SPECOPS KEY RECOVERY

Datasheet

ABOUT SPECOPS Specops Software is the leading provider of password management and authentication solutions. Specops protects your business data by blocking weak passwords and securing user authentication. Every day thousands of organizations use Specops Software to protect business data. For more information, please visit specopssoft.com

SPECOPS KEY RECOVERY

Specops Key Recovery is a self-service solution for unlocking computers encrypted by Microsoft BitLocker or Symantec Endpoint Encryption. A user who is locked out at the pre-boot authentication screen can use Specops Key Recovery to unlock their computer, without calling the helpdesk. For added security, users are verified with multi-factor authentication. The solution supports a number of authentication factors, including Duo Security, Symantec VIP, Okta, PingID and YubiKey.

To protect corporate data and address regulatory requirements, organizations are increasingly turning to endpoint encryption solutions. Encryption at the hardware level of a storage device, commonly referred to as full-disk encryption (FDE), protects confidential information from unauthorized access.

FDE solutions, such as BitLocker and Symantec Endpoint Encryption, create a pre-boot authentication environment that require a secret key every time the computer is started, or when a lockout is triggered. Without a self-service recovery solution, FDE will drive calls to the helpdesk.

Feature Highlights

FEATURES	BITLOCKER ALONE	BITLOCKER WITH SPECOPS	SYMANTEC ENDPOINT ENCRYPTION ALONE	SYMANTEC ENDPOINT ENCRYPTION WITH SPECOPS
Self-service key recovery	Yes (MBAM integrated with SCCM)	Yes	Yes	Yes
Remote self-service key recovery	No	Yes	No	Yes
Multi-factor authentication	No	Yes (20+ identity services)	No (security questions)	Yes (20+ identity services)
Integration with self-service password reset	No	Yes, with Specops uReset	No	Yes, with Specops uReset

How does it work?

You can configure Specops Key Recovery by installing the Gatekeeper component in your organization's corporate network. The Gatekeeper will access BitLocker and/or Symantec Endpoint Encryption to relay recovery keys for end users. The recovery key is encrypted inside the corporate network, and decrypted once it reaches the user's device. Specops Key Recovery does not access sensitive data from BitLocker or Symantec Endpoint Encryption.

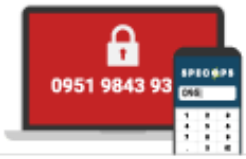
When a user attempts a self-driven key recovery, Specops Key Recovery will prompt the user to authenticate with the identity service(s) from their enrollment. The enrollment data is stored on a sub-object of their user account in the on-premises Active Directory.

The following takes place during a self-driven key recovery:

1. User is locked out at the pre-boot authentication screen. The preboot authentication screen prompts the user to visit Specops Key Recovery on a mobile device.

2. The user visits Specops Key Recovery and enters their corporate email address.

3. Specops Key Recovery displays the authentication rules to the user. The user authenticates with various identity services to fulfill the policy.

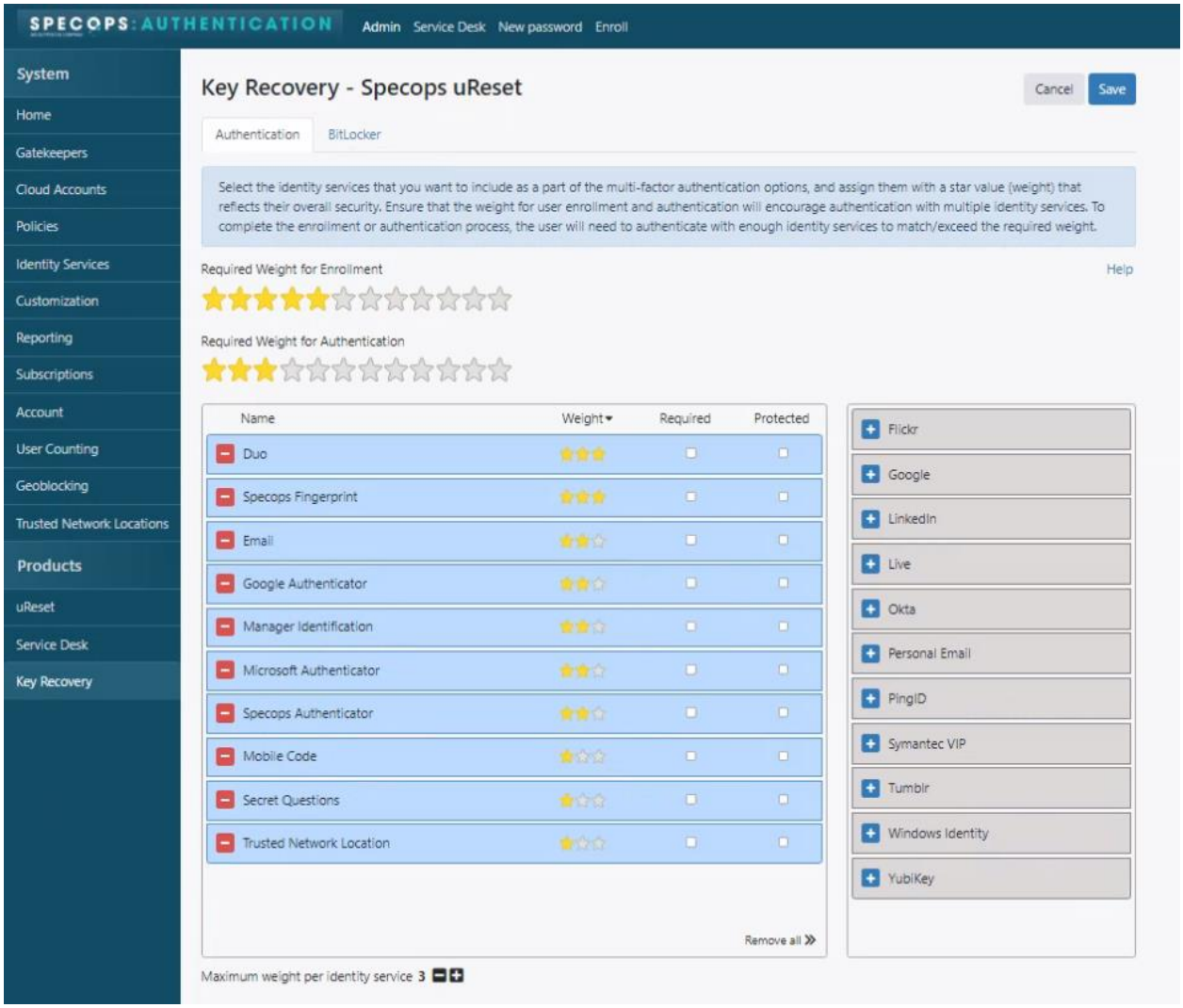


4. The user is asked for the sequence number or first 8 characters of the recovery key ID of the locked computer. The user enters the additional information on their mobile device.

5. Specops Key Recovery displays a recovery key for the locked computer on the user's mobile device. The user enters the recovery key on the locked computer to regain access.

What does it look like?

Admin Experience



Specops Key Recovery enhances security by extending multi-factor authentication to self-service key recovery. There are over 20 identity services available to ensure that you can select the best options for your users, including ID service options that require no end-user enrollment action. Lifting the burden of end user enrollment ensures your rollout of Specops Key Recovery is quick and easy.

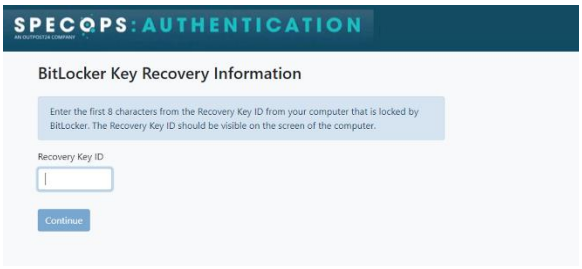
However, since not all identity services are equally secure, administrators can assign each identity service a trust value, based on their perceived level of security. The trust assignment is managed via stars, as shown in the administrator view above.

What does it look like?

End user experience

After verifying their identity via the methods configured by their administrator, the end user can follow the steps on screen to finish the recovery key process, as shown here.

The simple interface (available in multiple languages) helps minimize encryption lockout calls to the service desk.



What people are saying

Really great product

"Overall, I think that Specops Key Recovery is a really great product that will go a long way toward helping organizations prevent BitLocker-related data loss."

- Brien Posey, Microsoft MVP, Techgenix review

Really impressed with the management portal and support

"I was impressed with Specops Key Recovery for BitLocker, the management portal, and the support I received."

- Robert Pearman, Microsoft MVP, 4sysops review

Our Technology Partners

Our Technology partnerships ensure that organizations can confidently extend the value of their existing investments and systems to optimize password security– whether that's extending existing multi-factor authentication investments or extending Microsoft Active Directory functionality. Read more.

Get a Demo of Specops Key Recovery

Interested to see how Specops Key Recovery can work in your organization? Click here to start a demo or trial today.