SOPHOS

Cybersecurity made simple.

Sophos Central Device Encryption

Administratoranleitung

Inhalt

1 Über Sophos Central Device Encryption

Sophos Central Device Encryption ermöglicht Ihnen, die BitLocker-Laufwerkverschlüsselung auf Windows Endpoints sowie die FileVault-Verschlüsselung auf Mac Endpoints über Sophos Central zu verwalten.

Durch die Verschlüsselung von Festplatten sind Daten geschützt, auch wenn ein Gerät verloren geht oder gestohlen wird.

Diese Hilfe beschreibt, wie Sie Sophos Central Device Encryption einrichten und verwenden. Außerdem wird beschrieben, wie Sie den Wiederherstellungsschlüssel über das Self Service Portal abrufen können. Für weitere Informationen zu Richtlinieneinstellungen, Warnmeldungen und Recovery über Sophos Central, siehe Sophos Central Hilfe.

Verwandte Informationen

Sophos Central Admin Hilfe

2 Verwalten der BitLocker-Festplattenverschlüsselung

Dieser Abschnitt beschreibt die Voraussetzungen für die Verwendung der BitLocker Festplattenverschlüsselung auf Windows Endpoints in Ihrem Netzwerk sowie die verfügbaren Authentisierungsmodi deren Abhängigkeiten von den Windows Gruppenrichtlinien.

2.1 Migration zu Sophos Central Device Encryption

Wenn Sie bereits SafeGuard Enterprise mit BitLocker Drive Encryption oder Sophos Full Disk Encryption verwenden, lesen Sie in diesem Abschnitt, wie Sie zu Central Device Encryption migrieren können.

Folgende Fälle werden behandelt:

- SafeGuard Enterprise und BitLocker
- SafeGuard Enterprise und Sophos Full Disk Encryption
- Für Informationen zum Migrieren von Mac Endpoints, siehe Migration zu Sophos Central Device Encryption (Mac).

Zugehörige Aufgaben

Migration zu Sophos Central Device Encryption (Mac) (Seite 14)
Wenn Sie Sophos Central verwenden möchten, um Mac Endpoints zu verwalten, die bereits mit FileVault verschlüsselt sind, müssen Sie diesen Endpoints eine Sophos Central Device Encryption Richtlinie zuweisen.

2.1.1 Migration von SafeGuard Enterprise BitLocker

Führen Sie folgenden Schritte aus, um zu migrieren.

Hinweis
Wenn Sie BitLocker mit SafeGuard Enterprise Version 6.x oder 7.x verwenden, empfehlen wir, zuerst SafeGuard Enterprise auf die neueste Version zu aktualisieren.

Wenn Sie SafeGuard Enterprise Version 6.x oder 7.x verwenden, müssen Sie zuerst die Systemfestplatte gemäß SafeGuard Enterprise Administratorhilfe entschlüsseln bevor Sie zu Sophos Central Device Encryption migrieren können.

So migrieren Sie von SafeGuard Enterprise BitLocker Client (Version 8.0 oder höher) zu Sophos Central Device Encryption:

1. Öffnen Sie **Systemsteuerung > Programm deinstallieren** und klicken Sie mit der rechten Maustaste auf **Sophos SafeGuard Client**.
2. Wählen Sie im Kontextmenü **Ändern**.
   Der SafeGuard Enterprise Client Installationsassistent startet.
3. Deinstallieren Sie die BitLocker Komponente.

Hinweis
Durch die Deinstallation von BitLocker werden weder Volumes noch Dateien entschlüsselt.

4. Installieren Sie die Sophos Central Device Encryption Software.
5. Stellen Sie sicher, dass eine Sophos Central Device Encryption Richtlinie dem Endpoint zugewiesen und aktiviert ist.

Sie können nun BitLocker über Sophos Central verwalten. Es ist keine Neuverschlüsselung erforderlich. Sobald Sie dem Endpoint eine Sophos Central Device Encryption Richtlinie zugewiesen haben, wird der Wiederherstellungsschlüssel erneuert und in Sophos Central gespeichert. Die Funktion der Dateiverschlüsselung bleibt unverändert.

Verwandte Informationen
SafeGuard Enterprise Administratorhilfe

2.1.2 Migration von SafeGuard Enterprise Full Disk Encryption

Führen Sie folgenden Schritte aus, um zu migrieren.

So migrieren Sie von SafeGuard Enterprise Full Disk Encryption:

1. Deinstallieren Sie die Sophos SafeGuard Client Software.
   Verschlüsselte Volumes werden automatisch entschlüsselt. Verschlüsselte Dateien bleiben verschlüsselt.
2. Installieren Sie die Sophos Central Device Encryption Software.
3. Stellen Sie sicher, dass eine Sophos Central Device Encryption Richtlinie dem Endpoint zugewiesen und aktiviert ist.
4. Installieren Sie die benötigten SafeGuard Enterprise File Encryption Module neu (Synchronized Encryption oder Pfadbasierte Dateiverschlüsselung).

Sie können nun BitLocker über Sophos Central verwalten. Sobald Sie dem Endpoint eine Sophos Central Device Encryption Richtlinie zugewiesen haben, startet im Hintergrund die Verschlüsselung und der Wiederherstellungsschlüssel wird erneuert und in Sophos Central gespeichert.

2.2 Device Encryption vorbereiten

Standardmäßig sind die meisten Systemlaufwerke für die Verwendung von BitLocker vorbereitet. Ist dies nicht der Fall, führt Sophos Central Device Encryption automatisch das erforderliche Microsoft Befehlszeilentool `BdeHdCfg.exe` aus, um das Laufwerk vorzubereiten.

Das bedeutet, dass eine separate BitLocker-Partition auf dem Systemlaufwerk erzeugt wird.

Während der Einrichtung von Device Encryption werden Benutzer darüber informiert, dass ein Neustart erforderlich ist, um das Systemlaufwerk vorzubereiten. Benutzer können auswählen, ob sie den Computer sofort oder später neu starten möchten. Device Encryption kann nur gestartet werden, wenn der Computer neu gestartet wurde und die Vorbereitung des Systemlaufwerks erfolgreich war.

Die von Device Encryption benötigte Version von .NET Framework wird auf den Endpoints automatisch installiert.

2.3 Device Encryption Schritt für Schritt

Gehen Sie wie folgt vor, um Geräte zu verschlüsseln.

Voraussetzungen:

- Die Sophos Central Agent Software muss auf den Endpoints installiert sein.
- Eine Device Encryption Richtlinie muss in Sophos Central definiert und aktiviert sein.
- Benutzer müssen sich interaktiv an ihren Endpoints anmelden, um sie mit Sophos Central zu verbinden und zu synchronisieren. Beachten Sie, dass Remoteanmeldungen nicht unterstützt werden.
- Das Betriebssystem muss BitLocker-Laufwerkverschlüsselung unterstützen. Weitere Informationen finden Sie unter Device Encryption vorbereiten und Device Encryption Systemkompatibilität.

Im Folgenden erfahren Sie, was Benutzer sehen und wie sie vorgehen müssen.

1. Ist die TPM-Sicherheitshardware noch nicht aktiviert, wird eine BIOS-Aktion gestartet, um sie zu aktivieren. Dies erfordert einen Neustart. Benutzer können wählen, ob sie sofort oder später neu starten.
   Während des Neustarts werden Benutzer aufgefordert, das TPM zu aktivieren. Wenn das TPM nicht aktiviert werden kann oder der Benutzer nicht reagiert, wird eine Nachricht ausgegeben.
2. Ist das TPM aktiv, aber nicht im Besitz, so generiert die Sophos Central Agent Software automatisch neue TPM-Besitzerinformationen. Schlägt dies fehl, wird ein Warnhinweis an Sophos Central gesendet.
3. Fehlen TPM Endorsement Keys, so werden diese automatisch von der Sophos Central Agent Software erzeugt. Schlägt dies fehl, wird ein Warnhinweis an Sophos Central gesendet.
4. Wenn in der Device Encryption Richtlinie die Option **Authentifizierung bei Start erforderlich** deaktiviert ist, beginnt die Verschlüsselung der Festplatte automatisch. In diesem Fall müssen die Benutzer nichts weiter unternehmen. Springen Sie zu Schritt 8.
5. Wenn in der Device Encryption Richtlinie die Option **Authentifizierung bei Start erforderlich** aktiviert ist sehen die Benutzer den **Sophos Device Encryption** Dialog.
   - Schreibt die Device Encryption-Richtlinie eine PIN oder ein Kennwort für die Authentifizierung vor, müssen die Benutzer den Anweisungen auf dem Bildschirm folgen, um eine PIN oder ein Kennwort festzulegen. Wird TPM+PIN verwendet, wird der Schlüssel für die Verschlüsselung des Systemlaufwerks im TPM gespeichert.

     Hinweis
     Beim Erstellen eines Kennworts müssen Benutzer Folgendes beachten: In der Pre-Boot-Umgebung wird nur das US-Tastaturlayout (Englisch) unterstützt. Wenn sie jetzt eine PIN oder ein Kennwort mit Sonderzeichen festlegen, müssen sie später bei der Anmeldung möglicherweise andere Tasten für die Eingabe verwenden.

   - Wenn die Device Encryption-Richtlinie einen USB-Schlüssel für die Authentifizierung vorschreibt, müssen sie einen USB-Stick an ihren Computer anschließen. Der USB-Stick muss mit NTFS, FAT oder FAT32 formatiert sein.
6. Drückt der Benutzer auf **Neu starten und verschlüsseln**, startet der Computer neu und stellt sicher, dass Device Encryption funktioniert.
   Sie können **Später erinnern** auswählen, um den Dialog zu schließen. Der Dialog wird allerdings wieder angezeigt sobald sich Benutzer neu anmelden oder wenn Sie die Device Encryption-Richtlinie verändern.

7. Ist der Benutzer nicht in der Lage, PIN/Kennwort richtig einzugeben, kann er die Esc-Taste drücken. Das System startet normal, da noch keine Verschlüsselung durchführt wurde. Bei der nächsten Anmeldung wird der Benutzer erneut aufgefordert, PIN/Kennwort einzugeben.
8. Sie können sehen, welche Benutzer die Verschlüsselung noch nicht aktiviert haben. Das bedeutet, dass Benutzer ihren Computer noch nicht neu gestartet haben oder dass sie die Anweisungen noch nicht ausgeführt haben. Sehen Sie unter **Berichte** in Sophos Central nach.
9. War der Pre-Boot-Test erfolgreich, beginnt die Sophos Central Software mit der Verschlüsselung der lokalen Festplatten. Die Verschlüsselung passiert im Hintergrund, daher können Benutzer wie gewohnt mit dem Computer weiterarbeiten.
   Schlägt der Hardware-Test fehl, startet das System neu und es wird keine Verschlüsselung durchgeführt. Eine Ereignismeldung wird an Sophos Central gesendet, um Sie zu informieren.
10. Nachdem der Sophos Central Agent das Systemlaufwerk verschlüsselt hat, wird die Verschlüsselung der Datenvolumes gestartet, sofern dies in der Richtlinie definiert ist. Der Schutz für diese Volumes ist auf dem Systemlaufwerk gespeichert, so dass Datenvolumes automatisch nach dem Hochfahren verfügbar sind. Dass bedeutet, dass Benutzer nach der Anmeldung an ihrem Computer keine weiteren Schritte vornehmen müssen. Wechseldatenträger wie zum Beispiel USB-Speichersticks werden nicht verschlüsselt.

Auf dem Endpoint stehen die beiden Log-Dateien `CDE.log` und `CDE_trace.xml` unter `%ProgramData%\Sophos\Sophos Data Protection\Logs` zur Verfügung.

Zugehörige Konzepte

Device Encryption vorbereiten (Seite 3)
Standardmäßig sind die meisten Systemlaufwerke für die Verwendung von BitLocker vorbereitet. Ist dies nicht der Fall, führt Sophos Central Device Encryption automatisch das erforderliche Microsoft Befehlszeilentool `BdeHdCfg.exe` aus, um das Laufwerk vorzubereiten.

Device Encryption Systemkompatibilität (Seite 5)
Die folgende Tabelle bietet eine Übersicht, welche Authentisierungsmodi auf welchen Plattformen unterstützt werden. Welcher Modus zur Anwendung kommt hängt davon ab, welche Windows-Version installiert ist und ob TPM-Sicherheitshardware vorhanden ist.

TPM+PIN (Seite 7)
Dieser Modus verwendet die TPM-Sicherheitshardware des Computers sowie eine PIN für die Authentisierung.

2.4 Device Encryption Systemkompatibilität

Die folgende Tabelle bietet eine Übersicht, welche Authentisierungsmodi auf welchen Plattformen unterstützt werden. Welcher Modus zur Anwendung kommt hängt davon ab, welche Windows-Version installiert ist und ob TPM-Sicherheitshardware vorhanden ist.

Die Ziffer in Klammern gibt die Priorität an, mit der ein bestimmter Modus angewendet wird.

(*) Wenn **Authentifizierung bei Start erforderlich** aktiviert ist, kann der Modus "Nur TPM" nicht installiert werden und daher fällt die oberste Priorität an "TPM+PIN".

	Win 7 ohne TPM	Win 7 mit TPM	Win 8.1 ohne TPM	Win 8.1 mit TPM	Win 10 ohne TPM	Win 10 mit TPM
Nur TPM	-	ok (1*)	-	ok (1*)	-	ok (1*)
TPM+PIN	-	ok (2)	-	ok (2)	-	ok (2)

	Win 7 ohne TPM	Win 7 mit TPM	Win 8.1 ohne TPM	Win 8.1 mit TPM	Win 10 ohne TPM	Win 10 mit TPM
Passphrasen	-	-	ok (1)	ok (3)	ok (1)	ok (3)
USB-Stick	ok (1)	ok (3)	-	-	-	-

Möglicherweise müssen Sie TPM auf dem Endpoint-Computer konfigurieren, wenn Sie Central Device Encryption verwenden.

Wenn Sie TPM 2.0 oder höher verwenden, müssen Sie die Festplatte als GPT formatieren und das BIOS muss sich im UEFI-Modus befinden.

Wenn Sie TPM 1.2 verwenden, müssen Sie TPM im BIOS/UEFI aktivieren und es muss einsatzbereit sein. Sie können dies mit `TPM.MSC` überprüfen.

Es wird empfohlen, dass Sie Ihre Endpoint-Computer auf die neueste BIOS-/UEFI-Version aktualisieren, bevor Sie Central Device Encryption installieren.

Ist der Windows FIPS-Modus aktiviert, so wird BitLocker Verschlüsselung nur auf Systemen unterstützt, auf denen Windows 8.1 oder Windows 10 installiert ist. Ausführliche Informationen zu BitLocker im FIPS-Modus unter Windows 7 finden Sie unter Ein FIPS-konformes Wiederherstellungskennwort kann in AD DS für BitLocker unter Windows 7 oder Windows Server 2008 R2 nicht gespeichert werden.

Sie können verschlüsselte Festplatten mit Sophos Central Device Encryption verwenden. Für weitere Informationen, siehe Verschlüsselte Festplatte.

Central Device Encryption unterstützt die Vorabbereitstellung von BitLocker.

Verwandte Informationen

Ein FIPS-konformes Wiederherstellungskennwort kann in AD DS für BitLocker unter Windows 7 oder Windows Server 2008 R2 nicht gespeichert werden

Verschlüsselte Festplatte

2.5 Device Encryption Authentisierungsmodi

Sie können mit der Option **Authentifizierung bei Start erforderlich** in den Einstellungen unter Geräteverschlüsselung steuern, ob sich Benutzer bei jeder Anmeldung an ihrem Computer authentisieren müssen.

Welcher Authentisierungsmodus auf einem Computer installiert wird ist abhängig vom System, den BitLocker-Gruppenrichtlinien und der konfigurierten Device Encryption-Richtlinie. Abhängig von der Device Encryption Systemkompatibilität wird einer der folgenden Authentisierungsmodi auf den Endpoints installiert:

- TPM+PIN
- Passphrasen
- Nur TPM
- USB-Stick

Auf Endpoints, die bereits mit BitLocker verschlüsselt sind, werden Benutzer mittels einer Nachricht über die erforderlichen Schritte informiert.

Wenn Sie die Option **Authentifizierung bei Start erforderlich** aktivieren, werden Benutzer aufgefordert, PIN, Passphrase oder USB-Schlüssel zu definieren und auf **Anwenden** zu klicken. Die

PIN, die Passphrase oder der USB-Schlüssel muss dann bei jedem Start des Computers verwendet werden. Wenn Sie **Authentifizierung bei Start erforderlich** ausschalten, wird automatisch der Modus Nur TPM angewandt und es ist keine zusätzliche Authentisierung erforderlich. Benutzer werden informiert, dass ihr Laufwerk automatisch beim Start des Computers entsperrt wird.

Sophos Device Encryption kann das Gruppenrichtlinienobjekt (GPO) automatisch so konfigurieren, dass alle Authentisierungsmodi erlaubt sind, sofern die entsprechende Einstellung auf **Nicht konfiguriert** gesetzt ist. Wenn Sie die Einstellung manuell konfiguriert haben, werden diese Definitionen nicht überschrieben. Für weitere Informationen, siehe BitLocker-Gruppenrichtlinien.

Benutzer können die Installation der Authentisierungsmodi aufschieben. In diesem Fall findet keine Verschlüsselung statt. Sobald sich ein Benutzer wieder an Windows anmeldet oder wenn Sie eine neue Verschlüsselungsrichtlinie bereitstellen, wird der Benutzer aufgefordert, den Computer neu zu starten. Nach diesem Neustart ist der Authentisierungsmodus installiert und Device Encryption startet. Danach können Benutzer ihre Geräte nicht wieder entschlüsseln.

Zugehörige Konzepte

Device Encryption Systemkompatibilität (Seite 5)
Die folgende Tabelle bietet eine Übersicht, welche Authentisierungsmodi auf welchen Plattformen unterstützt werden. Welcher Modus zur Anwendung kommt hängt davon ab, welche Windows-Version installiert ist und ob TPM-Sicherheitshardware vorhanden ist.

BitLocker-Gruppenrichtlinien (Seite 8)
Sophos Central definiert einige Richtlinieneinstellungen automatisch, so dass Administratoren keine Vorbereitungen mehr für Device Encryption auf den Computern vornehmen müssen.

2.5.1 TPM+PIN

Dieser Modus verwendet die TPM-Sicherheitshardware des Computers sowie eine PIN für die Authentisierung.

Benutzer müssen diese PIN bei jedem Start des Computers in der Windows Pre-Boot-Umgebung eingeben.

"TPM+PIN" erfordert eine vorbereitete TPM und die GPO-Einstellungen des Systems müssen "TPM +PIN" zulassen.

Sind alle Bedingungen erfüllt, wird der Dialog für den "TPM+PIN"-Modus angezeigt und Benutzer werden aufgefordert, eine PIN zu definieren. Der Benutzer kann auf **Neu starten und verschlüsseln** klicken, um den Computer sofort neu zu starten und die Verschlüsselung zu starten.

Ist die GPO-Einstellung **Erweiterte PINs für Systemstart zulassen** aktiviert, darf die PIN Ziffern, Buchstaben und Sonderzeichen enthalten. Andernfalls sind nur Ziffern erlaubt.

PINs für BitLocker sind zwischen vier und zwanzig Zeichen lang. Sie können per Gruppenrichtlinie eine höhere Mindestlänge definieren. Die Sophos Central Agent Software definiert die Gruppenrichtlinie so, dass erweiterte PINs zugelassen sind. Der Dialog zeigt Hinweise für den Benutzer an, welche Zeichen verwendet werden dürfen und welche Mindest- bzw. Maximal-Länge erlaubt ist.

Hinweis
Alle Benutzer eines bestimmten Windows-Computers müssen dieselbe PIN verwenden, um das Systemlaufwerk zu entsperren. Anschließend können Sie sich mit ihren individuellen Anmeldeinformationen am Betriebssystem anmelden. Single Sign On wird auf Windows Computern nicht unterstützt.

2.5.2 Passphrasen

Für die Authentisierung an Endpoints ohne TPM-Sicherheitshardware kann eine Passphrase verwendet werden.

Benutzer müssen diese Passphrase bei jedem Start des Computers in der Windows Pre-Boot-Umgebung eingeben.

Der Schutz mit Passphrase erfordert Windows 8.0 oder höher und die GPO-Einstellungen des Systems müssen den Modus Passphrase erlauben.

Sind alle Bedingungen erfüllt, wird der Dialog für den "Passphrase"-Modus angezeigt und Benutzer werden aufgefordert, eine Passphrase mit 8-100 Zeichen zu definieren. Der Benutzer kann auf **Neu starten und verschlüsseln** klicken, um den Computer sofort neu zu starten und die Verschlüsselung zu starten.

2.5.3 Nur TPM

Dieser Modus verwendet die TPM-Sicherheitshardware des Computers ohne Authentisierung mit PIN.

Benutzer können den Computer starten ohne in der Windows Pre-Boot-Umgebung eine PIN eingeben zu müssen.

Der Modus erfordert eine vorbereitete TPM und die Device Encryption Richtlinieneinstellung **Authentifizierung bei Start erforderlich** muss deaktiviert sein. Außerdem müssen die GPO-Einstellungen des Systems "Nur TPM" zulassen.

Sind alle Bedingungen erfüllt, wird der Installationsdialog für den "Nur TPM"-Modus angezeigt. Benutzer können auf **Neu starten und verschlüsseln** klicken, um den Computer sofort neu zu starten und die Verschlüsselung zu starten.

2.5.4 USB-Stick

Dieser Modus verwendet für die Authentisierung einen Schlüssel, der auf einem USB-Stick gespeichert ist.

Der USB-Stick muss bei jedem Systemstart mit dem Computer verbunden werden.

Der USB-Stick-Modus wird auf Computern mit Windows 7 verwendet, wenn kein TPM vorhanden ist oder es per GPO deaktiviert ist.

Der USB-Stick muss mit NTFS, FAT oder FAT32 formatiert sein. Das Format exFAT wird nicht unterstützt. Außerdem muss der USB-Stick beschreibbar sein.

Sind alle Bedingungen erfüllt, wird der Dialog für den USB-Stick-Modus angezeigt und der Benutzer muss einen USB-Stick auswählen, auf dem der Schlüssel gespeichert werden soll.

Benutzer können auf **Neu starten und verschlüsseln** klicken, um den Computer sofort neu zu starten und die Verschlüsselung zu starten.

2.6 BitLocker-Gruppenrichtlinien

Sophos Central definiert einige Richtlinieneinstellungen automatisch, so dass Administratoren keine Vorbereitungen mehr für Device Encryption auf den Computern vornehmen müssen.

Einstellungen, die bereits von Administratoren getroffen wurden, werden dabei nicht überschrieben.

Im **Editor für lokale Gruppenrichtlinien** unter **Computerkonfiguration > Administrative Vorlagen > Windows-Komponenten > BitLocker- Laufwerksverschlüsselung > Betriebssystemlaufwerke** finden Sie folgende Richtlinien:

Richtlinie	Einstellung	Wert von Sophos Central festgelegt	Anmerkung
Netzwerkentsperrung beim Start zulassen		Aktiviert	Sie können erlauben, dass eine vordefinierte BitLocker-Netzwerkentsperrung nach der Aktivierung von Central Device Encryption wie vorher funktioniert.
Zusätzliche Authentifizierung beim Start anfordern	BitLocker ohne kompatibles TPM zulassen	Aktiviert	Erlaubt unter Windows 8 beim Systemstart die Verwendung eines Kennworts zum Entsperren des Systemlaufwerks wenn kein TPM verfügbar ist.
Zusätzliche Authentifizierung beim Start anfordern	TPM-Systemstart-PIN konfigurieren	Systemstart-PIN bei TPM zulassen	Wenn die Device Encryption-Richtlinieneinstellung **Authentifizierung bei Start erforderlich** aktiviert ist und das System über ein TPM verfügt, dann lässt diese Richtlinieneinstellung den Systemschutz mit TPM zu und der Benutzer zusätzlich nach einer PIN gefragt.
Erweiterte PINs für Systemstart zulassen	-	Aktiviert	Diese Einstellung erlaubt die Verwendung von alphanumerischen PINs, um das Systemlaufwerk mit TPM zu schützen. Kann diese Einstellung nicht definiert werden, sind nur Ziffern erlaubt.
Pre-Boot-Wiederherstellungsmeldung und -URL konfigurieren	Option für die Pre-Boot-Wiederherstellungsmeldung auswählen	Standardwiederherstellungsmeldung und -URL verwenden	Dabei wird die Standardmeldung und -URL von Sophos verwendet.

Richtlinie	Einstellung	Wert von Sophos Central festgelegt	Anmerkung
Pre-Boot-Wiederherstellungsmeldung und -URL konfigurieren	Selbstdefinierte Meldung	Sie haben keinen Wiederherstellungsschlüssel? Wenden Sie sich an den IT-Helpdesk oder gehen Sie zu Ihrem Self Service Portal: `https://sophos.com/ssp`	
Pre-Boot-Wiederherstellungsmeldung und -URL konfigurieren	Benutzerdefinierte Wiederherstellungs-URL-Option		
Konfigurieren der Verwendung hardwarebasierter Verschlüsselung für Datenlaufwerke	-	Deaktiviert	Hierdurch wird softwarebasierte Verschlüsselung erzwungen. Wenn eine vorhandene BitLocker-Gruppenrichtlinieneinstellung hardwarebasierte Verschlüsselung vorschreibt, wird diese Richtlinieneinstellung nicht überschrieben.
Konfigurieren der Verwendung hardwarebasierter Verschlüsselung für Betriebssystemlaufwerke	-	Deaktiviert	Hierdurch wird softwarebasierte Verschlüsselung erzwungen. Wenn eine vorhandene BitLocker-Gruppenrichtlinieneinstellung hardwarebasierte Verschlüsselung vorschreibt, wird diese Richtlinieneinstellung nicht überschrieben.

- Verschlüsselungsalgorithmus: Sophos Central Device Encryption verwendet standardmäßig AES-256. Über eine Gruppenrichtlinie kann auch AES-128 ausgewählt werden.
- PIN/Kennwortanforderungen: Gruppenrichtlinien können dazu verwendet werden, um die Mindestlänge von PIN/Kennwort zu definieren und die Verwendung von komplexen Kennwörtern zu verlangen.
- Nur genutzte Festplattenbereiche verschlüsseln: Ist die Gruppenrichtlinie für Startvolumes und/oder Datenvolumes so definiert, dass alle Daten verschlüsselt werden, so hat diese Richtlinie Vorrang gegenüber der Sophos Central-Richtlinie, die nur die Verschlüsselung der genutzten Festplattenbereiche vorsieht.

Manche Gruppenrichtlinien können im Widerspruch zu Sophos Central stehen, so dass die Verschlüsselung nicht durchgeführt werden kann. In diesem Fall wird eine Ereignismeldung an Sophos Central gesendet.

- Smartcard erforderlich: Sieht eine Gruppenrichtlinie die Verwendung von BitLocker mit Smartcard vor, wird eine Fehlermeldung ausgegeben, da dies von Sophos Central nicht unterstützt wird.
- Nur genutzte Festplattenbereiche verschlüsseln: Ist die Gruppenrichtlinie für Startvolumes und/ oder Datenvolumes so definiert, dass nur genutzte Festplattenbereiche verschlüsselt werden, aber die Sophos Central-Richtlinie erfordert die Verschlüsselung aller Daten, wird eine Fehlermeldung ausgegeben.

Wenn Sie Tablet-Computer (wie zum Beispiel das MS Surface Pro) verschlüsseln und die Authentifizierung bei Start verwenden möchten, müssen Sie folgende Gruppenrichtlinie aktivieren:

Verwendung der BitLocker-Authentifizierung mit erforderlicher Tastatureingabe vor dem Starten auf Slates aktivieren

Weitere Informationen finden Sie im Support-Artikel 125772.

Für weitere allgemeine Informationen zu den Einstellungen für BitLocker- und TPM-Gruppenrichtlinien, siehe BitLocker-Gruppenrichtlinien und Trusted Platform Module Services Group Policy Settings.

Zugehörige Konzepte

Verschlüsselungsmethode und Berichte (Seite 11)
Volumes können mit Software-basierter oder Hardware-basierter Verschlüsselung verschlüsselt werden.

Verwandte Informationen

BitLocker-Gruppenrichtlinien

TPM-Gruppenrichtlinien

Support-Artikel 125772

2.7 Einschränkungen

Dynamische Datenträger

BitLocker unterstützt keine dynamischen Datenträger. Endpoints senden eine Ereignismeldung an Sophos Central um Sie darüber zu informieren, dass die Verschlüsselung fehlgeschlagen ist. Systemvolumes auf dynamischen Datenträgern können nicht verschlüsselt werden. Datenvolumes auf dynamischen Datenträgern werden ignoriert.

Remotedesktop

Wenn Sie über Remotedesktop einen Windows-Endpoint verwenden, auf dem die Sophos Central Agent Software installiert ist, werden keine Dialoge angezeigt und Device Encryption wird NICHT ausgeführt wenn eine Richtlinie zugewiesen wird. Die Aktivierung der Verschlüsselung würde zu mehrmaligem Neustart zur Verifizierung der Kompatibilität der Hardware führen. Der Benutzer müsste dann in der Lage sein, die PIN / Passphrase in der Pre-Boot-Umgebung einzugeben, was aber über Remotedesktop nicht möglich ist.

2.8 Verschlüsselungsmethode und Berichte

Volumes können mit Software-basierter oder Hardware-basierter Verschlüsselung verschlüsselt werden.

Device Encryption verwendet für neue Volumes immer Software-basierte Verschlüsselung, auch wenn das Laufwerk Hardware-basierte Verschlüsselung unterstützt.

Wenn ein Laufwerk bereits mit Hardware-basierter Verschlüsselung verschlüsselt ist, wird die Verschlüsselung nicht geändert.

Wenn eine vorhandene BitLocker-Gruppenrichtlinieneinstellung Hardware-basierte Verschlüsselung vorschreibt, wird dies nicht geändert.

Auf der Seite **Computer** können Sie Computer nach ihrem Verschlüsselungsstatus filtern, z. B. Computer mit einer bestimmten Verschlüsselungsmethode oder unverschlüsselte Computer.

Auf der Detailseite eines Computers werden die Verschlüsselungsmethode und der Algorithmus angezeigt, die für ein Volume verwendet werden.

Für Windows-Computer können Sie auch **Verschlüsselt seit** sehen. Welche Information angezeigt wird, hängt vom Gerät ab.

- Für Computer, die vorher mit Sophos Central Device Encryption verschlüsselt waren, werden Datum und Uhrzeit des Upgrades auf Sophos Central Device Encryption 2.1 angezeigt.
- Für Computer, die vorher mit einer anderen Verschlüsselungssoftware verschlüsselt waren, werden Datum und Uhrzeit der Installation von Sophos Central Device Encryption angezeigt.
- Für neue mit Sophos Central Device Encryption 2.1 (oder später) verschlüsselte Computer werden Datum und Uhrzeit der Verschlüsselung angezeigt.

Der Bericht **Verschlüsselungsstatus** zeigt den Verschlüsselungsstatus Ihrer Computer an.

Sie können sehen, welche Computer verschlüsselt sind, welche Volume-Typen verschlüsselt sind und welche Computer Ihre Verschlüsselungsrichtlinien erfüllen. Sie können auch herausfinden, wie sich Ihre Computer authentisieren und wie sie verschlüsselt sind.

Zugehörige Konzepte

BitLocker-Gruppenrichtlinien (Seite 8)
Sophos Central definiert einige Richtlinieneinstellungen automatisch, so dass Administratoren keine Vorbereitungen mehr für Device Encryption auf den Computern vornehmen müssen.

Computer
Computer-Übersicht

2.9 Entschlüsselung

Normalerweise ist keine Entschlüsselung nötig. Wenn Sie einen bereits verschlüsselten Endpoint von der Verschlüsselung ausnehmen wollen, müssen Sie zuerst alle seine Benutzer aus der Richtlinie entfernen und anschließend die Verschlüsselung ausschalten.

Klicken Sie am Endpoint im Windows Explorer mit der rechten Maustaste auf das Systemlaufwerk und wählen Sie **BitLocker verwalten**. Klicken Sie im Dialog **BitLocker-Laufwerkverschlüsselung** auf **BitLocker deaktivieren**. Nur ein Windows Administrator kann diese Aktion durchführen.

Wenn ein Benutzer mit Administratorrechten versucht, seine Festplatte manuell zu entschlüsseln während eine Verschlüsselungsrichtlinie aktiv ist, hebt Sophos Central den Befehl des Benutzers auf und die Festplatte bleibt verschlüsselt.

2.10 Wiederherstellen von Windows Endpoints

Wenn Benutzer ihre BitLocker-PIN oder ihr BitLocker-Kennwort vergessen, haben sie zwei Möglichkeiten, wieder Zugriff auf ihren Computer zu erlangen.

- Benutzer können das Sophos Self Service Portal aufrufen, siehe Wiederherstellungsschlüssel über das Self Service Portal abrufen. Windows 10 Benutzer sehen Anweisungen auf dem Bildschirm **BitLocker-Wiederherstellung**.
- Sie können Benutzern dabei helfen, wieder Zugriff auf ihren Computer zu erlangen. Im Folgenden erfahren Sie, was Benutzer sehen und wie sie vorgehen müssen. Benutzer müssen:

1. Den Computer neu starten und die **Esc**-Taste drücken, wenn der **BitLocker**-Anmeldebildschirm erscheint.
2. Auf dem Bildschirm **BitLocker-Wiederherstellung** wird die **Wiederherstellungsschlüssel-ID** angezeigt.
3. Den Administrator kontaktieren und die Wiederherstellungsschlüssel-ID nennen.
   Sie können nun dem Benutzer den Wiederherstellungsschlüssel mitteilen. Eine Anleitung, wie Sie Wiederherstellungsschlüssel für Ihre Benutzer abrufen, finden Sie in der Sophos Central Hilfe.
4. Der Benutzer muss den Wiederherstellungsschlüssel eingeben und dann den Anweisungen auf dem Bildschirm folgen, um eine neue PIN oder ein neues Kennwort zu erstellen.

   Auf Computern mit Windows 7 werden keine Anweisungen angezeigt. Benutzer müssen ihre PIN oder ihr Kennwort selbst zurücksetzen.

Benutzer haben nun wieder Zugriff auf ihren Computer. Normalerweise werden Datenvolumes automatisch entsperrt sobald Benutzer auf das Startvolume zugreifen können. Ist dies nicht der Fall, können Sie für Datenvolumes auf demselben Weg einen Wiederherstellungsschlüssel in Sophos Central abrufen wie für Startvolumes.

Zugehörige Aufgaben

Wiederherstellungsschlüssel über das Self Service Portal abrufen (Seite 22)
Wenn Benutzer sich nicht an ihrem Computer anmelden können (BitLocker PIN bzw. macOS Passwort vergessen), können sie das Sophos Self Service Portal verwenden, um einen Wiederherstellungsschlüssel abzurufen.

Verwandte Informationen

Self-Service-Portal
Sophos Central Admin Hilfe

3 Verwalten der FileVault-Verschlüsselung

Sophos Central Device Encryption für Mac verwaltet die FileVault Verschlüsselungsfunktion auf Ihren Macs.

Benutzer müssen nur ihr macOS Anmeldepasswort eingeben, um ihre Daten zu verschlüsseln oder darauf zuzugreifen.

3.1 Migration zu Sophos Central Device Encryption (Mac)

Wenn Sie Sophos Central verwenden möchten, um Mac Endpoints zu verwalten, die bereits mit FileVault verschlüsselt sind, müssen Sie diesen Endpoints eine Sophos Central Device Encryption Richtlinie zuweisen.

Hinweis
Wenn Sie FileVault mit SafeGuard Enterprise verwenden, müssen Sie zuerst die **Sophos SafeGuard Device Encryption** Software deinstallieren.

Voraussetzungen:

- Sie müssen die Sophos-Central-Agent-Software auf den Endpoints installieren.
- Sie müssen eine Device Encryption Richtlinie in Sophos Central konfigurieren und aktivieren.
- Benutzer müssen sich an ihren Endpoints anmelden. Sie müssen mit Sophos Central verbunden und synchronisiert werden. Beachten Sie, dass Remoteanmeldungen nicht unterstützt werden.

Im Folgenden erfahren Sie, was Benutzer sehen und wie sie vorgehen müssen:

1. Sobald sich Benutzer anmelden oder wenn Sie eine Sophos Central Device Encryption Richtlinie zuweisen während sie angemeldet sind, werden die Benutzer informiert, dass Device Encryption zum Schutz ihres Computers eingerichtet wurde.
2. Um Sophos Central Device Encryption zu aktivieren müssen Benutzer ihr Anmeldepasswort eingeben und auf **Schlüssel erstellen** klicken.
   Ein neuer Wiederherstellungsschlüssel wird erzeugt und zentral gespeichert. Sind weitere unverschlüsselte interne Festplatten vorhanden, werden diese ebenfalls verschlüsselt. Sie benötigen dafür kein eigenes Festplatten-Passwort.
3. Bei internen Festplatten, die bereits mit einem Festplatten-Passwort verschlüsselt sind, müssen Benutzer das Festplatten-Passwort eingeben und auf **Weiter** klicken.
   Das Festplatten-Passwort wird nun von Sophos Central verwaltet. Die Festplatte wird beim Starten automatisch entsperrt.

Der Endpoint wird nun von Sophos Central Device Encryption verwaltet.

3.2 Device Encryption Schritt für Schritt (Mac)

Führen Sie die folgenden Schritte aus, um Macs zu verschlüsseln.

Voraussetzungen:

- Sie müssen die Sophos-Central-Agent-Software auf den Endpoints installieren.
- Sie müssen eine Device Encryption Richtlinie in Sophos Central konfigurieren und aktivieren.
- Benutzer müssen sich an ihren Endpoints anmelden. Sie müssen mit Sophos Central verbunden und synchronisiert werden. Beachten Sie, dass Remoteanmeldungen nicht unterstützt werden.

Im Folgenden erfahren Sie, was Benutzer sehen und wie sie vorgehen müssen.

1. Ihren Mac starten und ihr Anmeldepasswort eingeben.

   Dadurch wird Sophos Device Encryption aktiviert.
2. Entweder auf **Verschlüsseln** klicken, um die Verschlüsselung des Systemlaufwerks zu starten, oder auf **Später durchführen** klicken, um den Vorgang später zu starten.

   Wenn Benutzer ihr Anmeldepasswort eingeben und auf **Verschlüsseln** klicken, wird der Wiederherstellungsschlüssel sowohl lokal im Schlüsselbund als auch in Sophos Central gespeichert.

   Alle vorhandenen Benutzer eines Endpunkts werden automatisch zu FileVault hinzugefügt.

   Auf Endpoints mit macOS 10.12 oder älter muss sich jeder Benutzer extra anmelden, um zu FileVault hinzugefügt zu werden.

Sobald die Systemfestplatte verschlüsselt ist, werden automatisch interne Datenvolumes verschlüsselt. Verschlüsselte Festplatten werden beim Starten des Computers automatisch entsperrt.

Mitteilungen informieren Benutzer über den Verschlüsselungsstatus der einzelnen Volumes.

3.2.1 Neue Benutzer zu FileVault hinzufügen

Wenn Benutzer nicht automatisch zu FileVault hinzugefügt werden, gehen Sie wie folgt vor.

Sie müssen:

1. Benutzer müssen ihr Anmeldepasswort eingeben und auf **Weiter** klicken.
   Normalerweise können Benutzer ihr macOS Anmeldepasswort verwenden, um ihren Mac zu starten und FileVault zu verwenden.
2. Ist noch kein Wiederherstellungsschlüssel in Sophos Central gespeichert, müssen neue Benutzer einen existierenden Benutzer auswählen, der diesen Vorgang autorisieren kann.
3. Der existierende FileVault-Benutzer muss dann sein Anmeldepasswort eingeben und auf **Weiter** klicken.

Neue Benutzer können jetzt ihr macOS Anmeldepasswort verwenden, um ihren Mac zu starten und FileVault zu verwenden.

3.3 Wiederherstellen von Mac Endpoints

Führen Sie die folgenden Schritte aus, um Macs wiederherzustellen.

Wenn Benutzer ihr Anmeldepasswort vergessen, haben sie mehrere Möglichkeiten, wieder Zugriff auf ihren Computer zu erlangen.

- Mit dem Sophos Self Service Portal kann ein Benutzer seinen Computer wiederherstellen, wenn er als letzter an diesem Computer angemeldet war, siehe Wiederherstellungsschlüssel über das Self Service Portal abrufen.
- Benutzer können ihren Computer mit einem externen Mac Startvolume starten und dann mit Terminal-Befehlen entsperren.

- Benutzer können ihren Computer im Festplattenmodus starten und dann mit Terminal-Befehlen entsperren.
- Benutzer können ihren Computer mit macOS-Wiederherstellung starten und dann mit Terminal-Befehlen entsperren.

  Für Informationen zum Arbeiten mit Terminalbefehlen finden, siehe Verschlüsselte HFS+ Volumes über Terminal-Befehle entsperren und Verschlüsselte APFS Volumes über Terminal-Befehle entsperren.

Sie können Benutzern helfen, wieder Zugriff auf ihre Daten zu erlangen. Im Folgenden erfahren Sie, was Benutzer sehen und wie sie vorgehen müssen. Benutzer müssen:

1. Den Computer einschalten und warten, bis die **Wiederherstellungsschlüssel-ID** angezeigt wird. Die Wiederherstellungsschlüssel-ID wird nur für wenige Minuten angezeigt. Um sie erneut anzuzeigen, müssen Benutzer ihren Computer neu starten.
2. Den Administrator kontaktieren und die Wiederherstellungsschlüssel-ID nennen.
   Sie können nun dem Benutzer den Wiederherstellungsschlüssel mitteilen. Eine Anleitung, wie Sie Wiederherstellungsschlüssel für Ihre Benutzer abrufen, finden Sie in der Sophos Central Hilfe.
3. Auf das Fragezeichen im Feld **Passwort** klicken.
   Eine Meldung wird angezeigt.
4. Auf das Pfeilsymbol neben der Meldung klicken, um zum Feld Wiederherstellungsschlüssel zu wechseln.
5. Geben Sie den Wiederherstellungsschlüssel ein.

   Für Benutzer, die aus Active Directory importiert wurden, müssen Sie zusätzlich folgende Schritte ausführen:

   - Setzen Sie das bestehende Kennwort in der Active Directory zurück. Generieren Sie anschließend ein vorläufiges Kennwort und geben Sie dieses an den Benutzer weiter.
   - Bitten Sie den Benutzer, im Dialogfeld **Passwort zurücksetzen** auf **Abbrechen** zu klicken und stattdessen das vorläufige Kennwort einzugeben.
6. Den Anweisungen auf dem Bildschirm folgen, um ein neues Passwort zu erzeugen.
7. Benutzer müssen auf **Neuen Anmeldeschlüsselbund erstellen** klicken, falls sie dazu aufgefordert werden.

Benutzer haben nun wieder Zugriff auf das Startvolume ihres Computers.

Auf Endpoints mit macOS 10.12 oder älter wird ein neuer Wiederherstellungsschlüssel generiert und in Sophos Central gespeichert. Ein Wiederherstellungsschlüssel kann nur einmal verwendet werden. Wenn Sie einen Computer später erneut entsperren müssen, müssen Sie einen neuen Wiederherstellungsschlüssel abrufen.

Auf Endpoints mit macOS 10.13 und Apple File System (APFS) wird kein neuer Wiederherstellungsschlüssel generiert. Der vorhandene Wiederherstellungsschlüssel bleibt gültig.

Zugehörige Aufgaben

Wiederherstellungsschlüssel über das Self Service Portal abrufen (Seite 22)
Wenn Benutzer sich nicht an ihrem Computer anmelden können (BitLocker PIN bzw. macOS Passwort vergessen), können sie das Sophos Self Service Portal verwenden, um einen Wiederherstellungsschlüssel abzurufen.

Verschlüsselte HFS+ Volumes über Terminal-Befehle entsperren (Seite 17)
Sie können Terminal-Befehle verwenden, um verschlüsselte Laufwerke zu entsperren. Die Befehle in diesem Abschnitt gelten für Endpoints mit macOS 10.12 oder älter und Volumes, die mit HFS+ formatiert sind.

Verschlüsselte APFS Volumes über Terminal-Befehle entsperren (Seite 17)

Sie können Terminal-Befehle verwenden, um verschlüsselte Laufwerke zu entsperren. Die Befehle in diesem Abschnitt gelten für Endpoints mit macOS 10.13 und Apple File System (APFS).

Verwandte Informationen

Informationen zu macOS-Wiederherstellung
So wählen Sie ein anderes Startlaufwerk aus
Sophos Central Admin Hilfe

3.3.1 Verschlüsselte HFS+ Volumes über Terminal-Befehle entsperren

Sie können Terminal-Befehle verwenden, um verschlüsselte Laufwerke zu entsperren. Die Befehle in diesem Abschnitt gelten für Endpoints mit macOS 10.12 oder älter und Volumes, die mit HFS+ formatiert sind.

Im Folgenden erfahren Sie, was Benutzer sehen und wie sie vorgehen müssen. Benutzer müssen:

1. Die **Terminal** App öffnen und den Befehl `diskutil corestorage list` ausführen.
   Eine Liste mit allen verbundenen Volumes wird angezeigt.
2. Nach dem Volume suchen, das wiederhergestellt werden soll (`LV Name`), und die `Logical Volume` Identifikationsnummer notieren.
3. Den Administrator kontaktieren, die `Logical Volume` Identifikationsnummer als Wiederherstellungsschlüssel-ID nennen und nach dem Wiederherstellungsschlüssel fragen.
   Sie können nun dem Benutzer den Wiederherstellungsschlüssel mitteilen. Eine Anleitung, wie Sie Wiederherstellungsschlüssel für Ihre Benutzer abrufen, finden Sie in der Sophos Central Hilfe.
4. Den Wiederherstellungsschlüssel eingeben, wenn Sie nach dem Passwort für die Festplatte gefragt werden.
   Alternativ können Sie den Befehl `diskutil corestorage unlockVolume` sowie den Wiederherstellungsschlüssel in der **Terminal**-Anwendung eingeben, um die Festplatte zu entsperren.

Benutzer können nun im Finder auf die Festplatte zugreifen.

Verwandte Informationen

Sophos Central Admin Hilfe

3.3.2 Verschlüsselte APFS Volumes über Terminal-Befehle entsperren

Sie können Terminal-Befehle verwenden, um verschlüsselte Laufwerke zu entsperren. Die Befehle in diesem Abschnitt gelten für Endpoints mit macOS 10.13 und Apple File System (APFS).

Im Folgenden erfahren Sie, was Benutzer sehen und wie sie vorgehen müssen. Benutzer müssen:

1. Die **Terminal** App öffnen und den Befehl `diskutil apfs list` ausführen.
   Eine Liste mit allen verbundenen Volumes wird angezeigt.
2. Nach dem Volume suchen, das wiederhergestellt werden soll, und die Volume Identifikation notieren, zum Beispiel `Volume disk1s1`.
3. Den Administrator kontaktieren und die Volume Identifikation als Wiederherstellungsschlüssel-ID nennen.
   Sie können nun dem Benutzer den Wiederherstellungsschlüssel mitteilen. Eine Anleitung, wie Sie Wiederherstellungsschlüssel für Ihre Benutzer abrufen, finden Sie in der Sophos Central Hilfe.

4. Den Wiederherstellungsschlüssel eingeben, wenn Sie nach dem Passwort für die Festplatte gefragt werden.
   Alternativ können Benutzer den Befehl `diskutil apfs unlockVolume` sowie den Wiederherstellungsschlüssel in der **Terminal**-Anwendung eingeben, um die Festplatte zu entsperren.

Benutzer können nun im Finder auf die Festplatte zugreifen.

Verwandte Informationen
Sophos Central Admin Hilfe

3.3.3 Fehler: Speichern des Wiederherstellungsschlüssels fehlgeschlagen

In seltenen Fällen kann das Speichern des Wiederherstellungsschlüssels (lokal im Schlüsselbund oder in Sophos Central) fehlschlagen.

Das bedeutet, dass der Computer nicht wiederhergestellt werden kann, wenn Benutzer ihr Passwort vergessen. Um diesem Risiko entgegenzuwirken, wird eine Meldung mit dem Wiederherstellungsschlüssel angezeigt und die Benutzer werden aufgefordert, den Wiederherstellungsschlüssel zu notieren.

Das System versucht laufend, den Wiederherstellungsschlüssel in Sophos Central zu speichern. Sobald dies gelungen ist, werden die Benutzer informiert, dass ein neuer Wiederherstellungsschlüssel nun von Sophos Central verwaltet wird und sie ihre Kopie des Wiederherstellungsschlüssels vernichten können.

3.4 Device Encryption Status (Mac)

Benutzer können die **Sophos Device Encryption** App verwenden, um Informationen zum Verschlüsselungsstatus zu erhalten. Sie befindet sich im Verzeichnis `Programme` und kann über Finder, Launchpad oder Spotlight aufgerufen werden.

Die **Sophos Device Encryption** App zeigt folgende Informationen an:

- Richtlinienstatus: Die erste Zeile gibt darüber Auskunft, ob der Endpoint von Sophos Device Encryption verwaltet wird.
- Benutzerstatus: Die zweite Zeile gibt darüber Auskunft, was Benutzer tun oder nicht tun können.
- Festplattenstatus: Eine Liste aller internen Festplatten wird angezeigt. Ist der Festplattenname ausgegraut, ist die Festplatte nicht gemountet. Ein Symbol neben dem Namen der Festplatte zeigt den Status der Festplatte an. Folgende Status stehen zur Verfügung:
  - Grün: Die Festplatte ist vollständig verschlüsselt und der Wiederherstellungsschlüssel ist zentral gespeichert.
  - Gelb: Das Volume ist vollständig verschlüsselt, aber der Wiederherstellungsschlüssel ist nicht in Sophos Central gespeichert. Das kann vorkommen, wenn Sophos Central gerade nicht erreichbar ist. Wenn keine Verschlüsselung der Festplatte erforderlich ist, existiert möglicherweise kein Wiederherstellungsschlüssel. Dies ist normalerweise der Fall, wenn die Festplatte nicht von Sophos Central Device Encryption verwaltet wird und sie mit Betriebssystem-Tools verschlüsselt wurde.
  - Gelb + Ausrufezeichen Die Festplatte ist vollständig verschlüsselt, es ist eine Richtlinie vorhanden, die die Verschlüsselung der Platte vorsieht, jedoch ist kein Wiederherstellungsschlüssel verfügbar.

- Rot: Die Festplatte ist nicht verschlüsselt, es ist jedoch eine Richtlinie vorhanden, die die Verschlüsselung der Platte vorsieht.
- Grau: Die Festplatte ist nicht verschlüsselt und es ist keine Richtlinie vorhanden, die die Verschlüsselung der Platte vorsieht.
- Statusleiste + **Verschlüsseln**: Die Festplatte wird gerade verschlüsselt.
- Statusleiste + **Entschlüsseln**: Die Festplatte wird gerade entschlüsselt.

Hinweis
Wenn ein Benutzer mit Administratorrechten auf einem Mac Endpoint versucht, seine Festplatte manuell zu entschlüsseln während eine Verschlüsselungsrichtlinie aktiv ist, kann Sophos Central dies nicht verhindern und die Festplatte wird entschlüsselt. Sobald die Entschlüsselung abgeschlossen ist wird der Benutzer aber nach seinem Passwort gefragt um FileVault zu aktivieren und die Festplatte wird wieder verschlüsselt.

- Verschlüsselungsstatus: Im unteren Bereich des Fensters wird angezeigt, ob für die Festplatten Wiederherstellungsschlüssel verfügbar sind.

Alternativ können Informationen zum Device Encryption Status über das Kommandozeilen-Tool abgerufen werden. Das Tool ist im Verzeichnis `/usr/local/bin/seadmin` installiert. Folgende Befehle stehen zur Verfügung:

- `help`: Zeigt eine Liste aller verfügbaren Befehle an.
- `status`: Zeigt die letzte Synchronisierung der Verschlüsselungssoftware sowie das Intervall, in dem die Synchronisierung gestartet wird, an.
- `--device-encryption`: Zeigt die aktuelle Verschlüsselungsrichtlinie sowie den Status hinsichtlich Verschlüsselung und Wiederherstellung aller internen Festplatten an.

4 Dateien für den sicheren Austausch mit Kennwort schützen

Sie können diese Funktion in einer **Device Encryption** Richtlinie aktivieren.

Hinweis
Diese Funktion ist erst ab Central Device Encryption 2.0 verfügbar. Diese Funktion ist nur für Windows verfügbar.

Sie können Dateien bis zu 50 MB schützen.

Rechtsklick-Kontextmenü aktivieren: Wenn Sie diese Option aktivieren, wird die Option **Kennwortgeschützte Datei erstellen** dem Rechtsklick-Menü hinzugefügt. Benutzer können kennwortgeschützte Dateien an E-Mails anhängen, wenn Sie vertrauliche Daten an Empfänger außerhalb des Unternehmensnetzwerks senden. Die Dateien werden in eine neue HTML-Datei mit verschlüsseltem Inhalt verpackt.

Empfänger können die Datei öffnen, indem Sie darauf doppelklicken und das Kennwort eingeben. Sie können die empfangene Datei zurücksenden und sie mit demselben oder einem neuen Kennwort schützen oder eine neue kennwortgeschützte Datei erstellen.

Outlook Add-in aktivieren: Diese Option fügt die Verschlüsselung von E-Mail-Anhängen zu Outlook hinzu. Benutzer können Anhänge schützen, indem Sie im Outlook-Menüband **Anhänge schützen** auswählen. Alle ungeschützten Anhänge werden in eine neue HTML-Datei mit verschlüsseltem Inhalt verpackt und die E-Mail wird versendet.

Immer fragen, wie mit angehängten Dateien umgegangen werden soll: Wenn Sie diese Option aktivieren, müssen Benutzer festlegen, wie Anhänge gesendet werden sollen, wenn die Nachricht welche enthält. Sie können die Nachricht kennwortgeschützt oder ungeschützt versenden.

Sie können ausgeschlossene Domänen eingeben, für die die Option **Immer fragen, wie mit angehängten Dateien umgegangen werden soll** nicht gilt (beispielsweise die Domäne Ihrer Organisation). Wenn Empfänger zu einer solchen Domäne gehören, werden die Absender nicht gefragt, wie sie mit Anhängen umgehen möchten.

Geben Sie nur vollständige Domänennamen ein und trennen Sie diese durch Kommas.

Verwandte Informationen
Device Encryption Richtlinie

5 Benutzer auffordern, Passwort/PIN zu ändern

Es gibt zwei Möglichkeiten, Benutzer zur Änderung ihres Kennworts aufzufordern.

Hinweis
Diese Option ist nur für Windows verfügbar.

- Mit der Option **Ein neues Authentifizierungskennwort/eine neue PIN vom Benutzern anfordern** in der Verschlüsselungsrichtlinie.

  Diese Option ist standardmäßig deaktiviert. Sie erzwingt eine Änderung des BitLocker-Kennworts oder der PIN nach der angegebenen Zeitspanne. Ein Ereignis wird protokolliert, wenn Benutzer ihr Kennwort oder ihre PIN ändern.

  Hinweis
  Diese Funktion ist erst ab Central Device Encryption 2.0 verfügbar.

- Verwenden Sie die Option **Änderung des Passworts/der PIN auslösen** Option auf dem Tab **Zusammenfassung** der Detailseite eines Computers.

  Mit dieser Option können Benutzer aufgefordert werden, ihr BitLocker-Kennwort oder ihre BitLocker-PIN sofort zu ändern. Eine Nachricht wird angezeigt, wenn die Aufforderung erfolgreich gesendet wurde.

Auf dem Endpunkt werden Benutzer aufgefordert, ein neues BitLocker-Kennwort oder eine neue BitLocker-PIN festzulegen. Wenn Benutzer den Dialog schließen, ohne ein neues Kennwort oder eine neue PIN einzugeben, wird der Dialog nach 30 Sekunden erneut angezeigt. Dies endet, wenn Sie ein Kennwort eingeben. Nachdem Benutzer den Dialog fünfmal geschlossen haben, ohne das Kennwort oder die PIN zu ändern, wird ein Warnhinweis protokolliert.

Verwandte Informationen
Device Encryption Richtlinie
Computer-Übersicht

6 Wiederherstellungsschlüssel über das Self Service Portal abrufen

Wenn Benutzer sich nicht an ihrem Computer anmelden können (BitLocker PIN bzw. macOS Passwort vergessen), können sie das Sophos Self Service Portal verwenden, um einen Wiederherstellungsschlüssel abzurufen.

Mit dem Wiederherstellungsschlüssel können sie wieder auf ihren Computer zugreifen.

Um Benutzern zu ermöglichen, ihre Computer selbst über das Self Service Portal wiederherzustellen, öffnen Sie **Sophos Central > Personen > Benutzer**, wählen Sie einen oder mehrere Benutzer und klicken Sie auf die Schaltfläche **E-Mail-Einrichtungslink**. Wählen Sie im folgenden Dialog **E-Mail Sophos Central Self-Service Welcome/Setup**, um Benutzern einen Aktivierungslink per E-Mail zu senden. Wenn Benutzer den Anweisungen in der E-Mail folgen, können sie das Sophos Self Service Portal verwenden, um ihren Computer wiederherzustellen.

Im Folgenden erfahren Sie, was Benutzer sehen und wie sie vorgehen müssen. Benutzer müssen:

1. Verwenden Sie einen anderen Computer und melden Sie sich am Sophos Self Service Portal an.
2. Öffnen Sie die Seite **Device Encryption**.
   Eine Liste aller Computer, an denen Sie angemeldet waren, wird angezeigt. Wenn sich in der Zwischenzeit jemand an Ihrem Computer angemeldet hat, ist die Wiederherstellung über das Self Service Portal nicht möglich.
3. Wählen Sie einen Computer aus der Liste und klicken Sie auf die Schaltfläche **Abrufen** in der Spalte **WIEDERHERSTELLUNGSSCHLÜSSEL**.
   Ein Dialog mit dem Wiederherstellungsschlüssel wird angezeigt.
4. Starten Sie Ihren eigenen Computer und wechseln Sie zur Recovery-Seite.
   - Windows: Drücken Sie die **Esc**-Taste, um zum Bildschirm **BitLocker-Wiederherstellung** zu wechseln.
   - Mac: Klicken Sie auf das Fragezeichen im Feld **Passwort** um zur FileVault Recovery-Seite zu wechseln.
5. Geben Sie den Wiederherstellungsschlüssel ein.

Benutzer haben nun wieder Zugriff auf ihren Computer.

Verwandte Informationen

Self-Service-Portal

7 Weiterführende Informationen

Windows

- FAQs: Support-Artikel 124819
- Häufig gestellte Fragen (FAQ) zu BitLocker
- BitLocker-Gruppenrichtlinien
- TPM-Grundlagen
- TPM-Gruppenrichtlinien
- Trusted Platform Module Administration Technical Overview

Mac

- FAQs: Support-Artikel 125982
- FileVault-Setup: Das Startvolume Ihres Mac mit FileVault verschlüsseln
- FileVault Recovery-Schlüssel: Legen Sie einen FileVault-Recovery-Schlüssel für Computer in Ihrer Organisation fest
- Kennwortzurücksetzung: Passwort eines macOS-Benutzeraccounts ändern oder zurücksetzen

Verwandte Informationen

Häufig gestellte Fragen (FAQ) zu BitLocker
BitLocker-Gruppenrichtlinien
TPM-Gruppenrichtlinien
TPM-Grundlagen
Trusted Platform Module Administration Technical Overview
Das Startvolume Ihres Mac mit FileVault verschlüsseln
Einen FileVault-Wiederherstellungsschlüssel für Computer in deiner Einrichtung festlegen
Passwort eines macOS-Benutzeraccounts ändern oder zurücksetzen
Support-Artikel 124819
Support-Artikel 125982

8 Unterstützte Web-Browser

Die folgenden Browser werden aktuell unterstützt:

- Microsoft Internet Explorer 11 und Microsoft Edge.
- Google Chrome.
- Mozilla Firefox.
- Apple Safari (nur Mac).

Wir empfehlen die Installation oder ein Upgrade auf eine der unterstützten Versionen aus der obigen Liste sowie die Verwendung einer stets aktuellen Version. Wir planen, die jeweils neueste und vorherige Version von Google Chrome, Mozilla Firefox und Apple Safari zu unterstützen. Wird ein nicht unterstützter Browser erkannt, werden Sie zu https://central.sophos.com/unsupported weitergeleitet.

Hinweis
Sophos Central Admin wird auf Mobilgeräten nicht unterstützt.

9 Weitere Hilfe

So erhalten Sie Hilfe vom Sophos Support:

1. Klicken Sie oben rechts auf der Benutzeroberfläche auf **Hilfe** und wählen Sie **Support-Ticket erstellen**.
2. Füllen Sie das Formular aus. Bitte seien Sie so genau wie möglich, sodass der Support Ihnen bestmöglich helfen kann.
3. Optional können Sie die Option wählen, den Support direkt auf Ihre Sophos Central-Sitzung zugreifen zu lassen. Der Support kann Ihnen dadurch noch besser helfen.
4. Klicken Sie auf **Senden**.

Sophos wird Sie innerhalb von 24 Stunden kontaktieren.

Hinweis
Wenn Sie die Option gewählt haben, dem Support Zugriff auf Ihre Sophos Central Sitzung zu geben, wird diese Funktion aktiviert, wenn Sie auf **Senden** klicken. Die Remote-Unterstützung wird nach 72 Stunden automatisch deaktiviert. Um sie früher zu deaktivieren, klicken Sie auf Ihren Kontonamen (oben rechts in der Benutzeroberfläche), wählen Sie **Kontoinformationen** und klicken Sie auf den Tab **Sophos Support**.

Feedback geben

So reichen Sie beim Sophos Support Feedback oder einen Vorschlag ein:

1. Klicken Sie oben rechts auf der Benutzeroberfläche auf **Hilfe** und wählen Sie **Feedback geben**.
2. Füllen Sie das Formular aus.
3. Klicken Sie auf **Senden**.

Zusätzliche Hilfe

Sie können den technischen Support auch folgendermaßen anfordern:

- Tauschen Sie sich in der Sophos Community unter community.sophos.com mit anderen Benutzern aus, die dasselbe Problem haben.
- Durchsuchen Sie die Wissensdatenbank des Sophos Support unter www.sophos.com/de-de/support.aspx.

10 Rechtliche Hinweise