-factor information if you have that feature enabled. Once logged in, you will see the Secrets list.

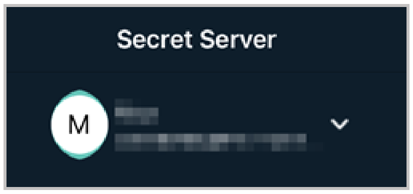
Switching Login Method

With Web Login enabled in the Secret Server Mobile app, the user can switch between standard and web login at any time. For example if your are logged in using the standard login method, you can switch to the web login method using the following procedure.

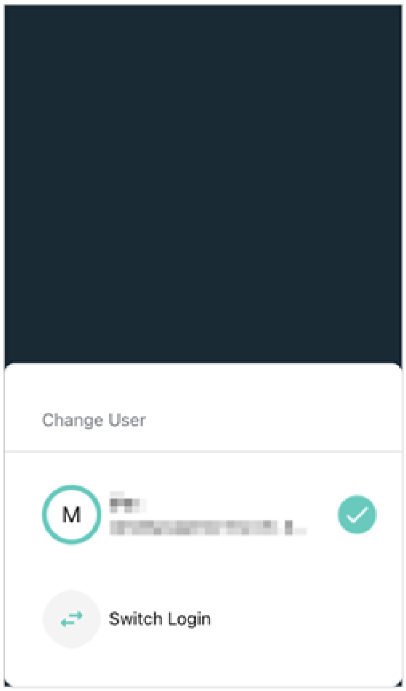
1. Select the Hamburger menu on the top left.



2. Click the currently logged in user.



3. On the **Change User** page, select **Switch Login**.

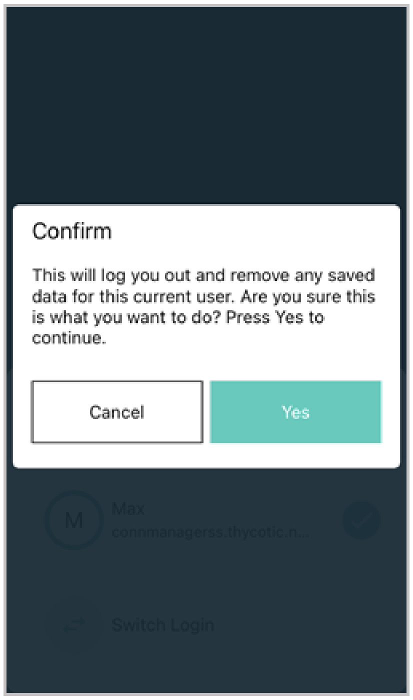


Change User

M [redacted]

Switch Login

A prompt appears with information about switching login methods.



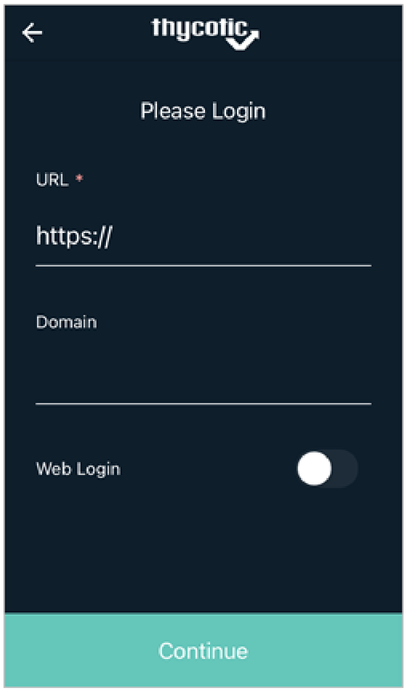
Confirm

This will log you out and remove any saved data for this current user. Are you sure this is what you want to do? Press Yes to continue.

4. Click **Yes**.
5. On the first **Please Login** screen, enter your **URL** and **Domain**
6. Click the switch next to **Web Login** to switch to the web login method.

7. Click **Continue**.

   Note: If you receive a message indicating that the HTTPS certificate for the Secret Server URL cannot be validated and you know the reason why (for example if you are working in a proof-of-concept environment with no external internet connection) you can bypass the message and proceed to connect anyway with an internal, self-signed, or enterprise certificate installed on your mobile device. Secret Server Mobile will remember your choice to bypass the warning so you won't need to manually bypass it each time. This capability is available for regular and web login methods on Android and iOS devices.



Please Login

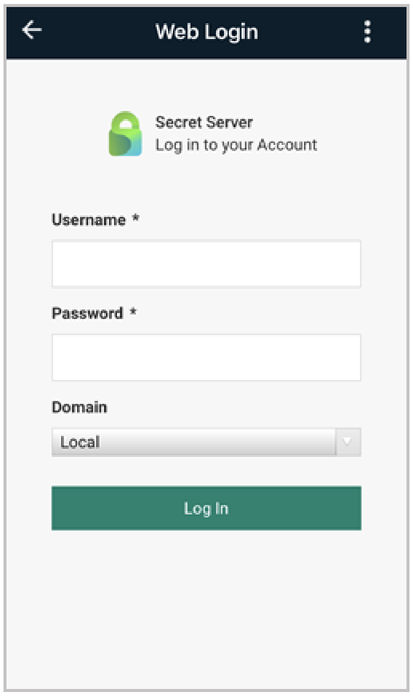
URL *

https://

Domain

Web Login

The **Web Login** page opens



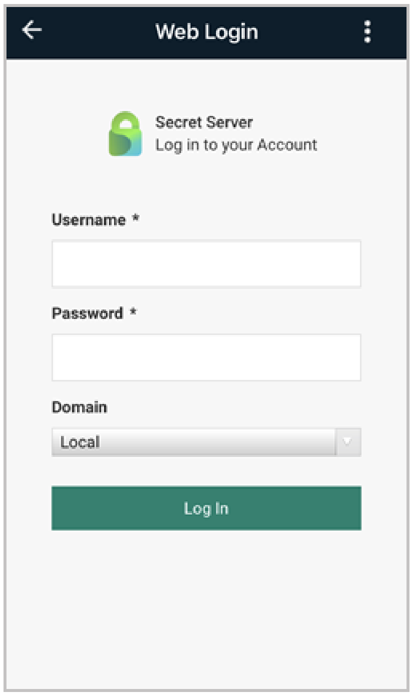
8. Enter your **Username** and **Password**.
9. Enter your **Domain** as appropriate.
10. Click **Log In**.

Refreshing Web Login

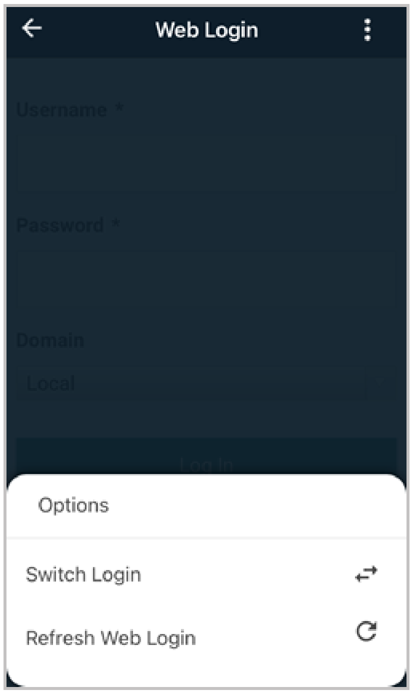
With the Web Login enabled in the Secret Server Mobile app, the user can manually refresh the SAML token.

Using the Application

1. On the Web Login page, click the **ellipsis** in the top right corner



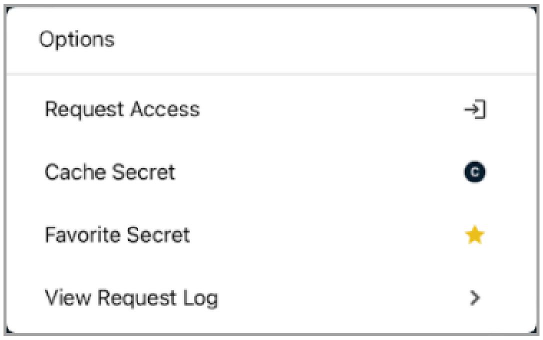
2. Under **Options**, select **Refresh Web Login**.



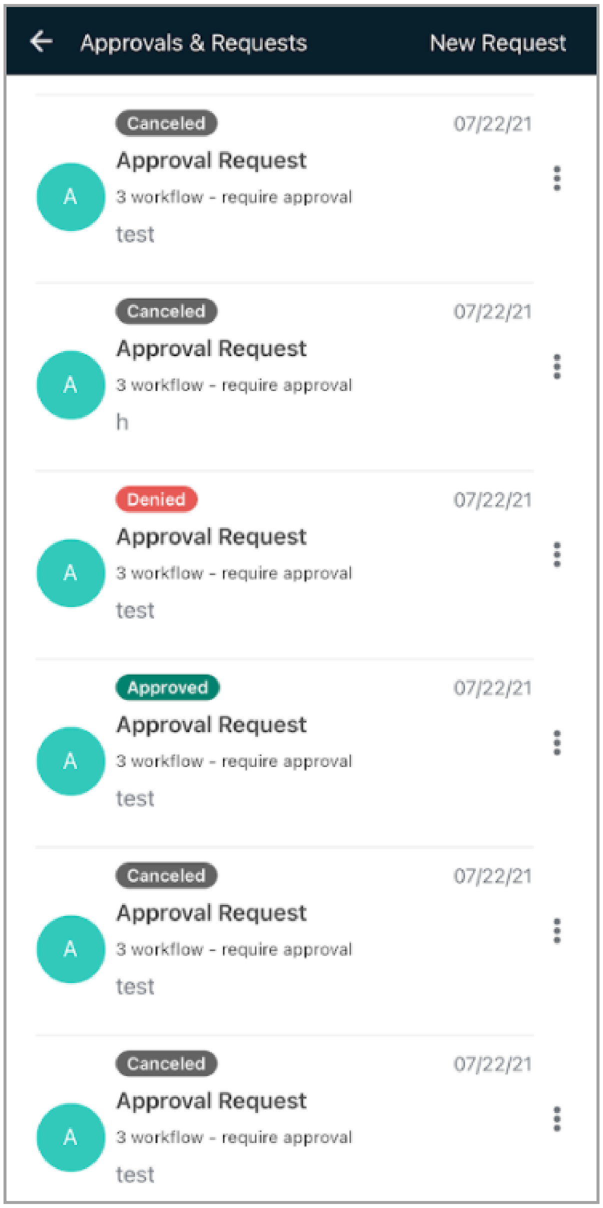
You will see a quick page flash when the app generates a new token.

Managing Multiple Access Requests

From any secret protected by a request access security workflow, users can click the secret's context menu (the three vertical dots on the right side) ⋮ to select options that include **Request Access** and **View Request Log**.



From the Approvals & Request Log, the user can view basic information at a glance about each access request, including the date it was initiated and its state (Pending Review, Canceled, Denied, or Approved). The user can also initiate a new request from the Request Log by clicking **New Request** at the top right.



Canceled 07/22/21
Approval Request
3 workflow - require approval
test

Canceled 07/22/21
Approval Request
3 workflow - require approval
h

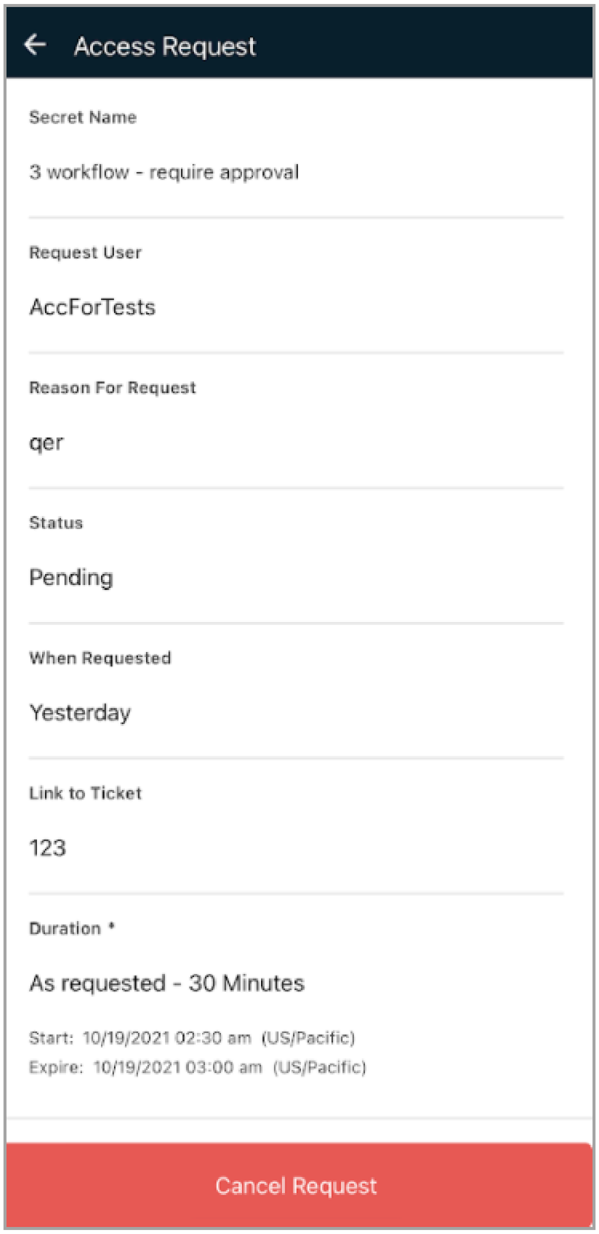
Denied 07/22/21
Approval Request
3 workflow - require approval
test

Approved 07/22/21
Approval Request
3 workflow - require approval
test

Canceled 07/22/21
Approval Request
3 workflow - require approval
test

Canceled 07/22/21
Approval Request
3 workflow - require approval
test

To see more detailed information on a request, the user can click the request or click the context menu on the right side. Details include the secret name, a link to the related ticket, the name of the person requesting access, the reason the request was made, the time the request was made, the length of time for which the user requested access, and the begin and end times of the requested access period. If the user has made two requests for different time slots, such as Saturday from 9:00 a.m. to 11:00 a.m. and Sunday from 2:00 p.m. to 4:00 p.m, both time slot requests will be shown. The request in the screen shot below is from the user viewing the screen, so the screen also displays an option at the bottom to cancel the request.



Secret Name

3 workflow - require approval

Request User

AccForTests

Reason For Request

qer

Status

Pending

When Requested

Yesterday

Link to Ticket

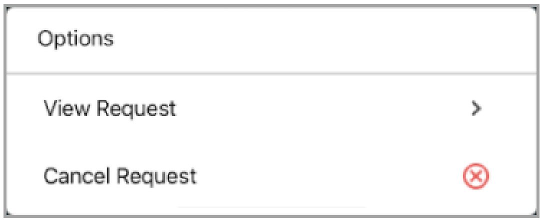
123

Duration *

As requested - 30 Minutes

Start: 10/19/2021 02:30 am (US/Pacific)
Expire: 10/19/2021 03:00 am (US/Pacific)

The user can also cancel the request from the context menu as shown below:



Offline Caching

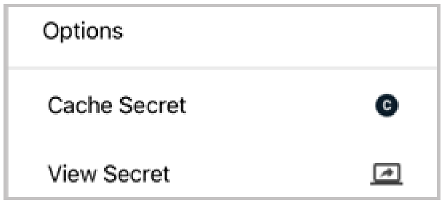
Mobile devices and applications can lose internet connectivity for a number of reasons. When Secret Server Mobile loses internet connectivity, users cannot access their secrets directly from Secret Server. But an organization can permit its Secret Server Mobile users to save secrets and secret folders to an offline cache. Offline caching stores secrets, secret folders, and all of their associated data to a password-protected, encrypted data file. When a network connection to Secret Server is unavailable, users can access secrets and folders cached offline for a maximum Time-To-Live (TTL) period. TTL and access to offline caching are controlled by an organization’s Secret Server administrator globally, for all mobile devices in the organization. If an organization does not allow offline caching, the administrator sets the TTL to zero.

Accessing secrets saved to an offline cache requires using biometric face or fingerprint recognition. The offline cache is automatically updated by default, but a user can turn off the auto-update feature. The offline cache is automatically cleared when the user logs out of the application or switches to another user identity.

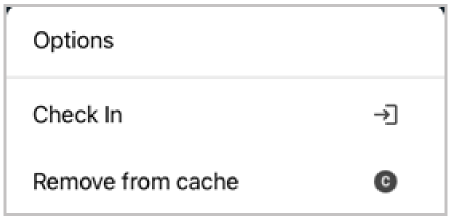
Add and Remove a Secret for Offline Caching

To add and remove a secret for offline caching, follow the procedure below:

1. Connect to Secret Server.
2. Select the secret and click the ellipsis on the side.
3. Click **Cache Secret**.



4. To remove the secret from offline cache, select the secret, click the ellipsis on the side, and click **Remove from cache**.

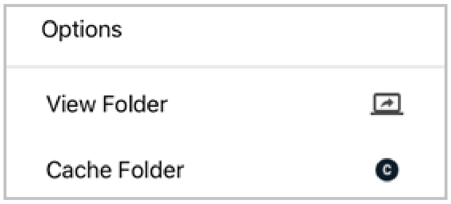


Add, Refresh, and Remove a Folder for Offline Caching

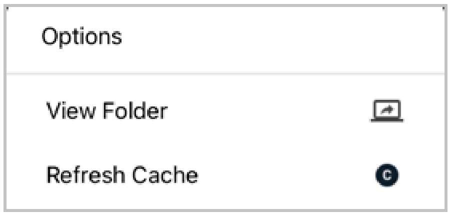
To add, refresh, and remove a secret folder for offline caching, follow the procedure below:

1. Connect to Secret Server.
2. Select the secret folder and click the ellipsis on the side.

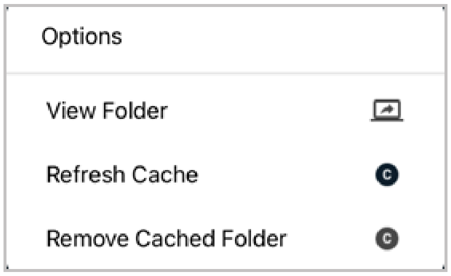
3. Select the **Cache Folder** option. When you cache a folder, the secrets in the folder are cached, but secrets in subfolders are not cached.



When you add a secret to a cached folder, you need to refresh the folder by clicking the ellipsis and clicking **Refresh Cache**.

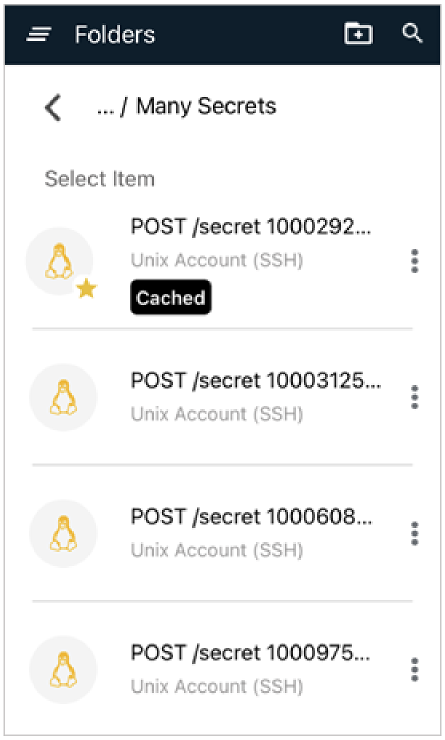


4. To remove a folder and all secrets inside it from the offline cache, select the folder and click the ellipsis on the side, then click **Remove Cached Folder**.



Identify Cached Secrets

When you have secrets saved to offline cache, they are marked with a "Cached" tag for easy identification.



Folders

... / Many Secrets

Select Item

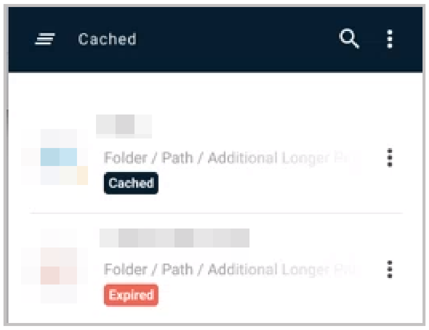
POST /secret 1000292...
Unix Account (SSH)
Cached

POST /secret 10003125...
Unix Account (SSH)

POST /secret 1000608...
Unix Account (SSH)

POST /secret 1000975...
Unix Account (SSH)

Cached secrets whose time has expired are marked with an "Expired" tag.



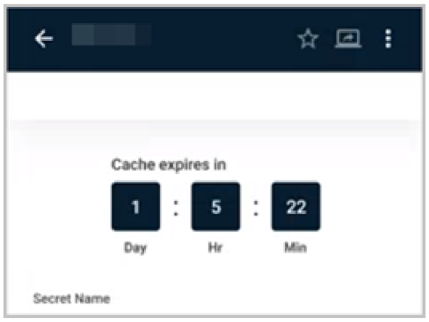
Cached

Folder / Path / Additional Longer Pa
Cached

Folder / Path / Additional Longer Pa
Expired

See How Much Time Remains for Accessing Secrets in the Offline Cache

When you open a secret, the time remaining until expiration is shown at the top of the screen. The default background is black.

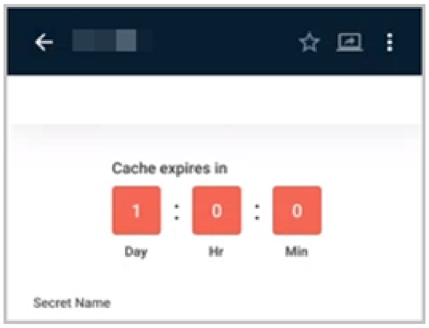


Cache expires in

1 : 5 : 22
Day Hr Min

Secret Name

When the secret has just 24 hours or less until expiration, the background changes to red for easy identification.



Troubleshooting

If you are unable to connect a client application or mobile device to your Secret Server instance please check the following:

If the Desktop Client is not starting or you are receiving a Login Failed error with your correct credentials you may need to uninstall and re-install Java.

For example:

- `https://secretserver/ss/Login.aspx` the URL to use is `https://secretserver/ss`
- `https://secretserver/Login.aspx` the URL to use is `https://secretserver/`
- `http://ss.myserver1.com/Login.aspx` the URL to use is `http://ss.myserver1.com/`

1. Are webservices enabled? Go to **Administration > Configuration** and ensure that "Enable Webservices" is set to "Yes".
2. Can you browse to Secret Server from the mobile device? If you are unable to browse to the Secret Server site using your mobile web browser, then that means that Secret Server is unreachable from your device. Ensure that you are on the wireless intranet, or that the Secret Server site is available from outside your internal network.
3. Check the URL you are using on the client application or mobile device - it should the URL of the Login.aspx without login.aspx
4. Are you using SSL? If so, is your certificate trusted? Check with your IIS administrator to get a valid certificate.
5. Are you working in an environment without access to the external Internet? If so you will receive a message indicating that the HTTPS certificate for the Secret Server URL cannot be validated. Since you know the message appears because you cannot access the Internet, you can bypass the message and proceed to connect anyway with an internal, self-signed, or enterprise certificate installed on your mobile device. This capability is available for regular and web login methods on Android and iOS devices.
6. A "you don't have permissions" message is usually due to workflows on the secret.

Release Notes

Secret Server Mobile Version Compatibility with Secret Server

Your Secret Server Mobile version is compatible with any Secret Server version released within the 12 months preceding the Secret Server Mobile release.

Changelog

This changelog is a chronological list of documentation changes to help track additions, deletions, and content edits other than spelling and grammar corrections.

Secret Server Mobile Version Compatibility with Secret Server

Your Secret Server Mobile version is compatible with any Secret Server version released within the 12 months preceding the Secret Server Mobile release.

February 2024

- 1.8.3 Release Notes, refer to "1.8.3 Release Notes " on the next page for details

December 2023

- 1.8.2 Release Notes, refer to "1.8.2 Release Notes" on the next page for details

August 29, 2023

- 1.8.1 Release Notes, refer to "1.8.1 Release Notes" on page 38 for details

February 22, 2022

- 1.8.0 Release Updates, refer to 1.8.0 Release Notes for details.

November 9, 2021

- 1.7.0 Release Updates, refer to 1.7.0 Release Notes for details.

August 10, 2021

- 1.6.1 Release Updates, refer to 1.6.1 Release Notes for details.

July 6, 2021

- 1.6.0 Release Updates, refer to 1.6.0 Release Notes for details.

March 16, 2021

- 1.5.0 Release Updates, refer to 1.5.0 Release Notes for details.

March 2, 2021

- 1.4.0 Release Updates, refer to 1.4.0 Release Notes for details.

November 2020

- 1.3.0 Release Updates, refer to 1.3.0 Release Notes for details.

October 2020

- 1.0.1 Release Updates, refer to 1.0.1 Release Notes for details.

September 2020

- 1.0.0 Release Notes, refer to 1.0.0 Release Notes - Initial Release for details.

1.8.5 Release Notes

Release Date: July 24th, 2024

Product Enhancements

- [[[Undefined variable global-vars.SecretServerMoble]]] upgraded to the latest target Android version.

Bug Fixes

- Fixed a bug where the app was showing offline mode after switching users.

1.8.4 Release Notes

Release Date: May 20th, 2024

Product Enhancements

- Resolved a bug that prevented the inbox from loading properly on iOS 17.4 devices.

1.8.3 Release Notes

February 13th, 2024

- Fixed a bug that prevented users without administrator permissions from caching secrets.
- Fixed a bug that allowed users to continue to cache secrets after having the "Access offline secrets on Mobile" permission removed.

1.8.2 Release Notes

Release Date: December 20th, 2023

Product Enhancements

- Thycotic [[[Undefined variable global-vars.SecretServerMoble]]] is now Delinea [[[Undefined variable global-vars.SecretServerMoble]]]. This release delivers a new icon and Delinea branding.

1.8.1 Release Notes

Release Date: August 29th, 2023

Bug Fixes

- Fixed an issue where Secret Server Mobile would display an "Invalid Response from Server" error when attempting to access a secret through a Secret Server Cloud tenant.

1.8.0 Release Notes

Release Date: February 22, 2022

Product Enhancements

- Made several performance updates to improve application performance and system response time.

Bug Fixes

- Fixed an issue accessing secrets in environments with a large or deep folder hierarchy.

Known Issues

- There is an issue with the unread notifications counter in Secret Server versions 11.1.000007 and above. Secret Server no longer displays the number of unread notifications in your Inbox.

  However, if you have Secret Sever versions 11.0.000008 and prior you will continue to see the notification counter.

iOS Specific

- The Notes label may be displayed in the local language if the system language is not English.

Android Specific

- When trying to type a comment in the Feedback section, the Send button may not appear.

1.7.0 Release Notes

Release Date: November 2, 2021

Product Enhancements

- A new Inbox serves as a central location for all notifications and all inbound and outbound access requests.
- Users can create a new access request directly from the navigation panel or from the secret's context menu.
- Users can update or cancel any pending access request for a secret from the requests log.
- Users can send several access requests for a secret, see a list of access requests for a secret, and see details of an access request.
- Users can now search for secret templates in addition to secrets.
- The Notes field for secrets now expands to accommodate multiple lines.
- Users who cannot access the internet for third-party certificate validation can now log into Secret Server using an internal, self-signed, or enterprise certificate installed on the user's device.

Known Issues

iOS Specific

When users try sending feedback about the application, the HTML tag <br/>, appears in the default iOS mail client. This issue can be resolved by simply upgrading to iOS version 15 and higher.

1.6.1 Release Notes

Release Date: August 10, 2021

Bug Fixes

- Fixed an issue where the secret list was getting duplicated in some instances after checkout/check-in.
- Fixed an issue where on some devices, the mobile app failed to get credentials from the secret during autofill.

1.6.0 Release Notes

Release Date: July 6, 2021

Feature Updates and Enhancements

- An organization can permit its Secret Server Mobile ("mobile app") users to save secrets and secret folders to an offline cache. When a network connection to Secret Server is unavailable, users can access secrets cached offline for a specified Time-To-Live (TTL) period. TTL and access to offline caching are controlled by an organization’s Secret Server administrator globally, for all mobile devices in the organization. Accessing secrets saved to an offline cache requires using biometric face or fingerprint recognition. If an organization does not allow offline caching, the administrator sets the TTL to zero. More information on offline caching is available in the publications set.
- Secret Server Mobile now permits Android users to log into Secret Server using a self-signed or internal certificate that cannot be validated by a third party or CA. Because this process bypasses CRL checking it is appropriate only for Proofs of Concept and other closed environments. It is not appropriate for production environments or other environments exposed to incoming internet traffic. The mobile app displays a warning

that the certificate cannot be validated with any CRL servers and that bypassing the CRL check may be harmful. The user can connect to Secret Server only if they acknowledge that they have read the warning and that they choose to proceed anyway at their own risk. The option to bypass CRL checking is not available on iOS devices.

Bug Fixes

- Radius authentication issues in the mobile app have been resolved in the current release.
- A user accessing a secret protected by the workflow, "Viewing Password Requires Edit," can now auto-fill their credentials without error, using a launcher or using web login credential fields that display the Delinea logo. The mobile application still bars users from viewing the password and from copying or pasting it using the clipboard function.

Known Issues

The mobile app does not support the following secret templates, and using them in SSM will result in errors:

- Google IAM Service Account
- Unix Account SSH Key Rotation - No Password

1.5.0 Release Notes

April 9, 2021

iOS Hotfix

Secret Server Mobile 1.5.0 is a hotfix release to support devices running the iOS update 14.4.1 and compatibility with the latest Secret Server release. For details about the features and functionality provided, see the 1.4.0 release notes.

Android Maintenance Release

Secret Server Mobile 1.5.0 is a maintenance release for Android to ensure compatibility with the latest Secret Server release. For details about the features and functionality provided, see the 1.4.0 release notes.

1.4.0 Release Notes

March 2, 2021

Features

Secret Server Mobile 1.4 provides users with the following enhanced capabilities, including workflows for the following actions:

- check in and check out Secrets
- provide a **Double Lock** password to access a Secret
- provide a **Comment** required to access a Secret
- provide a ticket Number required to access a Secret

- provide a Reason required to access a Secret
- receive a notification when you have requested access to a Secret twice in a row
- see a visual indication of each Secret you have checked out from both Secret Server Mobile and the Secret Server web interface
- see a visual indication when you request access to a Secret that is already checked out by another user
- set the beginning and end dates and times for checking out a Secret
- cancel requests for access to Secrets at any stage of the request process

User Interface Improvements

- Changed the password font to clearly distinguish between adjoining letters lowercase “l” (L) and uppercase “I” (I).

Bugs Fixed

- If your attempt to log into Secret Server fails, you now receive a message with the reason for the failure, such as incorrect username/password, failed 2FA/MFA input, no internet connectivity, incorrect Secret Server URL, 500 error from Secret Server, or no permissions/access to use the REST APIs.
- When you request access to the same Secret twice in a row, Secret Server Mobile now notifies you that you have already requested access to that Secret.
- In the **Title bar**, Secret names are no longer truncated when there is sufficient room to display them.
- When Secret Server Mobile cannot use **FaceID**, it now displays an appropriate notification.
- After a screen is minimized or maximized, the screen now retains all the information you already entered.
- After a screen is minimized or maximized, the keyboard is no longer displayed on the **Fingerprint ID** screen
- When a user cancels out of the **Fingerprint ID login** or the attempt has failed, the notification screen that appears no longer displays a keyboard.
- When a user cancels out of the **Fingerprint ID Login** and opens the **Password Login**, Secret Server Mobile no longer crashes.
- After Secret Server Mobile displays a **Face Not Recognized** message and the user taps **Enter Password**, the keyboard is now displayed.
- When API errors occur, Secret Server Mobile now displays relevant notifications.
- After a user deletes a Secret, Secret Server Mobile now displays a notification that the deletion was successful.
- When a site certificate is not valid, Secret Server Mobile now displays an appropriate message instead of **URL is not valid**.
- The **Home** screen now opens when expected, whereas in some cases the **Secrets** list screen appeared instead (SAML/Web Login)
- When you enter a correct Double Lock password for a Secret or Secrets, the Double Lock password is cached so you do not need to manually re-enter it for the remainder of the session. If the session expires, you will need to re-enter the Double Lock password.

Known Issues

- In some situations, when a user on an iOS device attempts to connect to a Secret Server Cloud using SAML (Web Login), the authentication token does not seem to successfully get back to the mobile app, resulting in a gray screen with a spinner icon.
- On iOS devices, a Toaster message at the top of the Secret Server Mobile **Home** screen overlaps the phone's system indicators such as the time and carrier.
- Users attempting to connect to an on-premises Secret Server configured with a Self-Signed/Internal certificate receive the message, **Unable to connect due to a self-signed or untrusted certificate**.
- When a user is creating a Secret using the template **Generic Discovery Credentials** and taps to enter a **Private Key Passphrase**, the input field should display **Enter** instead of **Current Password**, and the button label should read, **Generate** instead of **Generate Password**. It will generate a strong password.
- When Secret Server Mobile is auto-filling a password from a Secret that requires edit privileges to view it, the password field is filled with, **Not Valid for Display** instead of the actual password.
- Secret Server Mobile does not currently support deployment via MDM solutions (VMware workspace/AirWatch etc.)
- When a user attempting to access a Secret enters an incorrect alphanumeric value in the **Ticket Number** field, the error message, **Failed to send access request** appears.
- Secrets checked out by the current user via Autofill are not marked as **Checked Out** on the main screen. Likewise, Secrets marked as **Checked Out** on the main screen are not marked **Checked out** when using Autofill.

1.3.0 Release Notes

November 24th 2020

Features

- SAML Login Support (Web Login)
  - UI Option to use local login or Web Login (SAML)
  - On the login screen user has the option to Switch Login or Refresh Web Login.
  - When logging in via the Web Login (SAML) user does not have to manually click on “generate token” this is done for the user in the background (some users may see the page flash).

User Interface Improvements

- When Clicking on search (magnifying glass) and other options, the keyboard won't be active anymore when no text input is required.
- Moved the Home “+” button to the bottom of the screen.
- **Next** will only be enabled when all required fields are populated.
- **Save** will only be enabled when all required fields, for example the folder name when creating a folder, are populated.

Bugs Fixed

- Removed the invalid **Help** link, when using Auto-fill to fill passwords on an external application.
- Fixed an onboarding issue related to the FaceID/Fingerprint screen when biometrics have not been enabled on the device. Users are presented with a message recommending they enable biometrics for extra security.
- Fixed a defect where Autofill was not working after switching the logged in user to another user.

1.0.1 Release Notes

October 21st, 2020

Enhancements

- Onboarding:
  - Added a **Skip** option to the enable biometric page.
  - Resize toggle switch for using biometric options.
- Autofill service:
  - Improved alert message popup.
  - Updated spinner when loading search screen for autofill.
- Biometrics:
  - Updated default values based on Android/iOS platform for onboarding.
- General User Interface improvements:
  - Updated icons and adjusted alignments.
  - Reduced unnecessary spacing on multiple screens.
  - Modified the location of the **Cancel** button depending on screen size.
  - Modified size/shape of logged in user avatar on Menu screen.
  - Adjusted screen spacing for keyboard pop-up.
  - Added additional validation on **Edit Folder Name** field.

Bugs Fixed

- Fixed an issue where an SSL error is returned upon connecting to Cloud Secret Server instances depending on TLS version.
- Fixed an issue where the confirmation message pop-ups were cut off at the bottom of the dialog on some screens.
- Fixed an issue where the **Apply** button was enabled on the Password Change screen when no user modifications had been made.
- Fixed an issue with Secrets being listed but inaccessible on the All tab upon users switching accounts.

Android Specific

- Fixed an Autofill service issue that didn’t consistently open to **Search** when users were prompted with biometric verification.

iOS Specific

- Fixed an issue on the Secret Details page for the **Favorites** icon filling inconsistently when selected.
- Fixed an issue where the wrong message was displayed on an unsuccessful FaceID scan.

1.0.0 Initial Release

September 1st, 2020:

With this release, Delinea is rolling out the new **Secret Server Mobile Application** for iOS and Android devices.

- For Device Requirements, refer to Prerequisites.
- For steps required in Secret Server, refer to Configure Secret server.
- For the initial mobile setup and onboarding steps, refer to Mobile Setup.
- For a general UI reference, refer to Using the Application.