EXOSTAR

Secure Access Manager Passkey (FIDO2) User Guide

Activating and Using Passkeys and Security Keys

Version: 1.0

Date: 12 November 2026

Applies to: SAM 7.0 and later

1. REVISION HISTORY

Date	Version	Author	Description of Changes
12 November 2026	1.0	S. Torretti	Initial release of the end-user edition. Covers the FIDO2 credential types supported in SAM 7.0, activation of a hardware security key and of a passkey held on a phone, tablet or computer, credential management, signing in and stepping up, what to expect when an application requires FIDO2, troubleshooting, and frequently asked questions.

2. ABOUT THIS GUIDE

This guide explains how to activate and manage a passkey (FIDO2) credential on your Secure Access Manager (SAM) account, what to expect when you sign in or step up with one, and what to do when an application requires a passkey you do not yet hold.

Who this guide is for

This guide is for SAM users who sign in to applications through Secure Access Manager. It covers activating a passkey or a security key on your own account, managing the credentials you hold, and signing in with them. No administrative role is needed for anything described here.

What this guide covers

SAM 7.0 supports two kinds of FIDO2 credential — a shared passkey synced across your devices, and a device-bound hardware security key. Both are activated from the same place in SAM and both are managed the same way. This guide covers:

- The multi-factor credentials SAM supports after 7.0, and the two that are being withdrawn.
- Activating a hardware security key, step by step, with the screens you see.
- Activating a passkey stored on a phone, a tablet or the computer itself.
- Holding, naming, renaming, removing and replacing up to four passkeys on one account.
- Signing in with a passkey, and stepping up with one into an application that requires stronger authentication, including when identity proofing is required first.
- What to expect when an application requires FIDO2, and the "MFA Not Met" indicator shown when you do not yet hold the right credential.

The following are outside the scope of this guide:

- Phone OTP and e-mail OTP enrolment. See the SAM User Guide.
- Identity proofing in detail — the Experian credit questionnaire, the IAL2 workflow and Exostar webcam proofing. This guide states only where proofing sits in the passkey flow.
- Account recovery and recovery e-mail management. See the SAM Account Recovery Guide.
- Platform-wide Exostar FIDO policy and the Exostar Approved FIDO Authenticator List.
- Administrative configuration — the application settings by which FIDO2 is required, and step-up into administrative tabs.

Screens in this guide show SAM 7.0. Minor cosmetic differences from your own screens are possible.

Copyright © 2026 Exostar LLC. All rights reserved.

Conventions used in this guide

Convention	Meaning
Bold text	The exact label of a button, link, or field on the screen.
Passkey (FIDO2)	The collective term for both FIDO2 credential types supported by SAM.
Shared passkey	A FIDO2 credential created on a phone, tablet or computer and synced by a credential manager.
Security key	A device-bound FIDO2 hardware key, such as a YubiKey.
You	The SAM account holder activating or using a credential.

Note: Browser and operating system prompts shown in this guide are rendered by Windows and Chrome, not by SAM. Their wording and layout vary by browser and by operating system, and they may differ from the screens reproduced here.

3. KEY CONCEPTS

Credentials supported after SAM 7.0

SAM 7.0 modernises credential management and changes the set of multi-factor credentials SAM supports. Support for hardware tokens and Mobile ID is ending. After 7.0 the supported credentials are:

- Phone OTP — a one-time passcode sent to a registered mobile number.
- Email OTP — a one-time passcode sent to a registered e-mail address.
- FIDO2 shared passkey — a synced credential created on a phone, tablet or computer.
- FIDO2 security key — a device-bound hardware security key, such as a YubiKey.

FIDO2 is added alongside the existing OTP options, not as a replacement. You continue to sign in with a username and password plus a credential, unless an application you use requires FIDO2.

Why FIDO2 is phishing resistant

A FIDO2 credential is cryptographically bound to the SAM site, so it cannot be replayed against a look-alike site, and there is no shared secret for a user to disclose. At activation the device creates a key pair: the private key stays on the device or security key and never leaves it, and SAM stores only the matching public key.

The credential itself does not change. The same credential is used for every subsequent sign-in; what changes each time is the signed challenge — a fresh, single-use value that cannot be replayed. This is a different mechanism from a one-time passcode, where the code itself changes each time.

The two credential types

	Shared passkey	Security key
Where it lives	On a phone, tablet or computer, held by the device's credential manager and synced across the user's devices.	On the physical key itself. The private key never leaves the key.

Copyright © 2026 Exostar LLC. All rights reserved.

	Shared passkey	Security key
What you need	A device with a credential manager — for example Apple iCloud Keychain, Microsoft or Google.	The hardware key, a USB port, and the PIN set on the key.
How it is confirmed	Fingerprint, face or device PIN.	Key PIN plus a physical tap.
Typical assurance grade shown	UNATTESTED, where the credential manager supplies no attestation data.	FIDO_L2_HW for a certified hardware security key.

Which credential an application accepts

SAM treats a hardware security key as the stronger of the two types, because it is bound to that one device, whereas a shared passkey is synced across your devices. An application can therefore be set to accept either type, or to accept hardware security keys only. The table below shows which credential satisfies each requirement.

What the application requires	Satisfied by a security key	Satisfied by a shared passkey
FIDO2	Yes	Yes
FIDO2 - Passkeys	Yes	Yes
FIDO2 - YubiKeys	Yes	No

Note: Where you have access to applications with different FIDO2 requirements, SAM directs you to activate the highest credential any of those applications requires.

Assurance grades

Each activated credential card displays the credential's assurance grade — for example FIDO_L2_HW for a certified hardware security key, or UNATTESTED for a synced passkey from a mobile credential manager that does not supply attestation data. Exostar revalidates the authenticator on every registration and authentication, checking its identifier, certification level, key protection and attestation against the Exostar Approved FIDO Authenticator List, so a credential type that is later withdrawn stops being accepted.

4. BEFORE YOU BEGIN

What you need

Nothing is sent to you in advance. There is no key to distribute, no code to e-mail and no enrolment package — and therefore nothing that can be intercepted. To activate a credential you need one of the following:

- A hardware security key with a PIN already set on it, and a USB port to plug it into. No phone is required.
- A phone or tablet with a credential manager and a screen lock — fingerprint, face or PIN.
- A computer whose platform supports passkeys, for example Windows Hello on Windows or Touch ID and Face ID on a Mac.

Note: For users in environments where phones are not permitted, the hardware security key route is the recommended option.

Copyright © 2026 Exostar LLC. All rights reserved.

Register more than one credential

A single account can hold up to four passkeys, in any combination of hardware keys and shared passkeys. Register at least two. SAM has no separate recovery flow for a lost passkey — a lost credential is replaced by removing it and registering a new one, so if you hold only one credential and lose it, there is no self-service route back in.

Applications that require identity proofing

Where an application is set to Level 3, you must complete identity proofing before you can configure a credential for it. Proofing is reached from the **Get 2FA** prompt on the home page, from the credential management page, or from the manage 2FA credentials option. In SAM 7.0 this can be the Experian credit questionnaire, the IAL2 workflow where you photograph your driving licence and take a selfie on your phone, or Exostar webcam proofing for international users. Once proofing is complete you return to credential management and activate your passkey as described below.

5. ACTIVATING A PASSKEY

Credential management is reached from My Account, which opens the Activate your security methods page. Where a credential is mandatory, the page shows a required-credential counter.

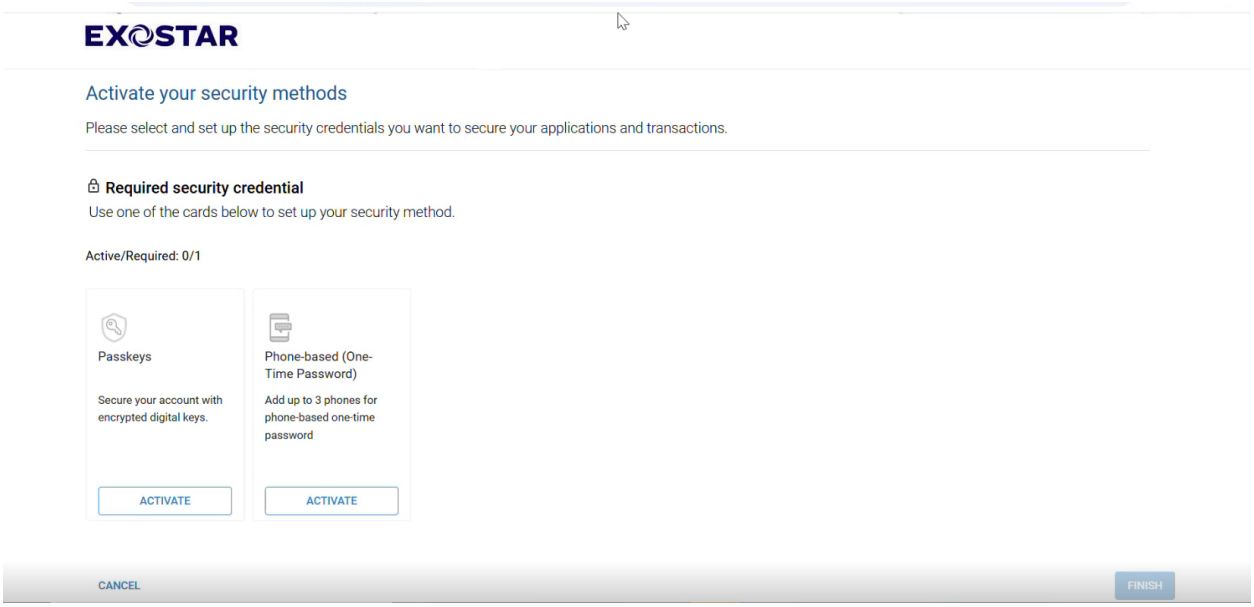


Figure 1. Activate your security methods, with the Passkeys and Phone-based (OTP) cards.

Selecting ACTIVATE on the Passkeys card hands off to the browser. Where the credential is stored is decided at the first browser prompt: continue for a hardware security key (Route A), or select Cancel to choose a phone, tablet or the computer itself (Route B).

Route A — a hardware security key

1. Security key setup. The browser confirms the site the credential is being created for. Continue to proceed.

Copyright © 2026 Exostar LLC. All rights reserved.

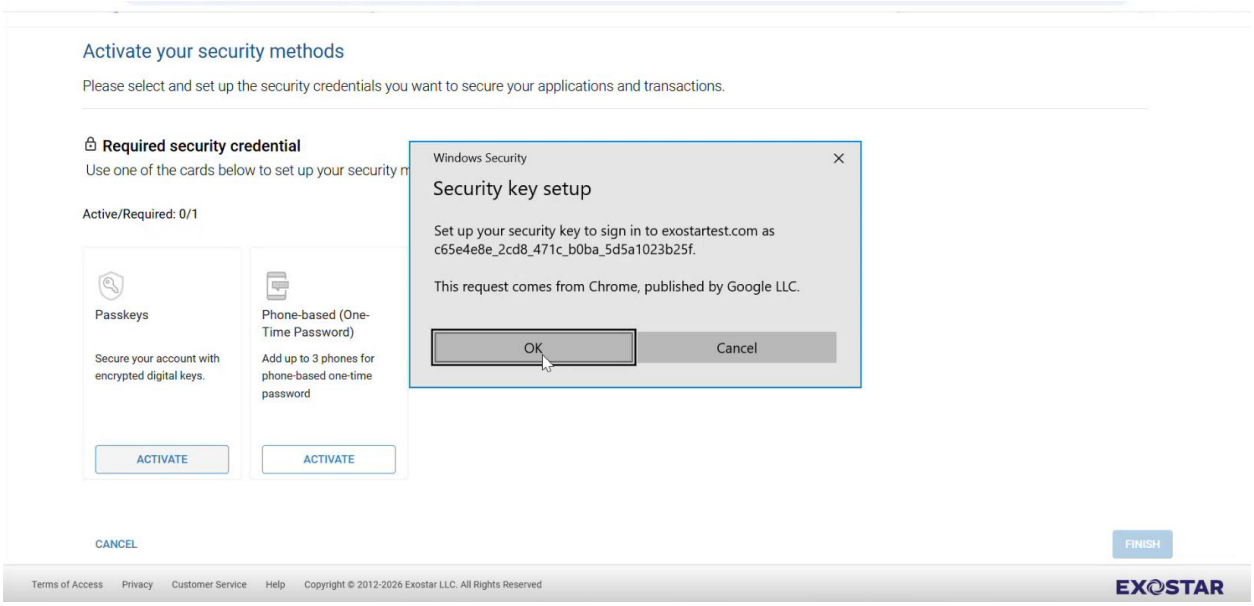


Figure 2. Browser prompt confirming credential creation for the SAM site.

2. Continue setup. Consent to the site seeing the make and model of the key.

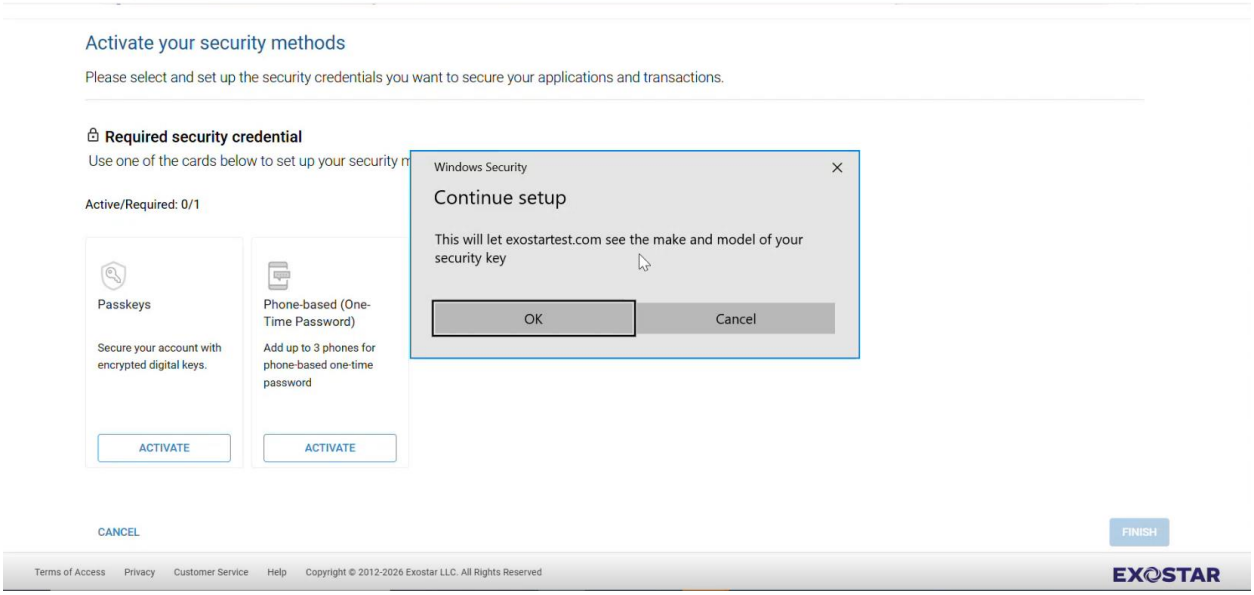


Figure 3. Consent to share the make and model of the security key.

3. Security key PIN. Enter the PIN set on the key.

Copyright © 2026 Exostar LLC. All rights reserved.

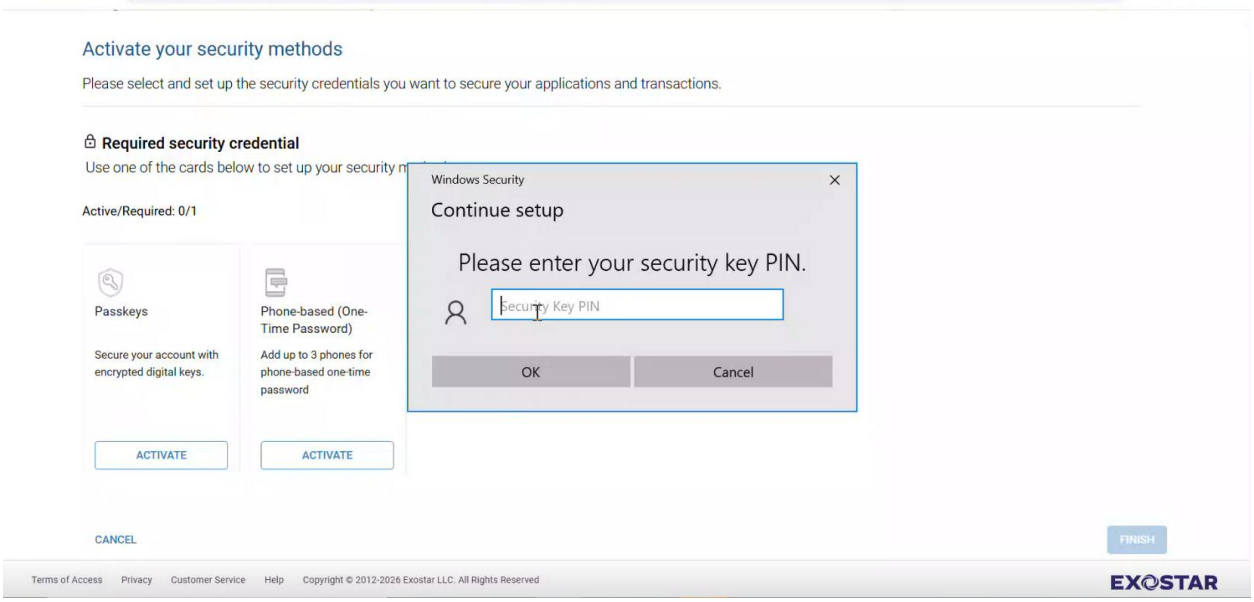


Figure 4. Security key PIN entry.

4. Touch the key. Tap the key to confirm physical presence.

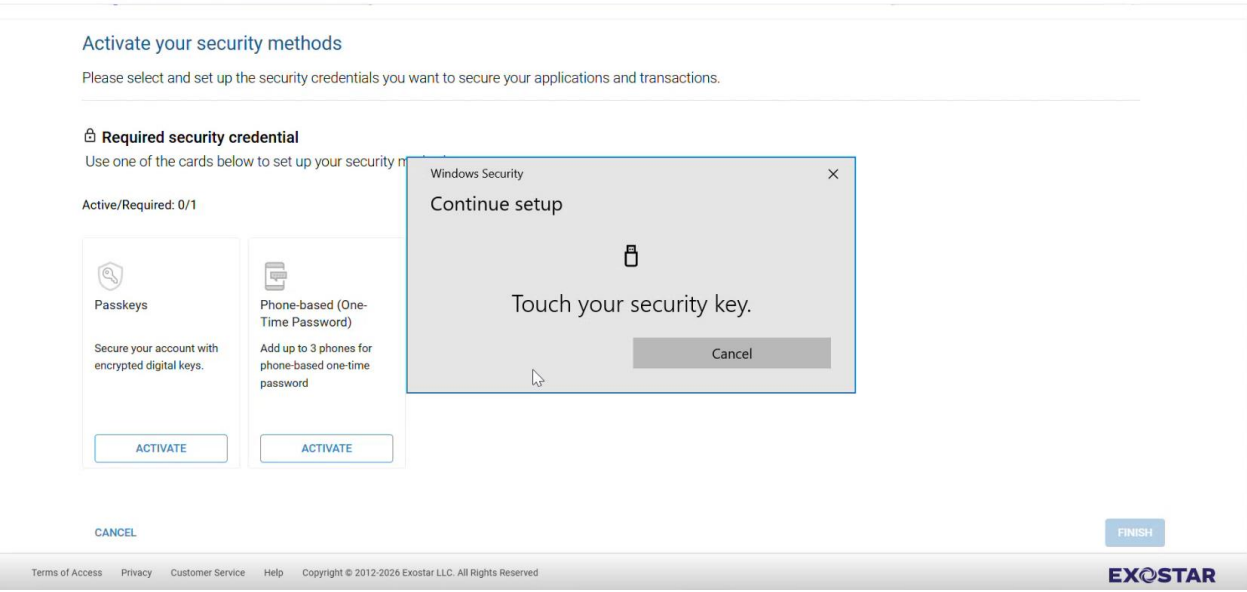


Figure 5. Physical presence check.

5. Add security key. SAM takes over again and asks for a nickname. A name is required.

Copyright © 2026 Exostar LLC. All rights reserved.

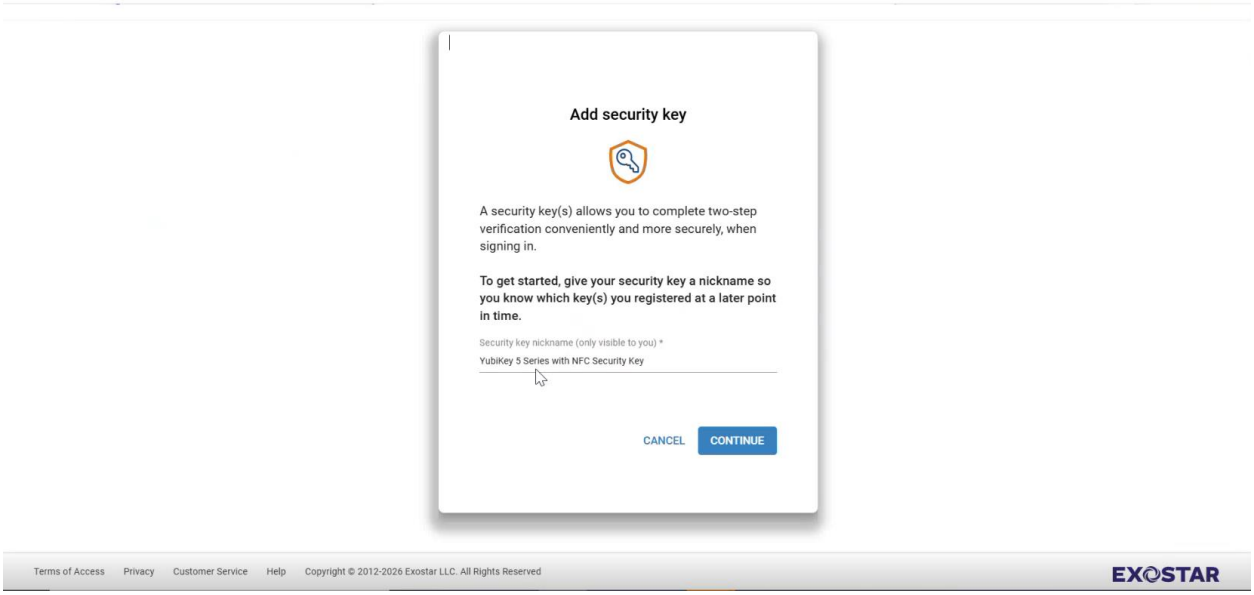


Figure 6. SAM's Add security key screen, where you name the credential.

The card then shows as Active with the nickname and the credential's assurance grade.

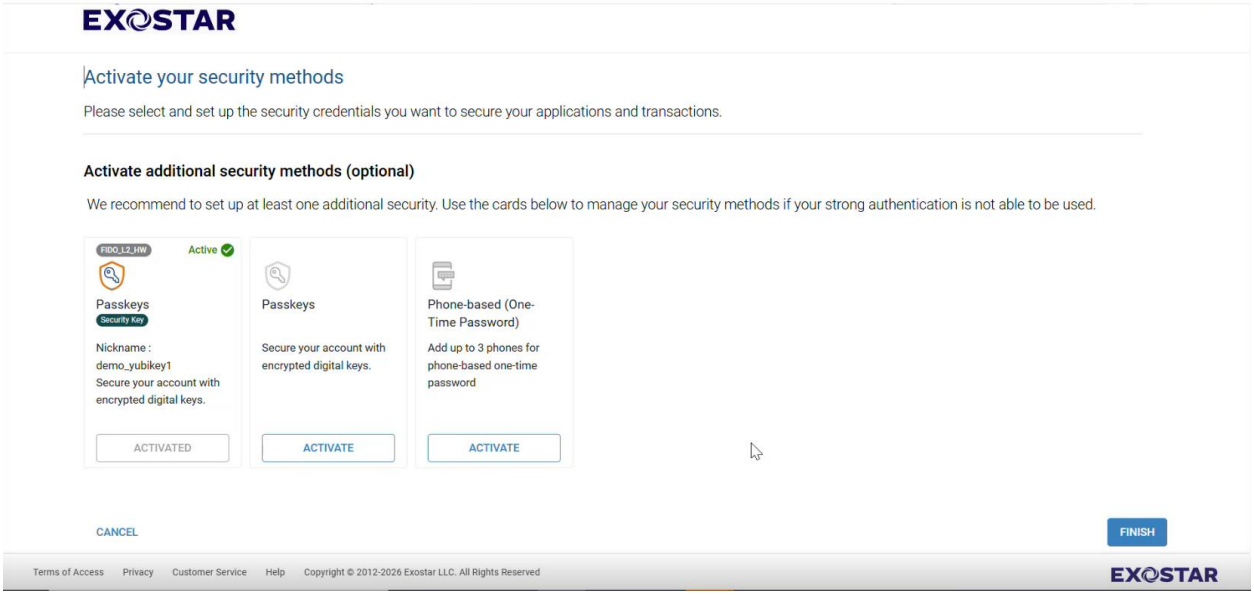


Figure 7. Activated security key, showing the nickname and the FIDO_L2_HW grade.

> **Note:** Steps 1 to 4 are rendered by the browser and the operating system, not by SAM. Their wording varies by browser and platform.

Route B — a passkey on a phone or tablet

To store the passkey on a phone instead, select Cancel at the first browser prompt. Chrome then offers a choice of where to save the passkey.

Copyright © 2026 Exostar LLC. All rights reserved.

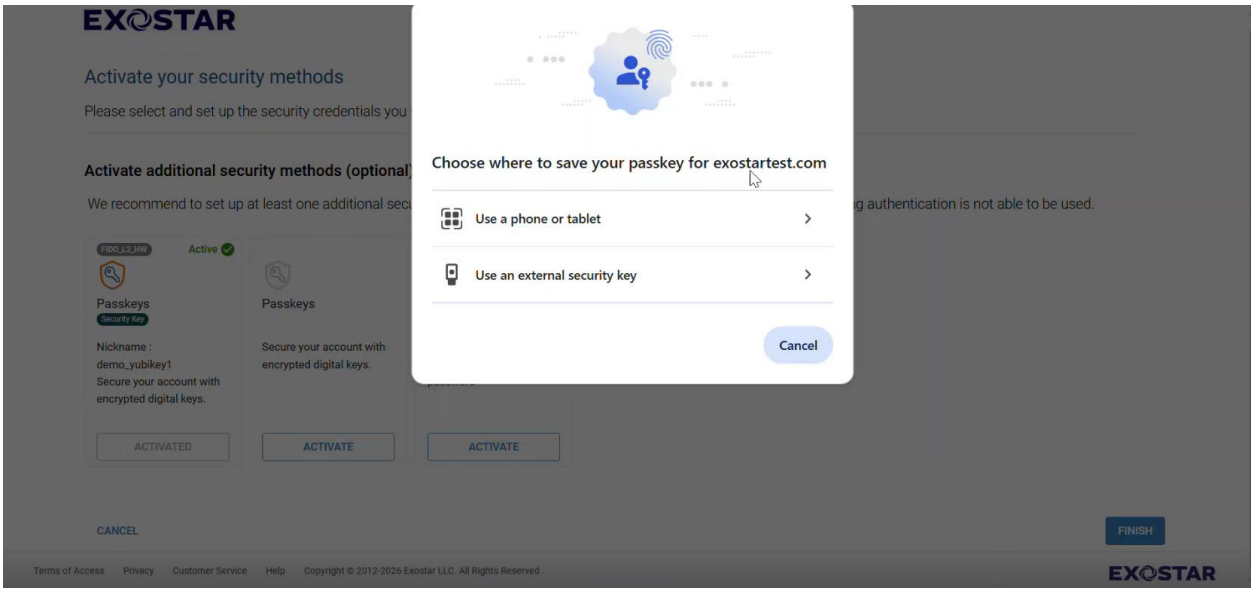


Figure 8. Choosing between a phone or tablet and an external security key.

1. Select Use a phone or tablet. A QR code is displayed.
2. Scan the QR code with the camera on the device where the passkey should live.
3. Confirm with the fingerprint, face or PIN set on that device. The passkey is created and stored there.

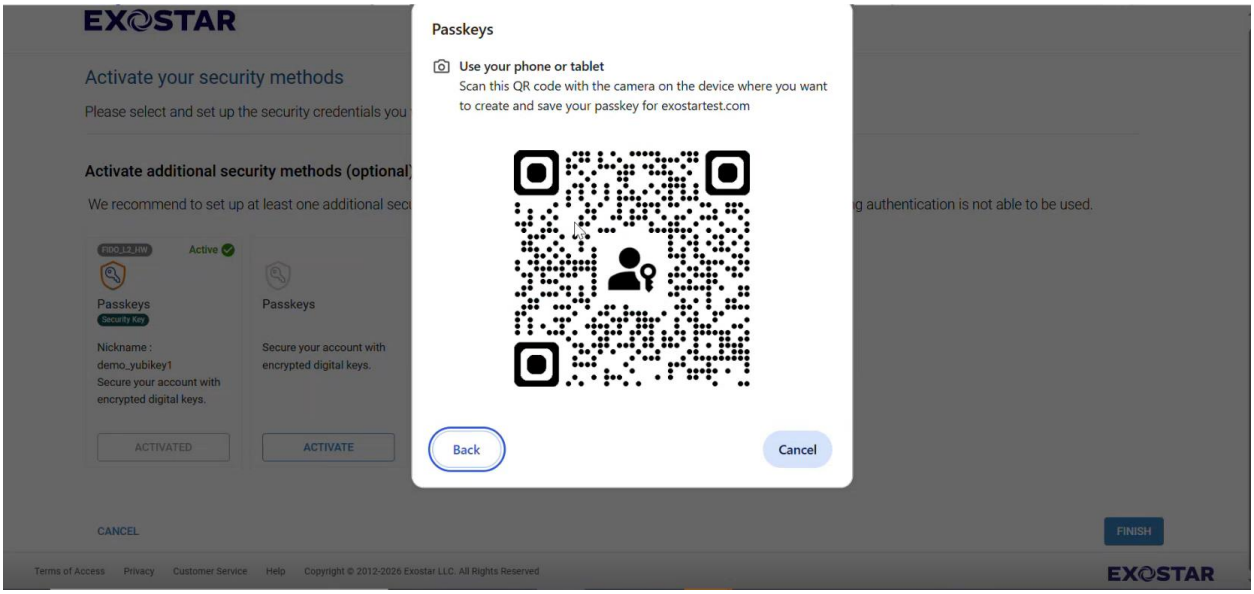


Figure 9. QR code for binding the passkey to a phone or tablet.

4. SAM then shows the same Add security key screen, pre-filled with a default name from the device's credential manager. Keep the name or replace it, then save.

Copyright © 2026 Exostar LLC. All rights reserved.

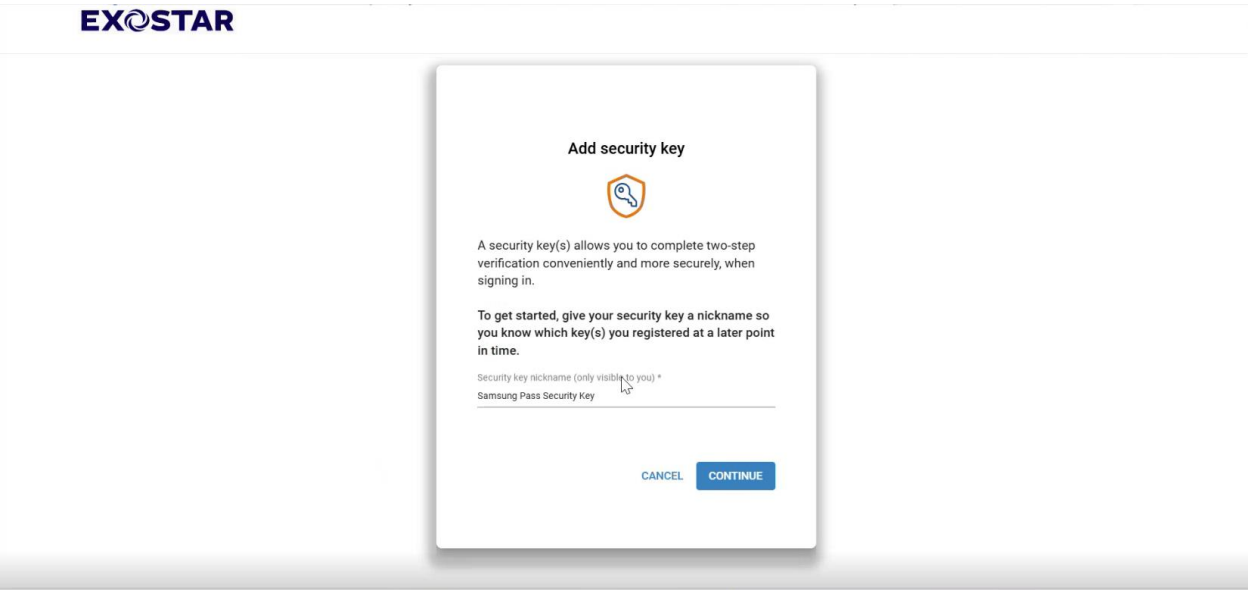


Figure 10. Naming a passkey created on a mobile device.

> **Note:** The QR code is displayed in two places: here, during activation, where it binds the device to the credential, and again at step-up when a shared passkey is the credential being used. It is not currently required to sign in to SAM.

Where the computer itself supports passkeys — Windows Hello on Windows, Touch ID or Face ID on a Mac — the passkey can be stored on the computer instead, and is presented directly at sign-in with a biometric or PIN prompt.

6. MANAGING YOUR PASSKEYS

An account can hold up to four passkeys, in any combination — all hardware keys, all mobile passkeys, or a mix of the two. Each activated card displays its own nickname and assurance grade.

Copyright © 2026 Exostar LLC. All rights reserved.

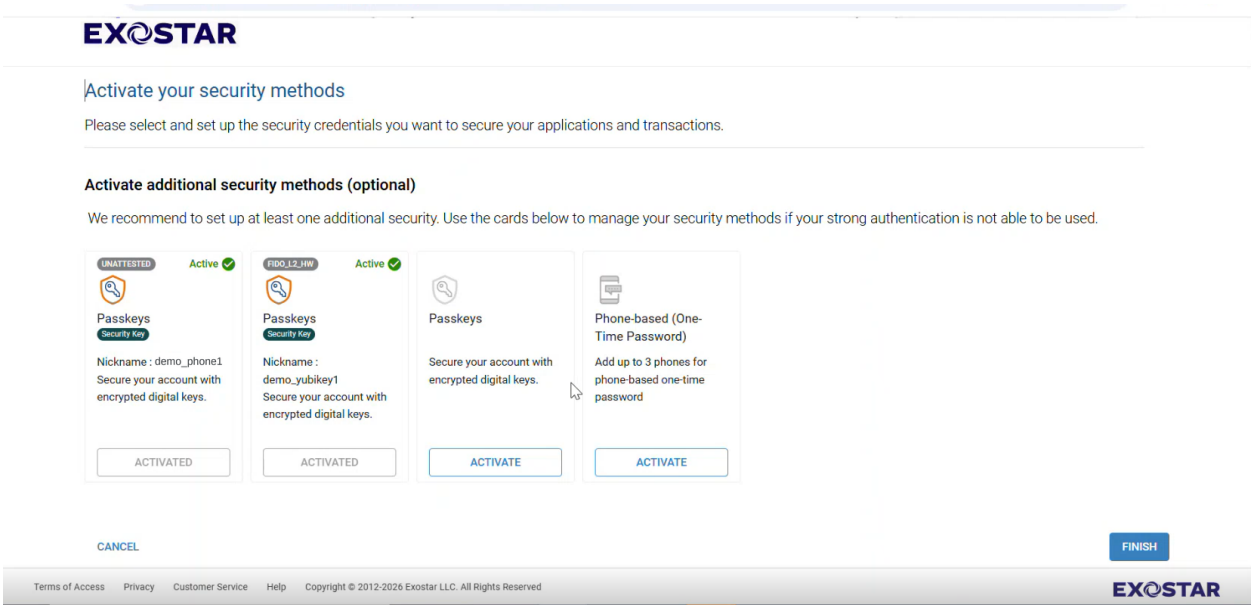


Figure 11. Two activated passkeys on one account, each showing its own grade and nickname.

Action	What you do	What to expect
Add another	Select ACTIVATE on the Passkeys card again.	The same activation sequence runs. Up to four passkeys in total.
Rename	Open the credential and enter a new nickname.	You must re-authenticate with that passkey before the new name is saved.
Remove	Remove the credential from credential management.	Step-up authentication is required and a removal reason is captured.
Replace a lost key	Remove the old credential and register a new one.	There is no recovery flow — a lost passkey is replaced by re-registering.

Important: SAM has no separate recovery flow for a lost or damaged passkey. Keep at least one spare credential registered so that losing one does not lock you out.

7. SIGNING IN AND STEPPING UP

Once a passkey is active it is used in two places: at sign-in, and when stepping up into an application that requires stronger authentication. Select the security key option and the browser takes over.

- With one hardware key, the browser prompts for the PIN and a tap, and the credential is used directly.
- With more than one hardware key, each key signals in turn and you tap whichever one you want to use.
- With a passkey held on a phone, the browser presents the device and you confirm with that phone's fingerprint, face or PIN.
- With a passkey held on the computer, it is presented directly with a biometric or PIN prompt.

Note: FIDO2 elevation is required once per session, not on every application launch.

Copyright © 2026 Exostar LLC. All rights reserved.

Where the QR code appears

The QR code is not limited to activation. It is displayed in two situations:

- At activation, when a passkey is being stored on a phone or tablet. Scanning the code binds that device to the credential.
- At step-up, when the credential being used is a shared passkey. The code is scanned with the device that holds the passkey, and the step-up is confirmed there.

A QR code is not currently required to sign in to SAM. A hardware security key never presents one, at sign-in or at step-up.

8. WHEN AN APPLICATION REQUIRES A PASSKEY

Some applications require a phishing-resistant credential. Where an application requires FIDO2, a passkey or a security key is the only step-up credential offered for it; Phone OTP is not presented as an alternative.

- If you do not yet hold the credential an application requires, an "MFA Not Met" indicator appears on that application's launch button on your SAM dashboard.
- Selecting the indicator takes you to credential management, where you activate the right credential. The application then launches normally.
- Some applications accept either credential type; others accept a hardware security key only — see Which credential an application accepts, under Key Concepts.

Note: SAM does not send a notification e-mail when an application begins to require FIDO2. You will see the requirement the next time you launch that application.

9. TROUBLESHOOTING

Issue	What is happening	What to do
An application's launch button shows "MFA Not Met".	The application requires a FIDO2 credential you do not yet hold.	Select the indicator to go to credential management and activate the required credential, then launch the application again.
A shared passkey is not accepted for an application.	The application is set to FIDO2 - YubiKeys, which accepts hardware security keys only.	Activate a hardware security key. A security key satisfies every FIDO2 requirement.
You have no phone, or phones are not permitted on site.	A phone is one storage option, not a requirement.	Use a hardware security key, or store the passkey on the computer where the platform supports it.
The Add security key screen will not save.	A nickname is required on this screen.	Enter a name for the credential and save again.
A passkey has been lost or damaged.	There is no recovery flow for a lost passkey.	Remove the old credential and register a replacement. Keep a second credential registered to avoid being locked out.
ACTIVATE does not add a fifth credential.	The account already holds the maximum of four passkeys.	Remove a credential that is no longer needed before registering another.

Copyright © 2026 Exostar LLC. All rights reserved.

Issue	What is happening	What to do
Identity proofing is requested before a credential can be configured.	The application is set to Level 3, which requires identity proofing first.	Complete proofing from the Get 2FA prompt or from credential management, then return and activate the credential.

Copyright © 2026 Exostar LLC. All rights reserved.

10. FREQUENTLY ASKED QUESTIONS

The questions below are the ones users most often ask about passkeys and security keys in SAM.

Can I activate a passkey without a phone?

Yes. A phone is one option, not a requirement. A hardware security key needs no phone at all — you plug it into a USB port, enter its PIN and tap it, as shown in Route A. The passkey can also be stored on the computer itself where the platform supports it, for example Windows Hello on Windows or Touch ID and Face ID on a Mac. If you work where phones are not permitted, the hardware key route is the recommended option.

Do I scan a QR code every time I sign in?

Not at sign-in. A QR code is not currently required to sign in to SAM. It is not, however, a one-off at activation either — the code appears in two situations:

- At activation, when you choose to store the passkey on a phone or tablet. Scanning the code binds that device to the credential.
- At step-up, when the credential being used is a shared passkey. The code is scanned with the device that holds the passkey, and the step-up is confirmed there.

A hardware security key never presents a QR code — it is a PIN and a tap, at sign-in and at step-up alike. A passkey held on the computer itself is presented directly with a biometric or PIN prompt.

Is the same key used every time, or does it change?

The credential itself stays the same. At activation, the device creates a key pair: the private key stays on the device or security key and never leaves it, and SAM stores only the matching public key. The same credential is then used for every subsequent sign-in. What changes on each authentication is the signed challenge — a fresh, single-use value that cannot be replayed. This is what makes FIDO2 phishing resistant, and it is a different mechanism from a one-time passcode, where the code itself changes each time.

How many passkeys can I hold?

Up to four, in any combination of hardware keys and passkeys held on a phone, tablet or computer. Register at least two, so that a lost or damaged credential does not lock you out.

What will I be sent before I can activate a passkey?

Nothing. You are never sent a key, a code or an enrolment package — there is nothing to distribute and nothing that can be intercepted. When an application begins to require FIDO2, you discover it the next time you try to launch that application: your dashboard shows "MFA Not Met", and one click takes you into the activation flow.

Do passkeys expire or need to be rotated?

No. FIDO2 credentials do not work like passwords, and there is no user-visible expiry: a registered credential stays valid until you remove it. Exostar does revalidate the authenticator on every registration and

Copyright © 2026 Exostar LLC. All rights reserved.

authentication, checking its identifier, certification level, key protection and attestation against the Exostar Approved FIDO Authenticator List, so a credential type that is later withdrawn stops being accepted.

Which passkey types does SAM accept?

SAM 7.0 accepts two kinds of FIDO2 credential:

- Shared passkeys synced through the Apple iCloud Keychain, Microsoft and Google credential managers.
- Hardware security keys (YubiKeys).

Copyright © 2026 Exostar LLC. All rights reserved.