Specops Key Recovery

Specops Key Recovery is a self-service solution for unlocking computers encrypted by Microsoft Bitlocker and 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 Symantec VIP, and Mobile Code.

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 when the computer is started, or when a lockout is triggered. Without a self-service recovery solution, FDE will drive calls to the helpdesk.

Features	BitLocker	BitLocker with Specops Key Recovery	Symantec Endpoint Encryption	Symantec Endpoint Encryption with Specops Key Recovery
Self-service key recovery	Yes	Yes	Yes	Yes
Self-service key recovery for remote users	No	Yes	No	Yes
Multi-factor authentication	No	Yes (15+ identity providers)	No (security questions)	Yes (15+ identity providers)
Integration with self-service password reset	No	Yes (Specops uReset)	No	Yes (Specops uReset)

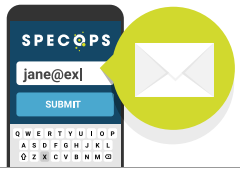
How does it work?

You can configure Specops Key Recovery by installing the Gatekeeper component in your organization's corporate network. The Gatekeeper will access Symantec Endpoint Encryption and/or Bitlocker 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 resources from Symantec Endpoint Encryption, or BitLocker.

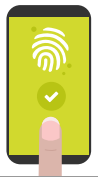
When a user attempts a self-driven key recovery, Specops Key Recovery will prompt the user to authenticate with the identity service(s) from their enrollment. The enrollment data is stored on a sub-object of their user account in the on-premises Active Directory.

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

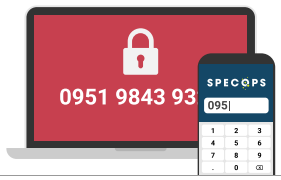
1. User is locked out at the pre-boot authentication screen. The pre-boot authentication screen prompts the user to visit Specops Key Recovery on a mobile device.



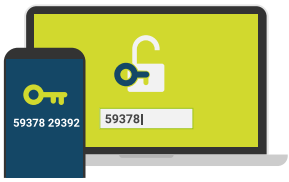
2. The user visits Specops Key Recovery and enters their corporate email address.



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.

Frequently Asked Questions

Q: What version of Symantec Endpoint Encryption does Specops Key Recovery support?

A: Version 11.0 and later.

Q: Does Specops Key Recovery store recovery keys?

A: No, recovery keys are stored and managed by Symantec Endpoint Encryption and/or Bitlocker.

Q: Can Specops Key Recovery reset passwords?

A: Specops Key Recovery can be used to get past the pre-boot authentication screen. A password reset solution, such as Specops uReset, can be used to enable self-service password resets. Specops Key Recovery uses the same authentication platform as Specops uReset, allowing users to use the same identity services to manage key recovery, and password resets.