Contents

- Information protection
  - BitLocker
    - Overview of BitLocker Device Encryption in Windows 10
    - BitLocker frequently asked questions (FAQ)
      - Overview and requirements
      - Upgrading
      - Deployment and administration
      - Key management
      - BitLocker To Go
      - Active Directory Domain Services
      - Security
      - BitLocker Network Unlock
      - General
    - Prepare your organization for BitLocker: Planning and policies
    - BitLocker basic deployment
    - BitLocker: How to deploy on Windows Server 2012 and later
    - BitLocker: Management for enterprises
    - BitLocker: How to enable Network Unlock
    - BitLocker: Use BitLocker Drive Encryption Tools to manage BitLocker
    - BitLocker: Use BitLocker Recovery Password Viewer
    - BitLocker Group Policy settings
    - BCD settings and BitLocker
    - BitLocker Recovery Guide
    - BitLocker Countermeasures
    - Protecting cluster shared volumes and storage area networks with BitLocker
    - Troubleshoot BitLocker
      - Troubleshoot BitLocker
      - BitLocker cannot encrypt a drive: known issues
      - Enforcing BitLocker policies by using Intune: known issues

BitLocker Network Unlock: known issues
BitLocker recovery: known issues
BitLocker configuration: known issues
Troubleshoot BitLocker and TPM issues
BitLocker cannot encrypt a drive: known TPM issues
BitLocker and TPM: other known issues
Decode Measured Boot logs to track PCR changes
Encrypted Hard Drive
Kernel DMA Protection for Thunderbolt™ 3
Protect your enterprise data using Windows Information Protection (WIP)
Create a WIP policy using Microsoft Intune
Create a WIP policy with MDM using the Azure portal for Microsoft Intune
Deploy your WIP policy using the Azure portal for Microsoft Intune
Associate and deploy a VPN policy for WIP using the Azure portal for Microsoft Intune
Create and verify an EFS Data Recovery Agent (DRA) certificate
Determine the Enterprise Context of an app running in WIP
Erstellen einer WIP-Richtlinie mit Microsoft Endpoint Configuration Manager
Erstellen und Bereitstellen einer WIP-Richtlinie mit Microsoft Endpoint Configuration Manager
Create and verify an EFS Data Recovery Agent (DRA) certificate
Determine the Enterprise Context of an app running in WIP
Mandatory tasks and settings required to turn on WIP
Testing scenarios for WIP
Limitations while using WIP
How to collect WIP audit event logs
General guidance and best practices for WIP
Enlightened apps for use with WIP
Unenlightened and enlightened app behavior while using WIP
Recommended Enterprise Cloud Resources and Neutral Resources network settings with WIP
Using Outlook Web Access with WIP
Fine-tune WIP Learning

How WIP works with sensitivity labels
Secure the Windows 10 boot process
Trusted Platform Module
Trusted Platform Module Overview
TPM fundamentals
How Windows 10 uses the TPM
TPM Group Policy settings
Back up the TPM recovery information to AD DS
View status, clear, or troubleshoot the TPM
Understanding PCR banks on TPM 2.0 devices
TPM recommendations

Informationsschutz

29.10.2019 • 2 minutes to read

Weitere Informationen zum Sichern von Dokumenten und anderen Daten in Ihrer Organisation.

ABSCHNITT	BESCHREIBUNG
BitLocker	Bietet Informationen zu BitLocker, einem Datenschutzfeature, das in das Betriebssystem integriert ist und die Bedrohungen durch Datendiebstahl oder Gefährdung durch verloren gegangene, gestohlene oder unangemessen deaktivierte Computer behandelt.
Verschlüsselte Festplatte	Verschlüsselte Festplatten verwenden die schnelle Verschlüsselung, die von der BitLocker-Laufwerkverschlüsselung bereitgestellt wird, um die Datensicherheit und-Verwaltung zu verbessern.
Kernel-DMA-Schutz für Thunderbolt™ 3	Der Kernel-DMA-Schutz schützt PCs vor Drive-through-DMA-Attacken (Direct Memory Access) mit PCI-HotPlug-Geräten, die mit Thunderbolt™ 3-Ports verbunden sind.
Schützen Ihrer Unternehmensdaten mit Windows Information Protection (WIP)	Bietet Informationen dazu, wie Sie eine Windows-Informationsschutz Richtlinie erstellen, die den Schutz vor potenziellen Unternehmensdaten Verlusten gewährleisten kann.
Sichern des Startvorgangs von Windows10	Windows 10 unterstützt Features, mit denen verhindert wird, dass Rootkits und Bootkits während des Startvorgangs geladen werden.
Trusted Platform Module	Die TPM-Technologie stellt hardwarebasierte, sicherheitsbezogene Funktionen bereit. Ein TPM-Chip ist ein sicherer Krypto-Prozessor, der Sie u.a. beim Erstellen und Speichern kryptografischer Schlüssel sowie beim Beschränken der Nutzung kryptografischer Schlüssel unterstützt.

BitLocker

06.03.2020 • 6 minutes to read

Betriff:

- Windows 10

Dieses Thema enthält eine grobe Übersicht über BitLocker, einschließlich einer Liste der Systemanforderungen, praktischer Anwendungen und veralteter Features.

Übersicht über BitLocker

Die BitLocker-Laufwerksverschlüsselung ist ein in das Betriebssystem integriertes Feature, das Daten vor Bedrohungen durch Datendiebstahl oder durch Offenlegung verlorener, gestohlener oder nicht ordnungsgemäß außer Betrieb gesetzter Computer schützt.

BitLocker bietet den größten Schutz bei Verwendung mit einem Trusted Platform Module (TPM) 1.2 oder höher. Das TPM ist eine Hardwarekomponente, die von vielen Computerherstellern auf vielen neueren Computern installiert wird. Es dient In Kombination mit BitLocker zum Schutz der Benutzerdaten und um sicherzustellen, dass ein Computer nicht manipuliert wurde, während das System offline geschaltet war.

Auf Computern ohne TPM-Version 1.2 oder höher können Sie BitLocker dennoch verwenden, um das Windows-Betriebssystemlaufwerk zu verschlüsseln. Allerdings muss der Benutzer für diese Implementierung einen USB-Systemstartschlüssel zum Starten des Computers oder Fortsetzen aus dem Ruhezustand einsetzen. Ab Windows 8 können Sie ein Betriebssystem-Volumekennwort verwenden, um das Betriebssystemvolume auf einem Computer ohne TPM zu schützen. Beide Optionen bieten nicht die Systemintegritätsprüfung vor dem Start, die BitLocker mit einem TPM anbietet.

Zusätzlich zu den TPM bietet BitLocker die Möglichkeit, den normalen Startvorgang zu sperren, bis der Benutzer eine persönliche Identifikationsnummer (PIN) angibt oder ein Wechselmedium einführt, z. B. einen USB-Speicherstick, der einen Systemstartschlüssel enthält. Diese zusätzlichen Sicherheitsmaßnahmen bieten eine mehrstufige Authentifizierung und sorgen dafür, dass der Computer nicht startet oder den Betrieb aus dem Ruhezustand fortsetzt, bis die richtige PIN oder ein Systemstartschlüssel bereitgestellt wird.

Praktische Anwendungsfälle

Daten auf einem verloren gegangenen oder gestohlenen Computer sind anfällig für nicht autorisierte Zugriffe durch das Ausführen eines Softwareangriffstools oder die Übertragung der Festplatte des Computers auf einen anderen Computer. BitLocker verringert das Risiko durch nicht autorisierten Datenzugriff, indem der Datei- und Computerschutz verbessert wird. BitLocker hilft auch dabei, den Zugriff auf Daten zu verhindern, wenn mit BitLocker geschützte Computer außer Betrieb genommen oder wiederverwendet werden.

Es gibt zwei zusätzliche Tools in den Remoteserver-Verwaltungstools, die Sie zum Verwalten von BitLocker verwenden können.

- **BitLocker-Wiederherstellungskennwort-Viewer**. Mit dem BitLocker-Wiederherstellungskennwort-Viewer können Sie die BitLocker-Laufwerksverschlüsselungswiederherstellungskennwörter auffinden und anzeigen, die in den Active Directory-Domänendiensten (AD DS) gesichert wurden. Sie können mit diesem Tool Daten wiederherstellen, die auf einem Laufwerk gespeichert sind, das mit BitLocker verschlüsselt wurde. Der BitLocker-Wiederherstellungskennwort-Viewer ist eine Erweiterung für Active Directory-Benutzer und das MMC-Snap-In. Mit diesem Tool können Sie das Dialogfeld **Eigenschaften** eines Computerobjekts überprüfen, um die entsprechenden BitLocker-Wiederherstellungskennwörter

anzuzeigen. Darüber hinaus können Sie mit der rechten Maustaste auf einen Domänencontainer klicken und dann über alle Domänen in der Active Directory-Gesamtstruktur hinweg nach einem BitLocker-Wiederherstellungskennwort suchen. Zum Anzeigen von Wiederherstellungskennwörtern müssen Sie ein Domänenadministrator sein oder von einem Domänenadministrator entsprechende Berechtigungen delegiert bekommen.

- **Tools zur BitLocker-Laufwerkverschlüsselung**. BitLocker-Laufwerksverschlüsselungstools umfassen die Befehlszeilentools manage-bde und repair-bde sowie die BitLocker-Cmdlets für Windows PowerShell. Sowohl manage-bde als auch die BitLocker-Cmdlets können zum Ausführen von Aufgaben verwendet werden, die über die BitLocker-Systemsteuerung ausgeführt werden können und sie sind für automatisierte Bereitstellungen und andere Scripting-Szenarien geeignet. Repair-bde wird für Notfallwiederherstellungsszenarien bereitgestellt, in denen ein durch BitLocker geschütztes Laufwerk nicht normal oder mithilfe der Wiederherstellungskonsole entsperrt werden kann.

Neue und geänderte Funktionalität

Informationen zu den Neuerungen in BitLocker für Windows10, wie die Unterstützung des XTS-AES-Verschlüsselungsalgorithmus, finden Sie im Abschnitt BitLocker unter "Neuerungen in Windows 10".

Systemanforderungen

BitLocker hat die folgenden Hardwareanforderungen:

Damit BitLocker die Systemintegritätsprüfung verwendet, die von einem Trusted Platform Module (TPM) bereitgestellt wird, muss der Computer über TPM 1.2 oder höher verfügen. Wenn Ihr Computer nicht über ein TPM verfügt, ist es für die Aktivierung von Bitlocker erforderlich, dass Sie einen Systemstartschlüssel auf einem Wechselmedium speichern, z. B. einem USB-Flashlaufwerk.

Ein Computer mit einem TPM muss außerdem eine Trusted Computing Group (TCG)-kompatible BIOS und UEFI-Firmware besitzen. Die BIOS- oder UEFI-Firmware stellt eine Vertrauenskette für vor dem Betriebssystemstart her, und die Unterstützung für TCG-spezifische Static Root of Trust Measurement TCG umfassen. Bei einem Computer ohne TPM ist keine TCG-konforme Firmware erforderlich.

Die System-BIOS- oder UEFI-Firmware (für Computer mit und ohne TPM) muss die Geräteklasse für USB-Massenspeicher unterstützen, einschließlich des Lesens kleiner Dateien auf einem USB-Speicherstick in der Vorabbetriebssystemumgebung.

> **IMPORTANT**
>
> Unter Windows 7 können Sie ein Betriebssystemlaufwerk ohne TPM und USB-Flashlaufwerk verschlüsseln. Dieses Verfahren finden Sie unter Tipp des Tages: BitLocker ohne TPM oder USB.

> **NOTE**
>
> TPM 2,0 wird im Legacy-und CSM-Modus des BIOS nicht unterstützt. Bei Geräten mit TPM 2,0 muss der BIOS-Modus nur als systemeigener UEFI konfiguriert sein. Die Optionen für Legacy-und Kompatibilitäts Unterstützungs Module (CSM) müssen deaktiviert sein. Für zusätzliche Sicherheit aktivieren Sie das Feature für sicheres Booten.
>
> Das installierte Betriebs System auf der Hardware im Legacy Modus verhindert das Booten des Betriebssystems, wenn der BIOS-Modus in UEFI geändert wird. Verwenden Sie das Tool MBR2GPT , bevor Sie den BIOS-Modus ändern, der das Betriebssystem und den Datenträger zur Unterstützung von UEFI vorbereitet.

Die Festplatte muss mit mindestens zwei Laufwerken partitioniert werden:

- Das Betriebssystemlaufwerk (oder Startlaufwerk) enthält das Betriebssystem und unterstützende Dateien. Es

muss mit dem NTFS-Dateisystem formatiert sein.

- Das Systemlaufwerk enthält die Dateien, die benötigt werden, um Windows zu laden, nachdem die Firmware die Systemhardware vorbereitet hat. BitLocker ist auf diesem Laufwerk nicht aktiviert. Damit BitLocker funktioniert, darf das Systemlaufwerk nicht verschlüsselt sein, muss vom Betriebssystemlaufwerk abweichen und auf Computern mit dem FAT32-Dateisystem formatiert sein, die UEFI-basierte Firmware verwenden oder auf Computern mit dem NTFS-Dateisystem formatiert sein, die BIOS-Firmware verwenden. Wir empfehlen, dass das Systemlaufwerk ungefähr 350 MB groß ist. Nachdem BitLocker aktiviert ist, sollten etwa 250 MB Speicherplatz frei sein.

Bei der Installation auf einem neuen Computer erstellt Windows die Partitionen automatisch, die für BitLocker erforderlich sind.

Bei der Installation der optionalen BitLocker-Komponente auf einem Server müssen Sie außerdem das Feature „Erweitertes Speichern" installieren, das für die Unterstützung hardwareverschlüsselter Laufwerke verwendet wird.

Inhalt dieses Abschnitts

THEMA	BESCHREIBUNG
Übersicht über die BitLocker-Geräteverschlüsselung in Windows10	Dieses Thema für IT-Spezialisten bietet eine Übersicht über die verschiedenen Möglichkeiten, mit denen Daten auf Geräten unter Windows10 mit BitLocker-Geräteverschlüsselung geschützt werden können.
Häufig gestellte Fragen (Frequently Asked Questions, FAQ) zu BitLocker	In diesem Thema für IT-Spezialisten werden häufig gestellte Fragen zu den Anforderungen für die Verwendung, Aktualisierung, Bereitstellung und Verwaltung von BitLocker sowie zu den Schlüsselverwaltungsrichtlinien für BitLocker beantwortet.
Vorbereiten Ihrer Organisation auf BitLocker: Planung und Richtlinien	In diesem Thema, das sich an IT-Experten richtet, wird erläutert, wie Sie Ihre BitLocker-Bereitstellung planen können.
Grundlegende Bereitstellung von BitLocker	Dieses Thema richtet sich an IT-Experten und beschreibt die Verwendung von BitLocker-Features für den Schutz Ihrer Daten mithilfe von Laufwerkverschlüsselung.
BitLocker: Bereitstellen unter Windows Server	In diesem Thema für IT-Experten wird erläutert, wie BitLocker auf Windows Server bereitgestellt wird.
BitLocker: Aktivieren der Netzwerkentsperrung	In diesem Thema für IT-Experten wird beschrieben, wie die BitLocker-Netzwerkentsperrung funktioniert und konfiguriert wird.
BitLocker: Verwenden von BitLocker-Laufwerksverschlüsselungstools zum Verwalten von BitLocker	In diesem Thema für IT-Spezialisten werden die Tools zum Verwalten von BitLocker beschrieben.
BitLocker: Verwenden des BitLocker-Wiederherstellungskennwort-Viewers	In diesem Thema für IT-Experten wird beschrieben, wie der BitLocker-Wiederherstellungskennwort-Viewer verwendet wird.
BitLocker-Gruppenrichtlinieneinstellungen	In diesem Thema für IT-Experten werden die Funktion, Position und der Effekt der einzelnen Gruppenrichtlinieneinstellungen zum Verwalten von BitLocker beschrieben.

THEMA	BESCHREIBUNG
BCD-Einstellungen und BitLocker	Dieses Thema für IT-Experten beschreibt die BCD-Einstellungen, die von BitLocker verwendet werden.
BitLocker-Wiederherstellungsleitfaden	In diesem Thema für IT-Experten wird beschrieben, wie BitLocker-Schlüssel aus AD DS wiederhergestellt werden.
Schützen von BitLocker vor Angriffen vor dem Start	Dieser detaillierte Leitfaden hilft Ihnen, die Umstände zu verstehen, unter denen die Verwendung der Pre-Boot-Authentifizierung für Geräte mit Windows10, Windows 8,1, Windows 8 oder Windows 7 empfohlen wird. und wenn Sie sicher von der Konfiguration eines Geräts weggelassen werden kann.
Problembehandlung für BitLocker	In diesem Leitfaden werden die Ressourcen beschrieben, die Ihnen bei der Behandlung von BitLocker-Problemen helfen können, und es werden Lösungen für verschiedene häufige BitLocker-Probleme bereitgestellt.
Schützen freigegebener Clustervolumes und SANs (Storage Area Networks) mit BitLocker	In diesem Thema für IT-Experten wird beschrieben, wie der Schutz von CSVs (Cluster Shared Volumes, freigegebene Clustervolumes) und SANs mit BitLocker erfolgt.
Sicherer Start und BitLocker-Geräteverschlüsselung unter Windows10 IoT Core aktivieren	In diesem Thema wird erläutert, wie Sie BitLocker mit Windows10 IoT Core verwenden

Übersicht über die BitLocker-Geräteverschlüsselung in Windows10

06.03.2020 • 12 minutes to read

Betriff:

- Windows 10

In diesem Thema wird erläutert, wie Sie mithilfe der BitLocker-Geräteverschlüsselung Daten auf Geräten mit Windows 10 schützen können. Eine allgemeine Übersicht und eine Liste der Themen zu BitLocker finden Sie unter BitLocker.

Wenn Benutzer unterwegs sind, haben sie die vertrauliche Daten ihrer Organisation dabei. Wenn vertrauliche Daten gespeichert werden, müssen sie vor unbefugtem Zugriff geschützt werden. Windows stellt bereits seit langem Lösungen zum Schutz von gespeicherten Daten bereit, die Schutz vor böswilligen Angriffen bieten; den Anfang stellte das verschlüsselnde Dateisystem (EFS) unter Windows 2000 dar. In letzter Zeit hat BitLocker Verschlüsselung für vollständige Laufwerke und tragbare Laufwerke bereitgestellt. Windows verbessert den Datenschutz konsistent, indem vorhandene Optionen verbessert und neue Strategien bereitgestellt werden.

In Tabelle 2 sind bestimmte Aspekte des Datenschutzes und ihre Adressierung in Windows10 und Windows7 aufgeführt.

Tabelle 2 Datenschutz in Windows10 und Windows7

WINDOWS7	WINDOWS 10
Wenn BitLocker mit einer PIN zum Schutz beim Systemstart verwendet wird, können PCs wie z. B. Kioske nicht remote neu gestartet werden.	Moderne Windows-Geräte werden zunehmend durch die BitLocker-Geräteverschlüsselung geschützt und unterstützen SSO, um die BitLocker-Verschlüsselungsschlüssel nahtlos vor Kaltstart-Angriffen zu schützen. Die Netzwerkentsperrung ermöglicht das automatische Starten von PCs, wenn diese mit dem internen Netzwerk verbunden sind.
Wenn BitLocker aktiviert ist, kann der Bereitstellungsprozess mehrere Stunden dauern.	Die Vorabbereitstellung von BitLocker, das Verschlüsseln von Festplatten und die auf den verwendeten Speicherplatz begrenzte Verschlüsselung ermöglichen Administratoren das schnelle Aktivieren von BitLocker auf neuen Computern.
Die Verwendung von BitLocker mit selbst verschlüsselnden Laufwerken (Self-Encrypting Drives, SEDs) wird nicht unterstützt.	BitLocker unterstützt das Auslagern von Verschlüsselungsvorgängen an verschlüsselte Festplatten.
Administratoren müssen separate Tools zum Verwalten von verschlüsselten Festplatten verwenden.	BitLocker unterstützt verschlüsselte Festplatten mit integrierter Verschlüsselungshardware, sodass Administratoren sie mithilfe der bekannten BitLocker-Verwaltungstools verwalten können.
Das Verschlüsseln eines neuen Flashlaufwerks kann länger als 20 Minuten dauern.	Die nur in BitLocker To Go verwendete Speicherplatz Verschlüsselung ermöglicht es Benutzern, Wechseldatenträger in Sekunden zu verschlüsseln.

WINDOWS7	WINDOWS 10
BitLocker kann Benutzer zur Eingabe eines Wiederherstellungsschlüssels auffordern, wenn die Systemkonfiguration geändert wird.	BitLocker fordert den Benutzer nur bei einer Datenträgerbeschädigung oder bei einem Verlust der PIN bzw. des Kennworts zur Eingabe eines Wiederherstellungsschlüssels auf.
Benutzer müssen zum Starten des PCs eine PIN und dann ihr Kennwort zum Anmelden bei Windows eingeben.	Moderne Windows-Geräte werden zunehmend durch die BitLocker-Geräteverschlüsselung geschützt und unterstützen SSO, um die BitLocker-Verschlüsselungsschlüssel vor Kaltstart-Angriffen zu schützen.

Vorbereitung der Laufwerk- und Dateiverschlüsselung

Die besten Sicherheitsmaßnahmen sind für den Benutzer während der Implementierung und Verwendung transparent. Bei jeder möglichen Verzögerung oder Schwierigkeit aufgrund einer Sicherheitsfunktion ist es sehr wahrscheinlich, dass Benutzer versuchen, die Sicherheit zu umgehen. Dies gilt insbesondere für den Datenschutz, und solche Situationen müssen von Unternehmen vermieden werden. Ganz gleich, ob Sie ganze Volumes, Wechselmedien oder einzelne Dateien verschlüsseln möchten: Windows10 erfüllt Ihre Anforderungen, indem es optimierte, nutzbare Lösungen bereitstellt. Tatsächlich können Sie bereits im Voraus mehrere Schritte zur Vorbereitung der Datenverschlüsselung durchführen, um eine schnelle und reibungslose Bereitstellung sicherzustellen.

Vorabbereitstellung von TPM

In Windows7 bot das Vorbereiten des TPM für die Verwendung einige Herausforderungen:

- Sie können das TPM im BIOS aktivieren. Dazu muss es entweder in den BIOS-Einstellungen aktiviert werden oder es muss ein Treiber zur Aktivierung innerhalb von Windows installiert werden.
- Bei der Aktivierung des TPM sind u.U. mehrere Neustarts erforderlich.

Einfach ausgedrückt: Der Aufwand war hoch. Bei der Bereitstellung neuer PCs kann dies alles von IT-Mitarbeitern übernommen werden. Wenn Sie BitLocker jedoch auf Geräten hinzufügen möchten, die bereits von Benutzern verwendet werden, hätten diese Benutzer mit den technischen Problemen zu kämpfen und würden entweder Hilfe von der IT-Abteilung anfordern oder BitLocker einfach deaktiviert lassen.

Microsoft umfasst die Instrumentation in Windows10, die es dem Betriebssystem ermöglicht, das TPM vollständig zu verwalten. Das Aufrufen des BIOS ist nicht mehr erforderlich, und alle Szenarien, die einen Neustart erfordern, wurden entfernt.

Bereitstellung von Festplattenverschlüsselung

BitLocker kann gesamte Festplatten verschlüsseln, darunter System- sowie Datenlaufwerke. Die Vorabbereitstellung von BitLocker kann die benötigte Zeit für die Bereitstellung neuer PCs mit BitLocker-Aktivierung erheblich reduzieren. Mit Windows10 können Administratoren BitLocker und das TPM in der Windows-Vorinstallationsumgebung aktivieren, bevor Sie Windows installieren, oder als Teil einer automatisierten Bereitstellungstasksequenz ohne Benutzerinteraktion. In Kombination mit der Verschlüsselungsoption „Nur verwendeten Speicherplatz verschlüsseln“ und einem fast leeren Laufwerk (da Windows noch nicht installiert ist) dauert die Aktivierung von BitLocker nur wenige Sekunden. In früheren Versionen von Windows mussten Administratoren BitLocker nach der Installation von Windows aktivieren. Obwohl dieser Prozess automatisiert werden konnte, musste BitLocker das gesamte Laufwerk verschlüsseln. Dieser Prozess nahm je nach Laufwerkgröße und -leistung mehrere Stunden bis zu über einen Tag in Anspruch und hat die Bereitstellung erheblich verzögert. Microsoft hat diesen Prozess durch mehrere Features in Windows10 verbessert.

BitLocker-Geräteverschlüsselung

Ab Windows 8.1 aktiviert Windows automatisch die BitLocker-Geräteverschlüsselung auf Geräten, die den modernen Standbymodus unterstützen. Mit Windows10 bietet Microsoft Unterstützung für BitLocker-Geräteverschlüsselung auf einem weitaus breiteren Bereich von Geräten, einschließlich der modernen Standbymodus, und Geräten, auf denen Windows 10 Home Edition ausgeführt wird.

Microsoft geht davon aus, dass die meisten Geräte in Zukunft die Testanforderungen bestehen, wodurch die BitLocker-Geräteverschlüsselung auf modernen Windows-Geräten allgegenwärtig ist. Die BitLocker-Geräteverschlüsselung schützt das System weiter, indem die Geräte weite Datenverschlüsselung transparent implementiert wird.

Im Gegensatz zu einer BitLocker-Standardimplementierung wird die BitLocker-Geräteverschlüsselung automatisch aktiviert, sodass das Gerät immer geschützt ist. In der folgenden Liste wird die Funktionsweise beschrieben:

- Wenn eine Neuinstallation von Windows10 abgeschlossen ist und die Out-of-Box-Erfahrung abgeschlossen ist, ist der Computer für die erste Verwendung vorbereitet. Im Rahmen dieser Vorbereitung wird die BitLocker-Geräteverschlüsselung auf dem Betriebssystemlaufwerk initialisiert und die Datenlaufwerke auf dem Computer mit einem leeren Schlüssel festgelegt (Dies entspricht dem standardmäßigen BitLocker-Status angehalten). In diesem Zustand wird das Laufwerk mit einem Warnungssymbol in Windows-Explorer angezeigt. Das gelbe Warnungssymbol wird entfernt, nachdem die TPM-Beschützer erstellt und der Wiederherstellungsschlüssel gesichert wurde, wie in den folgenden Aufzählungspunkten erläutert.
- Wenn das Gerät keiner Domäne angehört, ist ein Microsoft-Konto erforderlich, das über Administratorrechte auf dem Gerät verfügt. Wenn der Administrator ein Microsoft-Konto zur Anmeldung verwendet, wird der unverschlüsselte Schlüssel entfernt, ein Wiederherstellungsschlüssel wird in das Microsoft-Onlinekonto hochgeladen, und eine TPM-Schutzvorrichtung wird erstellt. Sollte ein Gerät einen Wiederherstellungsschlüssel benötigen, wird der Benutzer zunächst zur Nutzung eines anderen Geräts aufgefordert und navigiert dann zu einer Zugriffs-URL, von der er mithilfe seiner Anmeldeinformationen für das Microsoft-Konto den Wiederherstellungsschlüssel abrufen kann.
- Wenn der Benutzer sich mit einem Domänenkonto anmeldet, wird der unverschlüsselte Schlüssel erst dann entfernt, wenn der Benutzer das Gerät einer Domäne hinzufügt und der Wiederherstellungsschlüssel erfolgreich in den Active Directory-Domänendiensten (AD DS) gesichert ist. Die Gruppenrichtlinieneinstellung **Computerkonfiguration\Administrative Vorlagen\Windows-Komponenten\BitLocker-Laufwerkverschlüsselung\Betriebssystemlaufwerke** muss aktiviert sein, und die Option **BitLocker erst aktivieren, nachdem Wiederherstellungsinformationen für Betriebssystemlaufwerke in AD DS gespeichert wurden** muss ausgewählt sein. Mit dieser Konfiguration wird das Wiederherstellungskennwort automatisch erstellt, wenn der Computer der Domäne beitritt, und anschließend wird der Wiederherstellungsschlüssel in ADDS gesichert, die TPM-Schutzvorrichtung wird erstellt, und der unverschlüsselte Schlüssel wird entfernt.
- Ähnlich wie bei der Anmeldung mit einem Domänenkonto wird der unverschlüsselte Schlüssel entfernt, wenn sich der Benutzer auf dem Gerät bei einem Azure AD-Konto anmeldet. Wie im vorhergehenden Punkt beschrieben, wird das Wiederherstellungskennwort automatisch erstellt, wenn der Benutzer sich bei Azure AD authentifiziert. Anschließend wird der Wiederherstellungsschlüssel in Azure AD gesichert, die TPM-Schutzvorrichtung wird erstellt, und der unverschlüsselte Schlüssel wird entfernt.

Microsoft empfiehlt, die BitLocker-Geräteverschlüsselung auf allen Systemen zu aktivieren, die Sie unterstützen, aber der automatische BitLocker-Geräte Verschlüsselungsprozess kann durch Ändern der folgenden Registrierungseinstellung verhindert werden:

- **Unterschlüssel**: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\BitLocker
- **Wert**: PreventDeviceEncryption equal to True (1)
- **Typ**: REG_DWORD

Administratoren können Domänen verbundene Geräte verwalten, deren BitLocker-Geräteverschlüsselung über die Microsoft BitLocker-Verwaltung und-Überwachung (MBAM) aktiviert ist. In diesem Fall stellt die BitLocker-

Geräteverschlüsselung automatisch zusätzliche BitLocker-Optionen zur Verfügung. Eine Konvertierung oder Verschlüsselung ist nicht erforderlich, und MBAM kann den gesamten BitLocker-Richtliniensatz verwalten, wenn Konfigurationsänderungen erforderlich sind.

Verschlüsselungsoption „Nur verwendeten Speicherplatz verschlüsseln“

In früheren Windows-Versionen konnte das Verschlüsseln eines Laufwerks durch BitLocker viel Zeit in Anspruch nehmen, da jedes Byte auf dem Volume (einschließlich der Teile, die Daten enthalten) verschlüsselt wurde. Dies ist nach wie vor die sicherste Methode zum Verschlüsseln eines Laufwerks, insbesondere dann, wenn ein Laufwerk zuvor vertrauliche Daten enthalten hat, die seither verschoben oder gelöscht wurden. In diesem Fall können Spuren der vertraulichen Daten auf Teilen des Laufwerks verbleiben, die als nicht verwendet gekennzeichnet sind. Aber warum ein neues Laufwerk verschlüsseln, wenn man einfach die Daten beim Schreiben verschlüsseln kann? Um die Verschlüsselungs Zeit zu verringern, ermöglicht BitLocker in Windows10 Benutzern, nur Ihre Daten zu verschlüsseln. Je nach der Datenmenge auf dem Laufwerk kann diese Option die Verschlüsselungszeit um mehr als 99 % reduzieren. Seien Sie jedoch vorsichtig bei der auf den verwendeten Speicherplatz begrenzten Verschlüsselung auf einem vorhandenen Volume, auf dem u. U. bereits vertrauliche Daten in unverschlüsseltem Zustand gespeichert wurden, da diese Sektoren mithilfe von Tools zur Datenträgerwiederherstellung wiederhergestellt werden können, bis sie mit neuen verschlüsselten Daten überschrieben werden. Allerdings kann die Begrenzung der Verschlüsselung auf verwendeten Speicherplatz auf einem völlig neuen Volume die Bereitstellungszeit ohne Sicherheitsrisiko erheblich verringern, da sämtliche neue Daten beim Schreiben auf den Datenträger verschlüsselt werden.

Unterstützung für verschlüsselte Festplatten

Selbst verschlüsselnde Laufwerke (SEDs) sind bereits seit mehreren Jahren verfügbar, Microsoft konnte die Verwendung unter einigen früheren Windows-Versionen jedoch nicht unterstützen, da den Laufwerken wichtige Schlüsselverwaltungsfunktionen fehlten. Microsoft hat mit Speicherhersteller an einer Verbesserung der Hardwarefunktionen zusammengearbeitet, und BitLocker unterstützt jetzt die nächste Generation von SEDs, die als verschlüsselte Festplatten bezeichnet werden. Verschlüsselte Festplatten bieten integrierte kryptografische Funktionen zum Verschlüsseln von Daten auf Laufwerken. Dies verbessert die Laufwerk- und Systemleistung durch die Auslagerung kryptografischer Berechnungen vom Prozessor des PCs auf das Laufwerk selbst und durch die schnelle Verschlüsselung des Laufwerk mithilfe von dedizierter Hardware. Wenn Sie beabsichtigen, die vollständige Laufwerkverschlüsselung mit Windows10 zu verwenden, empfiehlt Microsoft, Festplattenhersteller und-Modelle zu untersuchen, um zu ermitteln, ob eine der verschlüsselten Festplattenlaufwerke Ihre Sicherheits- und Budgetanforderungen erfüllt. Weitere Informationen zu verschlüsselten Festplatten finden Sie unter Verschlüsselte Festplatte.

Schutz von Informationen vor dem Start

Eine effektive Implementierung des Informationsschutzes berücksichtigt, wie die meisten Sicherheitssteuerelemente, die Benutzerfreundlichkeit und Sicherheit. Benutzer bevorzugen in der Regel eine einfache Sicherheitsumgebung. Je transparenter eine Sicherheitslösung ist, desto höher ist die Wahrscheinlichkeit, dass Benutzer sich danach richten. Für Organisationen ist der Schutz von Informationen auf ihren PCs unabhängig vom Zustand des Computers oder der Absicht von Benutzern entscheidend. Dieser Schutz sollte für die Benutzer nicht beschwerlich sein. Eine unerwünschte und bisher alltägliche Situation ist, dass der Benutzer vor dem Start zu einer Eingabe aufgefordert wird, und dann erneut bei der Anmeldung an Windows. Das mehrfache Auffordern von Benutzern zu einer Eingabe sollte vermieden werden. Windows10 kann eine echte SSO-Funktion aus der Preboot-Umgebung auf modernen Geräten und in einigen Fällen sogar auf älteren Geräten aktivieren, wenn robuste Informationen Schutz Konfigurationen vorhanden sind. Das isolierte TPM kann den gespeicherten BitLocker-Verschlüsselungsschlüssel sicher schützen und das Betriebssystemlaufwerk sicher entsperren. Wenn der Schlüssel verwendet wird und sich somit im Speicher befindet, kann er durch eine Kombination aus Hardware und

Windows-Funktionen gesichert und der unbefugte Zugriff durch Kaltstartangriffe verhindert werden. Zwar sind weitere Gegenmaßnahmen wie die PIN-basierte Entsperrung verfügbar, diese sind jedoch weniger benutzerfreundlich; je nach Konfiguration der Geräte bieten sie u. U. keine zusätzliche Sicherheit, wenn es um den Schlüsselschutz geht. Weitere Informationen finden Sie unter BitLocker-Gegenmaßnahmen.

Verwalten von Kennwörtern und PINs

Wenn BitLocker auf einem Systemlaufwerk aktiviert ist und der PC über ein TPM verfügt, können Sie festlegen, dass Benutzer eine PIN eingeben müssen, damit BitLocker das Laufwerk entsperrt. Eine solche PIN-Anforderung kann verhindern, dass ein Angreifer, der physischen Zugriff auf einem PC hat, überhaupt zur Windows-Anmeldung gelangt. So ist es dem Angreifer nahezu unmöglich, auf Benutzerdaten und Systemdateien zuzugreifen und diese zu ändern.

Das Anfordern einer PIN beim Systemstart ist eine nützliche Sicherheitsfunktion, da es als zweiter Authentifizierungsfaktor fungiert (eine zweite Information, die man kennen muss). Diese Konfiguration hat jedoch einige Nachteile. Einer der größten Nachteile besteht darin, dass die PIN regelmäßig geändert werden muss. In Unternehmen, die BitLocker mit Windows7 und dem Windows Vista-Betriebssystem verwendet haben, mussten sich die Benutzer an Systemadministratoren wenden, um ihre BitLocker-PIN oder Ihr Kennwort zu aktualisieren. Dies führte nicht nur zu höheren Verwaltungskosten, sondern auch dazu, dass Benutzer weniger bereit waren, ihre BitLocker-PIN oder das Kennwort regelmäßig zu ändern. Windows10-Benutzer können ihre BitLocker-Pins und-Kennwörter selbst ohne Administratoranmeldeinformationen aktualisieren. Diese Funktion senkt die Supportkosten und kann auch die Sicherheit verbessern, da Benutzer häufiger zum Ändern ihrer PINs und Kennwörter aufgefordert werden. Darüber hinaus ist für moderne Standbygeräte keine PIN für den Start erforderlich: Sie sind so konzipiert, dass Sie nur selten gestartet werden und andere Eindämmungs Möglichkeiten aufweisen, die die Angriffsfläche des Systems weiter reduzieren. Weitere Informationen zur Funktionsweise der Startsicherheit und den von Windows10 bereitgestellten Gegenmaßnahmen finden Sie unter Schützen von BitLocker vor Angriffen vor dem Start.

Konfigurieren der Netzwerkentsperrung

Einige Organisationen haben standortspezifische Datensicherheitsanforderungen. Dies ist am häufigsten in Umgebungen der Fall, in denen Daten mit hohem Wert auf PCs gespeichert sind. Die Netzwerkumgebung bietet möglicherweise wesentlichen Datenschutz und erzwingt eine obligatorische Authentifizierung. Daher gibt die Richtlinie an, dass diese PCs nicht das Gebäude verlassen oder vom Unternehmensnetzwerk getrennt werden dürfen. Sicherheitsmaßnahmen wie physische Sicherheitsschlösser und Geofence können als reaktive Kontrollelemente zur Durchsetzung dieser Richtlinie beitragen. Darüber hinaus ist ein proaktives Sicherheitssteuerelement erforderlich, das den Zugriff auf Daten nur gewährt, wenn der PC mit dem Unternehmensnetzwerk verbunden ist.

Die Netzwerkentsperrung ermöglicht das automatische Starten von PCs mit BitLocker-Schutz, wenn diese mit einem verkabelten Unternehmensnetzwerk verbunden sind, in dem Windows-Bereitstellungsdienste ausgeführt werden. Immer wenn der PC nicht mit dem Unternehmensnetzwerk verbunden ist, muss ein Benutzer eine PIN zum Entsperren des Laufwerks eingeben (wenn die PIN-basierte Entsperrung aktiviert ist). Die Netzwerkentsperrung erfordert die folgende Infrastruktur:

- Client-PCs mit UEFI (Unified Extensible Firmware Interface (UEFI) Firmware-Version 2.3.1 oder höher, die das Dynamic Host Configuration-Protokoll (DHCP) unterstützen
- Ein Server, auf dem mindestens Windows Server 2012 mit der Rolle "Windows-Bereitstellungsdienste" ausgeführt wird
- Ein Server, auf dem die DHCP-Serverrolle installiert ist

Weitere Informationen zur Konfiguration der Netzwerkentsperrung finden Sie unter BitLocker: Aktivieren der Netzwerkentsperrung.

Microsoft BitLocker Administration and Monitoring

MBAM ist Teil von Microsoft Desktop Optimization Pack und vereinfacht die Verwaltung und Unterstützung von BitLocker und BitLocker To Go. MBAM 2.5 mit Service Pack 1 (aktuelle Version) weist folgende wichtige Features auf:

- Administratoren können die Verschlüsselung von Volumes auf Clientcomputern unternehmensweit automatisieren.
- Sicherheitsbeauftragte können den Kompatibilitätszustand einzelner Computer oder sogar des ganzen Unternehmens schnell ermitteln.
- Bietet zentralisierte Berichterstellung und Hardwareverwaltung mit Microsoft Endpoint Configuration Manager.
- Die Arbeitsbelastung des Helpdesk wird verringert, da Endbenutzer seltener Unterstützung bei BitLocker-Wiederherstellungsanforderungen benötigen.
- Endbenutzer können verschlüsselte Geräte mithilfe des Self-Service-Portals eigenständig wiederherstellen.
- Sicherheitsbeauftragte können problemlos den Zugriff auf Informationen zu Wiederherstellungsschlüsseln überwachen.
- Windows Enterprise-Benutzer können standortunabhängig arbeiten und sich dabei darauf verlassen, dass ihre Unternehmensdaten geschützt sind.
- MBAM erzwingt die Richtlinienoptionen der BitLocker-Verschlüsselung, die Sie für Ihr Unternehmen festlegen.
- Integration in vorhandene Verwaltungstools wie Microsoft Endpoint Configuration Manager
- Die Benutzeroberfläche für die Wiederherstellung kann von der IT angepasst werden.
- Unterstützt Windows10.

Weitere Informationen zu MBAM, einschließlich Informationen zum Abrufen, finden Sie unter Microsoft BitLocker Administration and Monitoring im MDOP-TechCenter.

Häufig gestellte Fragen (Frequently Asked Questions, FAQ) zu BitLocker

20.12.2019 • 2 minutes to read

Gilt für:

- Windows 10

Dieses Thema enthält Links zu häufig gestellten Fragen zu BitLocker. BitLocker ist ein Datenschutzfeature, das Laufwerke auf dem Computer verschlüsselt, um Datendiebstahl oder-Belichtung zu verhindern. Mit BitLocker geschützten Computern können Daten auch sicherer gelöscht werden, wenn Sie außer Betrieb genommen werden, da es viel schwieriger ist, gelöschte Daten von einem verschlüsselten Laufwerk zu wiederherstellen als von einem nicht verschlüsselten Laufwerk.

- Übersicht und Anforderungen
- Aktualisierung
- Bereitstellung und Verwaltung
- Schlüsselverwaltung
- BitLocker To Go
- Active Directory-Domänendienste (hinzugefügt)
- Sicherheit
- BitLocker-Netzwerkentsperrung
- Verwenden von BitLocker mit anderen Programmen und allgemeinen Fragen

Weitere Informationen

- Vorbereiten Ihrer Organisation auf BitLocker: Planung und Richtlinien
- BitLocker-Gruppenrichtlinieneinstellungen
- BCD-Einstellungen und BitLocker
- BitLocker: Aktivieren der Netzwerkentsperrung
- BitLocker: Bereitstellen auf Windows Server 2012
- BitLocker: Verwenden von BitLocker-Laufwerksverschlüsselungstools zum Verwalten von BitLocker
- BitLocker: Verwenden des BitLocker-Wiederherstellungskennwort-Viewers
- BitLocker Cmdlets in Windows PowerShell

Häufig gestellte Fragen zur BitLocker-Übersicht und-Anforderungen

27.10.2019 • 4 minutes to read

Betrifft

- Windows 10

Wie funktioniert BitLocker?

Funktionsweise von BitLocker mit Betriebssystemlaufwerken

Mit BitLocker können Sie nicht autorisierten Datenzugriff auf verloren gegangenen oder gestohlenen Computern verhindern, indem Sie alle Benutzerdateien und Systemdateien auf dem Betriebssystemlaufwerk verschlüsseln, einschließlich der Auslagerungsdateien und Ruhezustandsdateien, und die Integrität der vorrangigen Startkomponenten und Startkonfigurationsdaten überprüfen.

Funktionsweise von BitLocker mit Festplattenlaufwerken und Wechseldatenträgern

Mithilfe von BitLocker können Sie den gesamten Inhalt eines Datenlaufwerks verschlüsseln. Sie können eine Gruppenrichtlinie verwenden, um festzulegen, dass BitLocker auf einem Laufwerk aktiviert wird, bevor der Computer Daten auf das Laufwerk schreiben kann. BitLocker kann mit einer Vielzahl von Methoden zum Entsperren für Datenlaufwerke konfiguriert werden, und ein Datenlaufwerk unterstützt mehrere Methoden zum Entsperren.

Unterstützt BitLocker die mehrstufige Authentifizierung?

Ja, BitLocker unterstützt die mehrstufige Authentifizierung für Betriebssystemlaufwerke. Wenn Sie BitLocker auf einem Computer mit einer TPM-Version 1.2 oder höher aktivieren, können Sie zusätzliche Authentifizierungsformen mit dem TPM-Schutz verwenden.

Welche Hardware- und Softwareanforderungen müssen für die Verwendung von BitLocker erfüllt werden?

Informationen zu den Anforderungen finden Sie unter Systemanforderungen.

> **NOTE**
>
> Dynamische Datenträger werden von BitLocker nicht unterstützt. Dynamische Datenvolumes werden nicht in der Systemsteuerung angezeigt. Obwohl das Betriebssystemvolume immer in der Systemsteuerung angezeigt wird, unabhängig davon, ob es sich um einen dynamischen Datenträger handelt, kann es nicht von BitLocker geschützt werden, wenn es sich um einen dynamischen Datenträger handelt.

Warum sind zwei Partitionen erforderlich? Warum muss das Systemlaufwerk so groß sein?

Zwei Partitionen sind zum Ausführen von BitLocker erforderlich, weil die Authentifizierung vor dem Start und die Überprüfung der Systemintegrität auf einer separaten Partition des verschlüsselten Betriebssystemlaufwerks erfolgen müssen. Diese Konfiguration schützt das Betriebssystem und die Informationen auf dem verschlüsselten

Laufwerk.

Welche Trusted Platform Modules (TPMs) werden von BitLocker unterstützt?

BitLocker unterstützt die TPM-Version 1.2 oder höher. Die BitLocker-Unterstützung für TPM 2,0 erfordert Unified Extensible Firmware Interface (UEFI) für das Gerät.

> **NOTE**
>
> TPM 2,0 wird im Legacy-und CSM-Modus des BIOS nicht unterstützt. Bei Geräten mit TPM 2,0 muss der BIOS-Modus nur als systemeigener UEFI konfiguriert sein. Die Optionen für Legacy-und Kompatibilitäts Unterstützungs Module (CSM) müssen deaktiviert sein. Für zusätzliche Sicherheit aktivieren Sie das Feature für sicheres Booten.
>
> Das installierte Betriebs System auf der Hardware im Legacy Modus verhindert das Booten des Betriebssystems, wenn der BIOS-Modus in UEFI geändert wird. Verwenden Sie das Tool MBR2GPT , bevor Sie den BIOS-Modus ändern, der das Betriebssystem und den Datenträger zur Unterstützung von UEFI vorbereitet.

Wie kann ich feststellen, dass ein TPM auf meinem Computer vorhanden ist?

Ab Windows 10, Version 1803, können Sie den TPM-Status im **Windows Defender Security Center** > **Device Security** > **Security Processor Details**überprüfen. Öffnen Sie in früheren Versionen von Windows die TPM-MMC-Konsole (TPM. msc), und schauen Sie unter der **Status** Überschrift nach.

Kann BitLocker auf einem Betriebssystemlaufwerk ohne TPM verwendet werden?

Ja, Sie können BitLocker auf einem Betriebssystemlaufwerk ohne die TPM-Version 1.2 oder höher aktivieren, wenn die BIOS- oder UEFI-Firmware aus einem USB-Speicherstick in der Startumgebung lesen kann. Dies liegt daran, dass BitLocker das geschützte Laufwerk erst entsperrt, wenn der eigene Volumehauptschlüssel von BitLocker entweder durch das TPM des Computers oder über einen USB-Speicherstick mit dem BitLocker-Systemstartschlüssel für diesen Computer erstmals freigegeben wird. Allerdings können Computer ohne TPMs die Systemintegritätsüberprüfung nicht verwenden, die ebenfalls von BitLocker bereitgestellt werden kann. Um zu ermitteln, ob ein Computer während des Startvorgangs von einem USB-Gerät lesen kann, verwenden Sie die BitLocker-Systemüberprüfung als Teil des BitLocker-Setupprozesses. Diese Systemüberprüfung führt Tests durch, um sicherzustellen, dass der Computer zum entsprechenden Zeitpunkt ordnungsgemäß von den USB-Geräten lesen kann und dass der Computer weitere BitLocker-Anforderungen erfüllt.

Wie erhalte ich BIOS-Unterstützung für das TPM auf meinem Computer?

Wenden Sie sich an den Hersteller des Computers, um eine Trusted Computing Group (TCG)-kompatible BIOS- oder UEFI-Startfirmware anzufordern, die die folgenden Anforderungen erfüllt:

- Sie ist mit den TCG-Standards für einen Clientcomputer kompatibel.
- Sie verfügt über einen sicheren Aktualisierungsmechanismus, um zu verhindern, dass eine schädliche BIOS- oder Startfirmware auf dem Computer installiert wird.

Welche Anmeldeinformationen sind erforderlich, um BitLocker zu verwenden?

Zum Aktivieren, Deaktivieren oder Ändern der Konfiguration von BitLocker auf dem Betriebssystem und auf Festplattenlaufwerken ist die Mitgliedschaft in der lokalen Gruppe **Administratoren** erforderlich. Standardbenutzer können die Konfiguration von BitLocker auf Wechseldatenträgern aktivieren, deaktivieren oder ändern.

Wie lautet die empfohlene Startreihenfolge für Computer, die mit BitLocker geschützt werden sollen?

Sie sollten die Startoptionen Ihres Computers so konfigurieren, dass die Festplatte zuerst in der Startreihenfolge steht, bevor andere Laufwerke wie CD/DVD-Laufwerke oder USB-Laufwerke vorhanden sind. Wenn die Festplatte nicht an erster Stelle steht und Sie in der Regel von der Festplatte starten, kann eine Änderung der Startreihenfolge erkannt oder vorausgesetzt werden, wenn Wechselmedien während des Starts gefunden werden.Die Startreihenfolge wirkt sich in der Regel auf die Systemmessung aus, die mit BitLocker überprüft wird. Eine Änderung der Startreihenfolge bewirkt, dass Sie zur Angabe des BitLocker-Wiederherstellungsschlüssels aufgefordert werden. Wenn Sie einen Laptop mit einer Dockingstation besitzen, stellen Sie sicher, dass das Festplattenlaufwerk in der Startreihenfolge an erster Stelle steht, wenn sich der Laptop in der Dockingstation befindet und aus der Dockingstation entfernt wurde.

Häufig gestellte Fragen zur BitLocker-Aktualisierung

04.01.2020 • 2 minutes to read

Betrifft:

- Windows 10

Kann ich ein Upgrade auf Windows10 durchführen, wenn BitLocker aktiviert ist?

Ja.

Was ist der Unterschied zwischen Anhalten und Entschlüsseln von BitLocker?

Entschlüsseln entfernt den BitLocker-Schutz vollständig, und das Laufwerk wird vollständig entschlüsselt.

Anhalten behält die verschlüsselten Daten bei, aber der BitLocker-Volumehauptschlüssel wird mit einem unverschlüsselten Schlüssel verschlüsselt. Der unverschlüsselte Schlüssel ist ein kryptografischer Schlüssel, der auf dem Laufwerk unverschlüsselt und nicht geschützt gespeichert wird. Durch die unverschlüsselte Speicherung dieses Schlüssels können mit der Option **Anhalten** Änderungen oder Upgrades auf dem Computer ohne den Zeit- und Kostenaufwand für die Entschlüsselung und erneute Verschlüsselung des gesamten Laufwerks vorgenommen werden. Nachdem die Änderungen vorgenommen wurden und BitLocker erneut aktiviert ist, versiegelt BitLocker den Verschlüsselungsschlüssel erneut für die neuen Werte der gemessenen Komponenten, die als Teil des Upgrades geändert wurden. Der Volumehauptschlüssel wird geändert, die Schutzvorrichtungen werden entsprechend angepasst, und der unverschlüsselte Schlüssel wird gelöscht.

Muss ich mein BitLocker-geschütztes Laufwerk zum Herunterladen und Installieren der Systemupdates und -upgrades entschlüsseln?

Für BitLocker ist keine Benutzeraktion erforderlich, um Updates von Microsoft anzuwenden, einschließlich Windows-Qualitätsupdates und -Funktionsupdates. Für Softwareupdates, die nicht von Microsoft stammen, muss BitLocker angehalten werden. Dazu gehören Folgende:

- Firmwareupdates vom Computerhersteller
- TPM-Firmwareupdates
- Microsoft-fremde Anwendungsupdates, die die Startkomponenten ändern

> **NOTE**
>
> Wenn Sie BitLocker angehalten haben, können Sie den BitLocker-Schutz fortsetzen, nachdem Sie das Upgrade oder Update installiert haben. Beim Fortsetzen des Schutzes wird BitLocker den Verschlüsselungsschlüssel für die neuen Werte der gemessenen Komponenten, die als Teil des Upgrades oder Updates geändert wurden, erneut versiegeln. Wenn diese Arten von Upgrades oder Updates angewendet werden, ohne BitLocker anzuhalten, wechselt Ihr Computer beim Neustart in den Wiederherstellungsmodus und benötigt einen Wiederherstellungsschlüssel oder ein Kennwort, um auf den Computer zugreifen zu können.

Häufig gestellte Fragen (Frequently Asked Questions, FAQ) zu BitLocker

20.12.2019 • 5 minutes to read

Gilt für:

- Windows 10

Kann die BitLocker-Bereitstellung in einer Unternehmensumgebung automatisiert werden?

Ja, Sie können die Bereitstellung und Konfiguration von BitLocker sowie das TPM entweder mit WMI- oder Windows PowerShell-Skripts automatisieren. Die Implementierung der Skripts hängt von Ihrer Umgebung ab. Sie können auch „Manage-bde.exe" verwenden, um BitLocker lokal oder remote zu konfigurieren. Weitere Informationen zum Schreiben von Skripts, die die BitLocker-WMI-Anbieter verwenden, finden Sie unter BitLocker Drive Encryption Provider(nur in englischer Sprache verfügbar). Weitere Informationen zur Verwendung von Windows PowerShell-Cmdlets mit der BitLocker-Laufwerkverschlüsselung finden Sie unter BitLocker Cmdlets in Windows PowerShell(nur in englischer Sprache verfügbar).

Kann BitLocker mehr als nur das Betriebssystemlaufwerk verschlüsseln?

Ja.

Gibt es eine wahrnehmbare Auswirkung auf die Leistung, wenn BitLocker auf einem Computer aktiviert ist?

Im Allgemeinen gibt es eine Beeinträchtigung der Leistung im einstelligen Prozentbereich.

Wie lange dauert die anfängliche Verschlüsselung, wenn BitLocker aktiviert ist?

Obwohl die BitLocker-Verschlüsselung im Hintergrund ausgeführt wird, während Sie Ihre Arbeit fortsetzen und das System verwendbar bleibt, hängen die Verschlüsselungszeiten vom zu verschlüsselnden Laufwerktyp, von der Größe des Laufwerks und der Geschwindigkeit des Laufwerks ab. Wenn Sie sehr große Laufwerke verschlüsseln, sollte die Verschlüsselung zu Zeiten erfolgen, wenn Sie das Laufwerk nicht verwenden.

Sie können auch auswählen, ob BitLocker das gesamte Laufwerk oder nur den belegten Speicherplatz auf dem Laufwerk verschlüsseln soll, wenn Sie BitLocker aktivieren. Auf einer neuen Festplatte kann die Verschlüsselung des belegten Speicherplatzes wesentlich schneller erfolgen als die Verschlüsselung des gesamten Laufwerks. Wenn diese Verschlüsselungsoption ausgewählt wird, verschlüsselt BitLocker die Daten automatisch, wenn sie gespeichert werden. Dabei wird sichergestellt, dass keine Daten unverschlüsselt gespeichert werden.

Was geschieht, wenn der Computer während der Verschlüsselung oder Entschlüsselung ausgeschaltet wird?

Wenn der Computer ausgeschaltet wird oder in den Ruhezustand wechselt, wird der BitLocker-Verschlüsselungs- und Entschlüsselungsprozess beim nächsten Mal, wenn Windows gestartet wird, an der Stelle fortgesetzt, an der er angehalten wurde. Dies gilt auch, wenn die Stromversorgung plötzlich unterbrochen ist.

Verschlüsselt und entschlüsselt BitLocker das gesamte Laufwerk auf einmal, wenn Daten gelesen und geschrieben werden?

Nein, BitLocker verschlüsselt und entschlüsselt nicht das gesamte Laufwerk beim Lesen und Schreiben von Daten. Die verschlüsselten Sektoren auf dem BitLocker-geschützten Laufwerk werden nur entschlüsselt, wenn sie von Systemlesevorgängen angefordert werden. Blöcke, die auf das Laufwerk geschrieben werden, werden verschlüsselt, bevor das System diese auf den physischen Datenträger schreibt. Unverschlüsselte Daten werden niemals auf einem BitLocker-geschützten Laufwerk gespeichert.

Wie kann ich verhindern, dass Benutzer in einem Netzwerk Daten auf einem nicht verschlüsselten Laufwerk speichern?

Sie können Gruppenrichtlinieneinstellungen so konfigurieren, dass Datenlaufwerke mit BitLocker geschützt werden, bevor ein von BitLocker geschützter Computer Daten in Sie schreiben kann. Weitere Informationen finden Sie unter BitLocker-Gruppenrichtlinieneinstellungen. Wenn diese Richtlinieneinstellungen aktiviert sind, wird das BitLocker-geschützte Betriebssystem Datenlaufwerke bereitstellen, die durch BitLocker nicht als schreibgeschützt geschützt sind.

Was ist der verwendete Speicherplatz nur für die Verschlüsselung?

BitLocker in Windows10 ermöglicht es Benutzern, nur Ihre Daten zu verschlüsseln. Obwohl es sich nicht um die sicherste Methode zum Verschlüsseln eines Laufwerks handelt, kann diese Option die Verschlüsselungs Zeit um mehr als 99 Prozent verringern, je nachdem, wie viele Daten verschlüsselt werden müssen. Weitere Informationen finden Sie unter verwendete Speicherplatz Verschlüsselung.

Welche Systemänderungen führen dazu, dass die Überprüfung der Integrität auf meinem Betriebssystemlaufwerk fehlschlägt?

Die folgenden Systemänderungen können dazu führen, dass die Überprüfung der Integrität fehlschlägt und dass verhindert wird, dass das TPM den BitLocker-Schlüssel zum Entschlüsseln des geschützten Betriebssystemlaufwerks freigibt:

- Verschieben des BitLocker-geschützten Laufwerks in einen neuen Computer
- Installieren einer neue Hauptplatine mit einem neuen TPM
- Ausschalten, Deaktivieren oder Löschen des TPM
- Ändern der Startkonfigurationseinstellungen
- Ändern des BIOS, der UEFI-Firmware, des Master Boot Records, des Startsektors, des Start-Managers, des Options-ROMs oder anderer frühzeitiger Startkomponenten oder Startkonfigurationsdaten

Warum startet BitLocker im Wiederherstellungsmodus, wenn Sie versuchen, das Betriebssystemlaufwerk zu starten?

Da BitLocker so konzipiert ist, Ihren Computer vor zahlreichen Angriffen zu schützen, gibt es viele Gründe, warum BitLocker im Wiederherstellungsmodus startet. Zum Beispiel:

- Ändern der BIOS-Startreihenfolge, sodass ein anderes Laufwerk vor der Festplatte gestartet wird.
- Hinzufügen oder Entfernen von Hardware, z. B. Einsetzen einer neuen Karte in den Computer, einschließlich einiger PCMIA-Drahtloskarten.
- Entfernen, Einsetzen oder vollständiges Leeren der Ladung eines Smart-Akkus in einem tragbaren Computer.

Die Wiederherstellung besteht in BitLocker aus der Entschlüsselung einer Kopie des Volumehauptschlüssels mithilfe eines auf einem USB-Speicherstick gespeicherten Wiederherstellungsschlüssels oder eines von einem

Wiederherstellungskennwort abgeleiteten kryptografischen Schlüssels. Das TPM ist an den Wiederherstellungsszenarien nicht beteiligt. Folglich ist die Wiederherstellung weiterhin möglich, wenn das TPM die Startkomponenten nicht überprüfen kann, nicht ordnungsgemäß funktioniert oder entfernt wird.

Was kann verhindern, dass BitLocker an PCR 7 gebunden wird?

Dies geschieht, wenn ein nicht-Windows-Betriebssystem vor Windows gestartet wird oder wenn der sichere Start für das Gerät nicht zur Verfügung steht, weil es deaktiviert wurde oder von der Hardware nicht unterstützt wird.

Kann ich Festplatten auf demselben Computer austauschen, wenn BitLocker auf dem Betriebssystemlaufwerk aktiviert ist?

Ja, Sie können mehrere Festplatten auf demselben Computer austauschen, wenn BitLocker aktiviert ist, aber nur, wenn die Festplatten auf demselben Computer mit BitLocker geschützt wurden. Die BitLocker-Schlüssel sind spezifisch für das TPM und das Betriebssystemlaufwerk. Wenn Sie ein Sicherungsbetriebssystem oder Datenlaufwerk für die Verwendung bei einem Ausfall der Festplatte vorbereiten möchten, müssen Sie sicherstellen, dass das richtige TPM zugeordnet wurde. Sie können auch verschiedene Festplatten für verschiedene Betriebssysteme konfigurieren und BitLocker anschließend jeweils mit unterschiedlichen Authentifizierungsmethoden (z. B. eine nur mit TPM und eine mit TPM und PIN) ohne Konflikte aktivieren.

Kann ich auf mein BitLocker-geschütztes Laufwerk zugreifen, wenn ich die Festplatte in einen anderen Computer einsetze?

Ja, wenn das Laufwerk ein Datenlaufwerk ist, können Sie es mithilfe des Systemsteuerungselements **BitLocker-Laufwerkverschlüsselung** genau wie jedes andere Datenlaufwerk mit einem Kennwort oder einer Smartcard entsperren. Wenn das Datenlaufwerk nur für die automatische Entsperrung konfiguriert wurde, müssen Sie es mit dem Wiederherstellungsschlüssel entsperren. Die verschlüsselte Festplatte kann mithilfe eines Datenwiederherstellungs-Agents (sofern konfiguriert) oder eines Wiederherstellungsschlüssels entsperrt werden.

Warum ist „BitLocker aktivieren“ nicht verfügbar, wenn ich mit der rechten Maustaste auf ein Laufwerk klicke?

Einige Laufwerke können nicht mit BitLocker verschlüsselt werden. Ein Laufwerk kann nicht verschlüsselt werden, wenn nicht genügend Datenträgergröße oder ein inkompatibles Dateisystem vorhanden ist, wenn das Laufwerk ein dynamischer Datenträger ist oder ein Laufwerk als Systempartition festgelegt ist. Standardmäßig wird das Systemlaufwerk (oder die Systempartition) aus der Anzeige ausgeblendet. Wenn es allerdings nicht als ausgeblendetes Laufwerk erstellt wird, wenn das Betriebssystem aufgrund eines benutzerdefinierten Installationsvorgangs installiert wurde, wird dieses Laufwerk möglicherweise angezeigt, kann aber nicht verschlüsselt werden.

Welche Arten von Datenträgerkonfigurationen werden von BitLocker unterstützt?

Eine beliebige Anzahl von internen Festplattenlaufwerken kann mit BitLocker geschützt werden. Bei einigen Versionen werden ATA- und SATA-basierte, direkt angeschlossene Speichergeräte ebenfalls unterstützt.

Häufig gestellte Fragen zur BitLocker-Schlüsselverwaltung

20.12.2019 • 6 minutes to read

Gilt für:

- Windows 10

Wie kann ich mein Wechseldaten Laufwerk authentifizieren oder entsperren?

Sie können Wechseldatenträger mithilfe eines Kennworts oder einer Smartcard entsperren, oder Sie können eine SID-Beschützer-Datei so konfigurieren, dass ein Laufwerk mithilfe ihrer Domänenanmeldeinformationen freigegeben wird. Nachdem Sie die Verschlüsselung gestartet haben, kann das Laufwerk auch automatisch auf einem bestimmten Computer für ein bestimmtes Benutzerkonto freigegeben werden. System Administratoren können konfigurieren, welche Optionen für Benutzer zur Verfügung stehen, sowie die Kennwortkomplexität und die Mindestanforderungen für die Länge. Verwenden Sie zum Entsperren mithilfe einer SID-beschützerverwaltung-BDE:

```
Manage-bde -protectors -add e: -sid domain\username
```

Was ist der Unterschied zwischen einem Wiederherstellungskennwort, einem Wiederherstellungsschlüssel, einer PIN, einer erweiterten PIN und einem Systemstartschlüssel?

Tabellen, in denen Elemente wie Wiederherstellungskennwort, Wiederherstellungsschlüssel und PIN aufgeführt und beschrieben sind, finden Sie unter BitLocker-Schlüsselschutzvorrichtungen und BitLocker-Authentifizierungsmethoden.

Wie können das Wiederherstellungskennwort und der Wiederherstellungsschlüssel gespeichert werden?

Das Wiederherstellungskennwort und der Wiederherstellungsschlüssel für ein Betriebssystemlaufwerk oder ein Festplattenlaufwerk können in einem Ordner, auf einem oder mehreren USB-Geräten oder in Ihrem Microsoft-Konto gespeichert oder gedruckt werden.

Bei Wechseldatenträgern können das Wiederherstellungskennwort und der Wiederherstellungsschlüssel in einem Ordner oder in Ihrem Microsoft-Konto gespeichert oder gedruckt werden. Standardmäßig kann ein Wiederherstellungsschlüssel für einen Wechseldatenträger nicht auf einem Wechseldatenträger gespeichert werden.

Ein Domänenadministrator kann außerdem Gruppenrichtlinien so konfigurieren, dass Wiederherstellungskennwörter automatisch generiert und in Active Directory-Domänendienste (Adds) für jedes BitLocker-geschützte Laufwerk gespeichert werden.

Ist es möglich, eine weitere Authentifizierungsmethode hinzuzufügen, ohne das Laufwerk zu entschlüsseln, wenn nur die TPM-Authentifizierungsmethode aktiviert ist?

Sie können das Befehlszeilentool „Manage-bde.exe" verwenden, um den TPM-Authentifizierungsmodus durch einen mehrstufigen Authentifizierungsmodus zu ersetzen. Wenn BitLocker beispielsweise nur mit der TPM-Authentifizierung aktiviert ist und Sie die PIN-Authentifizierung hinzufügen möchten, verwenden Sie die folgenden Befehle einer Eingabeaufforderung mit erhöhten Rechten, die *4-20 digit numeric PIN* durch die zu verwendende numerische PIN ersetzt:

```
manage-bde –protectors –delete %systemdrive% -type tpm
```

```
manage-bde –protectors –add %systemdrive% -tpmandpin 4-20 digit numeric PIN
```

Wann sollte eine weitere Methode für die Authentifizierung berücksichtigt werden?

Aufgrund neuer Hardware, die die Anforderungen des Windows-Hardware-Kompatibilitätsprogramms erfüllt, haben PINs eine weniger kritische Bedeutung für die Risikominderung. Daher reicht der Schutz durch ein TPM in Verbindung mit Richtlinien wie der Gerätesperrung wahrscheinlich aus. Beispielsweise besitzen Surface Pro und Surface Book keine externen DMA-Ports, die angegriffen werden können. Im Fall älterer Hardware, für die eine PIN erforderlich sein kann, wird empfohlen, erweiterte PINs zu aktivieren, die nichtnumerische Zeichen wie Buchstaben und Satzzeichen zulassen, und die PIN-Länge auf der Basis Ihrer Risikotoleranz und der Anti-Hammering-Funktionen der Hardware festzulegen, die für die TPMs auf Ihren Computern verfügbar sind.

Können die durch BitLocker geschützten Daten nicht wiederhergestellt werden, wenn ich meine Wiederherstellungsinformationen verliere?

BitLocker ist so konzipiert, dass das verschlüsselte Laufwerk ohne die erforderliche Authentifizierung nicht wiederhergestellt werden kann. Im Wiederherstellungsmodus benötigt der Benutzer das Wiederherstellungskennwort oder den Wiederherstellungsschlüssel, um das verschlüsselte Laufwerk zu entsperren.

> **IMPORTANT**
>
> Speichern Sie die Wiederherstellungsinformationen in Adds zusammen mit Ihrem Microsoft-Konto oder einem anderen sicheren Speicherort.

Kann der USB-Speicherstick, der als Systemstartschlüssel genutzt wird, auch verwendet werden, um den Wiederherstellungsschlüssel zu speichern?

Obwohl dies technisch möglich ist, wird die Verwendung eines USB-Speichersticks zum Speichern beider Schlüssel nicht empfohlen. Wenn der USB-Speicherstick, der Ihren Systemstartschlüssel enthält, verloren geht oder gestohlen wird, verlieren Sie auch den Zugriff auf Ihren Wiederherstellungsschlüssel. Darüber hinaus würde der Computer durch das Einfügen dieses Schlüssels automatisch über den Wiederherstellungsschlüssel starten, auch wenn die TPM-gemessenen Dateien geändert wurden, wodurch die Systemintegritätsüberprüfung des TPMs umgangen wird.

Kann ich den Systemstartschlüssel auf mehreren USB-Speichersticks speichern?

Ja, Sie können den Systemstartschlüssel eines Computers auf mehreren USB-Speichersticks speichern. Wenn Sie mit der rechten Maustaste auf ein BitLocker-geschütztes Laufwerk klicken und **BitLocker verwalten** auswählen, stehen Optionen zur Verfügung, mit denen Sie die Wiederherstellungsschlüssel nach Bedarf duplizieren können.

Kann ich mehrere (verschiedene) Systemstartschlüssel auf dem gleichen USB-Speicherstick speichern?

Ja, Sie können BitLocker-Systemstartschlüssel für unterschiedliche Computer auf dem gleichen USB-Speicherstick speichern.

Kann ich mehrere (verschiedene) Systemstartschlüssel für denselben Computer erstellen?

Sie können verschiedene Systemstartschlüssel für denselben Computer mithilfe von Skripting erstellen. Bei Computern mit einem TPM wird durch das Erstellen von verschiedenen Systemstartschlüsseln verhindert, dass BitLocker die Systemintegritätsüberprüfung des TPMs verwendet.

Kann ich mehrere PIN-Kombinationen erstellen?

Sie können nicht mehrere PIN-Kombinationen erstellen.

Welche Verschlüsselungsschlüssel werden in BitLocker verwendet? Wie funktionieren sie zusammen?

Die Rohdaten werden mit dem vollständigen Volumeverschlüsselungsschlüssel verschlüsselt, welcher dann mit dem Volumehauptschlüssel verschlüsselt wird. Der Volumehauptschlüssel wird wiederum durch eine von mehreren möglichen Methoden abhängig von der Authentifizierung (d. h. Schlüsselschutzvorrichtungen oder TPM) und den Wiederherstellungsszenarien verschlüsselt.

Wo werden die Verschlüsselungsschlüssel gespeichert?

Der vollständige Volumeverschlüsselungsschlüssel wird mit dem Volumehauptschlüssel verschlüsselt und auf dem verschlüsselten Laufwerk gespeichert. Der Volumehauptschlüssel wird mit der entsprechenden Schlüsselschutzvorrichtung verschlüsselt und auf dem verschlüsselten Laufwerk gespeichert. Wenn BitLocker unterbrochen wurde, wird der unverschlüsselte Schlüssel, mit dem der Volumehauptschlüssel verschlüsselt wird, auch auf dem verschlüsselten Laufwerk zusammen mit dem verschlüsselten Volumehauptschlüssel gespeichert.

Durch diesen Speichervorgang wird sichergestellt, dass der Volumehauptschlüssel niemals unverschlüsselt gespeichert wird und geschützt ist, es sei denn, Sie deaktivieren BitLocker. Die Schlüssel werden auch an zwei zusätzlichen Speicherorten auf dem Laufwerk zwecks Redundanz gespeichert. Die Schlüssel können vom Start-Manager gelesen und verarbeitet werden.

Warum muss ich die Funktionstasten verwenden, um die PIN oder das Wiederherstellungskennwort mit 48 Zeichen einzugeben?

Die Tasten F1 bis F10 sind universell zugeordnete Abfragecodes, die in der Umgebung vor dem Start auf allen Computern und in allen Sprachen verfügbar sind. Die numerischen Tasten 0 bis 9 können in der Umgebung vor dem Start nicht auf allen Tastaturen verwendet werden.

Wenn Sie eine erweiterte PIN verwenden, sollten Benutzer während des BitLocker-Setupprozesses die optionale Systemüberprüfung ausführen, um sicherzustellen, dass die PIN in der Umgebung vor dem Start richtig eingegeben werden kann.

Wie trägt BitLocker dazu bei, dass ein Angreifer nicht die PIN ermitteln kann, mit der das Betriebssystemlaufwerk entsperrt wird?

Es ist möglich, dass eine persönliche Identifikationsnummer (PIN) durch einen Angreifer, der einen Brute-Force-

Angriff durchführt, ermittelt werden kann. Ein Brute-Force-Angriff liegt vor, wenn ein Angreifer ein automatisiertes Tool verwendet, um verschiedene PIN-Kombinationen auszuprobieren, bis die richtige PIN-Kombination gefunden wird. Bei BitLocker-geschützten Computern muss der Angreifer bei dieser Art von Angriff, auch bekannt als Wörterbuchangriff, über den physischen Zugriff auf den Computer verfügen.

Das TPM verfügt über die integrierte Funktion zum Erkennen und Reagieren auf diese Art von Angriffen. Da TPMs von verschiedenen Herstellern unterschiedliche PIN- und Angriffsausgleiche unterstützen können, wenden Sie sich an den TPM-Hersteller, um herauszufinden, wie das TPM Ihres Computers PIN-Brute-Force-Angriffe reduziert. Nachdem Sie den Hersteller Ihres TPMs ermittelt haben, wenden Sie sich an den Hersteller, um die herstellerspezifischen Informationen zum TPM einzuholen. Die meisten Hersteller verwenden die PIN-Authentifizierungsfehleranzahl, um die Sperrungszeit für die PIN-Schnittstelle exponentiell zu erhöhen. Jeder Hersteller hat jedoch unterschiedliche Richtlinien, wann und wie der Fehlerzähler verringert oder zurückgesetzt wird.

Wie kann ich den Hersteller meines TPMs ermitteln?

Sie können Ihren TPM-Hersteller im **Windows Defender Security Center** > **Device Security** > **Security Processor Details**ermitteln.

Wie kann ich den Mechanismus für den Wörterbuchangriffsausgleich eines TPMs beurteilen?

Die folgenden Fragen können nützlich sein, wenn Sie einen TPM-Hersteller nach dem Konzept des Mechanismus für den Wörterbuchangriffsausgleich fragen:

- Wie viele fehlgeschlagene Autorisierungsversuche können auftreten, bevor die Sperrung erfolgt?
- Wie lautet der Algorithmus für die Bestimmung der Sperrdauer basierend auf der Anzahl der fehlgeschlagenen Versuche und anderen relevanten Parametern?
- Welche Aktionen können dazu führen, dass die Fehleranzahl und die Sperrdauer verringert oder zurückgesetzt wird?

Können die Komplexität und die Länge der PIN mit der Gruppenrichtlinie verwaltet werden?

Ja und nein. Sie können die minimale Länge der persönlichen Identifikationsnummer (PIN) mithilfe der Gruppenrichtlinieneinstellung **Minimale PIN-Länge für Systemstart konfigurieren** festlegen und die Verwendung alphanumerischer PINs durch Aktivieren der Gruppenrichtlinieneinstellung **Erweiterte PINs für Systemstart zulassen** ermöglichen. Allerdings können Sie die PIN-Komplexität nicht durch eine Gruppenrichtlinie festlegen.

Weitere Informationen finden Sie unter BitLocker-Gruppenrichtlinieneinstellungen.

Häufig gestellte Fragen zu BitLocker To Go

20.12.2019 • 2 minutes to read

Gilt für:

- Windows 10

Was ist BitLocker To Go?

BitLocker To Go ist die BitLocker-Laufwerksverschlüsselung auf Wechseldatenträgern. Dazu zählt die Verschlüsselung von USB-Speichersticks, SD-Karten, externen Festplattenlaufwerken und anderen Laufwerken, die mithilfe des NTFS-, FAT16-, FAT32- oder exFAT-Dateisystems formatiert werden.

Wie bei BitLocker können Laufwerke, die mithilfe von BitLocker To Go verschlüsselt sind, mithilfe eines Kennworts oder einer Smartcard auf einem anderen Computer mithilfe der **BitLocker-Laufwerkverschlüsselung** in der Systemsteuerung geöffnet werden.

Häufig gestellte Fragen zu BitLocker und Active Directory-Domänendiensten (Adds)

20.12.2019 • 3 minutes to read

Gilt für:

- Windows 10

Welche Art von Informationen wird in AD DS gespeichert?

GESPEICHERTE INFORMATIONEN	BESCHREIBUNG
Hash des TPM-Besitzer Kennworts	Ab Windows 10 wird der Kennworthash nicht standardmäßig in AD DS gespeichert. Der Kennworthash kann nur gespeichert werden, wenn das TPM Besitzer ist und der Besitz mithilfe von Komponenten von Windows 8,1 oder früher, wie dem BitLocker-Setup-Assistenten oder dem TPM-Snap-in, übernommen wurde.
BitLocker-Wiederherstellungskennwort	Mit dem Wiederherstellungskennwort können Sie im Fall eines Wiederherstellungsereignisses die Sperre aufheben und auf das Laufwerk zugreifen. Domänenadministratoren können das BitLocker-Wiederherstellungskennwort mit dem BitLocker-Wiederherstellungskennwort-Viewer anzeigen. Weitere Informationen zu diesem Tool finden Sie unter BitLocker: Verwenden des BitLocker-Wiederherstellungskennwort-Anzeigeprogramms.
BitLocker-Schlüsselpaket	Das Schlüsselpaket hilft, Schäden an der Festplatte zu beheben, die andernfalls die Standardwiederherstellung verhindern würden. Für die Verwendung des Schlüsselpakets für die Wiederherstellung ist das BitLocker-Reparatur Tool Repair-bde erforderlich.

Was geschieht, wenn BitLocker auf einem Computer aktiviert ist, bevor der Computer der Domäne beigetreten ist?

Wenn BitLocker auf einem Laufwerk aktiviert ist, bevor Gruppenrichtlinien angewendet wurden, um eine Sicherung durchzusetzen, werden die Wiederherstellungsinformationen nicht automatisch gesichert, um hinzugefügt zu werden, wenn der Computer der Domäne Beitritt oder wenn anschließend Gruppenrichtlinien angewendet werden. Allerdings Sie können **auswählen, wie BitLocker-geschützte Betriebssystemlaufwerke wiederhergestellt werden können**, **auswählen, wie BitLocker-geschützte Festplatten wiederhergestellt** werden können, und **auswählen, wie BitLocker-geschützte Wechseldatenträger wiederhergestellt werden können** , um zu erzwingen, dass der Computer mit einer Domäne verbunden wird, bevor BitLocker aktiviert werden kann, um sicherzustellen, dass die Wiederherstellungsinformationen für von BitLocker geschützte Laufwerke in Ihrer Organisation

Weitere Informationen finden Sie unter BitLocker-Gruppenrichtlinieneinstellungen.

Mithilfe der Schnittstelle der BitLocker Windows-Verwaltungsinstrumentation (Windows Management Instrumentation, WMI) können Administratoren ein Skript schreiben, um die vorhandenen Wiederherstellungsinformationen eines Online-Clients zu sichern oder zu synchronisieren. Dieser Prozess wird

jedoch nicht automatisch von BitLocker verwaltet. Das Befehlszeilentool manage-bde kann auch dazu verwendet werden, Wiederherstellungsinformationen manuell zu sichern, um Sie hinzufügen zu können. Wenn Sie beispielsweise alle Wiederherstellungsinformationen für das `$env:SystemDrive` hinzufügen sichern möchten, verwenden Sie das folgende Befehlsskript an einer Eingabeaufforderung mit erhöhten Rechten:

```
$BitLocker = Get-BitLockerVolume -MountPoint $env:SystemDrive
$RecoveryProtector = $BitLocker.KeyProtector | Where-Object { $_.KeyProtectorType -eq 'RecoveryPassword' }

Backup-BitLockerKeyProtector -MountPoint $env:SystemDrive -KeyProtectorId $RecoveryProtector.KeyProtectorID
BackupToAAD-BitLockerKeyProtector -MountPoint $env:SystemDrive -KeyProtectorId
$RecoveryProtector.KeyProtectorID
```

IMPORTANT

Das beitreten zu einem Computer zur Domäne sollte der erste Schritt für neue Computer in einer Organisation sein. Nachdem Computer einer Domäne beigetreten sind, ist das Speichern des BitLocker-Wiederherstellungsschlüssels für "hinzufügen" automatisch (wenn dies in der Gruppenrichtlinie aktiviert ist).

Gibt es einen Ereignisprotokolleintrag auf dem Clientcomputer, um den Erfolg oder Misserfolg der Active Directory-Sicherung anzugeben?

Ja, es gibt einen Ereignisprotokolleintrag, der angibt, dass der Erfolg oder Misserfolg einer Active Directory-Sicherung auf dem Clientcomputer aufgezeichnet ist. Auch wenn in einem Ereignisprotokolleintrag "Erfolg" angezeigt wird, könnten die Informationen später aus "hinzufügen" entfernt werden, oder BitLocker könnte so konfiguriert werden, dass die Active Directory-Informationen das Laufwerk nicht mehr entsperren können (beispielsweisedurch Entfernen des Wiederherstellungskennwort-Schlüsselschutz). Darüber hinaus ist es auch möglich, dass der Protokolleintrag manipuliert worden sein könnte.

Um zu ermitteln, ob eine legitime Sicherung in Adds vorhanden ist, müssen Sie letztendlich mithilfe des BitLocker-Kennwortanzeige Tools Abfrage hinzufügen.

Wenn ich das BitLocker-Wiederherstellungskennwort auf meinem Computer ändere und das neue Kennwort in Adds speichere, fügt Adds das alte Kennwort überschrieben hinzu?

Nein. Nach dem Entwurf werden BitLocker-Wiederherstellungskennwort-Einträge nicht aus Adds gelöscht; Daher werden möglicherweise mehrere Kennwörter für die einzelnen Laufwerke angezeigt. Überprüfen Sie das Datum auf dem Objekt, um das aktuelle Kennwort zu ermitteln.

Was geschieht, wenn die Sicherung anfänglich fehlschlägt? Wird die Sicherung von BitLocker wiederholt?

Wenn die Sicherung anfänglich fehlschlägt, beispielsweise wenn ein Domänencontroller zum Zeitpunkt der Ausführung des BitLocker-Setup-Assistenten nicht erreichbar ist, versucht BitLocker nicht erneut, die Wiederherstellungsinformationen zu sichern, um Sie hinzufügen zu können.

Wenn ein Administrator das Kontrollkästchen **BitLocker-Sicherung zum Hinzufügen** von BitLocker für die **Speicherung von BitLocker-Wiederherstellungsinformationen in Active Directory-Domänendienst (Windows 2008 und Windows Vista)** aktiviert, oder das entsprechende Kontrollkästchen **BitLocker erst dann aktivieren, wenn die Wiederherstellungsinformationen in AD DS für (Betriebssystem | behobene Daten | Wechseldaten) Laufwerke** in einem der von **BitLocker-geschützten Betriebssystemlaufwerke wiederhergestellt werden können**, wählen Sie aus, **wie BitLocker-geschützt behobene Datenlaufwerke**

können wiederhergestellt werden, **Wählen Sie aus, wie BitLocker-geschützte Wechseldaten Laufwerke wiederhergestellt werden können** Richtlinieneinstellungen, dadurch wird verhindert, dass Benutzer BitLocker aktivieren, es sei denn, der Computer ist mit der Domäne verbunden, und die Backup-Informationen für BitLocker-Wiederherstellungsinformationen werden erfolgreich hinzugefügt. Wenn die Sicherung mit diesen konfigurierten Einstellungen nicht erfolgreich ist, kann BitLocker nicht aktiviert werden. Dadurch wird sichergestellt, dass Administratoren BitLocker-geschützte Laufwerke in der Organisation wiederherstellen können.

Weitere Informationen finden Sie unter BitLocker-Gruppenrichtlinieneinstellungen.

Wenn ein Administrator diese Kontrollkästchen deaktiviert, lässt der Administrator ein Laufwerk BitLocker-geschützt werden, ohne dass die Wiederherstellungsinformationen erfolgreich auf Adds gesichert werden können. BitLocker wird die Sicherung jedoch nicht automatisch wiederholen, wenn ein Fehler auftritt. Stattdessen können Administratoren ein Skript für die Sicherung erstellen (wie zuvor in Was geschieht, wenn BitLocker auf einem Computer aktiviert ist, bevor der Computer der Domäne beigetreten ist? beschrieben), um die Informationen zu erfassen, nachdem die Verbindung wiederhergestellt wurde.

Häufig gestellte Fragen zu BitLocker-Sicherheit

20.12.2019 • 2 minutes to read

Gilt für:

- Windows 10

Welche Art der Verschlüsselung verwendet BitLocker? Ist diese konfigurierbar?

BitLocker verwendet den erweiterten Verschlüsselungsstandard (Advanced Encryption Standard, AES) als Verschlüsselungsalgorithmus mit einer konfigurierbaren Schlüssellänge von 128 oder 256 Bits. Die Standardeinstellung für die Verschlüsselung lautet AES-128, allerdings können die Optionen mithilfe der Gruppenrichtlinie konfiguriert werden.

Wie lautet die beste Vorgehensweise für die Verwendung von BitLocker auf einem Betriebssystemlaufwerk?

Die empfohlene Vorgehensweise für die BitLocker-Konfiguration auf einem Betriebssystemlaufwerk besteht darin, BitLocker auf einem Computer mit einer TPM-Version 1.2 oder höher und einer TCG-kompatiblen BIOS-oder UEFI-Firmware-Implementierung sowie einer PIN zu implementieren. Durch die Verwendung einer PIN, die vom Benutzer zusätzlich zur TPM-Überprüfung festgelegt wurde, kann ein böswilliger Benutzer, der physischen Zugriff auf den Computer hat, nicht einfach den Computer starten.

Welche Auswirkungen resultieren aus der Verwendung der Energieverwaltungsoptionen „Energiesparmodus" oder „Ruhezustand"?

BitLocker auf Betriebssystemlaufwerken in der Grundkonfiguration (mit einem TPM, aber ohne zusätzliche Start Authentifizierung) bietet zusätzliche Sicherheit für den Ruhezustandsmodus. BitLocker bietet jedoch eine größere Sicherheit, wenn es für die Verwendung eines zusätzlichen Start Authentifizierungsfaktors (TPM + PIN, TPM + USB oder TPM + PIN + USB) mit dem Hibernate-Modus konfiguriert ist. Diese Methode ist sicherer, da für die Rückgabe aus dem Ruhezustand eine Authentifizierung erforderlich ist. Um die Sicherheit zu verbessern, empfehlen wir, den Ruhemodus zu deaktivieren und die TPM +-PIN für die Authentifizierungsmethode zu verwenden. Die Start Authentifizierung kann mithilfe der Gruppenrichtlinie oder der Verwaltung mobiler Geräte mit dem BitLocker-Kryptografiedienstanbieterkonfiguriert werden.

Welche Vorteile bietet ein TPM?

Die meisten Betriebssysteme verwenden einen freigegebenen Speicherbereich und sind vom Betriebssystem abhängig, um den physischen Speicher zu verwalten. Ein TPM ist eine Hardwarekomponente, die die eigene interne Firmware und logische Schaltungen zum Verarbeiten von Anweisungen verwendet. Auf diese Weise wird der Schutz vor Sicherheitslücken bei externer Software sichergestellt. Bei Angriffen auf das TPM ist physischer Zugriff auf den Computer erforderlich. Darüber hinaus sind die erforderlichen Tools und die Fähigkeiten für den Angriff auf die Hardware oftmals umfangreicher und stehen in der Regel nicht so zur Verfügung wie diejenigen, die für den Angriff auf die Software verwendet werden. Da jedes TPM für den Computer, auf dem es vorhanden ist, spezifisch ist, ist der Angriff auf mehrere TPM-Computer schwierig und zeitaufwendig.

NOTE

Das Konfigurieren von BitLocker mit einem zusätzlichen Authentifizierungs Faktor bietet noch mehr Schutz vor TPM-Hardware Angriffen.

Häufig gestellte Fragen zur BitLocker-Netzwerksperrung

20.12.2019 • 2 minutes to read

Gilt für:

- Windows 10

Die BitLocker-Netzwerkentsperrung ermöglicht die einfache Verwaltung für BitLocker-aktivierte Desktops und Server, die die Schutzmethode TPM und PIN in einer Domänenumgebung verwenden. Beim Neustart eines Computers, der mit einem verkabelten Unternehmensnetzwerk verbunden ist, ermöglicht die Netzwerkentsperrung, dass die Aufforderung zur PIN-Eingabe umgangen wird. BitLocker-geschützte Betriebssystemvolumes werden mit einem vertrauenswürdigen Schlüssel automatisch entsperrt. Dieser Schlüssel wird vom Windows-Bereitstellungsdiensteserver als sekundäre Authentifizierungsmethode bereitgestellt.

Damit Sie die Netzwerkentsperrung verwenden können, benötigen Sie auch eine PIN, die für den Computer konfiguriert ist. Wenn der Computer nicht mit dem Netzwerk verbunden ist, müssen Sie die PIN eingeben, um die Sperrung aufzuheben.

Die BitLocker-Netzwerkentsperrung verfügt über Software- und Hardwareanforderungen für Clientcomputer, Windows-Bereitstellungsdienste und Domänencontroller, die erfüllt sein müssen, bevor Sie sie verwenden können.

Die Netzwerkentsperrung verwendet zwei Schutzvorrichtungen, die TPM-Schutzvorrichtung und die Schutzvorrichtung, die durch das Netzwerk oder Ihre PIN bereitgestellt wird. Bei der automatischen Entsperrung wird hingegen eine einzelne Schutzvorrichtung verwendet und zwar die, die im TPM gespeichert ist. Wenn der Computer mit einem Netzwerk ohne die Schlüsselschutzvorrichtung verbunden ist, werden Sie zur Eingabe Ihrer PIN aufgefordert. Wenn die PIN nicht verfügbar ist, müssen Sie den Wiederherstellungsschlüssel verwenden, um den Computer zu entsperren, wenn keine Verbindung mit dem Netzwerk hergestellt werden kann.

Weitere Informationen finden Sie unter BitLocker: Aktivieren der Netzwerkentsperrung.

Häufig gestellte Fragen zur Verwendung von BitLocker mit anderen Programmen

20.12.2019 • 5 minutes to read

Gilt für:

- Windows 10

Kann ich EFS mit BitLocker verwenden?

Ja, Sie können EFS (Encrypting File System) verwenden, um Dateien auf einem mit BitLocker geschützten Laufwerk zu verschlüsseln. BitLocker hilft beim Schutz des gesamten Betriebssystemlaufwerks vor Offlineangriffen, während EFS eine zusätzliche benutzerbasierte Verschlüsselung auf Dateiebene bereitstellen kann, um die Sicherheits Trennung zwischen mehreren Benutzern desselben Computers zu gewährleisten. Sie können EFS in Windows auch zum Verschlüsseln von Dateien auf anderen Laufwerken verwenden, die nicht von BitLocker verschlüsselt wurden. Die Stamm Geheimnisse von EFS werden standardmäßig auf dem Betriebssystemlaufwerk gespeichert. Wenn BitLocker für das Betriebssystemlaufwerk aktiviert ist, werden daher auch Daten, die von EFS auf anderen Laufwerken verschlüsselt sind, indirekt durch BitLocker geschützt.

Kann ein Kerneldebugger mit BitLocker ausgeführt werden?

Ja. Der Debugger sollte jedoch vor der Aktivierung von BitLocker aktiviert sein. Durch das Aktivieren des Debuggers wird sichergestellt, dass die richtigen Maße beim Einfügen in das TPM berechnet werden, sodass der Computer ordnungsgemäß startet. Wenn Sie das Debuggen aktivieren oder deaktivieren müssen, wenn Sie BitLocker verwenden, müssen Sie zuerst BitLocker anhalten, um zu verhindern, dass der Computer in den Wiederherstellungsmodus versetzt wird.

Wie werden Speicherabbilder von BitLocker verarbeitet?

BitLocker verfügt über einen Speichertreiberstapel, der sicherstellt, dass Speicherabbilder verschlüsselt werden, wenn BitLocker aktiviert ist.

Unterstützt BitLocker Smartcards für die Authentifizierung vor dem Start?

BitLocker unterstützt Smartcards nicht für die Authentifizierung vor dem Start. Es gibt keinen einzigen Industriestandard für die Smartcard-Unterstützung in der Firmware, und die meisten Computern implementieren nicht den Firmwaresupport für Smartcards oder unterstützen nur bestimmte Smartcards und Leser. Durch diese mangelnde Standardisierung ist die Unterstützung sehr schwierig.

Kann ich einen nicht von Microsoft stammenden TPM-Treiber verwenden?

Microsoft bietet keine Unterstützung für nicht von Microsoft stammende TPM-Treiber und empfiehlt ausdrücklich, diese nicht mit BitLocker zu verwenden. Wenn Sie versuchen, einen nicht von Microsoft stammenden TPM-Treiber mit BitLocker zu verwenden, meldet BitLocker möglicherweise, dass kein TPM auf dem Computer vorhanden ist und dass das TPM nicht mit BitLocker verwendet werden kann.

Können andere Tools, die die Master Boot Record-Arbeit verwalten oder ändern, mit BitLocker verwendet werden?

Es wird nicht empfohlen, den Master Boot Record auf Computern zu ändern, deren Betriebssystemlaufwerke aus diversen Sicherheits-, Zuverlässigkeits- und Produktsupport-Gründen BitLocker-geschützt sind. Änderungen am Master Boot Record (MBR) können die Sicherheitsumgebung verändern und den normalen Start des Computers verhindern sowie alle Maßnahmen zur Wiederherstellung eines beschädigten MBR erschweren. Änderungen, die am MBR von einem anderen Programm als Windows vorgenommen wurden, können dazu führen, dass der Computer in den Wiederherstellungsmodus wechselt oder verhindern, dass er vollständig gestartet wird.

Warum schlägt die Systemüberprüfung fehl, wenn ich mein Betriebssystemlaufwerk verschlüssele?

Die Systemüberprüfung wurde entwickelt, um sicherzustellen, dass die BIOS- oder UEFI-Firmware Ihres Computers mit BitLocker kompatibel ist und dass das TPM ordnungsgemäß ausgeführt wird. Die Systemüberprüfung kann aus verschiedenen Gründen fehlschlagen:

- Die BIOS- oder UEFI-Firmware des Computers kann keine USB-Speichersticks lesen.
- Die BIOS- oder UEFI-Firmware des Computers oder das Startmenü ist nicht für das Lesen von USB-Speichersticks aktiviert.
- Es gibt mehrere in den Computer eingesetzte USB-Speichersticks.
- Die PIN wurde nicht richtig eingegeben.
- Die BIOS- oder UEFI-Firmware des Computers unterstützt nur die Verwendung der Funktionstasten (F1 bis F10), um Zahlen in der Umgebung vor dem Start einzugeben.
- Der Systemstartschlüssel wurde entfernt, bevor der Neustart des Computers abgeschlossen war.
- Das TPM hat nicht ordnungsgemäß funktioniert und kann die Versiegelung der Schlüssel nicht aufheben.

Was kann ich tun, wenn der Wiederherstellungsschlüssel auf dem USB-Speicherstick nicht gelesen werden kann?

Einige Computer sind nicht in der Lage, USB-Speichersticks in der Umgebung vor dem Start zu lesen. Überprüfen Sie zunächst Ihre BIOS- oder UEFI-Firmware und die Starteinstellungen, um sicherzustellen, dass die Verwendung von USB-Laufwerken aktiviert ist. Wenn die Option nicht aktiviert ist, aktivieren Sie die Verwendung von USB-Laufwerken in der BIOS- oder UEFI-Firmware und in den Starteinstellungen, und versuchen Sie anschließend, den Wiederherstellungsschlüssel erneut vom USB-Speicherstick zu lesen. Wenn der Lesevorgang noch immer nicht möglich ist, müssen Sie die Festplatte als Datenlaufwerk auf einem anderen Computer bereitstellen, sodass ein Betriebssystem vorhanden ist und versucht wird, den Wiederherstellungsschlüssel vom USB-Speicherstick zu lesen. Wenn der USB-Stick beschädigt oder beschädigt ist, müssen Sie möglicherweise ein Wiederherstellungskennwort angeben oder die wiederhergestellten Wiederherstellungsinformationen verwenden. Wenn Sie den Wiederherstellungsschlüssel in der Umgebung vor dem Start verwenden, stellen Sie sicher, dass das Laufwerk mithilfe des NTFS-, FAT16- oder FAT32-Dateisystems formatiert ist.

Warum kann ich meinen Wiederherstellungsschlüssel nicht auf dem USB-Speicherstick speichern?

Die Option **Auf USB-Speicherstick speichern** wird bei Wechseldatenträgern standardmäßig nicht angezeigt. Wenn die Option nicht verfügbar ist, bedeutet dies, dass ein Systemadministrator die Verwendung der Wiederherstellungsschlüssel nicht erlaubt hat.

Warum kann ich das Laufwerk nicht automatisch entsperren?

Für das automatische Entsperren von Festplattenlaufwerken muss das Betriebssystemlaufwerk auch durch BitLocker geschützt sein. Wenn Sie einen Computer verwenden, der nicht über ein BitLocker-geschütztes Betriebssystemlaufwerk verfügt, kann das Laufwerk nicht automatisch entsperrt werden. Bei Wechseldatenträgern können Sie die automatische Entsperrung hinzufügen, indem Sie mit der rechten Maustaste auf das Laufwerk in Windows Explorer klicken und dann **BitLocker verwalten**auswählen. Sie können weiterhin die Kennwort- oder Smartcard-Anmeldeinformationen verwenden, die Sie beim Aktivieren von BitLocker bereitgestellt haben, um den Wechseldatenträger auf anderen Computern zu entsperren.

Kann ich BitLocker im abgesicherten Modus verwenden?

Im abgesicherten Modus ist die eingeschränkte BitLocker-Funktionalität verfügbar. BitLocker-geschützte Laufwerke können mit dem Systemsteuerungselement **BitLocker-Laufwerksverschlüsselung** entsperrt und entschlüsselt werden. Im abgesicherten Modus gibt es nicht die Möglichkeit, mit der rechten Maustaste zu klicken, um auf die BitLocker-Optionen über Windows-Explorer zuzugreifen.

Wie sperre ich ein Datenlaufwerk?

Sowohl Festplattenlaufwerke als auch Wechseldatenträger können mithilfe des Befehlszeilentools „Manage-bde“ und des Befehls „–lock“ gesperrt werden.

> **NOTE**
> Stellen Sie sicher, dass alle Daten auf dem Laufwerk gespeichert sind, bevor Sie Sie sperren. Nachdem es gesperrt wurde, kann nicht mehr auf das Laufwerk zugegriffen werden.

Die Syntax dieses Befehls lautet:

```
manage-bde driveletter -lock
```

Abgesehen von der Verwendung dieses Befehls werden Datenlaufwerke beim Herunterfahren und Neustart des Betriebssystems gesperrt. Ein Wechseldatenträger wird auch automatisch gesperrt, wenn das Laufwerk vom Computer entfernt wird.

Kann ich BitLocker mit dem Volumenschattenkopie-Dienst verwenden?

Ja. Schattenkopien, die vor der Aktivierung von BitLocker erstellt wurden, werden automatisch gelöscht, wenn BitLocker auf softwareverschlüsselten Laufwerken aktiviert ist. Wenn Sie ein hardwareverschlüsseltes Laufwerk verwenden, werden die Schattenkopien beibehalten.

Unterstützt BitLocker virtuelle Festplatten (Virtual Hard Disks, VHDs)?

BitLocker sollte wie ein bestimmter physischer Computer innerhalb seiner Hardwareeinschränkungen funktionieren, solange die Umgebung (physisch oder virtuell) die Windows-Betriebs System Anforderungen erfüllt, um ausgeführt zu werden.

- Mit TPM-ja wird es unterstützt
- Ohne TPM-ja, es wird unterstützt (mit Kennwortschutz)

BitLocker wird auch für VHD-Datenmengen unterstützt, beispielsweise für die von Clustern verwendeten, wenn Sie Windows10, Windows 8,1, Windows 8, Windows Server 2016, Windows Server 2012 R2 oder Windows Server 2012 ausführen.

Kann ich BitLocker mit virtuellen Computern (VMs) verwenden?

Ja. Mit BitLocker können Kennwortschutz und virtuelle TPMs verwendet werden, um virtuelle Computer zu schützen. VMs können Domänen verbunden, Azure AD-Joined oder Workplace-Joined (über **Einstellungen** > **-Konten** > **Access work oder School** > **Connect**) sein, um Richtlinien zu empfangen. Sie können die Verschlüsselung beim Erstellen des virtuellen Computers oder über andere vorhandene Verwaltungstools wie BitLocker CSP aktivieren. Sie können sogar ein Start- oder Anmeldeskript verwenden, das von der Gruppenrichtlinie bereitgestellt wird. Windows Server2016 unterstützt darüber hinaus abgeschirmte VMs und geschütztes Fabric, um VMs vor böswilligen Administratoren zu schützen.

Vorbereiten Ihrer Organisation auf BitLocker: Planung und Richtlinien

06.03.2020 • 12 minutes to read

Betriff:

- Windows 10

In diesem Thema, das sich an IT-Experten richtet, wird erläutert, wie Sie Ihre BitLocker-Bereitstellung planen können.

Wenn Sie Ihre BitLocker-Bereitstellungsstrategie entwerfen, definieren Sie die geeigneten Richtlinien und Konfigurationsanforderungen basierend auf den Geschäftsanforderungen Ihrer Organisation. Die folgenden Themen unterstützen Sie beim Sammeln von Informationen, die Sie für die Gestaltung Ihres Entscheidungsprozesses zum Bereitstellen und Verwalten von BitLocker-Systemen verwenden können.

Überwachen Ihrer Umgebung

Wenn Sie Ihre Unternehmensbereitstellung von BitLocker planen möchten, müssen Sie zunächst die aktuelle Umgebung kennen. Führen Sie eine informelle Überprüfung durch, um Ihre aktuellen Richtlinien, Verfahren und Hardwareumgebungen zu definieren. Überprüfen Sie zunächst Ihre vorhandenen Unternehmenssicherheitsrichtlinien im Zusammenhang mit der datenträgerverschlüsselungssoftware. Wenn in Ihrer Organisation derzeit keine datenträgerverschlüsselungssoftware verwendet wird, gibt es keine dieser Richtlinien. Wenn Sie datenträgerverschlüsselungssoftware verwenden, müssen Sie möglicherweise die Richtlinien Ihrer Organisation ändern, um die Funktionen von BitLocker zu berücksichtigen.

Verwenden Sie die folgenden Fragen, damit Sie die aktuellen Sicherheitsrichtlinien für die Datenträgerverschlüsselung in Ihrer Organisation dokumentieren können:

1. Gibt es Richtlinien zur Behebung der Verwendung von BitLocker durch Computer, und auf welchen Computern wird BitLocker nicht verwendet?
2. Welche Richtlinien bestehen zum Steuern des Wiederherstellungskennworts und des Wiederherstellungsschlüssel Speichers?
3. Was sind die Richtlinien für die Überprüfung der Identität von Benutzern, die BitLocker-Wiederherstellung durchführen müssen?
4. Welche Richtlinien bestehen, um zu steuern, wer in der Organisation Zugriff auf Wiederherstellungsdaten hat?
5. Welche Richtlinien bestehen, um die Außerbetriebnahme von Computern oder den Ruhestand zu steuern?

Verschlüsselungsschlüssel und Authentifizierung

BitLocker verhindert unbefugten Zugriff auf Daten auf verlorenen oder gestohlenen Computern durch:

- Verschlüsseln des gesamten Windows-Betriebssystemdatenträgers auf der Festplatte.
- Überprüfen der Integrität des Startprozesses

Das Trusted Platform Module (TPM) ist eine Hardwarekomponente, die von den Computerherstellern auf vielen neueren Computern installiert ist. Es dient In Kombination mit BitLocker zum Schutz der Benutzerdaten und um sicherzustellen, dass ein Computer nicht manipuliert wurde, während das System offline geschaltet war.

Darüber hinaus bietet BitLocker die Option zum Sperren des normalen Startvorgangs, bis der Benutzer eine persönliche Identifikationsnummer (PIN) bereitstellt oder ein Wechselspeichergerät, beispielsweise ein

Flashlaufwerk, mit einem Startschlüssel, einfügt. Diese zusätzlichen Sicherheitsmaßnahmen bieten eine mehrstufige Authentifizierung und sorgen dafür, dass der Computer nicht startet oder den Betrieb aus dem Ruhezustand fortsetzt, bis die richtige PIN oder ein Systemstartschlüssel bereitgestellt wird.

Auf Computern, die nicht über eine TPM-Version 1.2 oder höher verfügen, können Sie weiterhin BitLocker verwenden, um das Windows-Betriebssystem zu verschlüsseln. Bei dieser Implementierung muss der Benutzer jedoch einen USB-Startschlüssel einfügen, um den Computer zu starten oder aus dem Ruhezustand zu starten, und bietet keine Überprüfung vor dem Start der Systemintegrität, die von BitLocker bei der Arbeit mit einem TPM angeboten wird.

BitLocker-Schlüssel Beschützer

SCHLÜSSELSCHUTZ	BESCHREIBUNG
TPM	Ein Hardwaregerät, das bei der Einrichtung einer sicheren Vertrauensbasis verwendet wird. BitLocker unterstützt nur TPM, Version 1,2 oder höher.
PIN	Eine vom Benutzer eingegebene numerische Schlüssel Beschützerin, die nur zusätzlich zum TPM verwendet werden kann.
Erweiterte PIN	Eine vom Benutzer eingegebene Alphanumerische Tasten Beschützer, die nur zusätzlich zum TPM verwendet werden kann.
Start Taste	Ein Verschlüsselungsschlüssel, der auf den meisten Wechselmedien gespeichert werden kann. Dieser Schlüsselschutz kann alleine auf nicht-TPM-Computern oder in Verbindung mit einem TPM für zusätzliche Sicherheit verwendet werden.
Wiederherstellungskennwort	Eine 48-stellige Nummer, die zum Entsperren eines Volumes verwendet wird, wenn es sich im Wiederherstellungsmodus befindet. Zahlen können oft auf einer normalen Tastatur eingegeben werden, wenn die Zahlen auf der normalen Tastatur nicht reagieren, können Sie immer die Funktionstasten (F1-F10) verwenden, um die Zahlen einzugeben.
Wiederherstellungsschlüssel	Ein auf Wechselmedien gespeicherter Verschlüsselungsschlüssel, der zum Wiederherstellen von auf einem BitLocker-Volume verschlüsselten Daten verwendet werden kann.

BitLocker-Authentifizierungsmethoden

AUTHENTIFIZIERUNGSMETHODE	ERFORDERT BENUTZERINTERAKTION	BESCHREIBUNG
Nur TPM	Nein	TPM überprüft frühe Startkomponenten.

AUTHENTIFIZIERUNGSMETHODE	ERFORDERT BENUTZERINTERAKTION	BESCHREIBUNG
TPM + PIN	Ja	TPM überprüft frühe Startkomponenten. Der Benutzer muss die richtige PIN eingeben, bevor der Startvorgang fortgesetzt werden kann, und bevor das Laufwerk freigegeben werden kann. Das TPM wird gesperrt, wenn die falsche PIN wiederholt eingegeben wird, um die PIN vor Brute-Force-Angriffen zu schützen. Die Anzahl wiederholter Versuche, die eine Sperrung auslösen, ist variabel.
TPM + Netzwerkschlüssel	Nein	Das TPM überprüft die frühen Startkomponenten erfolgreich, und ein gültiger verschlüsselter Netzwerkschlüssel wurde vom WDS-Server bereitgestellt. Diese Authentifizierungsmethode bietet automatisches Entsperren von Betriebssystem-Volumes beim Systemneustart, während die mehrstufige Authentifizierung weiterhin beibehalten wird.
TPM + Startschlüssel	Ja	Das TPM überprüft die frühen Startkomponenten erfolgreich, und es wurde ein USB-Flashlaufwerk mit dem Startschlüssel eingefügt.
Nur Startschlüssel	Ja	Der Benutzer wird aufgefordert, das USB-Flashlaufwerk einzufügen, das den Wiederherstellungsschlüssel und/oder den Startschlüssel enthält, und den Computer neu zu starten.

Werden Computer ohne TPM-Version 1,2 oder höher unterstützt?

Ermitteln Sie, ob Sie Computer unterstützen möchten, die in Ihrer Umgebung nicht über eine TPM-Version 1,2 oder höher verfügen. Wenn Sie BitLocker auf diesem Computertyp unterstützen möchten, muss ein Benutzer einen USB-Startschlüssel verwenden, um das System zu booten. Dies erfordert zusätzliche Support Prozesse, die mit der mehrstufigen Authentifizierung vergleichbar sind.

Welche Bereiche in Ihrer Organisation benötigen eine Baseline-Ebene des Datenschutzes?

Die TPM-Authentifizierungsmethode bietet für Organisationen, die eine Baseline-Ebene des Datenschutzes benötigen, um die Sicherheitsrichtlinien zu erfüllen, die am besten transparente Benutzeroberfläche. Sie hat die niedrigsten Gesamtbetriebskosten. TPM-only eignet sich möglicherweise auch für Computer, die unbeaufsichtigt sind oder die unbeaufsichtigt neu gestartet werden müssen.

Die TPM-Authentifizierungsmethode bietet jedoch die niedrigste Ebene des Datenschutzes. Diese Authentifizierungsmethode schützt vor Angriffen, bei denen frühe Startkomponenten geändert werden, doch der Schutzgrad kann durch mögliche Schwächen in der Hardware oder in den frühen Startkomponenten beeinträchtigt werden. Die mehrstufigen Authentifizierungsmethoden von BitLocker erhöhen die Gesamtdaten Sicherheit erheblich.

Welche Bereiche Ihrer Organisation benötigen ein sichereres Maß an Datenschutz?

Wenn es Bereiche in Ihrer Organisation gibt, in denen Daten auf Benutzercomputern als hoch sensibel eingestuft

werden, sollten Sie die bewährte Methode zum Bereitstellen von BitLocker mithilfe der mehrstufigen Authentifizierung auf diesen Systemen berücksichtigen. Wenn der Benutzer eine PIN eingeben muss, erhöht sich der Schutzgrad für das System erheblich. Sie können auch die BitLocker-Netzwerksperrung verwenden, damit diese Computer automatisch entsperrt werden, wenn Sie mit einem vertrauenswürdigen Kabelnetzwerk verbunden sind, das den Netzwerkfreigabe Schlüssel bereitstellen kann.

Welche mehrstufige Authentifizierungsmethode bevorzugt Ihre Organisation?

Die von mehrstufigen Authentifizierungsmethoden bereitgestellten Schutz Unterschiede können nicht einfach quantifiziert werden. Bedenken Sie die Auswirkungen jeder Authentifizierungsmethode auf Helpdesk-Support, Benutzerschulung, Benutzerproduktivität und automatisierte Systemverwaltungsprozesse.

TPM-Hardwarekonfigurationen

Ermitteln Sie in Ihrem Bereitstellungsplan, welche TPM-basierten Hardwareplattformen unterstützt werden. Dokumentieren Sie die Hardware Modelle von einem OEM Ihrer Wahl, damit Ihre Konfigurationen getestet und unterstützt werden können. TPM-Hardware erfordert besondere Berücksichtigung in allen Aspekten der Planung und Bereitstellung.

TPM-1,2-Zustände und-Initialisierung

Für TPM 1,2 gibt es mehrere mögliche Zustände. Windows 10 initialisiert das TPM automatisch, wodurch es in einen aktivierten, aktivierten und im Besitz befindlichen Zustand versetzt wird. Dies ist der Zustand, den BitLocker benötigt, bevor er das TPM verwenden kann.

Bestätigungsschlüssel

Damit ein TPM von BitLocker verwendet werden kann, muss es einen bestätigungsschlüssel enthalten, bei dem es sich um ein RSA-Schlüsselpaar handelt. Die private Hälfte des Schlüsselpaars befindet sich im TPM und wird niemals außerhalb des TPM offenbart oder darauf zugegriffen. Wenn das TPM keinen bestätigungsschlüssel enthält, wird es von BitLocker erzwungen, dass das TPM automatisch im Rahmen des BitLocker-Setups generiert wird.

Ein bestätigungsschlüssel kann an verschiedenen Stellen im TPM-Lebenszyklus erstellt werden, muss jedoch nur einmal für die Lebensdauer des TPMs erstellt werden. Wenn für das TPM kein bestätigungsschlüssel vorhanden ist, muss er erstellt werden, bevor TPM-Besitz übernommen werden kann.

Weitere Informationen zum TPM und zur TCG finden Sie in der Gruppe vertrauenswürdige Computer: Trusted Platform Module (TPM)https://go.microsoft.com/fwlink/p/?linkid=69584-Spezifikationen ().

Nicht-TPM-Hardwarekonfigurationen

Geräte, die kein TPM enthalten, können weiterhin durch die Laufwerkverschlüsselung geschützt werden. Windows to go-Arbeitsbereiche können mit einem Startkennwort mit BitLocker geschützt werden, und PCs ohne TPM können einen Startschlüssel verwenden.

Verwenden Sie die folgenden Fragen, um Probleme zu identifizieren, die sich auf die Bereitstellung in einer nicht-TPM-Konfiguration auswirken könnten:

- Sind Regeln für die Kennwortkomplexität vorhanden?
- Verfügen Sie über ein Budget für USB-Flash Laufwerke für jeden dieser Computer?
- Unterstützen Ihre vorhandenen nicht-TPM-Geräte USB-Geräte beim Booten?

Testen Sie Ihre einzelnen Hardwareplattformen mit der Option BitLocker-Systemüberprüfung, während Sie BitLocker aktivieren. Mit der Systemüberprüfung wird sichergestellt, dass BitLocker die Wiederherstellungsinformationen von einem USB-Gerät und die Verschlüsselungsschlüssel korrekt lesen kann, bevor Sie die Lautstärke verschlüsseln. CD-und DVD-Laufwerke können nicht als Blockspeicher Gerät fungieren und können nicht zum Speichern des BitLocker-Wiederherstellungs Materials verwendet werden.

Überlegungen zur Datenträgerkonfiguration

Um ordnungsgemäß zu funktionieren, erfordert BitLocker eine bestimmte Datenträgerkonfiguration. Für BitLocker sind zwei Partitionen erforderlich, die die folgenden Anforderungen erfüllen:

- Die Betriebssystempartition enthält das Betriebssystem und die zugehörigen Unterstützungsdateien. Sie muss mit dem NTFS-Dateisystem formatiert sein.
- Die Systempartition (oder Startpartition) enthält die Dateien, die erforderlich sind, um Windows zu laden, nachdem das BIOS oder UEFI-Firware die System Hardware vorbereitet hat. BitLocker ist auf dieser Partition nicht aktiviert. Damit BitLocker funktioniert, darf die Systempartition nicht verschlüsselt sein und sich auf einer anderen Partition als dem Betriebssystem befinden. Auf UEFI-Plattformen muss die Systempartition mit dem FAT 32-Dateisystem formatiert sein. Auf BIOS-Plattformen muss die Systempartition mit dem NTFS-Dateisystem formatiert sein. Es sollte mindestens 350 MB groß sein.

Windows Setup konfiguriert automatisch die Festplattenlaufwerke Ihres Computers, um die BitLocker-Verschlüsselung zu unterstützen.

Die Windows-Wiederherstellungsumgebung (Windows RE) ist eine erweiterbare Wiederherstellungsplattform, die auf der Windows-Vorinstallationsumgebung (Windows PE) basiert. Wenn der Computer nicht gestartet werden kann, wechselt Windows automatisch in diese Umgebung, und das Tool zum Starten der Reparatur in Windows RE automatisiert die Diagnose und Reparatur einer nicht startfähigen Windows-Installation. Windows RE enthält auch die Treiber und Tools, die zum Entsperren eines von BitLocker geschützten Volumes erforderlich sind, indem Sie einen Wiederherstellungsschlüssel oder ein Wiederherstellungskennwort angeben. Wenn Sie Windows RE in Verbindung mit BitLocker verwenden möchten, muss sich das Windows RE-Startabbild auf einem Volume befinden, das nicht von BitLocker geschützt ist.

Windows RE kann auch von anderen Startmedien als der lokalen Festplatte verwendet werden. Wenn Sie Windows RE nicht auf der lokalen Festplatte von BitLocker-aktivierten Computern installieren möchten, können Sie für die Wiederherstellung Alternative Startmethoden wie Windows-Bereitstellungsdienste, CD-ROM oder USB-Flashlaufwerk verwenden.

BitLocker-Bereitstellung

In Windows Vista und Windows 7 wurde BitLocker nach der Installation für System-und Daten Volumes über die Befehlszeilenschnittstelle manage-bde oder die Benutzeroberfläche der Systemsteuerung bereitgestellt. Bei neueren Betriebssystemen kann BitLocker vor der Installation des Betriebssystems problemlos bereitgestellt werden. Voraus setmungen erfordern, dass der Computer ein TPM besitzt.

Um den BitLocker-Status eines bestimmten Volumes zu überprüfen, können Administratoren den Status des Laufwerks in der BitLocker-Systemsteuerung oder in Windows-Explorer sehen. Der Status "warten auf Aktivierung" mit einem gelben Ausrufezeichen bedeutet, dass das Laufwerk für BitLocker bereitgestellt wurde. Dieser Status bedeutet, dass beim Verschlüsseln des Volumes nur ein klarer Schutz verwendet wurde. In diesem Fall ist die Lautstärke nicht geschützt und muss dem Volume einen sicheren Schlüssel hinzugefügt haben, bevor das Laufwerk als vollständig geschützt gilt. Administratoren können die Optionen für die Systemsteuerung, das Tool "Manage-BDE" oder WMI-APIs verwenden, um einen geeigneten Schlüsselschutz hinzuzufügen, und der Datenträgerstatus wird aktualisiert.

Wenn Sie die Systemsteuerungsoptionen verwenden, können Administratoren auswählen, dass **BitLocker aktiviert** werden soll, und den Schritten im Assistenten folgen, um einen Beschützer hinzuzufügen, beispielsweise eine PIN für ein Betriebssystemvolume (oder ein Kennwort, wenn kein TPM vorhanden ist), oder ein Kennwort oder eine Smartcard-Schutzvorrichtung für ein Datenvolumen. Das Fenster Laufwerksicherheit wird angezeigt, bevor Sie den Lautstärke Status ändern.

Administratoren können BitLocker vor der Betriebssystembereitstellung über die Windows-Pre-Installation-Umgebung (WinPE) aktivieren. Dies erfolgt mit einem nach dem Zufallsprinzip generierten Clear Key Protector,

der auf das formatierte Volume angewendet wurde, und die Verschlüsselung des Volumes vor der Ausführung des Windows-Setupprozesses. Wenn für die Verschlüsselung nur die Option verwendeter Speicherplatz verwendet wird, dauert dieser Schritt nur wenige Sekunden und ist daher auch in regelmäßigen Bereitstellungsprozessen integriert.

Verschlüsselungsoption „Nur verwendeten Speicherplatz verschlüsseln“

Der BitLocker-Setup-Assistent bietet Administratoren die Möglichkeit, nur den verwendeten Speicherplatz oder die vollständige Verschlüsselungsmethode auszuwählen, wenn BitLocker für ein Volume aktiviert wird. Administratoren können die neue BitLocker-Gruppenrichtlinieneinstellung verwenden, um entweder den verwendeten Speicherplatz oder die vollständige Datenträgerverschlüsselung zu erzwingen.

Beim Starten des BitLocker-Setup-Assistenten werden Sie aufgefordert, die zu verwendende Authentifizierungsmethode einzugeben (Kennwort und Smartcard sind für Datenmengen verfügbar). Nachdem die Methode ausgewählt wurde und der Wiederherstellungsschlüssel gespeichert wurde, werden Sie aufgefordert, den Laufwerk Verschlüsselungs auszuwählen, entweder verwendeter Speicherplatz oder vollständige Laufwerkverschlüsselung.

Verwendeter Speicherplatz bedeutet nur, dass nur der Teil des Laufwerks, der Daten enthält, verschlüsselt wird, ungenutzter Speicherplatz bleibt unverschlüsselt. Dies führt zu einem wesentlich schnelleren Verschlüsselungsprozess, insbesondere bei neuen PCs und Datenlaufwerken. Wenn BitLocker mit dieser Methode aktiviert wird, wenn dem Laufwerk Daten hinzugefügt werden, wird der Teil des verwendeten Laufwerks verschlüsselt, sodass nie unverschlüsselte Daten auf dem Laufwerk gespeichert werden.

Vollständige Laufwerkverschlüsselung bedeutet, dass das gesamte Laufwerk verschlüsselt wird, unabhängig davon, ob Daten darin gespeichert sind oder nicht. Dies ist nützlich für Laufwerke, die umfunktioniert wurden und Datenreste aus der vorherigen Verwendung enthalten können.

Überlegungen zu Active Directory-Domänendiensten

BitLocker wird in Active Directory-Domänendienste (AD DS) integriert, um eine zentralisierte Schlüsselverwaltung bereitzustellen. Standardmäßig werden keine Wiederherstellungsinformationen in Active Directory gesichert. Administratoren können die folgende Gruppenrichtlinieneinstellung für jeden Laufwerktyp konfigurieren, um die Sicherung der BitLocker-Wiederherstellungsinformationen zu aktivieren:

Computer Configuration\Administrative Templates\Windows Components\BitLocker Drive Encryption*Drive Type*\Choose wie BitLocker-geschützte Laufwerke wiederhergestellt werden können.

Standardmäßig haben nur Domänenadministratoren Zugriff auf BitLocker-Wiederherstellungsinformationen, der Zugriff kann jedoch an andere Personen delegiert werden.

Die folgenden Wiederherstellungsdaten werden für jedes Computerobjekt gespeichert:

- **Wiederherstellungskennwort**

  Ein 48-stelliges Wiederherstellungskennwort, das zum Wiederherstellen eines von BitLocker geschützten Volumes verwendet wird. Benutzer geben dieses Kennwort ein, um ein Volume zu entsperren, wenn BitLocker in den Wiederherstellungsmodus wechselt.

- **Schlüsselpaket Daten**

  Mit diesem Schlüsselpaket und dem Wiederherstellungskennwort können Sie Teile eines von BitLocker geschützten Volumes entschlüsseln, wenn der Datenträger schwer beschädigt ist. Jedes Schlüsselpaket funktioniert nur mit dem Volume, auf dem es erstellt wurde, was mit der entsprechenden Volumen-ID identifiziert werden kann.

FIPS-Unterstützung für die Kennwortschutz-Wiederherstellung

Mit der in Windows Server 2012 R2 und Windows 8,1 eingeführten Funktionalität kann BitLocker im FIPS-Modus voll funktionsfähig sein.

> **NOTE**
>
> Der United States Federal Information Processing Standard (FIPS) definiert Sicherheits-und Interoperabilitätsanforderungen für Computersysteme, die von der US-Bundesregierung verwendet werden. Der FIPS 140-Standard definiert genehmigte kryptografische Algorithmen. Der FIPS 140-Standard legt auch Anforderungen für die Schlüsselgenerierung und für die Schlüsselverwaltung fest. Das National Institute of Standards and Technology (NIST) verwendet das Cryptographic Module Validation Program (CMVP), um zu ermitteln, ob eine bestimmte Implementierung eines kryptografischen Algorithmus mit dem FIPS 140-Standard kompatibel ist. Eine Implementierung eines kryptografischen Algorithmus gilt nur dann als FIPS-140-kompatibel, wenn Sie übermittelt wurde und die NIST-Validierung durchgeführt hat. Ein Algorithmus, der nicht übermittelt wurde, kann nicht als FIPS-kompatibel angesehen werden, selbst wenn die Implementierung identische Daten als validierte Implementierung desselben Algorithmus erzeugt.

Vor diesen unterstützten Windows-Versionen verhinderte BitLocker, wenn sich Windows im FIPS-Modus befand, die Erstellung oder Verwendung von Wiederherstellungskennwörtern und zwang den Benutzer stattdessen, Wiederherstellungsschlüssel zu verwenden. Weitere Informationen zu diesen Problemen finden Sie im Support Artikel kb947249.

Aber auf Computern, auf denen diese unterstützten Systeme mit aktiviertem BitLocker ausgeführt werden:

- FIPS-konforme Wiederherstellungs-Kenn Wort Schützer können erstellt werden, wenn sich Windows im FIPS-Modus befindet. Diese Beschützer verwenden den FIPS 140 NIST SP800-132-Algorithmus.
- Im FIPS-Modus auf Windows 8,1 erstellte Wiederherstellungskennwörter können von auf anderen Systemen erstellten Wiederherstellungskennwörtern unterschieden werden.
- Wiederherstellungs Sperre mithilfe der FIPS-kompatiblen Algorithmus-basierter Recovery-Kennwortschutzfunktion in allen Fällen, die derzeit für Wiederherstellungskennwörter funktionieren.
- Wenn FIPS-konforme Wiederherstellungskennwörter Volumes entsperren, wird das Volume freigegeben, um Lese-/Schreibzugriff auch im FIPS-Modus zu ermöglichen.
- FIPS-konforme Wiederherstellungs-Kenn Wort Schutze können in AD a im FIPS-Modus exportiert und gespeichert werden.

Die BitLocker-Gruppenrichtlinieneinstellungen für Wiederherstellungskennwörter funktionieren für alle Windows-Versionen, die BitLocker unterstützen, unabhängig davon, ob Sie sich im FIPS-Modus befinden oder nicht.

Sie können jedoch keine Wiederherstellungskennwörter verwenden, die auf einem System im FIPS-Modus für Systeme, die älter als Windows Server 2012 R2 und Windows 8,1 sind, generiert wurden. Auf Windows Server 2012 R2 und Windows 8,1 erstellte Wiederherstellungskennwörter sind mit BitLocker unter Betriebssystemen vor Windows Server 2012 R2 und Windows 8,1 nicht kompatibel. Daher sollten stattdessen Wiederherstellungsschlüssel verwendet werden.

Weitere Informationen

- Trusted Platform Module
- Gruppenrichtlinieneinstellungen für TPM-Dienste
- Häufig gestellte Fragen (Frequently Asked Questions, FAQ) zu BitLocker
- BitLocker
- BitLocker-Gruppenrichtlinieneinstellungen
- Grundlegende Bereitstellung von BitLocker

Grundlegende Bereitstellung von BitLocker

27.10.2019 • 20 minutes to read

Betrifft

- Windows 10

Dieses Thema richtet sich an IT-Experten und beschreibt die Verwendung von BitLocker-Features für den Schutz Ihrer Daten mithilfe von Laufwerkverschlüsselung.

Verwenden von BitLocker zum Verschlüsseln von Volumes

BitLocker bietet die vollständige Volumen Verschlüsselung (FVE) für Betriebssystem-Volumes sowie fest-und Wechseldaten-Volumes. Um vollständig verschlüsselte Betriebssystemdatenträger zu unterstützen, verwendet BitLocker ein unverschlüsseltes System Volume für die Dateien, die zum Booten, entschlüsseln und Laden des Betriebssystems erforderlich sind. Dieser Datenträger wird bei einer Neuinstallation von Client-und Server Betriebssystemen automatisch erstellt.

Für den Fall, dass das Laufwerk als einzelner zusammenhängender Speicherplatz bereitgestellt wurde, erfordert BitLocker ein neues Volume, in dem die Startdateien gespeichert werden. Diese Volumes können von BdeHdCfg.exe erstellt werden.

> **Hinweis:** Weitere Informationen zur Verwendung dieses Tools finden Sie unter Bdehdcfg im Befehlszeilen Bezug.

Die BitLocker-Verschlüsselung kann mithilfe der folgenden Methoden ausgeführt werden:

- BitLocker-Systemsteuerung
- Windows-Explorer
- manage-bde-Befehlszeilenschnittstelle
- BitLocker-Cmdlets für Windows PowerShell

Verschlüsseln von Volumes mithilfe der BitLocker-Systemsteuerung

Verschlüsseln von Volumes mit der BitLocker-Systemsteuerung (Klicken Sie auf **Start**, geben Sie **BitLocker**ein, klicken Sie auf **BitLocker verwalten**) gibt an, wie viele Benutzer BitLocker verwenden werden. Der Name der BitLocker-Systemsteuerung ist die BitLocker-Laufwerkverschlüsselung. Das BitLocker-Control Panel unterstützt die Verschlüsselung von Betriebssystemen, festen Daten und Wechseldatenträgern. Das BitLocker-Control Panel organisiert die verfügbaren Laufwerke in der entsprechenden Kategorie, je nachdem, wie sich das Gerät an Windows anmeldet. Nur formatierte Volumes mit zugewiesenen Laufwerkbuchstaben werden im BitLocker Control Panel-Applet ordnungsgemäß angezeigt. Wenn Sie die Verschlüsselung für ein Volume starten möchten, wählen Sie BitLocker für das entsprechende Laufwerk **aktivieren** aus, um den BitLocker-Laufwerk Verschlüsselungs-Assistenten zu initialisieren. Die Optionen für den BitLocker-Laufwerk Verschlüsselungs-Assistenten variieren je nach Datenträgertyp (Betriebssystem Lautstärke oder Datenvolumen).

Betriebssystem Lautstärke

Beim Start überprüft der BitLocker Drive Encryption-Assistent, ob der Computer die BitLocker-Systemanforderungen zum Verschlüsseln eines Betriebssystemdatenträgers erfüllt. Standardmäßig gelten folgende Systemanforderungen:

ANFORDERUNG	BESCHREIBUNG
Hardwarekonfiguration	Der Computer muss die Mindestanforderungen für die unterstützten Windows-Versionen erfüllen.
Betriebssystem	BitLocker ist ein optionales Feature, das vom Server-Manager unter Windows Server 2012 und höher installiert werden kann.
Hardware-TPM	TPM, Version 1.2 oder 2,0 Für BitLocker ist kein TPM erforderlich; Allerdings kann nur ein Computer mit einem TPM die zusätzliche Sicherheit der System Integritätsüberprüfung vor dem Start und der mehrstufigen Authentifizierung bieten.
BIOS-Konfiguration	• Eine TCG (Trusted Computing Group)-kompatibles BIOS oder UEFI-Firmware. • Die Startreihenfolge muss so fest eingestellt sein, dass Sie zuerst auf der Festplatte und nicht auf dem USB-oder CD-Laufwerk gestartet wird. • Die Firmware muss während des Starts von einem USB-Flashlaufwerk gelesen werden können.
Dateisystem	Für Computer, die nativ mit UEFI-Firmware Booten, mindestens eine FAT32-Partition für das Systemlaufwerk und eine NTFS-Partition für das Betriebssystemlaufwerk. Für Computer mit Legacy-BIOS-Firmware, mindestens zwei NTFS-Festplattenpartitionen, eine für das Systemlaufwerk und eine für das Betriebssystemlaufwerk. Bei beiden Firmware-Systemen muss die Systemlaufwerk Partition mindestens 350 Megabyte (MB) betragen und als aktive Partition festzulegen.
Voraussetzungen für Hardware verschlüsselte Laufwerke (optional)	Wenn Sie ein Hardware verschlüsselte Laufwerk als Startlaufwerk verwenden möchten, muss sich das Laufwerk im Zustand "nicht initialisiert" und im Status "Sicherheit inaktiv" befinden. Darüber hinaus muss das System immer mit der systemeigenen UEFI-Version 2.3.1 oder höher Booten, und die CSM (sofern vorhanden) ist deaktiviert.

Wenn die ursprüngliche Konfiguration übergeben wird, müssen die Benutzer ein Kennwort für die Lautstärke eingeben. Wenn das Volume nicht die anfängliche Konfiguration für BitLocker übergibt, wird der Benutzer mit einem Fehlerdialogfeld angezeigt, in dem die entsprechenden zu ergreifenden Aktionen beschrieben sind. Nachdem für das Volume ein sicheres Kennwort erstellt wurde, wird ein Wiederherstellungsschlüssel generiert. Der BitLocker-Laufwerk Verschlüsselungs-Assistent fordert zur Eingabe eines Speicherorts auf, um diesen Schlüssel zu speichern. Ein BitLocker-Wiederherstellungsschlüssel ist ein spezieller Schlüssel, den Sie erstellen können, wenn Sie die BitLocker-Laufwerkverschlüsselung zum ersten Mal auf jedem von Ihnen verschlüsselten Laufwerk aktivieren. Sie können den Wiederherstellungsschlüssel verwenden, um Zugriff auf Ihren Computer zu erhalten, wenn das Laufwerk, auf dem Windows installiert ist (das Betriebssystemlaufwerk), mithilfe der BitLocker-Laufwerkverschlüsselung verschlüsselt wird und BitLocker eine Bedingung erkennt, die verhindert, dass

das Laufwerk aufgehoben wird, wenn die der Computer wird gestartet. Ein Wiederherstellungsschlüssel kann auch verwendet werden, um auf einem Wechseldatenträger (wie einer externen Festplatte oder einem USB-Flashlaufwerk) Zugriff auf Dateien und Ordner zu erhalten, die mithilfe von BitLocker To Go verschlüsselt sind, wenn Sie aus irgendeinem Grund das Kennwort vergessen oder Ihr Computer nicht auf das Laufwerk zugreifen kann. .

Sie sollten den Wiederherstellungsschlüssel speichern, indem Sie ihn drucken, auf Wechselmedien speichern oder als Datei in einem Netzwerkordner oder auf Ihrem OneDrive oder auf einem anderen Laufwerk Ihres Computers speichern, das Sie nicht verschlüsseln. Sie können den Wiederherstellungsschlüssel nicht im Stammverzeichnis eines nicht austauschbaren Laufwerks speichern und können nicht auf dem verschlüsselten Volume gespeichert werden. Sie können den Wiederherstellungsschlüssel für ein Wechseldatenträger (wie etwa einen USB-Stick) auf Wechselmedien nicht speichern. Im Idealfall sollten Sie den Wiederherstellungsschlüssel separat von Ihrem Computer speichern. Nachdem Sie einen Wiederherstellungsschlüssel erstellt haben, können Sie die BitLocker-Systemsteuerung verwenden, um zusätzliche Kopien zu erstellen.

Wenn der Wiederherstellungsschlüssel ordnungsgemäß gespeichert wurde, fordert der BitLocker-Laufwerk Verschlüsselungs Assistent den Benutzer auf, das Laufwerk zu verschlüsseln. Es gibt zwei Möglichkeiten:

- Nur verwendeter Speicherplatz verschlüsseln – verschlüsselt nur Speicherplatz, der Daten enthält
- Gesamtes Laufwerk verschlüsseln – verschlüsselt das gesamte Volume einschließlich des freien Speicherplatzes

Es wird empfohlen, dass Laufwerke mit wenig bis gar keine Daten die Verschlüsselungsoption **verwendeter Speicherplatz** verwenden und dass Laufwerke mit Daten oder einem Betriebssystem die Option **gesamtes Laufwerk verschlüsseln** verwenden.

> **Hinweis:** gelöschte Dateien werden als freier Speicherplatz im Dateisystem angezeigt, der nicht nur von **verwendetem Speicherplatz**verschlüsselt wird. Bis Sie gelöscht oder überschrieben werden, enthalten gelöschte Dateien Informationen, die mit gängigen forensischen Datentools wiederhergestellt werden können.

Wenn Sie einen Verschlüsselungstyp auswählen und " **weiter** " auswählen, erhält der Benutzer die Möglichkeit, eine BitLocker-Systemprüfung auszuführen (standardmäßig aktiviert), die sicherstellt, dass BitLocker auf die Wiederherstellungs-und Verschlüsselungsschlüssel vor der Datenträgerverschlüsselung zugreifen kann. beginnt. Es wird empfohlen, diese Systemüberprüfung auszuführen, bevor Sie den Verschlüsselungsvorgang starten. Wenn die Systemprüfung nicht ausgeführt wird und ein Problem auftritt, wenn das Betriebssystem versucht zu starten, muss der Benutzer den Wiederherstellungsschlüssel bereitstellen, um Windows zu starten.

Nachdem Sie die Systemprüfung abgeschlossen haben (falls aktiviert), startet der BitLocker-Laufwerk Verschlüsselungs Assistent den Computer neu, um die Verschlüsselung zu starten. Beim Neustart müssen Benutzer das Kennwort eingeben, das zum Booten des Betriebssystemdatenträgers ausgewählt wurde. Benutzer können den Verschlüsselungsstatus überprüfen, indem Sie den System Benachrichtigungsbereich oder die BitLocker-Systemsteuerung überprüfen.

Bis die Verschlüsselung abgeschlossen ist, sind die einzigen verfügbaren Optionen für die Verwaltung von BitLocker die Manipulation des Kennworts, das das Betriebssystemvolume schützt, Sichern des Wiederherstellungsschlüssels und Deaktivieren von BitLocker.

Datenvolumen

Das Verschlüsseln von Datenmengen mithilfe der BitLocker-System Steuerungsschnittstelle funktioniert auf ähnliche Weise wie die Verschlüsselung der Betriebssystemdatenträger. Benutzer wählen **BitLocker** in der Systemsteuerung aktivieren aus, um den BitLocker-Laufwerk Verschlüsselungs-Assistenten zu starten. Anders als bei Betriebssystem-Volumes müssen Daten-Volumes keine Konfigurationstests für den Assistenten übergeben, um fortzufahren. Beim Starten des Assistenten wird eine Auswahl von Authentifizierungsmethoden zum Entsperren des Laufwerks angezeigt. Die verfügbaren Optionen sind **Kennwort** und **Smartcard** und **entsperren dieses Laufwerk automatisch auf diesem Computer**. Standardmäßig deaktiviert, wird die letztere Option das

Datenvolumen ohne Benutzereingabe entsperren, wenn das Betriebssystemvolume entsperrt ist.

Nachdem Sie die gewünschte Authentifizierungsmethode ausgewählt und **weiter**ausgewählt haben, stellt der Assistent Optionen für die Speicherung des Wiederherstellungsschlüssels dar. Diese Optionen sind dieselben wie für die Volumes des Betriebssystems. Wenn der Wiederherstellungsschlüssel gespeichert ist, **werden im Assistenten** die verfügbaren Optionen für die Verschlüsselung angezeigt. Diese Optionen sind identisch mit den Betriebssystem-Volumes; **nur verwendeter Speicherplatz** und **vollständige Laufwerkverschlüsselung**. Wenn der zu verschlüsselnde Datenträger neu oder leer ist, wird empfohlen, dass nur die Verschlüsselung nur für Speicherplatz ausgewählt ist.

Wenn eine Verschlüsselungsmethode ausgewählt ist, wird vor dem Beginn des Verschlüsselungsprozesses ein letzter Bestätigungsbildschirm angezeigt. Die Auswahl von "Verschlüsselung **starten** " beginnt mit der Verschlüsselung.

Der Verschlüsselungsstatus wird im Infobereich oder in der BitLocker-Systemsteuerung angezeigt.

OneDrive-Option

Es gibt eine neue Option zum Speichern des BitLocker-Wiederherstellungsschlüssels mithilfe des OneDrive. Diese Option erfordert, dass Computer keine Mitglieder einer Domäne sind und dass der Benutzer ein Microsoft-Konto verwendet. Lokale Konten bieten keine Möglichkeit zur Nutzung von OneDrive. Die Option OneDrive ist die standardmäßig Empfohlene Wiederherstellungsschlüssel-Speichermethode für Computer, die nicht mit einer Domäne verbunden sind.

Benutzer können überprüfen, ob der Wiederherstellungsschlüssel ordnungsgemäß gespeichert wurde, indem Sie deren OneDrive für den BitLocker-Ordner überprüfen, der während des Speichervorgangs automatisch erstellt wird. Der Ordner enthält zwei Dateien, eine Readme. txt und den Wiederherstellungsschlüssel. Für Benutzer, die mehr als ein Wiederherstellungskennwort auf Ihrem OneDrive speichern, können Sie den erforderlichen Wiederherstellungsschlüssel identifizieren, indem Sie den Dateinamen betrachten. Die Wiederherstellungsschlüssel-ID wird an das Ende des Datei namens angefügt.

Verwenden von BitLocker in Windows-Explorer

Windows-Explorer ermöglicht Benutzern das Starten des BitLocker-Laufwerk Verschlüsselungs-Assistenten, indem Sie mit der rechten Maustaste auf ein Volume klicken und **BitLocker aktivieren**auswählen. Diese Option steht standardmäßig auf Clientcomputern zur Verfügung. Auf Servern müssen Sie zuerst die BitLocker-und Desktop Features installieren, damit diese Option zur Verfügung steht. Nachdem Sie **BitLocker aktiviert**haben, funktioniert der Assistent genauso wie beim Starten mithilfe der BitLocker-Systemsteuerung.

Kompatibilität auf abwärts Ebene

Die folgende Tabelle zeigt die Kompatibilitätsmatrix für Systeme, die BitLocker aktiviert und dann einer anderen Version von Windows präsentiert wurden.

Tabelle 1: quer Kompatibilität für Windows10-, Windows 8,1-, Windows 8-und Windows 7-verschlüsselte Volumes

Verschlüsselungstyp	Windows10 und Windows 8,1	Windows 8	Windows 7
Vollständig verschlüsselt unter Windows 8	Als vollständig verschlüsselt dargestellt	n.v.	Als vollständig verschlüsselt dargestellt

Verwendeter Speicherplatz nur verschlüsselt unter Windows 8	Als Verschlüsselung beim Schreiben präsentieren	n.v.	Als vollständig verschlüsselt dargestellt
Vollständig verschlüsselte Volumes von Windows 7	Als vollständig verschlüsselt dargestellt	Als vollständig verschlüsselt dargestellt	n.v.
Teilweise verschlüsselte Volumes von Windows 7	Windows10 und Windows 8,1 vervollständigen die Verschlüsselung unabhängig von der Richtlinie.	Windows 8 vervollständigen die Verschlüsselung unabhängig von der Richtlinie	n.v.

Verschlüsseln von Volumes mithilfe der Befehlszeilenoberfläche von manage-bde

Manage-bde ist ein Befehlszeilendienstprogramm, das für das Skripting von BitLocker-Vorgängen verwendet werden kann. Manage-bde bietet zusätzliche Optionen, die nicht in der BitLocker-Systemsteuerung angezeigt werden. Eine vollständige Liste der Optionen finden Sie unter Verwalten von BDE. Manage-bde bietet eine Vielzahl weiterer Optionen für die Konfiguration von BitLocker. Dies bedeutet, dass die Verwendung der Befehlssyntax möglicherweise eine sorgfältige und eventuell spätere Anpassung durch den Benutzer erfordert. Beispielsweise wird durch die Verwendung `manage-bde -on` von nur dem Befehl auf einem Datenvolumen die Lautstärke ohne Authentifizierungsschutz vollständig verschlüsselt. Für einen auf diese Weise verschlüsselten Datenträger ist weiterhin die Benutzerinteraktion erforderlich, um den BitLocker-Schutz zu aktivieren, auch wenn der Befehl erfolgreich abgeschlossen wurde, weil dem Volume eine Authentifizierungsmethode hinzugefügt werden muss, damit Sie vollständig geschützt ist. Befehlszeilen Benutzer müssen die geeignete Syntax für eine bestimmte Situation ermitteln. Der folgende Abschnitt behandelt die allgemeine Verschlüsselung für Betriebssystem-Volumes und-Datenmengen.

Betriebssystem Lautstärke

Nachfolgend finden Sie Beispiele für grundlegende gültige Befehle für Betriebssystem-Volumes. Im allgemeinen verschlüsselt die Verwendung des `manage-bde -on <drive letter>` Befehls nur den Betriebssystemdatenträger mit einem nur-TPM-Schutz und ohne Wiederherstellungsschlüssel. Viele Umgebungen erfordern jedoch mehr sichere Schutzvorrichtungen wie Kennwörter oder PIN und erwarten, dass Sie Informationen mit einem Wiederherstellungsschlüssel wiederherstellen können.

Ermitteln des Datenträgerstatus

Bei der Verwendung von manage-bde empfiehlt es sich, den Lautstärke Status im Zielsystem zu ermitteln. Verwenden Sie den folgenden Befehl, um den Lautstärke Status zu ermitteln:

```
manage-bde -status
```

Dieser Befehl gibt die Volumes für das Ziel, den aktuellen Verschlüsselungsstatus und den Volume-Typ (Betriebssystem oder Daten) für die einzelnen Volumes zurück. Mithilfe dieser Informationen können Benutzer die optimale Verschlüsselungsmethode für Ihre Umgebung ermitteln.

Aktivieren von BitLocker ohne TPM

Nehmen wir beispielsweise an, dass Sie BitLocker auf einem Computer ohne TPM-Chip aktivieren möchten. Um

BitLocker für das Betriebssystemvolume ordnungsgemäß zu aktivieren, müssen Sie ein USB-Flashlaufwerk als Startschlüssel zum Booten verwenden (in diesem Beispiel der Laufwerkbuchstabe E). Zuerst erstellen Sie den für BitLocker erforderlichen Startschlüssel mithilfe der Option – Protektoren, und speichern Sie ihn auf dem USB-Laufwerk auf E:, und beginnen Sie dann mit dem Verschlüsselungsprozess. Sie müssen den Computer neu starten, wenn Sie dazu aufgefordert werden, den Verschlüsselungsvorgang abzuschließen.

```
manage-bde –protectors -add C: -startupkey E:
manage-bde -on C:
```

Aktivieren von BitLocker nur mit einem TPM

Mithilfe von manage-bde ist es möglich, das Betriebssystemvolume ohne definierte Schutzvorrichtungen zu verschlüsseln. Der folgende Befehl lautet:

```
manage-bde -on C:
```

Dadurch wird das Laufwerk mit dem TPM als Protector verschlüsselt. Wenn ein Benutzer die Beschützer für ein Volume unsicher ist, können Sie die Option-Protectors in manage-bde verwenden, um diese Informationen mit dem folgenden Befehl aufzulisten:

```
manage-bde -protectors -get <volume>
```

Bereitstellen von BitLocker mit zwei Schutzvorrichtungen

Ein weiteres Beispiel ist ein Benutzer auf nicht-TPM-Hardware, der dem Betriebssystemvolume ein Kennwort und eine SID-basierte Schutzvorrichtung hinzufügen möchte. In diesem Fall fügt der Benutzer zuerst die Beschützer hinzu. Dies erfolgt über den folgenden Befehl:

```
manage-bde -protectors -add C: -pw -sid <user or group>
```

Dieser Befehl fordert den Benutzer auf, die Kennwortschutz Taste einzugeben und dann zu bestätigen, bevor Sie dem Volume hinzugefügt wird. Wenn die Beschützer auf dem Volume aktiviert sind, muss der Benutzer nur BitLocker aktivieren.

Datenvolumen

Daten-Volumes verwenden dieselbe Syntax für die Verschlüsselung als Betriebssystem-Volumes, erfordern aber keine Schutzvorrichtungen, damit der Vorgang abgeschlossen werden kann. Das Verschlüsseln von Daten-Volumes kann mithilfe des Basis `manage-bde -on <drive letter>` Befehls erfolgen: oder Benutzer können dem Volume Protektoren hinzufügen. Es wird empfohlen, dass mindestens ein primärer Schutz und ein Wiederherstellungs-Protector zu einem Datenvolumen hinzugefügt werden.

Aktivieren von BitLocker mit einem Kennwort

Eine allgemeine Schutzvorrichtung für ein Datenvolumen ist die Kennwortschutz-Komponente. Im folgenden Beispiel fügen wir dem Volume eine Kennwortschutzfunktion hinzu und aktivieren BitLocker.

```
manage-bde -protectors -add -pw C:
manage-bde -on C:
```

Verschlüsseln von Volumes mithilfe der BitLocker Windows PowerShell-Cmdlets

Windows PowerShell-Cmdlets stellen eine alternative Möglichkeit zum Arbeiten mit BitLocker dar. Mithilfe der Skriptfunktionen von Windows PowerShell können Administratoren BitLocker-Optionen problemlos in vorhandene Skripts integrieren. In der folgenden Liste werden die verfügbaren BitLocker-Cmdlets angezeigt.

Name	Parameter
Add-BitLockerKeyProtector	-ADAccountOrGroup -ADAccountOrGroupProtector -Bestätigen -MountPoint -Kennwort -PasswordProtector -PIN -RecoveryKeyPath -RecoveryKeyProtector -RecoveryPassword) angegeben -RecoveryPasswordProtector -Service -StartupKeyPath -StartupKeyProtector -TpmAndPinAndStartupKeyProtector -TpmAndPinProtector -TpmAndStartupKeyProtector -TpmProtector -WhatIf
Backup-BitLockerKeyProtector	-Bestätigen -Keyprotector-Nr. -MountPoint -WhatIf
Deaktivieren-BitLocker	-Bestätigen -MountPoint -WhatIf
Deaktivieren-BitLockerAutoUnlock	-Bestätigen -MountPoint -WhatIf

Enable-BitLocker	-AdAccountOrGroup -AdAccountOrGroupProtector -Bestätigen -EncryptionMethod -HardwareEncryption -Kennwort -PasswordProtector -PIN -RecoveryKeyPath -RecoveryKeyProtector -RecoveryPassword) angegeben -RecoveryPasswordProtector -Service -SkipHardwareTest -StartupKeyPath -StartupKeyProtector -TpmAndPinAndStartupKeyProtector -TpmAndPinProtector -TpmAndStartupKeyProtector -TpmProtector -UsedSpaceOnly -WhatIf
Enable-BitLockerAutoUnlock	-Bestätigen -MountPoint -WhatIf
Get-BitLockerVolume	-MountPoint
Sperren – BitLocker	-Bestätigen -ForceDismount -MountPoint -WhatIf
Remove-BitLockerKeyProtector	-Bestätigen -Keyprotector-Nr. -MountPoint -WhatIf

Fortsetzen – BitLocker	-Bestätigen -MountPoint -WhatIf
Anhalten – BitLocker	-Bestätigen -MountPoint -RebootCount -WhatIf
Entsperren – BitLocker	-AdAccountOrGroup -Bestätigen -MountPoint -Kennwort -RecoveryKeyPath -RecoveryPassword) angegeben -RecoveryPassword) angegeben -WhatIf

Ähnlich wie manage-bde ermöglichen die Windows PowerShell-Cmdlets die Konfiguration über die in der Systemsteuerung angebotenen Optionen hinaus. Wie bei manage-bde müssen die Benutzer die spezifischen Anforderungen des Volumes, das Sie verschlüsseln, vor der Ausführung von Windows PowerShell-Cmdlets in Frage stellen. Ein guter erster Schritt besteht darin, den aktuellen Zustand der Volumes auf dem Computer zu ermitteln. Dazu können Sie das Cmdlet " `Get-BitLocker` Volume" verwenden. Die Ausgabe dieses Cmdlets zeigt Informationen zu den Datenträgertypen, Beschützer, Schutzstatus und anderen nützlichen Informationen an. Gelegentlich werden alle Schutzvorrichtungen möglicherweise nicht **angezeigt, wenn** Sie "Get-BitLockerVolume" wegen fehlender Leertaste in der Ausgabe Anzeige verwenden. Wenn nicht alle Schutzvorrichtungen für ein Volume angezeigt werden, können Sie den Windows PowerShell-Pipe-Befehl (|) verwenden, um eine Liste der Beschützer zu formatieren.

> **Hinweis:** für den Fall, dass mehr als vier Schutzvorrichtungen für ein Volume vorhanden sind, kann für den Befehl Pipe der Anzeigebereich nicht mehr angezeigt werden. Verwenden Sie für Volumes mit mehr als vier Beschützern die im folgenden Abschnitt beschriebene Methode, um eine Auflistung aller Schutzvorrichtungen mit der Schutz-ID zu generieren.

```
Get-BitLockerVolume C: | fl
```

Wenn Sie die vorhandenen Schutzvorrichtungen entfernen möchten, bevor BitLocker auf dem Datenträger bereitgestellt wird, können Sie `Remove-BitLockerKeyProtector` das Cmdlet verwenden. Hierzu muss die GUID, die dem Protector zugeordnet ist, entfernt werden. Mit einem einfachen Skript können die Werte jedes **Get-BitLockerVolume-Steuer** Zeichens an eine andere Variable weitergegeben werden, wie unten zu sehen ist:

```
$vol = Get-BitLockerVolume
$keyprotectors = $vol.KeyProtector
```

Mithilfe dieser Informationen können wir die Informationen in der **$keyprotectors** -Variable anzeigen, um die GUID für jeden Protector zu ermitteln. Mithilfe dieser Informationen können wir dann den Schlüsselschutz für ein

bestimmtes Volume mithilfe des Befehls entfernen:

```
Remove-BitLockerKeyProtector <volume>: -KeyProtectorID "{GUID}"
```

> **Hinweis:** das BitLocker-Cmdlet setzt voraus, dass die Schlüssel-Beschützer-GUID in Anführungszeichen eingeschlossen ist. Stellen Sie sicher, dass die gesamte GUID mit geschweiften Klammern in den Befehl eingeschlossen ist.

Betriebssystem Lautstärke

Die Verwendung der BitLocker-Cmdlets für Windows PowerShell ähnelt dem Arbeiten mit dem Manage-BDE-Tool zum Verschlüsseln von Betriebssystem-Volumes. Windows PowerShell bietet Benutzern viel Flexibilität. Beispielsweise können Benutzer den gewünschten Protector als Teilbefehl zum Verschlüsseln des Volumes hinzufügen. Nachfolgend finden Sie Beispiele für häufige Benutzerszenarien und Schritte, die Sie mithilfe der BitLocker-Cmdlets für Windows PowerShell ausführen können. So aktivieren Sie BitLocker nur mit dem TPM-Schutz. Dies kann mithilfe des Befehls erfolgen:

```
Enable-BitLocker C:
```

Im folgenden Beispiel wird ein zusätzlicher Protector, die StartupKey-Schutzvorrichtungen, hinzugefügt, und es wird der BitLocker-Hardware Test übersprungen. In diesem Beispiel wird die Verschlüsselung sofort gestartet, ohne dass ein Neustart erforderlich ist.

```
Enable-BitLocker C: -StartupKeyProtector -StartupKeyPath <path> -SkipHardwareTest
```

Datenvolumen

Die Datenvolume-Verschlüsselung mit Windows PowerShell entspricht den für Betriebssystemdatenträger. Bevor Sie die Lautstärke verschlüsseln, sollten Sie die gewünschten Schutzvorrichtungen hinzufügen. Im folgenden Beispiel wird dem E:-Volume eine Kennwortschutz Komponente mithilfe der Variablen $PW als Kennwort hinzugefügt. Die $PW-Variable wird als SecureString-Wert gespeichert, um das benutzerdefinierte Kennwort zu speichern. Zuletzt beginnt die Verschlüsselung.

```
$pw = Read-Host -AsSecureString
<user inputs password>
Enable-BitLockerKeyProtector E: -PasswordProtector -Password $pw
```

Verwenden eines sid-basierten Beschützers in Windows PowerShell

Der ADAccountOrGroup Protector ist ein sid-basierter Active Directory-Schutz. Dieser Schutz kann sowohl auf Betriebssystem-als auch auf Daten-Volumes hinzugefügt werden, obwohl er die Betriebssystem-Volumes in der Pre-Boot-Umgebung nicht entsperrt. Für den Protector muss die sid für das Domänenkonto oder die Gruppe mit dem Protector verknüpft werden. BitLocker kann einen clusterfähigen Datenträger schützen, indem ein sid-basierter Schutz für das Cluster Name Object (CNO) hinzugefügt wird, mit dem der Datenträger ordnungsgemäß Failover und auf einen beliebigen Mitgliedscomputer des Clusters freigegeben werden kann.

> **Warnung:** die SID-basierte Schutzkomponente erfordert die Verwendung einer zusätzlichen Schutzkomponente (wie TPM, PIN, Wiederherstellungsschlüssel usw.), wenn Sie auf Betriebssystemdatenträgern verwendet wird.

Zum Hinzufügen eines ADAccountOrGroup-Beschützers zu einem Volume müssen entweder die tatsächliche Domänen-SID oder der Gruppenname, dem die Domäne vorangestellt ist, und ein umgekehrter Schrägstrich eingegeben werden. Im folgenden Beispiel wird das CONTOSO\Administrator-Konto als Protector zum

Datenvolumen G hinzugefügt.

```
Enable-BitLocker G: -AdAccountOrGroupProtector -AdAccountOrGroup CONTOSO\Administrator
```

Für Benutzer, die die sid für das Konto oder die Gruppe verwenden möchten, besteht der erste Schritt darin, die dem Konto zugeordnete sid zu ermitteln. Um die spezifische sid für ein Benutzerkonto in Windows PowerShell abzurufen, verwenden Sie den folgenden Befehl:

```
get-aduser -filter {samaccountname -eq "administrator"}
```

> **Hinweis:** die Verwendung dieses Befehls erfordert das Feature Remote Remote-AD-PowerShell.
>
> **Tipp:** zusätzlich zum oben genannten Windows PowerShell-Befehl können Informationen zu den lokal angemeldeten Benutzern und Gruppenmitgliedschaften mithilfe von: WHOAMI/all. gefunden werden. Dies erfordert keine Verwendung zusätzlicher Funktionen.

Im folgenden Beispiel möchte der Benutzer dem zuvor verschlüsselten Betriebssystemdatenträger einen Domänen-SID-basierten Schutz hinzufügen. Der Benutzer kennt die sid für das Benutzerkonto oder die Gruppe, die Sie hinzufügen möchten, und verwendet den folgenden Befehl:

```
Add-BitLockerKeyProtector C: -ADAccountOrGroupProtector -ADAccountOrGroup "<SID>"
```

> **Hinweis:** Active Directory-basierte Schutzfunktionen werden normalerweise zum Entsperren von Failover-Cluster fähigen Volumes verwendet.

Überprüfen des BitLocker-Status

Zum Überprüfen des BitLocker-Status eines bestimmten Volumes können Administratoren den Status des Laufwerks im BitLocker-Applet "Systemsteuerung", Windows-Explorer, Befehlszeilentool "Manage-BDE" oder Windows PowerShell-Cmdlets anzeigen. Jede Option bietet unterschiedliche Detailebenen und einfache Bedienung. Wir werden uns mit den einzelnen verfügbaren Methoden im folgenden Abschnitt befassen.

Überprüfen des BitLocker-Status mit der Systemsteuerung

Die Überprüfung des BitLocker-Status mit der Systemsteuerung ist die häufigste Methode, die die meisten Benutzer verwenden. Nach dem Öffnen wird der Status für jedes Volume neben der Datenträgerbeschreibung und dem Laufwerkbuchstaben angezeigt. Zu den verfügbaren Statusrückgabe Werten mit der Systemsteuerung gehören:

STATUS	BESCHREIBUNG
Ein	BitLocker ist für das Volume aktiviert.
Aus	BitLocker ist für das Volume nicht aktiviert.
Suspended	BitLocker wird angehalten und schützt die Lautstärke nicht aktiv.
Warten auf Aktivierung	BitLocker ist mit einem klaren Protector-Schlüssel aktiviert und erfordert, dass weitere Aktionen vollständig geschützt sind.

Wenn ein Laufwerk mit BitLocker vorab bereitgestellt wurde, wird der Status "warten auf Aktivierung" mit einem gelben Ausrufezeichen auf Volume E angezeigt. Dieser Status bedeutet, dass beim Verschlüsseln des Volumes nur ein klarer Schutz verwendet wurde. In diesem Fall befindet sich das Volume nicht in einem geschützten Zustand und muss dem Volume einen sicheren Schlüssel hinzugefügt haben, bevor das Laufwerk vollständig geschützt ist. Administratoren können die Systemsteuerung, das Manage-BDE-Tool oder WMI-APIs verwenden, um einen geeigneten Schlüsselschutz hinzuzufügen. Nachdem der Vorgang abgeschlossen ist, wird das Control Panel aktualisiert, um den neuen Status wiederzugeben. Über die Systemsteuerung können Administratoren **BitLocker aktivieren** , um den BitLocker-Laufwerk Verschlüsselungs-Assistenten zu starten und einen Schutz, wie PIN für ein Betriebssystemvolume (oder ein Kennwort, wenn kein TPM vorhanden ist) oder ein Kennwort oder eine Smartcard-Beschützer für Daten hinzufügen. Volumen. Das Fenster "Laufwerksicherheit" wird vor dem Ändern des Lautstärke Status angezeigt. Durch Auswählen von **BitLocker aktivieren** wird der Verschlüsselungsvorgang abgeschlossen.

Sobald die BitLocker-Protector-Aktivierung abgeschlossen ist, wird der Fertigstellungshinweis angezeigt.

Überprüfen des BitLocker-Status mit manage-bde

Administratoren, die eine Befehlszeilenschnittstelle bevorzugen, können manage-bde verwenden, um den Volumen Status zu überprüfen. Manage-bde ist in der Lage, weitere Informationen über das Volume zurückzugeben, als die grafischen Benutzeroberflächentools in der Systemsteuerung. So kann beispielsweise manage-bde die verwendete BitLocker-Version, den Verschlüsselungstyp und die einem Datenträger zugeordneten Schutzfolien anzeigen.

Verwenden Sie den folgenden Befehl, um den Status eines Volumes mithilfe von manage-bde zu überprüfen:

```
manage-bde -status <volume>
```

> **Hinweis:** wenn dem Befehl-Status kein Volumen Buchstabe zugeordnet ist, wird der Status aller Volumes auf dem Computer angezeigt.

Überprüfen des BitLocker-Status mit Windows PowerShell

Windows PowerShell-Befehle bieten eine weitere Möglichkeit zum Abfragen des BitLocker-Status für Volumes. Wie manage-bde bietet Windows PowerShell den Vorteil, dass Sie den Status eines Volumes auf einem Remotecomputer überprüfen können.

Mit dem Cmdlet Get-BitLockerVolume wird für jedes Volume im System der aktuelle BitLocker-Status angezeigt. Verwenden Sie den folgenden Befehl, um Informationen zu erhalten, die für ein bestimmtes Volume detaillierter sind:

```
Get-BitLockerVolume <volume> -Verbose | fl
```

Mit diesem Befehl werden Informationen zur Verschlüsselungsmethode, zum Datenträgertyp, zu den Schlüssel Beschützern usw. angezeigt.

Bereitstellen von BitLocker während der Betriebssystembereitstellung

Administratoren können BitLocker vor der Betriebssystembereitstellung in der Windows-Vorinstallationsumgebung aktivieren. Dies erfolgt mit einem nach dem Zufallsprinzip generierten Clear Key Protector, der auf das formatierte Volume angewendet wurde, und die Verschlüsselung des Volumes vor der Ausführung des Windows-Setupprozesses. Wenn die Verschlüsselung die in diesem Dokument weiter unten beschriebene Option verwendeter Speicherplatz verwendet, dauert dieser Schritt nur wenige Sekunden und ist in normalen Bereitstellungsprozessen gut integriert.

Entschlüsseln von BitLocker-Volumes

Beim Entschlüsseln von Volumes werden BitLocker und alle zugehörigen Schutzvorrichtungen aus den Volumes entfernt. Die Entschlüsselung sollte erfolgen, wenn kein Schutz mehr erforderlich ist. Die BitLocker-Entschlüsselung sollte nicht als Schritt zur Problembehandlung erfolgen. BitLocker kann mithilfe der BitLocker Control Panel-Applet-, manage-bde-oder Windows PowerShell-Cmdlets aus einem Volume entfernt werden. Wir werden die einzelnen Methoden weiter unten erläutern.

Entschlüsseln von Volumes mithilfe des BitLocker-Systemsteuerungs-Applet

Die BitLocker-Entschlüsselung mithilfe der Systemsteuerung erfolgt mithilfe eines Assistenten. Die Systemsteuerung kann über den Windows-Explorer aufgerufen werden oder durch Öffnen der direkt. Nach dem Öffnen der BitLocker-Systemsteuerung wählen Benutzer die Option BitLocker deaktivieren aus, um den Vorgang zu starten. Nach der Auswahl wählt der Benutzer den Vorgang fortsetzen, indem er auf das Bestätigungsdialogfeld klickt. Wenn BitLocker deaktivieren bestätigt ist, wird der Laufwerk Entschlüsselungsvorgang gestartet, und der Status wird dem Control Panel gemeldet.

In der Systemsteuerung wird der Entschlüsselungs Fortschritt nicht gemeldet, sondern im Infobereich der Taskleiste angezeigt. Wenn Sie das Symbol für den Benachrichtigungsbereich auswählen, wird ein modales Dialogfeld mit Fortschritt geöffnet.

Nach Abschluss der Entschlüsselung aktualisiert das Laufwerk seinen Status in der Systemsteuerung und steht für die Verschlüsselung zur Verfügung.

Entschlüsseln von Volumes mithilfe der Befehlszeilenoberfläche von manage-bde

Das Entschlüsseln von Volumes mithilfe von manage-bde ist sehr einfach. Die Entschlüsselung mit manage-bde bietet den Vorteil, dass keine Bestätigung des Benutzers erforderlich ist, um den Prozess zu starten. Manage-bde verwendet den-Off-Befehl, um den Entschlüsselungsprozess zu starten. Ein Beispielbefehl für die Entschlüsselung lautet:

```
manage-bde -off C:
```

Dieser Befehl deaktiviert den Schutz, während er die Lautstärke entschlüsselt und alle Beschützer entfernt, wenn die Entschlüsselung abgeschlossen ist. Wenn ein Benutzer den Status der Entschlüsselung überprüfen möchte, kann er den folgenden Befehl verwenden:

```
manage-bde -status C:
```

Entschlüsseln von Volumes mithilfe der BitLocker Windows PowerShell-Cmdlets

Die Entschlüsselung mit Windows PowerShell-Cmdlets ist einfach, ähnlich wie manage-bde. Der zusätzliche Vorteil von Windows PowerShell bietet die Möglichkeit, mehrere Laufwerke in einem Durchgang zu entschlüsseln. Im folgenden Beispiel verfügt der Benutzer über drei verschlüsselte Volumes, die Sie entschlüsseln möchten.

Mit dem Befehl Disable-BitLocker können Sie alle Beschützer und die Verschlüsselung gleichzeitig entfernen, ohne dass zusätzliche Befehle erforderlich sind. Ein Beispiel für diesen Befehl ist:

```
Disable-BitLocker
```

Wenn ein Benutzer die einzelnen Bereitstellungspunkte nicht einzeln eingeben möchte, kann mit `-MountPoint` dem Parameter in einem Array derselbe Befehl in einer Zeile sequenziert werden, ohne dass eine zusätzliche Benutzereingabe erforderlich ist. Ein Beispielbefehl lautet:

```
Disable-BitLocker -MountPoint E:,F:,G:
```

Weitere Informationen

- Vorbereiten Ihrer Organisation auf BitLocker: Planung und Richtlinien
- BitLocker-Wiederherstellungs Handbuch
- BitLocker: Aktivieren der Netzwerkentsperrung
- Übersicht über BitLocker

BitLocker: Bereitstellen auf Windows Server 2012 und höher

27.10.2019 • 4 minutes to read

Gilt für: Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019

In diesem Thema für IT-Experten wird erläutert, wie BitLocker unter Windows Server 2012 und höher bereitgestellt wird. Für alle Windows Server-Editionen kann BitLocker mithilfe von Server-Manager-oder Windows PowerShell-Cmdlets installiert werden. BitLocker erfordert Administratorrechte auf dem Server für die Installation.

Installieren von BitLocker

So installieren Sie BitLocker mit dem Server-Manager

1. Öffnen Sie den Server-Manager, indem Sie das Server-Manager-Symbol auswählen oder "Server Manager. exe" ausführen.
2. Wählen Sie in der **Navigationsleiste des Server-Managers Verwalten** aus, und wählen Sie **Rollen und Features hinzufügen** aus, um den **Assistenten zum Hinzufügen von Rollen und Features** zu starten.
3. Wenn der **Assistent zum Hinzufügen von Rollen und Features** geöffnet ist, wählen Sie im Bereich **vor dem Beginn** (sofern angezeigt) die Option **weiter** aus.
4. Wählen Sie auf **Rollen-oder Feature-basierter Installation** im Bereich " **Installationstyp** " des **Assistenten "Rollen und Features hinzufügen** " aus, und wählen Sie **weiter** aus, um fortzufahren.
5. Wählen Sie im Bereich **Serverauswahl** die **Option Server aus dem Serverpool auswählen aus** , und bestätigen Sie den Server für die BitLocker-Feature-Installation.
6. Serverrollen und Features werden mithilfe desselben Assistenten im Server-Manager installiert. Wählen Sie im Bereich " **Server Rollen** " des Assistenten zum **Hinzufügen von Rollen und Features weiter** aus, um zum Bereich **Features** zu gelangen.
7. Aktivieren Sie das Kontrollkästchen neben **BitLocker-Laufwerkverschlüsselung** im Bereich " **Features** " des **Assistenten zum Hinzufügen von Rollen und Features**. Der Assistent zeigt die zusätzlichen Verwaltungsfeatures an, die für BitLocker verfügbar sind. Wenn Sie diese Funktionen nicht installieren möchten, deaktivieren Sie die **Option Verwaltungstools einbeziehen** , und wählen Sie **Features hinzufügen**aus. Sobald die optionale Auswahl der Features abgeschlossen ist, wählen Sie **weiter** aus, um den Assistenten fortzusetzen.

   > **Hinweis:** die **Erweiterte Speicher** Funktion ist ein erforderliches Feature zum Aktivieren von BitLocker. Dieses Feature ermöglicht die Unterstützung für verschlüsselte Festplatten auf fähigen Systemen.

8. Wählen Sie im **Bestätigungs** Bereich des **Assistenten zum Hinzufügen von Rollen und Features** die Option **Installieren** aus, um die BitLocker-Feature-Installation zu starten. Für das BitLocker-Feature ist ein Neustart erforderlich. Wenn Sie im **Bestätigungs** Bereich die Option " **Zielserver automatisch starten, wenn erforderlich** " auswählen, wird nach Abschluss der Installation ein Neustart des Computers erzwungen.
9. Wenn das Kontrollkästchen **Zielserver automatisch bei Bedarf neu starten** nicht aktiviert ist, zeigt der **Ergebnisbereich** des **Assistenten zum Hinzufügen von Rollen und Features** den Erfolg oder Misserfolg der BitLocker-Feature-Installation an. Falls erforderlich, wird eine Benachrichtigung über zusätzliche Aktionen, die erforderlich sind, um die Feature-Installation abzuschließen, wie etwa den Neustart des Computers, im

Ergebnistext angezeigt.

So installieren Sie BitLocker mithilfe von Windows PowerShell

Windows PowerShell bietet Administratoren eine weitere Option für die BitLocker-Feature-Installation. Windows PowerShell installiert Features mithilfe des `servermanager` oder `dism` -Moduls. die und- `servermanager` `dism` Module geben jedoch nicht immer die Funktion Namen Parität frei. Aus diesem Grund empfiehlt es sich, vor der Installation das Feature oder den Rollennamen zu bestätigen.

> **Hinweis:** Sie müssen den Server neu starten, um die Installation von BitLocker abzuschließen.

Verwenden des Server-Moduls zum Installieren von BitLocker

Das `servermanager` Windows PowerShell-Modul kann entweder das `Install-WindowsFeature` oder `Add-WindowsFeature` zum Installieren des BitLocker-Features verwenden. Das `Add-WindowsFeature` Cmdlet ist lediglich ein Stub für `Install-WindowsFeature`. In diesem Beispiel wird `Install-WindowsFeature` das Cmdlet verwendet. Der Funktionsname für BitLocker im `servermanager` Modul lautet. `BitLocker`

Die Installation von Features in Windows PowerShell umfasst standardmäßig keine optionalen unter Features oder Verwaltungstools im Rahmen des Installationsprozesses. Dies kann mithilfe der `-WhatIf` Option in Windows PowerShell angezeigt werden.

```
Install-WindowsFeature BitLocker -WhatIf
```

Die Ergebnisse dieses Befehls zeigen, dass nur das BitLocker-Laufwerk Verschlüsselungsfeature mithilfe dieses Befehls installiert wird.

Wenn Sie sehen möchten, was mit dem BitLocker-Feature einschließlich aller verfügbaren Verwaltungstools und unter Features installiert wird, verwenden Sie den folgenden Befehl:

```
Install-WindowsFeature BitLocker -IncludeAllSubFeature -IncludeManagementTools -WhatIf | fl
```

Das Ergebnis dieses Befehls zeigt die folgende Liste aller Verwaltungstools für BitLocker an, die zusammen mit dem Feature installiert werden, einschließlich Tools für die Verwendung mit Active Directory-Domänendiensten (AD DS) und Active Directory Lightweight Directory Dienste (AD LDS).

- BitLocker-Laufwerkverschlüsselung
- Tools zur BitLocker-Laufwerkverschlüsselung
- Verwaltungsdienstprogramme für die BitLocker-Laufwerkverschlüsselung
- BitLocker-Wiederherstellungskennwort-Viewer
- AD DS-Snap-Ins und Befehlszeilen Tools
- AD DS-Tools
- AD DS-und AD LDS-Tools

Der Befehl, um eine vollständige Installation des BitLocker-Features mit allen verfügbaren Features abzuschließen und den Server nach Abschluss neu zu starten, lautet wie folgt:

```
Install-WindowsFeature BitLocker -IncludeAllSubFeature -IncludeManagementTools -Restart
```

> **Wichtig:** Wenn Sie das BitLocker-Feature mithilfe von Windows PowerShell installieren, wird die erweiterte Speicherfunktion nicht installiert. Administratoren, die verschlüsselte Festplatten in Ihrer Umgebung unterstützen möchten, müssen das erweiterte Speicherfeature separat installieren.

Verwenden des DISM-Moduls zum Installieren von BitLocker

Das `dism` Windows PowerShell-Modul verwendet `Enable-WindowsOptionalFeature` das Cmdlet, um Features zu installieren. Der BitLocker-Funktionsname für BitLocker `BitLocker` ist. Bei `dism` der Suche nach Funktionsnamen unterstützt das Modul keine Platzhalter. Verwenden Sie das `Get-WindowsOptionalFeatures` Cmdlet, um `dism` Funktionsnamen für das Modul aufzulisten. Mit dem folgenden Befehl werden alle optionalen Features in einem Online-Betriebssystem (ausgeführt) aufgelistet.

```
Get-WindowsOptionalFeature -Online | ft
```

Aus dieser Ausgabe können wir sehen, dass es drei optionale BitLocker-Funktionsnamen gibt: BitLocker, BitLocker-Dienstprogramme und BitLocker-NetworkUnlock. Zum Installieren des BitLocker-Features sind die Features BitLocker und BitLocker-Dienstprogramme die einzigen erforderlichen Elemente.

Verwenden Sie den folgenden Befehl `dism`, um BitLocker mithilfe des Moduls zu installieren:

```
Enable-WindowsOptionalFeature -Online -FeatureName BitLocker -All
```

Mit diesem Befehl wird der Benutzer aufgefordert, einen Neustart durchführen. Das Cmdlet Enable-WindowsOptionalFeature bietet keine Unterstützung für das Erzwingen eines Neustart des Computers. Dieser Befehl enthält keine Installation der Verwaltungstools für BitLocker. Verwenden Sie den folgenden Befehl für eine vollständige Installation von BitLocker und aller verfügbaren Verwaltungstools:

```
Enable-WindowsOptionalFeature -Online -FeatureName BitLocker, BitLocker-Utilities -All
```

Weitere Informationen

- Übersicht über BitLocker
- Häufig gestellte Fragen (Frequently Asked Questions, FAQ) zu BitLocker
- Vorbereiten Ihrer Organisation auf BitLocker: Planung und Richtlinien
- BitLocker: Aktivieren der Netzwerkentsperrung

BitLocker-Verwaltung für Unternehmen

07.12.2019 • 5 minutes to read

Das ideal für die BitLocker-Verwaltung besteht darin, die Notwendigkeit von IT-Administratoren zum Einrichten von Verwaltungsrichtlinien mithilfe von Tools oder anderen Mechanismen zu eliminieren, indem Windows Aufgaben ausführt, die praktischer zu automatisieren sind. Diese Vision nutzt moderne Entwicklungen im Bereich Hardware. Die zunehmende Verbreitung von TPM 2.0, sicherem Start und weiteren Hardwareverbesserungen hat beispielsweise zur Entlastung von Helpdesks beigetragen. Es konnte eine konsistente Abnahme der Zahl von Supportanrufen festgestellt werden, was zu einer größeren Benutzerzufriedenheit führt. Windows bleibt weiterhin der Fokus für neue Features und Verbesserungen bei der integrierten Verschlüsselungs Verwaltung, wie beispielsweise die automatische Aktivierung der Verschlüsselung auf Geräten, die den modernen Standbymodus ab Windows 8,1 unterstützen.

Obwohl viel Windows BitLocker- Dokumentation veröffentlicht wurde, fordern Kunden häufig Empfehlungen und Hinweise zu einer bestimmten, aufgabenorientierten Dokumentation, die sowohl einfach zu verdauen als auch auf die Bereitstellung und Verwaltung von BitLocker ausgerichtet ist. Dieser Artikel enthält Links zu relevanten Dokumentationen, Produkten und Diensten, die Ihnen bei der Beantwortung dieser und anderer verwandter häufig gestellter Fragen helfen, und stellt auch BitLocker-Empfehlungen für verschiedene Computertypen zur Verfügung.

> **IMPORTANT**
>
> Die Funktionen für die Microsoft BitLocker-Verwaltung und-Überwachung (MBAM) werden in Zukunft von ConfigMgr in den Szenarien für die Zukunft von Prem bereitgestellt.

Verwalten von Domänen verbundenen Computern und wechseln in die Cloud

Unternehmen, die mit Microsoft System Center2012 Configuration Manager SP1 (SCCM) oder höher Images ihrer Computer erstellen, können eine vorhandene Tasksequenz für die Vorabbereitstellung von BitLocker zur Verschlüsselung in Windows Preinstallation Environment (WinPE) verwenden und anschließend den Schutz aktivieren. Dies kann helfen, sicherzustellen, dass Computer von Anfang verschlüsselt sind, schon bevor Benutzer sie erhalten. Im Rahmen der Imageerstellung könnte ein Unternehmen SCCM auch verwenden, um die gewünschte BitLocker-Gruppenrichtlinie vorab festzulegen.

Unternehmen können Microsoft BitLocker-Verwaltung und-Überwachung (MBAM) verwenden, um Clientcomputer mit BitLocker zu verwalten, die lokal einer Domäne angehören, bis die Mainstream-Unterstützung im Juli 2019 endet oder Sie bis April 2026 erweiterten Support erhalten können. Daher wird es in den nächsten Jahren eine gute Strategie für Unternehmen sein, auf Cloud-basiertes Management für BitLocker zu planen und zu wechseln. Informationen zum Speichern von Wiederherstellungsschlüsseln in Azure Active Directory (Azure AD) finden Sie in den PowerShell-Beispielen .

Verwalten von Geräten, die mit Azure Active Directory verbunden sind

Geräte, die mit Azure AD verbunden sind, werden mithilfe der Mobile Device Management (MDM)-Richtlinie aus einer MDM-Lösung wie Microsoft InTune verwaltet. Ohne Windows 10, Version 1809, können nur lokale Administratoren BitLocker über die Intune-Richtlinie aktivieren. Ab Windows 10, Version 1809, kann InTune BitLocker für Standardbenutzer aktivieren. Der BitLocker-Geräte Verschlüsselungs Status kann über den Richtlinien-Konfigurations Einstellungsanbieter (CSP)von verwalteten Computern abgefragt werden, der meldet, ob die BitLocker-Geräteverschlüsselung auf dem Gerät aktiviert ist. Die Kompatibilität mit der Richtlinie für die

BitLocker-Geräteverschlüsselung kann eine Voraussetzung für den bedingten Zugriff auf Dienste wie Exchange Online und SharePoint Online sein.

Ab Windows10, Version 1703, (auch bekannt als Windows Creators Update) kann die Aktivierung von BitLocker MDM ausgelöst werden, entweder über den Richtlinien-CSP oder den BitLocker-CSP. Der BitLocker-CSP fügt Richtlinienoptionen hinzu, die über die Sicherstellung der Verschlüsselung hinausgehen und auf Computern unter Windows 10 und Windows phones verfügbar sind.

Bei Hardware, die mit modernen Standby-und HSTI kompatibel ist, wird bei Verwendung einer dieser Funktionen die BitLocker-Geräteverschlüsselung automatisch aktiviert, wenn der Benutzer ein Gerät mit Azure AD verknüpft. Azure AD bietet ein Portal, in dem Wiederherstellungsschlüssel auch gesichert werden, damit Benutzer ihre eigenen Wiederherstellungsschlüssel zu Self-Service-Zwecken abrufen können, wenn erforderlich. Für ältere Geräte, die noch nicht verschlüsselt werden, können Administratoren ab Windows10, Version 1703, (das Windows10 Creators Update) den BitLocker-CSP verwenden, um die Verschlüsselung auszulösen und den Wiederherstellungsschlüssel in Azure AD speichern.

Dies gilt auch für Azure Hybrid AD.

Verwalten von Arbeitsplatz verbundenen PCs und Smartphones

Für Windows-PCs und Windows-Smartphones, die sich über die Verbindung mit dem Geschäfts- **oder Schulkonto verbinden**, wird die BitLocker-Geräteverschlüsselung über MDM verwaltet, genauso wie Geräte, die mit Azure AD verbunden sind.

Verwalten von Servern

Server werden häufig mittels PowerShell installiert, konfiguriert und bereitgestellt. Daher besteht die Empfehlung darin, PowerShell zum Aktivieren von BitLocker auf einem Server zu verwenden, idealerweise als Teil der anfänglichen Einrichtung. BitLocker ist eine optionale Komponente (OC) in Windows Server. Folgen Sie daher den Anweisungen in BitLocker: Bereitstellen von Windows Server2012 und höher, um die BitLocker-OC hinzuzufügen.

Die minimale Serverschnittstelle ist eine Voraussetzung für einige BitLocker-Verwaltungstools. In einer Server Core-Installation müssen Sie zunächst die erforderlichen GUI-Komponenten hinzufügen. Die Schrittezum Hinzufügen von Shellkomponenten zu Server Core werden in Verwenden von bedarfsbasierten Features mit aktualisierten Systemen und gepatchten Images und Aktualisieren von lokalen Quellmedien, um Rollen und Features hinzuzufügen beschrieben.

Wenn Sie einen Server manuell installieren, z.B. einen eigenständigen Server, ist die Wahl von Server mit Desktopdarstellung der einfachste Weg, da Sie so die Schritte für das Hinzufügen einer GUI zu Server Core vermeiden können.

Darüber hinaus können Lights-Out-Rechenzentren die erweiterte Sicherheit eines zweiten Faktors nutzen und gleichzeitig die Notwendigkeit vermeiden, dass Benutzer während Neustarts eingreifen müssen, indem optional eine Kombination von BitLocker (TPM + PIN) und BitLocker-Netzwerkentsperrung verwendet wird. Die BitLocker-Netzwerkentsperrung vereint die besten Merkmale von Hardwareschutz, Standortabhängigkeit und automatischer Entsperrung, während sie sich am vertrauenswürdigen Speicherort befindet. Weitere Informationen zu den Konfigurationsschritten finden Sie unter BitLocker: Aktivieren der Netzwerkentsperrung.

Weitere Informationen finden Sie im BitLocker-FAQ-Artikel und unter anderen nützlichen Links in Verwandte Artikel.

PowerShell-Beispiele

Für Computer einschließlich virtueller Computer, die Azure AD-beigetreten sind, sollte das Kennwort für die Wiederherstellung in Azure Active Directory gespeichert werden.

Beispiel: Verwenden von PowerShell zum Hinzufügen eines Wiederherstellungskennworts und Sichern des Wiederherstellungskennworts in Azure AD, bevor BitLocker aktiviert wird

```
Add-BitLockerKeyProtector -MountPoint "C:" -RecoveryPasswordProtector

$BLV = Get-BitLockerVolume -MountPoint "C:"

BackupToAAD-BitLockerKeyProtector -MountPoint "C:" -KeyProtectorId $BLV.KeyProtector[0].KeyProtectorId
```

Für Computer einschließlich Servern, die einer Domäne beigetreten sind, sollte das Kennwort für die Wiederherstellung in Active Directory Domain Services (AD DS) gespeichert werden.

Beispiel: Verwenden von PowerShell zum Hinzufügen eines Wiederherstellungskennworts und Sichern des Wiederherstellungskennworts in AD DS, bevor BitLocker aktiviert wird

```
Add-BitLockerKeyProtector -MountPoint "C:" -RecoveryPasswordProtector

$BLV = Get-BitLockerVolume -MountPoint "C:"

Backup-BitLockerKeyProtector -MountPoint "C:" -KeyProtectorId $BLV.KeyProtector[0].KeyProtectorId
```

Anschließend können Sie PowerShell verwenden, um BitLocker zu aktivieren.

Beispiel: Verwenden von PowerShell zum Aktivieren von BitLocker mit TPM-Schutz

```
Enable-BitLocker -MountPoint "D:" -EncryptionMethod XtsAes256 -UsedSpaceOnly -TpmProtector
```

Beispiel: Verwenden von PowerShell zum Aktivieren von BitLocker mit einem TPM + PIN-Schutz, in diesem Fall mit einer auf 123456 festgelegten PIN

```
$SecureString = ConvertTo-SecureString "123456" -AsPlainText -Force

Enable-BitLocker -MountPoint "C:" -EncryptionMethod XtsAes256 -UsedSpaceOnly -Pin $SecureString -
TPMandPinProtector
```

Verwandte Artikel

BitLocker: FAQ

Microsoft BitLocker Administration and Monitoring (MBAM)

Übersicht über die BitLocker-Geräteverschlüsselung in Windows10

BitLocker-Gruppenrichtlinieneinstellungen

Microsoft Intune *(Übersicht)*

Einstellungskonfigurationsanbieter *(Richtlinien-CSP: siehe Security-RequireDeviceEncryption)*

BitLocker-CSP

Windows Server-Einrichtungstools

Windows Server-Installationsoptionen

Aktualisieren lokaler Quellmedien, um Rollen und Features hinzuzufügen

Hinzufügen oder Entfernen optionaler Komponenten auf Server Core *(bedarfsbasierte Features)*

BitLocker: Bereitstellen auf Windows Server 2012 und höher

BitLocker: Aktivieren der Netzwerkentsperrung

Abgeschirmte VMs und geschütztes Fabric

PowerShell

BitLocker-Cmdlets für Windows PowerShell

Surface Pro-Spezifikationen

BitLocker: Aktivieren der Netzwerkentsperrung

11.02.2020 • 20 minutes to read

Betrifft

- Windows 10

In diesem Thema für IT-Experten wird beschrieben, wie die BitLocker-Netzwerkentsperrung funktioniert und konfiguriert wird.

Die Netzwerksperrung wurde in Windows 8 und Windows Server 2012 als BitLocker-Schutzoption für die Volumes des Betriebssystems eingeführt. Die Netzwerksperre ermöglicht eine einfachere Verwaltung für BitLocker-fähige Desktops und Server in einer Domänenumgebung, indem die Betriebssystem-Volumes beim Systemneustart automatisch freigegeben werden, wenn Sie mit einem drahtgebundenen Unternehmensnetzwerk verbunden sind. Für dieses Feature muss die Clienthardware einen DHCP-Treiber in der UEFI-Firmware implementieren. Ohne Netzwerksperrung ist für Betriebssystem-Volumes, die durch TPM + PIN-Protektoren geschützt sind, eine PIN erforderlich, wenn ein Computer neu gestartet oder aus dem Ruhezustand fortgesetzt wird (beispielsweisedurch Wake-on-LAN). Dies kann Unternehmen erschweren, Software-Patches auf unbeaufsichtigten Desktops und Remote verwalteten Servern bereitzustellen.

Mit der Netzwerksperrung können BitLocker-fähige Systeme mit TPM + PIN und die Hardwareanforderungen für den Start in Windows ohne Benutzereingriff erfüllt werden. Die Netzwerksperrung funktioniert auf ähnliche Weise wie das TPM + StartupKey beim Booten. Anstatt die StartupKey von USB-Medien zu lesen, besteht der Schlüssel für die Netzwerksperrung jedoch aus einem im TPM gespeicherten Schlüssel und einem verschlüsselten Netzwerkschlüssel, der an den Server gesendet, entschlüsselt und in einer sicheren Sitzung an den Client zurückgegeben wird.

Dieses Thema enthält:

- Kernanforderungen für Netzwerksperrung
- Netzwerk Sperrungs Sequenz
- Konfigurieren der Netzwerkentsperrung
- Erstellen der Zertifikatvorlage für die Netzwerksperrung
- Deaktivieren der Netzwerksperrung
- Aktualisieren von Netzwerkfreigabe Zertifikaten
- Problembehandlung bei der Netzwerksperrung
- Konfigurieren der Netzwerksperrung auf nicht unterstützten Systemen

Kernanforderungen für Netzwerksperrung

Die Netzwerksperrung muss obligatorische Hardware-und Softwareanforderungen erfüllen, bevor das Feature Domänen verbundene Systeme automatisch entsperren kann. Zu diesen Anforderungen gehören:

- Sie müssen mindestens Windows 8 oder Windows Server 2012 ausführen.
- Alle unterstützten Betriebssysteme mit UEFI-DHCP-Treibern können Netzwerk-Unlock-Clients sein.
- Netzwerk Sperrungs Clients müssen über einen TPM-Chip und mindestens eine TPM-Schutzkomponente verfügen.
- Ein Server, auf dem die Windows-Bereitstellungsdienste-Rolle (WDS) auf einem beliebigen unterstützten Server Betriebssystem ausgeführt wird.
- Optionales Feature für BitLocker-Netzwerksperrung, das auf einem beliebigen unterstützten Server

Betriebssystem installiert ist.

- Ein vom WDS-Server getrennter DHCP-Server.
- Ordnungsgemäß konfigurierte öffentliche/private Schlüssel Kopplung.
- Netzwerk Sperrungseinstellungen für Gruppenrichtlinien konfiguriert.

Der Netzwerkstapel muss aktiviert sein, damit das Feature Netzwerksperre verwendet werden kann. Gerätehersteller liefern Ihre Produkte in verschiedenen Zuständen und mit unterschiedlichen BIOS-Menüs, daher müssen Sie sicherstellen, dass der Netzwerkstapel im BIOS aktiviert ist, bevor Sie den Computer starten.

> **NOTE**
> Damit DHCP in UEFI ordnungsgemäß unterstützt wird, sollte das UEFI-basierte System im einheitlichen Modus sein, ohne dass ein Kompatibilitäts Support Modul (CSM) aktiviert ist.

Damit die Netzwerksperrung auf Computern mit Windows 8 und höher zuverlässig funktioniert, muss der erste Netzwerkadapter auf dem Computer, in der Regel der integrierte Adapter, für die Unterstützung von DHCP konfiguriert und für die Netzwerksperrung verwendet werden. Dies ist besonders erwähnenswert, wenn Sie über mehrere Adapter verfügen und eine ohne DHCP konfigurieren möchten, beispielsweise für ein Lights-Out-Verwaltungsprotokoll. Diese Konfiguration ist erforderlich, da die Netzwerksperre das Auflisten von Adaptern beendet, wenn eine Verbindung mit einem DHCP-Portfehler aus irgendeinem Grund erreicht wird. Wenn also der erste Aufzählungs Adapter DHCP nicht unterstützt, nicht an das Netzwerk angeschlossen ist oder die Verfügbarkeit des DHCP-Ports aus irgendeinem Grund nicht meldet, schlägt die Netzwerksperrung fehl.

Die Netzwerk Sperrungs Serverkomponente wird unter unterstützten Versionen von Windows Server 2012 und höher als Windows-Feature mithilfe von Server-Manager-oder Windows PowerShell-Cmdlets installiert. Der Funktionsname ist die BitLocker-Netzwerksperrung im Server-Manager und BitLocker-NetworkUnlock in Windows PowerShell. Dieses Feature ist eine Hauptanforderung.

Für die Netzwerksperrung sind Windows-Bereitstellungsdienste (WDS) in der Umgebung erforderlich, in der das Feature verwendet wird. Die Konfiguration der WDS-Installation ist nicht erforderlich; der WDS-Dienst muss jedoch auf dem Server ausgeführt werden.

Der Netzwerkschlüssel wird auf dem Systemlaufwerk zusammen mit einem AES 256-Sitzungsschlüssel gespeichert und mit dem 2048-Bit-RSA-öffentlichen Schlüssel des Zertifikats des Unlock-Servers verschlüsselt. Der Netzwerkschlüssel wird mit der Hilfe eines Anbieters für eine unterstützte Version von Windows Server mit WDS entschlüsselt und mit dem zugehörigen Sitzungsschlüssel verschlüsselt zurückgegeben.

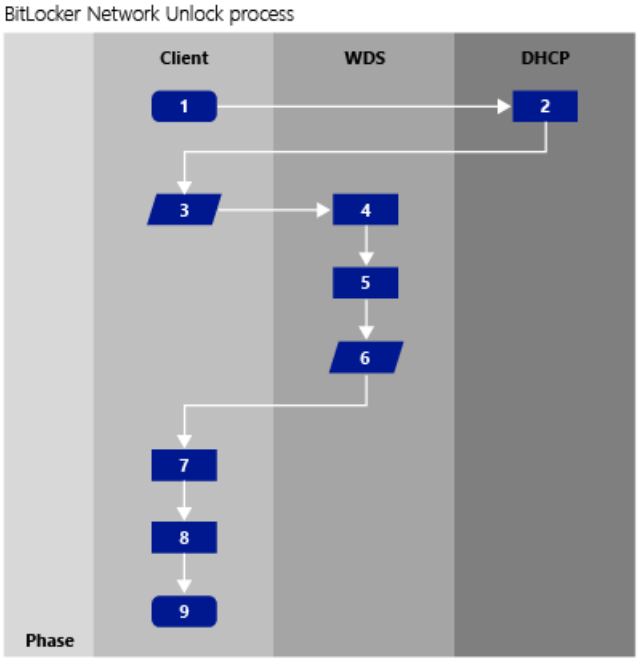
Netzwerk Sperrungs Sequenz

Die Unlock-Sequenz wird auf der Clientseite gestartet, wenn der Windows-Start-Manager feststellt, dass die Netzwerksperre Protector vorhanden ist. Es nutzt den DHCP-Treiber in UEFI, um eine IP-Adresse für IPv4 abzurufen, und sendet dann eine herstellerspezifische DHCP-Anforderung, die den Netzwerkschlüssel und einen Sitzungsschlüssel für die Antwort enthält, die alle durch das Netzwerksperre-Zertifikat des Servers verschlüsselt sind, wie oben beschrieben. Der Netzwerk-Unlock-Anbieter auf dem unterstützten WDS-Server erkennt die herstellerspezifische Anforderung, entschlüsselt ihn mit dem privaten RSA-Schlüssel und gibt den mit dem Sitzungsschlüssel verschlüsselten Netzwerkschlüssel über seine eigene herstellerspezifische DHCP-Antwort zurück.

Auf der Serverseite verfügt die WDS-Serverrolle über eine optionale Plug-in-Komponente, wie einen PXE-Anbieter, der die Anforderungen für eingehende Netzwerk Sperrungen übernimmt. Der Anbieter kann auch mit Subnetz-Einschränkungen konfiguriert werden, was erfordert, dass die IP-Adresse, die vom Client in der Netzwerkfreigabe Anforderung bereitgestellt wird, zu einem zulässigen Subnetz gehört, um den Netzwerkschlüssel für den Client freizugeben. In Fällen, in denen der Netzwerk-Unlock-Anbieter nicht verfügbar ist, schlägt BitLocker einen Failover zum nächsten verfügbaren Protector durch, um das Laufwerk zu entsperren.

In einer typischen Konfiguration bedeutet dies, dass der standardmäßige TPM + PIN Unlock-Bildschirm angezeigt wird, um das Laufwerk zu entsperren.

Die serverseitige Konfiguration zum Aktivieren der Netzwerksperrung erfordert auch die Bereitstellungeines 2048-Bit-RSA-Paars aus öffentlichen/privaten Schlüsseln in Form eines X. 509-Zertifikats und die Verteilung des Zertifikats des öffentlichen Schlüssels an die Clients. Dieses Zertifikat muss über den Gruppenrichtlinien-Editor direkt auf einem Domänencontroller mit mindestens einer Domänenfunktionsebene von Windows Server 2012 verwaltet und bereitgestellt werden. Bei diesem Zertifikat handelt es sich um den öffentlichen Schlüssel, der den zwischen Netzwerkschlüssel verschlüsselt (bei dem es sich um eines der beiden Geheimnisse handelt, die zum Entsperren des Laufwerks erforderlich sind, das andere Geheimnis wird im TPM gespeichert).



Phasen des Netzwerkfreigabe Prozesses

1. Der Windows-Start-Manager erkennt, dass in der BitLocker-Konfiguration eine Netzwerkschutz Sperre vorhanden ist.
2. Der Clientcomputer verwendet seinen DHCP-Treiber im UEFI, um eine gültige IPv4-IP-Adresse abzurufen.
3. Der Clientcomputer sendet eine herstellerspezifische DHCP-Anforderung aus, die den Netzwerkschlüssel (einen 256-Bit-zwischen Schlüssel) und einen AES-256-Sitzungsschlüssel für die Antwort enthält. Beide Schlüssel werden mit dem 2048-Bit-RSA-öffentlichen Schlüssel des Netzwerkfreigabe Zertifikats vom WDS-Server verschlüsselt.
4. Der Netzwerk-Unlock-Anbieter auf dem WDS-Server erkennt die herstellerspezifische Anforderung.
5. Der Anbieter entschlüsselt ihn mit dem BitLocker-Netzwerksperre-Zertifikat RSA-privater Schlüssel des WDS-Servers.
6. Der WDS-Anbieter gibt dann den mit dem Sitzungsschlüssel verschlüsselten Netzwerkschlüssel unter Verwendung seiner eigenen herstellerspezifischen DHCP-Antwort an den Clientcomputer zurück. Dies bildet einen zwischen Schlüssel.
7. Der zurückgegebene zwischen Schlüssel wird dann mit einem anderen lokalen 256-Bit-zwischen Schlüssel kombiniert, der nur vom TPM entschlüsselt werden kann.
8. Dieser kombinierte Schlüssel wird verwendet, um einen AES-256-Schlüssel zu erstellen, mit dem die Sperre des Volumes aufgehoben wird.
9. Die Startsequenz wird von Windows fortgesetzt.

Konfigurieren der Netzwerkentsperrung

Mit den folgenden Schritten kann ein Administrator die Netzwerksperrung in einer Domäne konfigurieren, in

der die Domänenfunktionsebene mindestens Windows Server 2012 ist.

Installieren der WDS-Server Rolle

Das Feature "BitLocker-Netzwerksperrung" installiert die WDS-Rolle, wenn Sie noch nicht installiert ist. Wenn Sie es separat installieren möchten, bevor Sie die BitLocker-Netzwerksperre installieren, können Sie den Server-Manager oder Windows PowerShell verwenden. Wenn Sie die Rolle mit dem Server-Manager installieren möchten, wählen Sie im Server-Manager die Rolle **Windows-Bereitstellungsdienste** aus.

Verwenden Sie den folgenden Befehl, um die Rolle unter Verwendung von Windows PowerShell zu installieren:

```
Install-WindowsFeature WDS-Deployment
```

Sie müssen den WDS-Server so konfigurieren, dass er mit DHCP (und optional mit Active Directory-Domänendiensten) und dem Clientcomputer kommunizieren kann. Sie können das WDS-Verwaltungstool WdsMgmt. msc verwenden, das den Konfigurations-Assistenten für Windows-Bereitstellungsdienste startet.

Bestätigen, dass der WDS-Dienst ausgeführt wird

Um zu bestätigen, dass der WDS-Dienst ausgeführt wird, verwenden Sie die Dienste-Verwaltungskonsole oder Windows PowerShell. Um zu bestätigen, dass der Dienst in der Dienste-Verwaltungskonsole ausgeführt wird, öffnen Sie die Konsole mithilfe von **Services. msc** , und überprüfen Sie den Status des Diensts für Windows-Bereitstellungsdienste.

Um zu bestätigen, dass der Dienst mit Windows PowerShell ausgeführt wird, verwenden Sie den folgenden Befehl:

```
Get-Service WDSServer
```

Installieren der Netzwerk Sperrungs Funktion

Verwenden Sie den Server-Manager oder Windows PowerShell, um das Feature Netzwerksperrung zu installieren. Wenn Sie das Feature mithilfe des Server-Managers installieren möchten, wählen Sie in der Server-Manager-Konsole das Feature **BitLocker-Netzwerksperrung** aus.

Verwenden Sie den folgenden Befehl, um das Feature mithilfe von Windows PowerShell zu installieren:

```
Install-WindowsFeature BitLocker-NetworkUnlock
```

Erstellen der Zertifikatvorlage für die Netzwerksperrung

Eine ordnungsgemäß konfigurierte Active Directory Services-Zertifizierungsstelle kann diese Zertifikatvorlage verwenden, um Netzwerkfreigabe Zertifikate zu erstellen und auszustellen.

1. Öffnen Sie das Zertifikatvorlagen-Snap-in (certtmpl. msc).
2. Suchen Sie die Benutzervorlage. Klicken Sie mit der rechten Maustaste auf den Vorlagennamen, und wählen Sie **Vorlage duplizieren**aus.
3. Ändern Sie auf der Registerkarte **Kompatibilität** die Felder **Zertifizierungsstelle** und **Zertifikat Empfänger** auf Windows Server 2012 und Windows 8. Stellen Sie sicher, dass das Dialogfeld **resultierende Änderungen anzeigen** aktiviert ist.
4. Wählen Sie die Registerkarte **Allgemein** der Vorlage aus. Der **Anzeigename** und der **Vorlagenname** der Vorlage sollten eindeutig erkennen, dass die Vorlage für die Netzwerksperrung verwendet wird. Deaktivieren Sie das Kontrollkästchen für die Option **Zertifikat in Active Directory veröffentlichen** .
5. Wählen Sie die Registerkarte **Anforderungsbehandlung** aus. Wählen Sie im Dropdownmenü **Zweck** die Option **Verschlüsselung** aus. Stellen Sie sicher, dass die Option **privater Schlüssel kann exportiert werden** aktiviert ist.

6. Wählen Sie die Registerkarte **Kryptografie** aus. Legen Sie die **minimale Schlüsselgröße** auf 2048. (Jeder Microsoft Cryptographic Provider, der RSA unterstützt, kann für diese Vorlage verwendet werden, aber für Einfachheit und Aufwärtskompatibilität empfehlen wir die Verwendung des **Microsoft-Software-Schlüsselspeicheranbieters**.)
7. Wählen Sie die Option **Anforderungen müssen eine der folgenden Anbietern verwenden aus** , und deaktivieren Sie alle Optionen, mit Ausnahme des von Ihnen ausgewählten Kryptographie-Anbieters, beispielsweise des **Microsoft Software Key-Speicheranbieters**.
8. Wählen Sie die Registerkarte **Antragsteller Name** aus. Wählen Sie **in der Anfrage Supply**aus. Wählen Sie **OK** aus, wenn das Dialogfeld Zertifikatvorlagen eingeblendet wird.
9. Wählen Sie die Registerkarte **Ausstellungsanforderungen** aus. Wählen Sie die Optionen **Zertifizierungsstelle Zertifikat-Manager-Genehmigung** und **gültige vorhandene Zertifikate** aus.
10. Wählen Sie die Registerkarte **Erweiterungen** aus. Wählen Sie **Anwendungsrichtlinien** und dann **Bearbeiten...** aus.
11. Wählen Sie im Dialogfeld Erweiterungsoptionen für **Anwendungsrichtlinien bearbeiten** die Option **Client Authentifizierung**, **Datei System verschlüsseln und sichere e-Mail** aus, und wählen Sie **Entfernen**aus.
12. Wählen Sie im Dialogfeld **Anwendungsrichtlinienerweiterung bearbeiten** die Option **Hinzufügen**aus.
13. Wählen Sie im Dialogfeld **Anwendungsrichtlinie hinzufügen** die Option **neu**aus. Geben Sie im Dialogfeld **neue Anwendungsrichtlinie** die folgenden Informationen in den bereitgestellten Bereich ein, und klicken Sie dann auf **OK** , um die BitLocker-Netzwerksperre-Anwendungsrichtlinie zu erstellen:
    - **Name: BitLocker-Netzwerksperre**
    - **Objekt-ID: 1.3.6.1.4.1.311.67.1.1**
14. Wählen Sie die neu erstellte **BitLocker-Netzwerk Sperrungs** Anwendungsrichtlinie aus, und wählen Sie **OK**aus.
15. Wenn die Registerkarte **Erweiterungen** weiterhin geöffnet ist, wählen Sie das Dialogfeld **Schlüsselverwendungserweiterung bearbeiten** aus, und wählen Sie die Option **Schlüsselaustausch nur mit Schlüssel Verschlüsselung zulassen (Schlüssel Verschlüsselung)** aus. Aktivieren Sie das Kontrollkästchen **Diese Erweiterung als kritisch festlegen** .
16. Wählen Sie die Registerkarte **Sicherheit** aus. bestätigen Sie, dass der Gruppe der **Domänenadministratoren** die Berechtigung zum **registrieren** erteilt wurde.
17. Wählen Sie **OK** aus, um die Konfiguration der Vorlage abzuschließen.

Wenn Sie die Vorlage für das Netzwerk entsperren zur Zertifizierungsstelle hinzufügen möchten, öffnen Sie das Zertifizierungsstellen-Snap-in (certsrv. msc). Klicken Sie mit der rechten Maustaste auf das Element **Zertifikatvorlagen** , und wählen Sie **neu aus, Zertifikatvorlage zum ausgeben**. Wählen Sie das zuvor erstellte BitLocker-Netzwerk Sperrungs Zertifikat aus.

Nach dem Hinzufügen der Vorlage für das Netzwerk entsperren zur Zertifizierungsstelle kann dieses Zertifikat verwendet werden, um die BitLocker-Netzwerksperrung zu konfigurieren.

Erstellen des Netzwerkfreigabe Zertifikats

Die Netzwerksperrung kann importierte Zertifikate aus einer vorhandenen PKI-Infrastruktur verwenden, oder Sie können ein selbstsigniertes Zertifikat verwenden.

Gehen Sie wie folgt vor, um ein Zertifikat von einer vorhandenen Zertifizierungsstelle (Certification Authority, ca) zu registrieren:

1. Öffnen des Zertifikats-Managers auf dem WDS-Server mithilfe von **Certmgr. msc**
2. Klicken Sie unter dem Element Zertifikate-Aktueller Benutzer mit der rechten Maustaste auf persönlich.
3. Wählen Sie alle Aufgaben und dann **Neues Zertifikat anfordern** aus.
4. Wählen Sie **weiter** aus, wenn der Zertifikat Registrierungs-Assistent geöffnet wird.
5. Active Directory-Registrierungsrichtlinie auswählen

6. Wählen Sie die Zertifikatvorlage aus, die für die Netzwerksperrung auf dem Domänencontroller erstellt wurde, und wählen Sie **registrieren**aus. Wenn Sie dazu aufgefordert werden, weitere Informationen zu erhalten, fügen Sie dem Zertifikat das folgende Attribut hinzu:
   - Wählen Sie den Bereich **Subject Name** aus, und geben Sie einen Anzeigenamen-Wert an. Es wird empfohlen, dass dieser Anzeigename Informationen für die Domäne oder Organisationseinheit für das Zertifikat enthält. Beispiel: "BitLocker-Netzwerk Sperrungs Zertifikat für Contoso-Domäne"
7. Erstellen Sie das Zertifikat. Stellen Sie sicher, dass das Zertifikat im Ordner "persönlich" angezeigt wird.
8. Exportieren des Zertifikats des öffentlichen Schlüssels für die Netzwerksperrung
   a. Erstellen Sie eine CER-Datei, indem Sie mit der rechten Maustaste auf das zuvor erstellte Zertifikat klicken, dann **alle Aufgaben**auswählen und dann **exportieren**.
   b. Wählen Sie **Nein, privaten Schlüssel nicht exportieren**aus.
   c. Wählen Sie **der codierte binäre X. 509** aus, und führen Sie den Export des Zertifikats in eine Datei aus.
   d. Geben Sie der Datei einen Namen wie BitLocker-NetworkUnlock. cer.
9. Exportieren des öffentlichen Schlüssels mit einem privaten Schlüssel für die Netzwerksperrung
   a. Erstellen Sie eine PFX-Datei, indem Sie mit der rechten Maustaste auf das zuvor erstellte Zertifikat klicken, dann **alle Aufgaben**auswählen und dann **exportieren**.
   b. Wählen Sie **Ja, privaten Schlüssel exportieren**aus.
   c. Führen Sie den Assistenten aus, um die PFX-Datei zu erstellen.

Zum Erstellen eines selbstsignierten Zertifikats können Sie entweder das Cmdlet New-SelfSignedCertificate in Windows PowerShell verwenden oder Certreq verwenden.

Beispiel für Windows PowerShell:

```
New-SelfSignedCertificate -CertStoreLocation Cert:\LocalMachine\My -Subject "CN=BitLocker Network Unlock
certificate" -Provider "Microsoft Software Key Storage Provider" -KeyUsage KeyEncipherment -KeyUsageProperty
Decrypt,Sign -KeyLength 2048 -HashAlgorithm sha512 -TextExtension @("1.3.6.1.4.1.311.21.10=
{text}OID=1.3.6.1.4.1.311.67.1.1","2.5.29.37={text}1.3.6.1.4.1.311.67.1.1")
```

Certreq-Beispiel:

1. Erstellen Sie eine Textdatei mit der Erweiterung. inf. Beispiel: Notepad. exe BitLocker-NetworkUnlock. inf.
2. Fügen Sie der zuvor erstellten Datei den folgenden Inhalt hinzu:

```
[NewRequest]
Subject="CN=BitLocker Network Unlock certificate"
ProviderType=0
MachineKeySet=True
Exportable=true
RequestType=Cert
KeyUsage="CERT_KEY_ENCIPHERMENT_KEY_USAGE"
KeyUsageProperty="NCRYPT_ALLOW_DECRYPT_FLAG | NCRYPT_ALLOW_SIGNING_FLAG"
KeyLength=2048
SMIME=FALSE
HashAlgorithm=sha512
[Extensions]
1.3.6.1.4.1.311.21.10 = "{text}"
_continue_ = "OID=1.3.6.1.4.1.311.67.1.1"
2.5.29.37 = "{text}"
_continue_ = "1.3.6.1.4.1.311.67.1.1"
```

3. Öffnen Sie eine Eingabeaufforderung mit erhöhten Rechten, und verwenden Sie das Certreq-Tool, um ein

neues Zertifikat mithilfe des folgenden Befehls zu erstellen und den vollständigen Pfad zu der zuvor erstellten Datei zusammen mit dem Dateinamen anzugeben:

```
certreq -new BitLocker-NetworkUnlock.inf BitLocker-NetworkUnlock.cer
```

4. Überprüfen Sie, ob der vorherige Befehl das Zertifikat ordnungsgemäß erstellt hat, indem Sie bestätigen, dass die CER-Datei vorhanden ist.

5. Starten Sie Zertifikate – lokaler Computer, indem Sie **certlm. msc**ausführen.
6. Erstellen Sie eine PFX-Datei, indem Sie im Navigationsbereich den Pfad **Zertifikate – lokaler Computer\Personal\Certificates** öffnen, mit der rechten Maustaste auf das zuvor importierte Zertifikat klicken, dann **alle Aufgaben**auswählen und dann **exportieren**. Führen Sie den Assistenten aus, um die PFX-Datei zu erstellen.

Bereitstellen des privaten Schlüssels und des Zertifikats auf dem WDS-Server

Stellen Sie mit dem erstellten Zertifikat und Schlüssel in der Infrastruktur bereit, um Systeme ordnungsgemäß zu entsperren. Gehen Sie zum Bereitstellen der Zertifikate wie folgt vor:

1. Öffnen Sie auf dem WDS-Server eine neue MMC, und fügen Sie das Zertifikat-Snap-in hinzu. Wählen Sie das Computerkonto und den lokalen Computer aus, wenn die Optionen angegeben sind.
2. Klicken Sie mit der rechten Maustaste auf das Zertifikat (lokaler Computer) – BitLocker-Laufwerk Verschlüsselungs Netzwerk entsperren, wählen Sie alle Aufgaben und dann **importieren**aus.
3. Wählen Sie im Dialogfeld **zu importierende Datei** die zuvor erstellte PFX-Datei aus.
4. Geben Sie das Kennwort ein, das zum Erstellen der PFX-Anwendung verwendet wird, und führen Sie den Assistenten aus.

Konfigurieren von Gruppenrichtlinieneinstellungen für die Netzwerksperrung

Wenn Zertifikat und Schlüssel auf dem WDS-Server für die Netzwerksperrung bereitgestellt werden, besteht der letzte Schritt darin, die Gruppenrichtlinieneinstellungen zum Bereitstellen des Zertifikats für öffentliche Schlüssel auf Computern zu verwenden, deren Sperrung mithilfe des Netzwerkfreigabe Schlüssels aufgehoben werden soll. Gruppenrichtlinieneinstellungen für BitLocker finden Sie unter **\Computer Configuration\Administrative Templates\Windows Components\BitLocker Drive Encryption** mithilfe des lokalen Gruppenrichtlinien-Editors oder der Microsoft Management Console.

In den folgenden Schritten wird beschrieben, wie Sie die Gruppenrichtlinieneinstellung aktivieren, die für die Konfiguration der Netzwerksperrung erforderlich ist.

1. Öffnen Sie die Gruppenrichtlinien-Verwaltungskonsole (GPMC. msc).
2. Aktivieren Sie die Richtlinie **erfordert beim Start eine zusätzliche Authentifizierung** , und aktivieren Sie die Option **Start-PIN mit TPM anfordern** oder **Start-PIN mit TPM zulassen** .
3. Aktivieren Sie BitLocker mit TPM + PIN-Schutz auf allen Computern, die mit der Domäne verbunden sind.

In den folgenden Schritten wird beschrieben, wie die erforderliche Gruppenrichtlinieneinstellung bereitgestellt wird:

> **NOTE**
>
> Die Gruppenrichtlinieneinstellungen **ermöglichen die Netzwerksperrung beim Start** und das **Hinzufügen eines Netzwerkfreigabe Zertifikats** in Windows Server 2012.

1. Kopieren Sie die für Netzwerksperrung erstellte CER-Datei auf den Domänencontroller.
2. Starten Sie auf dem Domänencontroller die Gruppenrichtlinien-Verwaltungskonsole (GPMC. msc).
3. Erstellen Sie ein neues Gruppenrichtlinienobjekt, oder ändern Sie ein vorhandenes Objekt, um die Einstellung

Netzwerksperrung beim Start zulassen zu aktivieren.

4. Bereitstellen des öffentlichen Zertifikats für Clients:

   a. Navigieren Sie in der Gruppenrichtlinien-Verwaltungskonsole zum folgenden Speicherort: **Computer Configuration\Policies\Windows Settings\Security Settings\Public Schlüssel Policies\BitLocker Laufwerk Verschlüsselungs Netzwerk Zertifikat entsperren**.
   b. Klicken Sie mit der rechten Maustaste auf den Ordner, und wählen Sie **Netzwerkfreigabe Zertifikat hinzufügen**aus.
   c. Führen Sie die Schritte des Assistenten aus, und importieren Sie die CER-Datei, die zuvor kopiert wurde.

> **NOTE**
> Es kann jeweils nur ein Netzwerk Sperrungs Zertifikat zur Verfügung stehen. Wenn ein neues Zertifikat erforderlich ist, löschen Sie das aktuelle Zertifikat, bevor Sie ein neues Zertifikat bereitstellen. Das Netzwerk Sperrungs Zertifikat befindet sich im **HKEY \ _LOCAL \ _MACHINE \software\policies\microsoft\systemcertificates\fve\ _NKP** -Schlüssel auf dem Clientcomputer.

1. Starten Sie die Clients nach der Bereitstellung der Gruppenrichtlinie neu. > [!NOTE] > Das **Netzwerk (Zertifikat basiert)** Protector wird erst nach einem Neustart mit aktivierter Richtlinie und einem gültigen Zertifikat im FVE_NKP Store hinzugefügt.

Konfigurationsdateien für Subnet-Richtlinien auf dem WDS-Server (optional)

Standardmäßig werden alle Clients mit dem richtigen Netzwerk Sperrungs Zertifikat und den gültigen Netzwerk Sperrungs Beschützern, die kabelgebundenen Zugriff auf einen Netzwerk entsperren-aktivierten WDS-Server über DHCP haben, vom Server freigegeben. Es kann eine Konfigurationsdatei für eine Subnetz-Richtlinie auf dem WDS-Server erstellt werden, um zu begrenzen, welche Subnetz-Netzwerk Sperrungs Clients zum Entsperren verwenden können.

Die Konfigurationsdatei mit dem Namen "BDE-Network-Unlock. ini" muss sich im gleichen Verzeichnis wie die Netzwerk-Unlock-Anbieter-DLL (%windir%\System32\Nkpprov.dll) befinden und sowohl für IPv6-als auch für IPv4-DHCP-Implementierungen verwendet werden. Wenn die Richtlinie für die Subnet-Konfiguration beschädigt wird, schlägt der Anbieter fehl und reagiert nicht mehr auf Anfragen.

Die Konfigurationsdatei der Subnet-Richtlinie muss einen Abschnitt "\ [Subnetze]" verwenden, um die einzelnen Subnetze zu identifizieren. Die benannten Subnets können dann verwendet werden, um Einschränkungen in Zertifikat Unterabschnitten festzulegen. Subnets werden als einfache Name-Wert-Paare im allgemeinen INI-Format definiert, wobei jedes Subnetz eine eigene Zeile hat, mit dem Namen auf der linken Seite des Gleichheitszeichens und dem auf der rechten Seite des Gleichheitszeichens angegebenen Subnetz als CIDR-Adresse oder-Bereich (klassenübergreifend). Das Schlüsselwort "aktiviert" ist für Subnet-Namen nicht zulässig.

```
[SUBNETS]
SUBNET1=10.185.250.0/24 ; comment about this subrange could be here, after the semi-colon
SUBNET2=10.185.252.200/28
SUBNET3= 2001:4898:a:2::/64 ; an IPv6 subnet
SUBNET4=2001:4898:a:3::/64; in production, the admin would likely give more useful names, like BUILDING9-
EXCEPT-RECEP.
```

Nach dem Abschnitt \ [Subnets] können für jedes Netzwerk Sperrungs Zertifikat Abschnitte vorhanden sein, die durch den ohne Leerzeichen formatierten Zertifikat Fingerabdruck identifiziert werden, in dem Subnetze definiert werden, von denen Clients mit diesem Zertifikat freigegeben werden können.

> **NOTE**
> Wenn Sie den Fingerabdruck des Zertifikats angeben, schließen Sie keine Leerzeichen ein. Wenn Leerzeichen im Fingerabdruck enthalten sind, schlägt die Subnetz-Konfiguration fehl, da der Fingerabdruck nicht als gültig erkannt wird.

Subnet-Einschränkungen werden innerhalb der einzelnen Zertifikat Abschnitte definiert, indem die Liste der zulässigen Subnetze angegeben wird. Wenn ein Subnetz in einem Zertifikat Abschnitt aufgeführt ist, sind nur die aufgeführten Subnets für dieses Zertifikat zugelassen. Wenn kein Subnetz in einem Zertifikat Abschnitt aufgeführt ist, sind alle Subnets für dieses Zertifikat zugelassen. Wenn ein Zertifikat keinen Abschnitt in der Konfigurationsdatei der Subnet-Richtlinie enthält, werden keine Subnetz-Einschränkungen für die Freigabe mit diesem Zertifikat angewendet. Dies bedeutet, dass für jedes Zertifikat ein Zertifikat Abschnitt vorhanden sein muss, damit alle Zertifikate auf dem Server für jedes Netzwerk freigegeben werden können, und dass für jeden Zertifikat Abschnitt eine explizite Liste der zulässigen Listen eingerichtet wird. Subnetlisten werden erstellt, indem der Name eines Subnetzes aus dem Abschnitt \ [Subnetze] in einer eigenen Zeile unterhalb der Kopfzeile des Zertifikat Abschnitts angegeben wird. Auf dem Server werden dann nur die Clients mit diesem Zertifikat auf den in der Liste angegebenen Subnetz (en) freigegeben. Zur Problembehandlung kann ein Subnetz schnell ausgeschlossen werden, ohne es aus dem Abschnitt zu löschen, indem Sie es einfach mit einem vorangestellten Semikolon kommentieren.

```
[2158a767e1c14e88e27a4c0aee111d2de2eafe60]
;Comments could be added here to indicate when the cert was issued, which Group Policy should get it, and so
on.
;This list shows this cert is only allowed to unlock clients on SUBNET1 and SUBNET3 subnets. In this
example, SUBNET2 is commented out.
SUBNET1
;SUBNET2
SUBNET3
```

Um die Verwendung eines Zertifikats überhaupt nicht zu unterbinden, kann seine Subnetliste die Zeile "disabled" enthalten.

Deaktivieren der Netzwerksperrung

Um den Unlock-Server zu deaktivieren, kann der PXE-Anbieter vom WDS-Server aufgehoben oder ganz deinstalliert werden. Wenn Sie jedoch verhindern möchten, dass Clients Netzwerk entsperren-Schutzvorrichtungen erstellen, sollte die Gruppenrichtlinieneinstellung **Netzwerksperrung beim Start zulassen** deaktiviert sein. Wenn diese Richtlinieneinstellung auf Clientcomputern auf "deaktiviert" aktualisiert wird, werden alle auf dem Computer vorhandenen Netzwerk Sperrungs Schlüssel gelöscht. Alternativ kann die BitLocker-Netzwerk Sperrungs Zertifikatrichtlinie auf dem Domänencontroller gelöscht werden, um dieselbe Aufgabe für eine gesamte Domäne auszuführen.

> **NOTE**
> Durch das Entfernen des FVE_NKP Zertifikatspeichers, der das Netzwerk Zertifikat und den Schlüssel auf dem WDS-Server enthält, wird auch die Fähigkeit des Servers, auf Unlock-Anforderungen für dieses Zertifikat zu reagieren, effektiv deaktiviert. Dies wird jedoch als Fehlerbedingung angesehen und ist keine unterstützte oder empfohlene Methode zum Deaktivieren des Netzwerk Sperrungs Servers.

Aktualisieren von Netzwerkfreigabe Zertifikaten

Um die von der Netzwerksperrung verwendeten Zertifikate zu aktualisieren, müssen Administratoren das neue Zertifikat für den Server importieren oder generieren und dann die Gruppenrichtlinieneinstellung Netzwerk Sperrungs Zertifikat auf dem Domänencontroller aktualisieren.

Problembehandlung bei der Netzwerksperrung

Das Beheben von Problemen mit der Netzwerksperrung beginnt mit der Überprüfung der Umgebung. Oft ist ein kleines Konfigurationsproblem die Ursache für den Fehler. Zu überprüfende Elemente sind:

- Überprüfen Sie, ob die Clienthardware UEFI-basiert ist und die Firmware-Version 2.3.1 lautet und dass sich die UEFI-Firmware im einheitlichen Modus befindet, ohne dass ein Kompatibilitäts Support Modul (CSM) für den BIOS-Modus aktiviert ist. Überprüfen Sie dazu, ob für die Firmware keine Option wie "Legacy-Modus" oder "Kompatibilitätsmodus" aktiviert ist oder dass sich die Firmware nicht in einem BIOS-ähnlichen Modus befindet.
- Alle erforderlichen Rollen und Dienste werden installiert und gestartet
- Öffentliche und private Zertifikate wurden veröffentlicht und befinden sich im richtigen Zertifikat Container. Das vorhanden sein des Netzwerkfreigabe Zertifikats kann in der Microsoft Management Console (MMC. exe) auf dem WDS-Server überprüft werden, wobei die Zertifikat-Snap-Ins für den lokalen Computer aktiviert sind. Das Clientzertifikat kann überprüft werden, indem der Registrierungsschlüssel **HKEY \ _LOCAL \ _MACHINE \software\policies\microsoft\systemcertificates\fve\ _NKP** auf dem Clientcomputer überprüft wird.
- Gruppenrichtlinien für die Netzwerksperrung sind aktiviert und mit den entsprechenden Domänen verknüpft.
- Überprüfen Sie, ob die Gruppenrichtlinien die Clients ordnungsgemäß erreichen. Dies kann mithilfe der Dienstprogramme Gpresult. exe oder RSoP. msc erfolgen.
- Überprüfen Sie, ob die Clients nach der Anwendung der Richtlinie neu gestartet wurden.
- Überprüfen Sie, ob das **Netzwerk (Certificate based)** Protector auf dem Client aufgeführt ist. Dies kann entweder mithilfe von manage-bde-oder Windows PowerShell-Cmdlets erfolgen. Mit dem folgenden Befehl werden beispielsweise die auf dem Laufwerk C: des lokalen Computers konfigurierten Schlüssel Beschützer aufgelistet:

  ```
  manage-bde -protectors -get C:
  ```

  > **NOTE**
  > Verwenden Sie die Ausgabe von manage-bde zusammen mit dem WDS-Debug-Protokoll, um festzustellen, ob der richtige Fingerabdruck des Zertifikats für die Netzwerksperrung verwendet wird.

Dateien, die bei der Problembehandlung bei der BitLocker-Netzwerksperrung erfasst werden sollen:

1. Die Windows-Ereignisprotokolle. Insbesondere die BitLocker-Ereignisprotokolle und das Microsoft-Windows-Deployment-Services-Diagnostics-Debug-Protokoll

   Die Debug-Protokollierung ist standardmäßig für die WDS-Serverrolle deaktiviert, daher müssen Sie Sie zuerst aktivieren. Sie können eine der beiden folgenden Methoden verwenden, um die WDS-Debug-Protokollierung zu aktivieren.

   a. Starten Sie eine Eingabeaufforderung mit erhöhten Rechten, und führen Sie den folgenden Befehl aus:

      ```
      wevtutil sl Microsoft-Windows-Deployment-Services-Diagnostics/Debug /e:true
      ```

   b. Öffnen Sie die Ereignisanzeige auf dem WDS-Server.

      Klicken Sie im linken Bereich auf **Anwendungen und Dienstprotokolle**, klicken Sie auf **Microsoft**, klicken Sie auf **Windows**, klicken Sie auf **Bereitstellungsdienste-Diagnose**, und klicken Sie dann auf **Debuggen**.

Klicken Sie im rechten Bereich auf **Protokoll aktivieren**.

2. Die DHCP-Subnet-Konfigurationsdatei (sofern vorhanden).

3. Die Ausgabe des BitLocker-Status auf dem Volume kann in einer Textdatei mithilfe von **manage-bde-Status** oder **Get-BitLockerVolume** in Windows PowerShell erfasst werden.
4. Netzwerk Monitor Erfassung auf dem Server, auf dem die WDS-Rolle gehostet wird, gefiltert nach Client-IP-Adresse.

Konfigurieren von Gruppenrichtlinieneinstellungen für die Netzwerksperrung in früheren Versionen

Die Netzwerksperrung und die zugehörigen Gruppenrichtlinieneinstellungen wurden in Windows Server 2012 eingeführt, können aber unter Verwendung von Betriebssystemen mit Windows Server2008R2 und Windows Server2008 bereitgestellt werden.

Anforderungen

- Auf dem Server, auf dem WDS gehostet wird, müssen alle Server Betriebssysteme ausgeführt werden, die in der Liste **gilt für zu** Beginn dieses Themas angegeben sind.
- Auf Clientcomputern muss eines der Clientbetriebssysteme ausgeführt werden, die in der Liste " **gilt für** " am Anfang dieses Themas angegeben sind.

Die folgenden Schritte können verwendet werden, um die Netzwerksperrung auf diesen älteren Systemen zu konfigurieren.

1. Installieren der WDS-Server Rolle
2. Bestätigen, dass der WDS-Dienst ausgeführt wird
3. Installieren der Netzwerk Sperrungs Funktion
4. Erstellen des Netzwerkfreigabe Zertifikats
5. Bereitstellen des privaten Schlüssels und des Zertifikats auf dem WDS-Server
6. Konfigurieren der Registrierungseinstellungen für die Netzwerksperrung:

   Wenden Sie die Registrierungseinstellungen an, indem Sie das folgende certutil-Skript ausführen (vorausgesetzt, die Zertifikatdatei für das Netzwerk entsperren heißt " **BitLocker-NetworkUnlock.CER**") auf jedem Computer, auf dem eines der Clientbetriebssysteme ausgeführt wird, die in der Liste " **gilt für** " am Anfang dieses Themas angegeben sind.

   ```
   certutil -f -grouppolicy -addstore FVE_NKP BitLocker-NetworkUnlock.cer
   reg add "HKLM\SOFTWARE\Policies\Microsoft\FVE" /v OSManageNKP /t REG_DWORD /d 1 /f
   reg add "HKLM\SOFTWARE\Policies\Microsoft\FVE" /v UseAdvancedStartup /t REG_DWORD /d 1 /f
   reg add "HKLM\SOFTWARE\Policies\Microsoft\FVE" /v UsePIN /t REG_DWORD /d 2 /f
   reg add "HKLM\SOFTWARE\Policies\Microsoft\FVE" /v UseTPMPIN /t REG_DWORD /d 2 /f
   reg add "HKLM\SOFTWARE\Policies\Microsoft\FVE" /v UseTPM /t REG_DWORD /d 2 /f
   reg add "HKLM\SOFTWARE\Policies\Microsoft\FVE" /v UseTPMKey /t REG_DWORD /d 2 /f
   reg add "HKLM\SOFTWARE\Policies\Microsoft\FVE" /v UseTPMKeyPIN /t REG_DWORD /d 2 /f
   ```

7. Einrichten eines TPM-Beschützers auf den Clients

8. Starten Sie die Clients neu, um das Netzwerk (Zertifikat basiert) Protector hinzuzufügen.

Weitere Informationen:

- Übersicht über BitLocker
- Häufig gestellte Fragen (Frequently Asked Questions, FAQ) zu BitLocker
- Vorbereiten Ihrer Organisation auf BitLocker: Planung und Richtlinien

BitLocker: Verwenden von BitLocker-Laufwerksverschlüsselungstools zum Verwalten von BitLocker

06.03.2020 • 9 minutes to read

Betriff:

- Windows 10

In diesem Thema für IT-Spezialisten werden die Tools zum Verwalten von BitLocker beschrieben.

Zu den BitLocker-Laufwerk Verschlüsselungstools gehören die Befehlszeilentools manage-bde und Repair-bde sowie die BitLocker-Cmdlets für Windows PowerShell.

Sowohl manage-bde als auch die BitLocker-Cmdlets können verwendet werden, um alle Aufgaben auszuführen, die über die BitLocker-Systemsteuerung ausgeführt werden können und für automatisierte Bereitstellungen und andere Skript Szenarien geeignet sind.

Repair-bde ist ein spezielles Umstands Tool, das für Disaster Recovery-Szenarien bereitgestellt wird, bei denen ein geschütztes BitLocker-Laufwerk nicht normal oder mithilfe der Wiederherstellungskonsole freigegeben werden kann.

1. Manage-bde
2. Reparieren-BDE
3. BitLocker-Cmdlets für Windows PowerShell

Manage-bde

Manage-bde ist ein Befehlszeilentool, das für das Skripting von BitLocker-Vorgängen verwendet werden kann. Manage-bde bietet zusätzliche Optionen, die nicht in der BitLocker-Systemsteuerung angezeigt werden. Eine vollständige Liste der Optionen für manage-bde finden Sie unter Verwalten-BDE -Befehlszeilenreferenz.

Manage-bde umfasst geringere Standardeinstellungen und erfordert eine größere Anpassung für die Konfiguration von BitLocker. Beispielsweise wird durch die Verwendung `manage-bde -on` von nur dem Befehl auf einem Datenvolumen die Lautstärke ohne Authentifizierungsschutz vollständig verschlüsselt. Für einen auf diese Weise verschlüsselten Datenträger ist weiterhin die Benutzerinteraktion erforderlich, um den BitLocker-Schutz zu aktivieren, auch wenn der Befehl erfolgreich abgeschlossen wurde, weil dem Volume eine Authentifizierungsmethode hinzugefügt werden muss, damit Sie vollständig geschützt ist. Die folgenden Abschnitte enthalten Beispiele für häufige Verwendungsszenarien für manage-bde.

Verwenden von manage-bde mit Betriebssystem-Volumes

Nachfolgend finden Sie Beispiele für grundlegende gültige Befehle für Betriebssystem-Volumes. Im allgemeinen verschlüsselt die Verwendung des `manage-bde -on <drive letter>` Befehls nur den Betriebssystemdatenträger mit einem nur-TPM-Schutz und ohne Wiederherstellungsschlüssel. Viele Umgebungen erfordern jedoch mehr sichere Schutzvorrichtungen wie Kennwörter oder PIN und erwarten, dass Sie Informationen mit einem Wiederherstellungsschlüssel wiederherstellen können. Es wird empfohlen, dass mindestens ein primärer Schutz und ein Wiederherstellungs-Protector zu einem Betriebssystemdatenträger hinzugefügt werden.

Bei der Verwendung von manage-bde empfiehlt es sich, den Lautstärke Status im Zielsystem zu ermitteln. Verwenden Sie den folgenden Befehl, um den Lautstärke Status zu ermitteln:

```
manage-bde -status
```

Dieser Befehl gibt die Volumes für das Ziel, den aktuellen Verschlüsselungsstatus, die Verschlüsselungsmethode und den Volume-Typ (Betriebssystem oder Daten) für die einzelnen Volumes zurück:

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.15063]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\windows\system32>manage-bde -status
BitLocker Drive Encryption: Configuration Tool version 10.0.15063
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

Disk volumes that can be protected with
BitLocker Drive Encryption:
Volume C: [OSDisk]
[OS Volume]

    Size:                 465.27 GB
    BitLocker Version:    2.0
    Conversion Status:    Fully Encrypted
    Percentage Encrypted: 100.0%
    Encryption Method:    XTS-AES 128
    Protection Status:    Protection On
    Lock Status:          Unlocked
    Identification Field: Unknown
    Key Protectors:
        Numerical Password
        TPM
```

Im folgenden Beispiel wird das Aktivieren von BitLocker auf einem Computer ohne TPM-Chip veranschaulicht. Bevor Sie den Verschlüsselungsprozess starten, müssen Sie den für BitLocker erforderlichen Startschlüssel erstellen und auf dem USB-Laufwerk speichern. Wenn BitLocker für das Betriebssystemvolume aktiviert ist, muss BitLocker auf das USB-Flashlaufwerk zugreifen, um den Verschlüsselungsschlüssel zu erhalten (in diesem Beispiel steht der Laufwerkbuchstabe E für das USB-Laufwerk). Sie werden aufgefordert, den Computer neu zu starten, um den Verschlüsselungsvorgang abzuschließen.

```
manage-bde –protectors -add C: -startupkey E:
manage-bde -on C:
```

> **Hinweis:** nachdem die Verschlüsselung abgeschlossen ist, muss der USB-Startschlüssel eingefügt werden, bevor das Betriebssystem gestartet werden kann.

Eine Alternative zum Startschlüssel Schutz auf nicht-TPM-Hardware ist die Verwendung eines Kennworts und eines **ADaccountorgroup** -Beschützers zum Schutz des Betriebssystemdatenträgers. In diesem Szenario fügen Sie zuerst die Beschützer hinzu. Dies erfolgt über den folgenden Befehl:

```
manage-bde -protectors -add C: -pw -sid <user or group>
```

Für diesen Befehl müssen Sie die Kennwortschutz Taste eingeben und dann bestätigen, bevor Sie Sie dem Volume hinzufügen. Wenn die Schutzvorrichtungen auf dem Volume aktiviert sind, können Sie BitLocker aktivieren.

Auf Computern mit einem TPM ist es möglich, das Betriebssystemvolume ohne definierte Schutzvorrichtungen mithilfe von manage-bde zu verschlüsseln. Der folgende Befehl lautet:

```
manage-bde -on C:
```

Dadurch wird das Laufwerk mit dem TPM als Standardschutz verschlüsselt. Wenn Sie nicht sicher sind, ob eine

TPM-Beschützer verfügbar ist, führen Sie den folgenden Befehl aus, um die für ein Volume verfügbaren Schutzvorrichtungen aufzulisten:

```
manage-bde -protectors -get <volume>
```

Verwenden von manage-bde mit Daten-Volumes

Daten-Volumes verwenden dieselbe Syntax für die Verschlüsselung als Betriebssystem-Volumes, erfordern aber keine Schutzvorrichtungen, damit der Vorgang abgeschlossen werden kann. Das Verschlüsseln von Daten-Volumes kann mithilfe des Befehls `manage-bde -on <drive letter>` Base erfolgen: oder Sie können zunächst zusätzliche Schutzvorrichtungen hinzufügen. Es wird empfohlen, dass mindestens ein primärer Schutz und ein Wiederherstellungs-Protector zu einem Datenvolumen hinzugefügt werden.

Eine allgemeine Schutzvorrichtung für ein Datenvolumen ist die Kennwortschutz-Komponente. Im folgenden Beispiel fügen wir dem Volume eine Kennwortschutzfunktion hinzu und aktivieren BitLocker.

```
manage-bde -protectors -add -pw C:
manage-bde -on C:
```

Reparieren-BDE

Möglicherweise wird ein Problem auftreten, das einen Bereich einer Festplatte schädigt, auf dem BitLocker wichtige Informationen speichert. Diese Art von Problem kann durch einen Festplattenfehler verursacht werden oder wenn Windows unerwartet beendet wird.

Das BitLocker-Reparatur Tool (Repair-BDE) kann verwendet werden, um auf verschlüsselte Daten auf einer schwer beschädigten Festplatte zuzugreifen, wenn das Laufwerk mithilfe von BitLocker verschlüsselt wurde. Repair-bde kann wichtige Teile des Laufwerks wiederherstellen und wiederherstellbare Daten retten, solange ein gültiges Wiederherstellungskennwort oder Wiederherstellungsschlüssel verwendet wird, um die Daten zu entschlüsseln. Wenn die BitLocker-metadatendaten auf dem Laufwerk beschädigt sind, müssen Sie zusätzlich zum Wiederherstellungskennwort oder Wiederherstellungsschlüssel ein Sicherungsschlüssel Paket bereitstellen können. Dieses Schlüsselpaket wird in den Active Directory-Domänendiensten (Adds) gesichert, wenn Sie die Standardeinstellung für Adds-Sicherung verwendet haben. Mit diesem Schlüsselpaket und entweder dem Wiederherstellungskennwort oder dem Wiederherstellungsschlüssel können Sie Teile eines durch BitLocker geschützten Laufwerks entschlüsseln, wenn der Datenträger beschädigt ist. Jedes Schlüsselpaket funktioniert nur für ein Laufwerk, das über die entsprechende laufwerkskennung verfügt. Sie können das BitLocker-Wiederherstellungskennwort-Viewer verwenden, um dieses Schlüsselpaket von Adds abzurufen.

> **Tipp:** Wenn Sie keine Wiederherstellungsinformationen hinzufügen oder wenn Sie Schlüsselpakete Alternativ speichern möchten, können Sie den Befehl `manage-bde -KeyPackage` verwenden, um ein Schlüsselpaket für ein Volume zu generieren.

Das Befehlszeilentool Repair-bde ist für die Verwendung vorgesehen, wenn das Betriebssystem nicht gestartet wird oder wenn Sie die BitLocker-Wiederherstellungskonsole nicht starten können. Sie sollten Repair-bde verwenden, wenn die folgenden Bedingungen zutreffen:

1. Sie haben das Laufwerk mithilfe der BitLocker-Laufwerkverschlüsselung verschlüsselt.
2. Windows wird nicht gestartet, oder Sie können die BitLocker-Wiederherstellungskonsole nicht starten.
3. Sie verfügen nicht über eine Kopie der Daten, die auf dem verschlüsselten Laufwerk enthalten sind.

> **Hinweis:** Schäden am Laufwerk sind möglicherweise nicht mit BitLocker verbunden. Daher empfiehlt es sich, andere Tools zu testen, um das Problem mit dem Laufwerk zu diagnostizieren und zu beheben, bevor Sie das BitLocker-Reparatur Tool verwenden. Die Windows-Wiederherstellungsumgebung (WindowsRE) bietet

> zusätzliche Optionen zum Reparieren von Computern.

Für Repair-bde sind die folgenden Einschränkungen vorhanden:

- Das Befehlszeilentool Repair-bde kann ein Laufwerk, das während des Verschlüsselungs-oder Entschlüsselungsvorgangs nicht funktioniert hat, nicht reparieren.
- Das Befehlszeilentool Repair-bde geht davon aus, dass das Laufwerk vollständig verschlüsselt wurde, wenn das Laufwerk eine Verschlüsselung aufweist.

Weitere Informationen zur Verwendung von Repair-bde finden Sie unter Repair-bde.

BitLocker-Cmdlets für Windows PowerShell

Windows PowerShell-Cmdlets bieten Administratoren eine neue Möglichkeit, wenn Sie mit BitLocker arbeiten. Mithilfe der Skriptfunktionen von Windows PowerShell können Administratoren BitLocker-Optionen problemlos in vorhandene Skripts integrieren. In der folgenden Liste werden die verfügbaren BitLocker-Cmdlets angezeigt.

Name	Parameter
Add-BitLockerKeyProtector	-ADAccountOrGroup -ADAccountOrGroupProtector -Bestätigen -MountPoint -Kennwort -PasswordProtector -PIN -RecoveryKeyPath -RecoveryKeyProtector -RecoveryPassword) angegeben -RecoveryPasswordProtector -Service -StartupKeyPath -StartupKeyProtector -TpmAndPinAndStartupKeyProtector -TpmAndPinProtector -TpmAndStartupKeyProtector -TpmProtector -WhatIf
Backup-BitLockerKeyProtector	-Bestätigen -Keyprotector-Nr. -MountPoint -WhatIf

Deaktivieren-BitLocker	-Bestätigen -MountPoint -WhatIf
Deaktivieren-BitLockerAutoUnlock	-Bestätigen -MountPoint -WhatIf
Enable-BitLocker	-AdAccountOrGroup -AdAccountOrGroupProtector -Bestätigen -EncryptionMethod -HardwareEncryption -Kennwort -PasswordProtector -PIN -RecoveryKeyPath -RecoveryKeyProtector -RecoveryPassword) angegeben -RecoveryPasswordProtector -Service -SkipHardwareTest -StartupKeyPath -StartupKeyProtector -TpmAndPinAndStartupKeyProtector -TpmAndPinProtector -TpmAndStartupKeyProtector -TpmProtector -UsedSpaceOnly -WhatIf
Enable-BitLockerAutoUnlock	-Bestätigen -MountPoint -WhatIf
Get-BitLockerVolume	-MountPoint

Sperren – BitLocker	-Bestätigen -ForceDismount -MountPoint -WhatIf
Remove-BitLockerKeyProtector	-Bestätigen -Keyprotector-Nr. -MountPoint -WhatIf
Fortsetzen – BitLocker	-Bestätigen -MountPoint -WhatIf
Anhalten – BitLocker	-Bestätigen -MountPoint -RebootCount -WhatIf
Entsperren – BitLocker	-AdAccountOrGroup -Bestätigen -MountPoint -Kennwort -RecoveryKeyPath -RecoveryPassword) angegeben -RecoveryPassword) angegeben -WhatIf

Ähnlich wie manage-bde ermöglichen die Windows PowerShell-Cmdlets die Konfiguration über die in der Systemsteuerung angebotenen Optionen hinaus. Wie bei manage-bde müssen die Benutzer die spezifischen Anforderungen des Volumes, das Sie verschlüsseln, vor der Ausführung von Windows PowerShell-Cmdlets in Frage stellen. Ein guter erster Schritt besteht darin, den aktuellen Zustand der Volumes auf dem Computer zu ermitteln. Sie können dies mit dem `Get-BitLockerVolume` Cmdlet tun. Die `Get-BitLockerVolume` Ausgabe des Cmdlets gibt Informationen zu den Datenträgertypen,-Beschützern, zum Schutzstatus und zu anderen Details.

> **Tipp:** gelegentlich werden alle Protektoren möglicherweise nicht angezeigt, `Get-BitLockerVolume` Wenn Sie aufgrund von Platzmangel in der Ausgabe Anzeige verwendet werden. Wenn nicht alle Schutzvorrichtungen für ein Volume angezeigt werden, können Sie den Windows PowerShell-Pipe-Befehl (|) verwenden, um eine vollständige Liste der Beschützer zu formatieren. `Get-BitLockerVolume C: | fl`

Wenn Sie die vorhandenen Schutzvorrichtungen entfernen möchten, bevor BitLocker auf dem Datenträger bereitgestellt wird, können Sie `Remove-BitLockerKeyProtector` das Cmdlet verwenden. Hierzu muss die GUID, die dem Protector zugeordnet ist, entfernt werden.

Mit einem einfachen Skript können die Werte jedes Get-BitLockerVolume-Steuerzeichens an eine andere Variable weitergegeben werden, wie unten zu sehen ist:

```
$vol = Get-BitLockerVolume
$keyprotectors = $vol.KeyProtector
```

Mithilfe dieser Informationen können Sie die Informationen in der $keyprotectors-Variable anzeigen, um die GUID für jeden Protector zu ermitteln.

Mithilfe dieser Informationen können Sie die Schlüssel Beschützer für ein bestimmtes Volume mithilfe des Befehls entfernen:

```
Remove-BitLockerKeyProtector <volume>: -KeyProtectorID "{GUID}"
```

> **Hinweis:** das BitLocker-Cmdlet setzt voraus, dass die Schlüssel-Beschützer-GUID in Anführungszeichen eingeschlossen ist. Stellen Sie sicher, dass die gesamte GUID mit geschweiften Klammern in den Befehl eingeschlossen ist.

Verwenden der BitLocker Windows PowerShell-Cmdlets mit Betriebssystemdatenträgern

Die Verwendung der BitLocker-Cmdlets für Windows PowerShell ähnelt dem Arbeiten mit dem Manage-BDE-Tool zum Verschlüsseln von Betriebssystem-Volumes. Windows PowerShell bietet Benutzern viel Flexibilität. Beispielsweise können Benutzer den gewünschten Protector als Teilbefehl zum Verschlüsseln des Volumes hinzufügen. Nachfolgend finden Sie Beispiele für häufige Benutzerszenarien und Schritte, um Sie in BitLocker Windows PowerShell zu erreichen.

Im folgenden Beispiel wird gezeigt, wie Sie BitLocker auf einem Betriebssystemlaufwerk nur mit dem TPM-Schutz aktivieren:

```
Enable-BitLocker C:
```

Im folgenden Beispiel wird ein zusätzlicher Protector, der StartupKey-Protector, hinzugefügt, und es wird der BitLocker-Hardware Test übersprungen. In diesem Beispiel wird die Verschlüsselung sofort gestartet, ohne dass ein Neustart erforderlich ist.

```
Enable-BitLocker C: -StartupKeyProtector -StartupKeyPath <path> -SkipHardwareTest
```

Verwenden der BitLocker Windows PowerShell-Cmdlets mit Datenvolumen

Die Datenvolume-Verschlüsselung mit Windows PowerShell entspricht den für Betriebssystemdatenträger. Bevor Sie die Lautstärke verschlüsseln, sollten Sie die gewünschten Schutzvorrichtungen hinzufügen. Im folgenden Beispiel wird dem E:-Volume eine Kennwortschutz Komponente mithilfe der Variablen $PW als Kennwort hinzugefügt. Die $PW-Variable wird als SecureString-Wert gespeichert, um das benutzerdefinierte Kennwort zu speichern.

```
$pw = Read-Host -AsSecureString
<user inputs password>
Enable-BitLockerKeyProtector E: -PasswordProtector -Password $pw
```

Verwenden eines anzeigen Kontos oder Gruppen Beschützers in Windows PowerShell

Der in Windows 8 und Windows Server 2012 eingeführte **ADAccountOrGroup** -Protector ist ein sid-basierter Active Directory-Schutz. Dieser Schutz kann sowohl auf Betriebssystem-als auch auf Daten-Volumes hinzugefügt

werden, obwohl er die Betriebssystem-Volumes in der Pre-Boot-Umgebung nicht entsperrt. Für den Protector muss die sid für das Domänenkonto oder die Gruppe mit dem Protector verknüpft werden. BitLocker kann einen clusterfähigen Datenträger schützen, indem ein sid-basierter Schutz für das Cluster Name Object (CNO) hinzugefügt wird, mit dem der Datenträger ordnungsgemäß Failover und von einem beliebigen Mitgliedscomputer des Clusters freigegeben werden kann.

> **Warnung:** der **ADAccountOrGroup** -Schutz erfordert die Verwendung eines zusätzlichen Beschützers für die Verwendung (wie TPM, PIN oder Wiederherstellungsschlüssel) bei Verwendung auf Betriebssystem-Volumes.

Zum Hinzufügen eines **ADAccountOrGroup** -Beschützers zu einem Volume müssen entweder die tatsächliche Domänen-SID oder der Gruppenname, dem die Domäne vorangestellt ist, und ein umgekehrter Schrägstrich eingegeben werden. Im folgenden Beispiel wird das CONTOSO\Administrator-Konto als Protector zum Datenvolumen G hinzugefügt.

```
Enable-BitLocker G: -AdAccountOrGroupProtector -AdAccountOrGroup CONTOSO\Administrator
```

Für Benutzer, die die sid für das Konto oder die Gruppe verwenden möchten, besteht der erste Schritt darin, die dem Konto zugeordnete sid zu ermitteln. Um die spezifische sid für ein Benutzerkonto in Windows PowerShell abzurufen, verwenden Sie den folgenden Befehl:

> **Hinweis:** die Verwendung dieses Befehls erfordert das Feature Remote Remote-AD-PowerShell.

```
get-aduser -filter {samaccountname -eq "administrator"}
```

> **Tipp:** zusätzlich zum oben angegebenen PowerShell-Befehl können Informationen zu den lokal angemeldeten Benutzern und Gruppenmitgliedschaften mithilfe von: WHOAMI/all. gefunden werden. Dies erfordert keine Verwendung zusätzlicher Funktionen.

Im folgenden Beispiel wird dem zuvor verschlüsselten Betriebssystemvolume mithilfe der SID des Kontos ein **ADAccountOrGroup** -Protector hinzugefügt:

```
Add-BitLockerKeyProtector C: -ADAccountOrGroupProtector -ADAccountOrGroup S-1-5-21-3651336348-8937238915-
291003330-500
```

> **Hinweis:** Active Directory-basierte Schutzfunktionen werden normalerweise zum Entsperren von Failover-Cluster fähigen Volumes verwendet.

Weitere Informationen

- Übersicht über BitLocker
- Häufig gestellte Fragen (Frequently Asked Questions, FAQ) zu BitLocker
- Vorbereiten Ihrer Organisation auf BitLocker: Planung und Richtlinien
- BitLocker: Aktivieren der Netzwerkentsperrung
- BitLocker: Bereitstellen auf Windows Server 2012

BitLocker: Verwenden des BitLocker-Wiederherstellungskennwort-Viewers

27.10.2019 • 2 minutes to read

Betrifft

- Windows 10

In diesem Thema für IT-Experten wird beschrieben, wie der BitLocker-Wiederherstellungskennwort-Viewer verwendet wird.

Das BitLocker-Wiederherstellungskennwort-Viewer-Tool ist ein optionales Tool, das im Lieferumfang der Remote Server-Verwaltungs Tools enthalten ist. Damit können Sie BitLocker-Wiederherstellungskennwörter suchen und anzeigen, die in Active Directory-Domänendiensten (AD DS) gespeichert sind. Sie können mit diesem Tool Daten wiederherstellen, die auf einem Laufwerk gespeichert sind, das mit BitLocker verschlüsselt wurde. Das BitLocker-Tool für die Active Directory-Wiederherstellungskennwort-Anzeige ist eine Erweiterung für das MMC-Snap-in "Active Directory-Benutzer und-Computer". Mit diesem Tool können Sie das Dialogfeld **Eigenschaften** eines Computerobjekts überprüfen, um die entsprechenden BitLocker-Wiederherstellungskennwörter anzuzeigen. Darüber hinaus können Sie mit der rechten Maustaste auf einen Domänencontainer klicken und dann über alle Domänen in der Active Directory-Gesamtstruktur hinweg nach einem BitLocker-Wiederherstellungskennwort suchen. Sie können auch nach einem Kennwort anhand der Kenn Wort Kennung (ID) suchen.

Vorbereitung

So führen Sie die Verfahren in diesem Szenario aus:

- Sie müssen über die Anmeldeinformationen des Domänenadministrators verfügen.
- Ihre Testcomputer müssen der Domäne beigetreten sein.
- Auf den Testcomputern muss BitLocker aktiviert sein, nachdem Sie der Domäne beigetreten sind.

Die folgenden Verfahren beschreiben die am häufigsten ausgeführten Aufgaben mit dem BitLocker-Wiederherstellungskennwort-Viewer.

So zeigen Sie die Wiederherstellungskennwörter für einen Computer an

1. Suchen Sie in **Active Directory-Benutzer und-Computer**nach dem Container, in dem sich der Computer befindet, und klicken Sie darauf.
2. Klicken Sie mit der rechten Maustaste auf das Computerobjekt, und klicken Sie dann auf **Eigenschaften**.
3. Klicken Sie im Dialogfeld **Eigenschaften** auf die Registerkarte **BitLocker-Wiederherstellung** , um die BitLocker-Wiederherstellungskennwörter anzuzeigen, die dem Computer zugeordnet sind.

So kopieren Sie die Wiederherstellungskennwörter für einen Computer

1. Führen Sie die Schritte im vorherigen Verfahren aus, um die BitLocker-Wiederherstellungskennwörter anzuzeigen.
2. Klicken Sie im Dialogfeld **Eigenschaften** auf der Registerkarte **BitLocker-Wiederherstellung** mit der rechten Maustaste auf das BitLocker-Wiederherstellungskennwort, das Sie kopieren möchten, und klicken Sie dann auf **Details kopieren**.
3. Drücken Sie STRG + V, um den kopierten Text an einen Zielspeicherort, beispielsweise eine Textdatei oder eine Kalkulationstabelle, einzufügen.

So suchen Sie ein Wiederherstellungskennwort mithilfe einer Kenn Wort Kennung

1. Klicken Sie in Active Directory-Benutzer und-Computer mit der rechten Maustaste auf den Domänencontainer, und klicken Sie dann auf **BitLocker-Wiederherstellungskennwort suchen**.
2. Geben Sie im Dialogfeld **BitLocker-Wiederherstellungskennwort suchen** die ersten acht Zeichen des Wiederherstellungskennworts in das Feld **Kenn Wort Kennung (erste 8 Zeichen)** ein, und klicken Sie dann auf **Suchen**. Indem Sie die Verfahren in diesem Szenario durchführen, haben Sie die Wiederherstellungskennwörter für einen Computer angezeigt und kopiert und eine Kennwort-ID verwendet, um ein Wiederherstellungskennwort zu finden.

Weitere Informationen

- Übersicht über BitLocker
- Häufig gestellte Fragen (Frequently Asked Questions, FAQ) zu BitLocker
- Vorbereiten Ihrer Organisation auf BitLocker: Planung und Richtlinien
- BitLocker: Bereitstellen auf Windows Server 2012
- BitLocker: Verwenden von BitLocker-Laufwerksverschlüsselungstools zum Verwalten von BitLocker

BitLocker-Gruppenrichtlinieneinstellungen

06.03.2020 • 73 minutes to read

Betriff:

- Windows 10

In diesem Thema für IT-Experten werden die Funktion, der Standort und der Effekt der einzelnen Gruppenrichtlinieneinstellungen beschrieben, die zum Verwalten der BitLocker-Laufwerkverschlüsselung verwendet werden.

Um zu steuern, welche Laufwerk Verschlüsselungsaufgaben der Benutzer in der Windows-Systemsteuerung ausführen kann, oder um andere Konfigurationsoptionen zu ändern, können Sie Gruppenrichtlinien-administrative Vorlagen oder Richtlinieneinstellungen für lokale Computer verwenden. Wie Sie diese Richtlinieneinstellungen konfigurieren, hängt davon ab, wie Sie BitLocker implementieren und welche Ebene von Benutzerinteraktionen zulässig ist.

> **Hinweis:** Ein separater Satz von Gruppenrichtlinieneinstellungen unterstützt die Verwendung des Trusted Platform Module (TPM). Ausführliche Informationen zu diesen Einstellungen finden Sie unter Gruppenrichtlinieneinstellungen für vertrauenswürdige Platt Form Module.

Auf die BitLocker-Gruppenrichtlinieneinstellungen kann über den lokalen Gruppenrichtlinien-Editor und die Gruppenrichtlinien-Verwaltungskonsole (Group Policy Management Console, GPMC) unter **Computer Configuration\Administrative Templates\Windows Components\BitLocker Drive Encryption**zugegriffen werden. Die meisten BitLocker-Gruppenrichtlinieneinstellungen werden angewendet, wenn BitLocker zunächst für ein Laufwerk aktiviert ist. Wenn ein Computer nicht mit vorhandenen Gruppenrichtlinieneinstellungen kompatibel ist, ist BitLocker möglicherweise erst aktiviert oder geändert, wenn sich der Computer in einem kompatiblen Zustand befindet. Wenn ein Laufwerk nicht mit den Gruppenrichtlinieneinstellungen übereinstimmt (Wenn beispielsweise eine Gruppenrichtlinieneinstellung nach der anfänglichen BitLocker-Bereitstellung in Ihrer Organisation geändert wurde und die Einstellung auf zuvor verschlüsselte Laufwerke angewendet wurde), kann keine Änderung an der BitLocker-Konfiguration dieses Laufwerks mit Ausnahme einer Änderung, die Sie in die Compliance einführt.

Wenn mehrere Änderungen erforderlich sind, um die Kompatibilität des Laufwerks zu gewährleisten, müssen Sie den BitLocker-Schutz sperren, die erforderlichen Änderungen vornehmen und dann den Schutz fortsetzen. Diese Situation kann beispielsweise auftreten, wenn ein Wechseldatenträger ursprünglich für die Entsperrung mit einem Kennwort konfiguriert wurde und dann die Gruppenrichtlinieneinstellungen geändert werden, um Kennwörter zu unterbinden und Smartcards zu erfordern. In diesem Fall müssen Sie den BitLocker-Schutz unterbrechen, indem Sie das Befehlszeilentool manage-bde verwenden, die Methode zum Entsperren des Kennworts löschen und die Smartcard-Methode hinzufügen. Nachdem dies abgeschlossen ist, ist BitLocker mit der Gruppenrichtlinieneinstellung kompatibel, und der BitLocker-Schutz auf dem Laufwerk kann fortgesetzt werden.

BitLocker-Gruppenrichtlinieneinstellungen

Die folgenden Abschnitte enthalten eine umfassende Liste der BitLocker-Gruppenrichtlinieneinstellungen, die nach Verwendung organisiert sind. Zu den BitLocker-Gruppenrichtlinieneinstellungen gehören Einstellungen für bestimmte Laufwerktypen (Betriebssystemlaufwerke, fest Netzlaufwerke und Wechseldatenträger) sowie Einstellungen, die auf alle Laufwerke angewendet werden.

Die folgenden Richtlinieneinstellungen können verwendet werden, um zu ermitteln, wie ein mit BitLocker

geschütztes Laufwerk entsperrt werden kann.

- Zulassen, dass Geräte mit sicheren Start-und geschützten DMA-Anschlüssen den Preboot-PIN deaktivieren
- Netzwerksperre beim Start zulassen
- Zusätzliche Authentifizierung beim Start erforderlich
- Erweiterte Pins für den Start zulassen
- Konfigurieren der Mindest-PIN-Länge für den Start
- Neue DMA-Geräte deaktivieren, wenn dieser Computer gesperrt ist
- Verhindern, dass Standardbenutzer die PIN oder das Kennwort ändern
- Konfigurieren der Verwendung von Kennwörtern für Betriebssystemlaufwerke
- Anfordern zusätzlicher Authentifizierung beim Start (Windows Server 2008 und Windows Vista)
- Konfigurieren der Verwendung von Smartcards auf festen Datenlaufwerken
- Konfigurieren der Verwendung von Kennwörtern auf festen Datenlaufwerken
- Konfigurieren der Verwendung von Smartcards auf wechselbaren Datenlaufwerken
- Konfigurieren der Verwendung von Kennwörtern auf austauschbaren Datenlaufwerken
- Überprüfen der Kompatibilität von Smartcard-Zertifikat Nutzungsregeln
- Aktivieren der Verwendung der BitLocker-Authentifizierung, die eine Vorstart Tastatureingabe auf Schiefer erfordert

Die folgenden Richtlinieneinstellungen werden verwendet, um zu steuern, wie Benutzer auf Laufwerke zugreifen können und wie Sie BitLocker auf ihren Computern verwenden können.

- Schreibzugriff auf Festplattenlaufwerke verweigern, die nicht durch BitLocker geschützt sind
- Schreibzugriff auf Wechseldatenträger verweigern, die nicht durch BitLocker geschützt sind
- Steuern der Verwendung von BitLocker auf Wechseldatenträgern

Die folgenden Richtlinieneinstellungen legen die für BitLocker verwendeten Verschlüsselungsmethoden und Verschlüsselungstypen fest.

- Wählen Sie Laufwerk Verschlüsselungsmethode und Verschlüsselungsstärke aus.
- Konfigurieren der Verwendung von hardwarebasierter Verschlüsselung für fest Netzlaufwerke
- Konfigurieren der Verwendung von hardwarebasierter Verschlüsselung für Betriebssystemlaufwerke
- Konfigurieren der Verwendung von hardwarebasierter Verschlüsselung für Wechseldaten Laufwerke
- Erzwingen des Laufwerk Verschlüsselungstyps auf festen Datenlaufwerken
- Erzwingen des Laufwerk Verschlüsselungstyps auf Betriebssystemlaufwerken
- Erzwingen des Laufwerk Verschlüsselungstyps auf Wechseldatenträgern

Die folgenden Richtlinieneinstellungen definieren die Wiederherstellungsmethoden, die zum Wiederherstellen des Zugriffs auf ein mit BitLocker geschütztes Laufwerk verwendet werden können, wenn eine Authentifizierungsmethode fehlschlägt oder nicht verwendet werden kann.

- Auswählen, wie BitLocker-geschützte Betriebssystemlaufwerke wiederhergestellt werden können
- Auswählen, wie Benutzer BitLocker-geschützte Laufwerke wiederherstellen können (Windows Server 2008 und Windows Vista)
- Speichern von BitLocker-Wiederherstellungsinformationen in den Active Directory-Domänendiensten (Windows Server 2008 und Windows Vista)
- Standardordner für Wiederherstellungskennwort auswählen
- Auswählen, wie BitLocker-geschützte Festplatten wiederhergestellt werden können
- Auswählen, wie BitLocker-geschützte Wechsellaufwerke wiederhergestellt werden können
- Konfigurieren der Nachricht und der URL für die Pre-Boot-Wiederherstellung

Die folgenden Richtlinien werden verwendet, um benutzerdefinierte Bereitstellungsszenarien in Ihrer

Organisation zu unterstützen.

- Sicheren Start für Integritätsüberprüfung zulassen
- Bereitstellen der eindeutigen Bezeichner für Ihre Organisation
- Verhindern, dass beim Neustart Speicher überschrieben wird
- Konfigurieren des TPM-Platt Form Überprüfungsprofils für BIOS-basierte Firmware-Konfigurationen
- Konfigurieren des TPM-Platt Form Überprüfungsprofils (Windows Vista, Windows Server 2008, Windows 7, Windows Server 2008 R2)
- Konfigurieren des TPM-Platt Form Prüfungs Profils für systemeigene UEFI-Firmware-Konfigurationen
- Zurücksetzen von Platt Form Überprüfungsdaten nach BitLocker-Wiederherstellung
- Verwenden des erweiterten Startkonfigurationsdaten Überprüfungsprofils
- Gewähren des Zugriffs auf von BitLocker geschützte fest Netzlaufwerke aus früheren Versionen von Windows
- Gewähren des Zugriffs auf von BitLocker geschützte Wechseldaten Laufwerke aus früheren Versionen von Windows

Zulassen, dass Geräte mit sicheren Start-und geschützten DMA-Anschlüssen den Preboot-PIN deaktivieren

Diese Richtlinieneinstellung ermöglicht Benutzern auf Geräten, die mit dem modernen Standby-Modus kompatibel sind, oder mit der Microsoft-Hardware Sicherheits Test-Schnittstelle (HSTI) keine PIN für die Preboot-Authentifizierung.

Richtlinienbeschreibung	Mit dieser Richtlinieneinstellung können Sie einen nur-TPM-Schutz für neuere, sicherere Geräte zulassen, beispielsweise für Geräte, die modernen Standby-oder HSTI unterstützen, während eine PIN auf älteren Geräten erforderlich ist.
Eingeführt	Windows10, Version1703
Laufwerktyp	Betriebssystemlaufwerke
Richtlinienpfad	Computer Configuration\Administrative Vorlagen\Windows-Komponenten\Internet BitLocker-Laufwerkverschlüsselung Drive Encryption\Operating System Laufwerke
Konflikte	Diese Einstellung setzt die **Option Start-PIN mit** TPM erfordern für die Richtlinie erfordern zusätzlicher Authentifizierung beim Start auf kompatible Hardware außer Kraft.
Wenn aktiviert	Benutzer auf modernen Standby-und HSTI-kompatiblen Geräten können BitLocker ohne Preboot-Authentifizierung aktivieren.
Wenn deaktiviert oder nicht konfiguriert	Es gelten die Optionen für die Richtlinie erfordern zusätzlicher Authentifizierung beim Start.

Referenz

Die Option für die Voreinstellungs **Authentifizierung erfordert die** Start-PIN mit TPM der Richtlinie erfordern zusätzlicher Authentifizierung beim Start ist häufig aktiviert, um die Sicherheit älterer Geräte zu gewährleisten, die den modernen Standbymodus nicht unterstützen. Sehbehinderte Benutzer haben jedoch keine hörbare Möglichkeit, zu wissen, wann eine PIN eingegeben werden muss. Diese Einstellung ermöglicht eine Ausnahme von der PIN-erforderlichen Richtlinie für sichere Hardware.

Netzwerksperre beim Start zulassen

Diese Richtlinie steuert einen Teil des Verhaltens des Features Netzwerksperrung in BitLocker. Diese Richtlinie ist erforderlich, um die BitLocker-Netzwerksperrung in einem Netzwerk zu aktivieren, da Clients, die BitLocker ausführen, die erforderliche Netzwerkschlüssel Schutzfunktion während der Verschlüsselung erstellen können. Diese Richtlinie wird zusätzlich zur BitLocker-Laufwerk Verschlüsselungs Netzwerk Sperrungs Zertifikat-Sicherheitsrichtlinie (im Ordner " **Richtlinien für öffentliche Schlüssel** " der Richtlinie für lokale Computer) verwendet, damit Systeme, die mit einem vertrauenswürdigen Netzwerk verbunden sind, das Feature für die Netzwerksperrung ordnungsgemäß verwenden können.

Richtlinienbeschreibung	Mit dieser Richtlinieneinstellung können Sie steuern, ob ein mit BitLocker geschützter Computer, der mit einem vertrauenswürdigen lokalen Netzwerk verbunden ist und zu einer Domäne gehört, Netzwerkschlüssel Schutz auf Computern mit TPM erstellen und verwenden kann, um das Betriebssystem automatisch aufzuheben. Laufwerk, wenn der Computer gestartet wird.
Eingeführt	Windows Server 2012 und Windows 8
Laufwerktyp	Betriebssystemlaufwerke
Richtlinienpfad	Computer Configuration\Administrative Vorlagen\Windows-Komponenten\Internet BitLocker-Laufwerkverschlüsselung Drive Encryption\Operating System Laufwerke
Konflikte	Keine
Wenn aktiviert	Clients, die mit einem BitLocker-Netzwerksperre-Zertifikat konfiguriert sind, können Netzwerkschlüssel-Schutzvorrichtungen erstellen und verwenden.
Wenn deaktiviert oder nicht konfiguriert	Clients können keine Netzwerkschlüssel-Schutzvorrichtungen erstellen und verwenden

Referenz

Wenn Sie zum Entsperren des Computers eine Netzwerkschlüssel Schutzkomponente verwenden möchten, müssen der Computer und der Server, auf dem die BitLocker-Laufwerk Verschlüsselungs Netzwerksperre gehostet wird, mit einem Netzwerksperre-Zertifikat bereitgestellt werden. Das Netzwerk Sperrungs Zertifikat wird verwendet, um einen Netzwerkschlüssel Schutz zu erstellen und den Informationsaustausch mit dem Server zu schützen, um den Computer zu entsperren. Sie können das Zertifikat für die Gruppenrichtlinieneinstellung **Computer Configuration\Windows Settings\Security Settings\Public Schlüssel Policies\BitLocker Laufwerk Verschlüsselungs Netzwerk entsperren** auf dem Domänencontroller verwenden, um dieses Zertifikat an Computer in Ihrer Organisation zu verteilen. Diese

Unlock-Methode verwendet das TPM auf dem Computer, sodass Computer, die kein TPM besitzen, keine Netzwerkschlüssel Schutzfunktionen erstellen können, um mithilfe der Netzwerksperrung automatisch zu entsperren.

> **Hinweis:** Für Zuverlässigkeit und Sicherheit sollten Computer auch über eine TPM-Start-PIN verfügen, die verwendet werden kann, wenn der Computer vom kabelgebundenen Netzwerk getrennt wird oder beim Start keine Verbindung mit dem Domänencontroller hergestellt wird.

Weitere Informationen zur Netzwerksperrung finden Sie unter BitLocker: Aktivieren der Netzwerksperrung.

Zusätzliche Authentifizierung beim Start erforderlich

Mithilfe dieser Richtlinieneinstellung wird gesteuert, welche Unlock-Optionen für Betriebssystemlaufwerke verfügbar sind.

Richtlinienbeschreibung	Mit dieser Richtlinieneinstellung können Sie konfigurieren, ob BitLocker bei jedem Start des Computers eine zusätzliche Authentifizierung erfordert und ob Sie BitLocker mit einem Trusted Platform Module (TPM) verwenden. Diese Richtlinieneinstellung wird angewendet, wenn Sie BitLocker aktivieren.
Eingeführt	Windows Server 2008 R2 und Windows 7
Laufwerktyp	Betriebssystemlaufwerke
Richtlinienpfad	Computer Configuration\Administrative Vorlagen\Windows-Komponenten\Internet BitLocker-Laufwerkverschlüsselung Drive Encryption\Operating System Laufwerke
Konflikte	Wenn eine Authentifizierungsmethode erforderlich ist, können die anderen Methoden nicht zugelassen werden. Die Verwendung von BitLocker mit einem TPM-Startschlüssel oder einem TPM-Startschlüssel und einer PIN muss nicht zulässig sein, **wenn die Einstellung Schreibzugriff auf Wechsellaufwerke, die nicht** durch BitLocker geschützt sind, aktiviert ist.
Wenn aktiviert	Benutzer können Erweiterte Startoptionen im BitLocker-Setup-Assistenten konfigurieren.
Wenn deaktiviert oder nicht konfiguriert	Benutzer können nur grundlegende Optionen auf Computern mit einem TPM konfigurieren. Beim Start kann nur eine der zusätzlichen Authentifizierungsoptionen erforderlich sein. Andernfalls tritt ein Richtlinienfehler auf.

Referenz

Wenn Sie BitLocker auf einem Computer ohne TPM verwenden möchten, wählen Sie **BitLocker ohne kompatibles TPM zulassen**aus. In diesem Modus ist für den Start ein Kennwort oder ein USB-Laufwerk

erforderlich. Das USB-Laufwerk speichert den Startschlüssel, der zum Verschlüsseln des Laufwerks verwendet wird. Wenn das USB-Laufwerk eingefügt wird, wird der Startschlüssel authentifiziert, und auf das Betriebssystemlaufwerk kann zugegriffen werden. Wenn das USB-Laufwerk verloren geht oder nicht verfügbar ist, ist die BitLocker-Wiederherstellung für den Zugriff auf das Laufwerk erforderlich.

Auf einem Computer mit einem kompatiblen TPM können beim Starten zusätzliche Authentifizierungsmethoden verwendet werden, um den Schutz für verschlüsselte Daten zu verbessern. Wenn der Computer gestartet wird, kann er Folgendes verwenden:

- nur das TPM
- Einfügen eines USB-Flashlaufwerks mit dem Startschlüssel
- die Eingabe einer 4-stelligen bis 20-stelligen Personal Identification Number (PIN)
- eine Kombination aus PIN und USB-Speicherstick

Es gibt vier Optionen für TPM-fähige Computer oder Geräte:

- Konfigurieren des TPM-Starts
  - TPM zulassen
  - TPM anfordern
  - TPM nicht zulassen
- Konfigurieren der TPM-Start-PIN
  - Start-PIN mit TPM zulassen
  - Start-PIN mit TPM erforderlich
  - Start-PIN mit TPM nicht zulassen
- Konfigurieren des TPM-Startschlüssels
  - Autostart-Schlüssel mit TPM zulassen
  - Starten des Schlüssels mit TPM erforderlich
  - Startschlüssel nicht mit TPM zulassen
- Konfigurieren des TPM-Startschlüssels und der PIN
  - TPM-Startschlüssel mit PIN zulassen
  - Starten des Schlüssels und anheften mit TPM erforderlich
  - TPM-Startschlüssel mit PIN nicht zulassen

Erweiterte Pins für den Start zulassen

Diese Richtlinieneinstellung ermöglicht die Verwendung von erweiterten Pins, wenn Sie eine Unlock-Methode verwenden, die eine PIN enthält.

Richtlinienbeschreibung	Mit dieser Richtlinieneinstellung können Sie konfigurieren, ob erweiterte Start Pins für BitLocker verwendet werden.
Eingeführt	Windows Server 2008 R2 und Windows 7
Laufwerktyp	Betriebssystemlaufwerke

Richtlinienpfad	Computer Configuration\Administrative Vorlagen\Windows-Komponenten\Internet BitLocker-Laufwerkverschlüsselung Drive Encryption\Operating System Laufwerke
Konflikte	Keine
Wenn aktiviert	Alle neuen BitLocker-Start Pins, die festzulegen sind, sind erweiterte Pins. Vorhandene Laufwerke, die mit Standard Start Pins geschützt wurden, sind davon nicht betroffen.
Wenn deaktiviert oder nicht konfiguriert	Erweiterte Pins werden nicht verwendet.

Referenz

Erweiterte Start Pins ermöglichen die Verwendung von Zeichen (einschließlich Groß-und Kleinbuchstaben, Symbolen, Zahlen und Leerzeichen). Diese Richtlinieneinstellung wird angewendet, wenn Sie BitLocker aktivieren.

> **Wichtig:** Nicht alle Computer unterstützen erweiterte Pin-Zeichen in der Preboot-Umgebung. Es wird dringend empfohlen, dass Benutzer während des BitLocker-Setups eine Systemüberprüfung durchführen, um zu überprüfen, ob erweiterte Pin-Zeichen verwendet werden können.

Konfigurieren der Mindest-PIN-Länge für den Start

Diese Richtlinieneinstellung wird verwendet, um eine minimale PIN-Länge festzulegen, wenn Sie eine Unlock-Methode verwenden, die eine PIN enthält.

Richtlinienbeschreibung	Mit dieser Richtlinieneinstellung können Sie eine Mindestlänge für eine TPM-Start-Pin konfigurieren. Diese Richtlinieneinstellung wird angewendet, wenn Sie BitLocker aktivieren. Die Start-PIN muss eine Mindestlänge von 4 Ziffern aufweisen, und Sie kann eine maximale Länge von 20 Ziffern aufweisen. Standardmäßig ist die minimale PIN-Länge 6.
Eingeführt	Windows Server 2008 R2 und Windows 7
Laufwerktyp	Betriebssystemlaufwerke
Richtlinienpfad	Computer Configuration\Administrative Vorlagen\Windows-Komponenten\Internet BitLocker-Laufwerkverschlüsselung Drive Encryption\Operating System Laufwerke
Konflikte	Keine

Wenn aktiviert	Sie können festlegen, dass von Benutzern festgelegte Start Pins eine Mindestlänge von 4 bis 20 Stellen aufweisen müssen.
Wenn deaktiviert oder nicht konfiguriert	Benutzer können eine Start-PIN mit einer beliebigen Länge zwischen 6 und 20 Ziffern konfigurieren.

Referenz

Diese Richtlinieneinstellung wird angewendet, wenn Sie BitLocker aktivieren. Die Start-PIN muss eine Mindestlänge von 4 Ziffern aufweisen und eine maximale Länge von 20 Ziffern aufweisen.

Ursprünglich war BitLocker für eine PIN von 4 bis 20 Zeichen zulässig. Windows Hello hat eine eigene PIN für die Anmeldung, die 4 bis 127 Zeichen umfassen kann. Sowohl BitLocker als auch Windows Hello verwenden das TPM, um Angriffe durch Brute-Force-Angriffe zu verhindern.

Das TPM kann so konfiguriert werden, dass Wörterbuchangriffs Verhütungs Parameter (Sperrschwelle und Sperrdauer) verwendet werden, um zu steuern, wie viele fehlerhafte Autorisierungsversuche zulässig sind, bevor das TPM gesperrt wird, und wie viel Zeit verstreichen muss, bevor ein weiterer Versuch ausgeführt werden kann.

Die Parameter für die Verhinderung von Wörterbuchangriffen bieten eine Möglichkeit, Sicherheitsanforderungen mit Usability auszugleichen. Wenn BitLocker beispielsweise mit einer TPM + PIN-Konfiguration verwendet wird, ist die Anzahl der PIN-Vermutungen im Laufe der zeitlimitiert. Ein TPM-2,0 in diesem Beispiel kann so konfiguriert werden, dass nur 32-Pin-Vermutungen sofort zulässig sind, und dann nur noch eine Vermutung alle zwei Stunden. Dies summiert sich auf maximal ungefähr 4415 Vermutungen pro Jahr. Wenn die Pin 4 Ziffern umfasst, können alle 9999 möglichen Pin-Kombinationen in etwas mehr als zwei Jahren versucht werden.

Das Erhöhen der PIN-Länge erfordert eine größere Anzahl von Vermutungen für einen Angreifer. In diesem Fall kann die Sperrdauer zwischen den einzelnen Vermutungen verkürzt werden, damit legitime Benutzer einen fehlgeschlagenen Versuch schneller wiederholen können, während gleichzeitig ein ähnliches Schutzniveau beibehalten wird.

Ab Windows 10, Version 1703, wurde die Mindestlänge für die BitLocker-PIN auf 6 Zeichen erhöht, um besser mit anderen Windows-Features auszurichten, die TPM 2,0 nutzen, einschließlich Windows Hello. Um Organisationen beim Übergang zu unterstützen, beginnend mit Windows 10, Version 1709 und Windows 10, Version 1703, bei dem das kumulative Update vom Oktober 2017 installiert ist, ist die BitLocker-PIN-Länge standardmäßig 6 Zeichen, kann aber auf vier Zeichen reduziert werden. Wenn die minimale PIN-Länge vom Standardwert von sechs Zeichen reduziert wird, wird der TPM-2,0-Sperrzeitraum verlängert.

Neue DMA-Geräte deaktivieren, wenn dieser Computer gesperrt ist

Mit dieser Richtlinieneinstellung können Sie den direkten Speicherzugriff (DMA) für alle Hot-Plug-fähigen PCI-Anschlüsse sperren, bis sich ein Benutzer bei Windows anmeldet.

Richtlinienbeschreibung	Mit dieser Einstellung können Angriffe verhindert werden, die externe PCI-basierte Geräte verwenden, um auf BitLocker-Schlüssel zuzugreifen.
Eingeführt	Windows10, Version1703
Laufwerktyp	Betriebssystemlaufwerke

Richtlinienpfad	Computer Configuration\Administrative Vorlagen\Windows-Komponenten\Internet BitLocker-Laufwerkverschlüsselung Drive Encryption
Konflikte	Keine
Wenn aktiviert	Jedes Mal, wenn der Benutzer den Bildschirm sperrt, wird DMA auf Hot-Pluggable-PCI-Ports blockiert, bis sich der Benutzer erneut anmeldet.
Wenn deaktiviert oder nicht konfiguriert	DMA ist auf Hot-Pluggable-PCI-Geräten verfügbar, wenn das Gerät aktiviert ist, unabhängig davon, ob ein Benutzer angemeldet ist.

Referenz

Diese Richtlinieneinstellung wird nur erzwungen, wenn BitLocker oder Geräteverschlüsselung aktiviert ist. Wie im Blog zum Microsoft-Sicherheitsleitfadenerläutert, kann in einigen Fällen, wenn diese Einstellung aktiviert ist, interne, PCI-basierte Peripheriegeräte fehlschlagen, einschließlich Wireless-Netzwerktreibern sowie Eingabe-und Audio-Peripheriegeräten. Dieses Problem ist im April 2018 Quality Updatebehoben.

Verhindern, dass Standardbenutzer die PIN oder das Kennwort ändern

Mit dieser Richtlinieneinstellung können Sie konfigurieren, ob Standardbenutzer die PIN oder das Kennwort ändern dürfen, die zum Schützen des Betriebssystemlaufwerks verwendet wird.

Richtlinienbeschreibung	Mit dieser Richtlinieneinstellung können Sie konfigurieren, ob Standardbenutzer die PIN oder das Kennwort ändern dürfen, die zum Schützen des Betriebssystemlaufwerks verwendet werden.
Eingeführt	Windows Server 2012 und Windows 8
Laufwerktyp	Betriebssystemlaufwerke
Richtlinienpfad	Computer Configuration\Administrative Vorlagen\Windows-Komponenten\Internet BitLocker-Laufwerkverschlüsselung Drive Encryption\Operating System Laufwerke
Konflikte	Keine
Wenn aktiviert	Standard Benutzer sind nicht berechtigt, BitLocker-Pins oder-Kennwörter zu ändern.
Wenn deaktiviert oder nicht konfiguriert	Standard Benutzern ist es gestattet, BitLocker-Pins oder-Kennwörter zu ändern.

Referenz

Um die PIN oder das Kennwort zu ändern, muss der Benutzer in der Lage sein, die aktuelle PIN oder das

Kennwort anzugeben. Diese Richtlinieneinstellung wird angewendet, wenn Sie BitLocker aktivieren.

Konfigurieren der Verwendung von Kennwörtern für Betriebssystemlaufwerke

Diese Richtlinie steuert, wie nicht-TPM-basierte Systeme die Kennwortschutz Komponente verwenden. In Verbindung mit der Verwendung des Kennworts muss die Richtlinie für **Komplexitätsanforderungen erfüllen** , mit dieser Richtlinie können Administratoren die Kennwortlänge und-Komplexität für die Verwendung des Kennwortschutzes anfordern. Standardmäßig müssen Kennwörter acht Zeichen lang sein. Die Optionen für die Komplexitäts Konfiguration legen fest, wie wichtig die Domänen Konnektivität für den Client ist. Für die sicherste Kennwortsicherheit sollten Administratoren die Option **Kennwortkomplexität anfordern** auswählen, da Sie eine Domänen Konnektivität erfordert und das BitLocker-Kennwort die gleichen Anforderungen an die Kennwortkomplexität erfüllt wie Domänenanmelde Kennwörter.

Richtlinienbeschreibung	Mit dieser Richtlinieneinstellung können Sie die Einschränkungen für Kennwörter angeben, die zum Entsperren von Betriebssystemlaufwerken verwendet werden, die mit BitLocker geschützt sind.
Eingeführt	Windows Server 2012 und Windows 8
Laufwerktyp	Betriebssystemlaufwerke
Richtlinienpfad	Computer Configuration\Administrative Vorlagen\Windows-Komponenten\Internet BitLocker-Laufwerkverschlüsselung Drive Encryption\Operating System Laufwerke
Konflikte	Kennwörter können nicht verwendet werden, wenn FIPS-Compliance aktiviert ist. **Hinweis:** Die **System Kryptografie: Verwenden der FIPS-kompatiblen Algorithmen für Verschlüsselung, Hashing und Signatur** Richtlinieneinstellung, die sich unter **Computer Computerkonfiguration\Windows-Einstellungen Richtlinien\Zuweisen Computerkonfiguration\Windows-Einstellungen\Sicherheitseinstellungen\Lokale Richtlinien\Sicherheitsoptionen-Optionen** befindet, gibt an, ob die FIPS-Konformität aktiviert ist.
Wenn aktiviert	Benutzer können ein Kennwort konfigurieren, das die von Ihnen definierten Anforderungen erfüllt. Um die Komplexitätsanforderungen für das Kennwort zu **erzwingen,**wählen Sie Komplexität anfordern aus.
Wenn deaktiviert oder nicht konfiguriert	Die standardmäßige Längenbeschränkung von 8 Zeichen gilt für Kennwörter des Betriebssystemlaufwerks, und es werden keine Komplexitätsüberprüfungen ausgeführt.

Referenz

Wenn nicht-TPM-Beschützer auf Betriebssystemlaufwerken zulässig sind, können Sie ein Kennwort bereitstellen,

Komplexitätsanforderungen für das Kennwort erzwingen und eine Mindestlänge für das Kennwort konfigurieren. Damit die Komplexitäts Anforderungs Einstellung effektiv ist, muss das Kennwort für die Gruppenrichtlinieneinstellung den **Komplexitätsanforderungen entsprechen**, die sich auf **Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy** müssen ebenfalls aktiviert sein.

> **Hinweis:** Diese Einstellungen werden beim Aktivieren von BitLocker erzwungen, nicht beim Entsperren eines Volumes. BitLocker ermöglicht das Entsperren eines Laufwerks mit einem der auf dem Laufwerk verfügbaren Schutzvorrichtungen.

Wenn die Option " **Komplexität erforderlich**" lautet, ist eine Verbindung mit einem Domänencontroller erforderlich, wenn BitLocker aktiviert ist, um die Komplexität des Kennworts zu überprüfen. Wenn Sie auf **Komplexität zulassen**festzulegen, versucht eine Verbindung mit einem Domänencontroller, zu überprüfen, ob die Komplexität den von der Richtlinie festgelegten Regeln entspricht. Wenn keine Domänencontroller gefunden werden, wird das Kennwort unabhängig von der tatsächlichen Kennwortkomplexität akzeptiert, und das Laufwerk wird mithilfe dieses Kennworts als Beschützer verschlüsselt. Wenn die Einstellung auf **Komplexität nicht zulassen**eingestellt ist, wird keine Kenn Wort Komplexitäts Überprüfung durchgesetzt. Kennwörter müssen aus mindestens 8 Zeichen bestehen. Wenn Sie eine größere Mindestlänge für das Kennwort konfigurieren möchten, geben Sie die gewünschte Anzahl von Zeichen in das Feld **minimale Kennwortlänge** ein.

Wenn diese Richtlinieneinstellung aktiviert ist, können Sie die Option **Konfigurieren der Kennwortkomplexität für Betriebssystemlaufwerke** auf Folgendes festlegen:

- Kennwortkomplexität zulassen
- Kennwortkomplexität nicht zulassen
- Kennwortkomplexität anfordern

Anfordern zusätzlicher Authentifizierung beim Start (Windows Server 2008 und Windows Vista)

Diese Richtlinieneinstellung wird verwendet, um zu steuern, welche Unlock-Optionen für Computer mit Windows Server 2008 oder Windows Vista verfügbar sind.

Richtlinienbeschreibung	Mit dieser Richtlinieneinstellung können Sie steuern, ob der BitLocker-Setup-Assistent auf Computern unter Windows Vista oder Windows Server 2008 eine zusätzliche Authentifizierungsmethode einrichten kann, die bei jedem Start des Computers erforderlich ist.
Eingeführt	Windows Server 2008 und Windows Vista
Laufwerktyp	Betriebssystemlaufwerke (Windows Server 2008 und Windows Vista)
Richtlinienpfad	Computer Configuration\Administrative Vorlagen\Windows-Komponenten\Internet BitLocker-Laufwerkverschlüsselung Drive Encryption\Operating System Laufwerke
Konflikte	Wenn Sie eine zusätzliche Authentifizierungsmethode anfordern, können keine anderen Authentifizierungsmethoden zugelassen werden.

Wenn aktiviert	Der BitLocker-Setup-Assistent zeigt die Seite an, auf der der Benutzer Erweiterte Startoptionen für BitLocker konfigurieren kann. Sie können die Einstellungsoptionen für Computer mit oder ohne TPM weiter konfigurieren.
Wenn deaktiviert oder nicht konfiguriert	Der BitLocker-Setup-Assistent zeigt grundlegende Schritte an, mit denen Benutzer BitLocker auf Computern mit einem TPM aktivieren können. In diesem einfachen Assistenten kann kein zusätzlicher Start-oder Startcode konfiguriert werden.

Referenz

Auf einem Computer mit einem kompatiblen TPM können zwei Authentifizierungsmethoden beim Start verwendet werden, um zusätzlichen Schutz für verschlüsselte Daten bereitzustellen. Wenn der Computer gestartet wird, kann es erforderlich sein, dass Benutzer ein USB-Laufwerk einfügen, das einen Startschlüssel enthält. Darüber hinaus kann es erforderlich sein, dass Benutzer eine sechsstellige bis 20-stellige Start-PIN eingeben.

Ein USB-Laufwerk mit einem Startschlüssel ist auf Computern ohne kompatibles TPM erforderlich. Ohne ein TPM werden BitLocker-verschlüsselte Daten ausschließlich durch das Schlüsselmaterial geschützt, das sich auf diesem USB-Laufwerk befindet.

Es gibt zwei Optionen für TPM-fähige Computer oder Geräte:

- Konfigurieren der TPM-Start-PIN
  - Start-PIN mit TPM zulassen
  - Start-PIN mit TPM erforderlich
  - Start-PIN mit TPM nicht zulassen
- Konfigurieren des TPM-Startschlüssels
  - Autostart-Schlüssel mit TPM zulassen
  - Starten des Schlüssels mit TPM erforderlich
  - Startschlüssel nicht mit TPM zulassen

Diese Optionen schließen sich gegenseitig aus. Wenn Sie den Startschlüssel benötigen, dürfen Sie die Start-PIN nicht zulassen. Wenn Sie die Start-PIN benötigen, dürfen Sie den Startschlüssel nicht zulassen. Andernfalls tritt ein Richtlinienfehler auf.

Wenn Sie die Seite erweitert auf einem TPM-fähigen Computer oder Gerät ausblenden möchten, setzen Sie diese Optionen auf **nicht zulassen** für den Startschlüssel und für die Start-PIN.

Konfigurieren der Verwendung von Smartcards auf festen Datenlaufwerken

Diese Richtlinieneinstellung wird verwendet, um die Verwendung von Smartcards mit festen Datenlaufwerken zu erzwingen, zu genehmigen oder abzulehnen.

Richtlinienbeschreibung	Mit dieser Richtlinieneinstellung können Sie angeben, ob Smartcards zum Authentifizieren des Benutzerzugriffs auf die mit BitLocker geschützten Datenlaufwerke auf einem Computer verwendet werden können.
Eingeführt	Windows Server 2008 R2 und Windows 7

Laufwerktyp	Feste Datenlaufwerke
Richtlinienpfad	Computer Configuration\Administrative Vorlagen\Windows-Komponenten\Internet BitLocker-Laufwerkverschlüsselung Drive Encryption\Fixed Datenlaufwerke
Konflikte	Um Smartcards mit BitLocker verwenden zu können, müssen Sie möglicherweise auch die Einstellung Objekt-**ID in der Configuration\Administrative Templates\BitLocker Drive Encryption\Validate Smartcard-Zertifikat Nutzungs** Regel-Kompatibilitätsrichtlinien Einstellung so ändern, dass Sie der Objekt-ID Ihrer Smartcard-Zertifikate entspricht.
Wenn aktiviert	Smartcards können verwendet werden, um den Benutzer Zugriff auf das Laufwerk zu authentifizieren. Sie können Smartcard-Authentifizierung anfordern, indem Sie **das Kontrollkästchen Verwenden von Smartcards auf festen** Datenlaufwerken anfordern aktivieren.
Wenn deaktiviert	Benutzer können keine Smartcards verwenden, um Ihren Zugriff auf von BitLocker geschützte fest Netzlaufwerke zu authentifizieren.
Wenn nicht konfiguriert	Smartcards können verwendet werden, um den Benutzer Zugriff auf ein mit BitLocker geschütztes Laufwerk zu authentifizieren.

Referenz

> **Hinweis:** Diese Einstellungen werden beim Aktivieren von BitLocker erzwungen, nicht beim Entsperren eines Laufwerks. BitLocker ermöglicht das Entsperren eines Laufwerks mithilfe eines der auf dem Laufwerk verfügbaren Schutzvorrichtungen.

Konfigurieren der Verwendung von Kennwörtern auf festen Datenlaufwerken

Diese Richtlinieneinstellung wird verwendet, um die Verwendung von Kennwörtern mit festen Datenlaufwerken zu erzwingen, zu genehmigen oder abzulehnen.

Richtlinienbeschreibung	Mit dieser Richtlinieneinstellung können Sie angeben, ob ein Kennwort zum Entsperren von BitLocker-geschützten festen Datenlaufwerken erforderlich ist.
Eingeführt	Windows Server 2008 R2 und Windows 7
Laufwerktyp	Feste Datenlaufwerke

Richtlinienpfad	Computer Configuration\Administrative Vorlagen\Windows-Komponenten\Internet BitLocker-Laufwerkverschlüsselung Drive Encryption\Fixed Datenlaufwerke
Konflikte	Um die Kennwortkomplexität verwenden **zu können, muss die Richtlinieneinstellung Computer Computerkonfiguration\Windows-Einstellungen Richtlinien\Zuweisen** Settings\Account Policies\Password Policy\Password den Anforderungen für die Komplexitäts Anforderung genügen.
Wenn aktiviert	Benutzer können ein Kennwort konfigurieren, das die von Ihnen definierten Anforderungen erfüllt. Um die Verwendung eines Kennworts zu erzwingen, **wählen Sie Kennwort für festes**Datenlaufwerk anfordern aus. Um die Komplexitätsanforderungen für das Kennwort zu **erzwingen,**wählen Sie Komplexität anfordern aus.
Wenn deaktiviert	Dem Benutzer ist es nicht gestattet, ein Kennwort zu verwenden.
Wenn nicht konfiguriert	Kennwörter werden mit den Standardeinstellungen unterstützt, die keine Anforderungen an die Kennwortkomplexität enthalten und nur 8 Zeichen erfordern.

Referenz

Wenn Sie auf **Komplexität anfordern**festlegen, ist eine Verbindung mit einem Domänencontroller erforderlich, um die Komplexität des Kennworts zu überprüfen, wenn BitLocker aktiviert ist.

Wenn Sie auf **Komplexität zulassen**festzulegen, versucht eine Verbindung mit einem Domänencontroller, zu überprüfen, ob die Komplexität den von der Richtlinie festgelegten Regeln entspricht. Wenn jedoch keine Domänencontroller gefunden werden, wird das Kennwort unabhängig von der tatsächlichen Kennwortkomplexität akzeptiert, und das Laufwerk wird mithilfe dieses Kennworts als Beschützer verschlüsselt.

Wenn auf **Komplexität nicht zulassen**eingestellt ist, wird keine Überprüfung der Kennwortkomplexität durchgeführt.

Kennwörter müssen aus mindestens 8 Zeichen bestehen. Wenn Sie eine größere Mindestlänge für das Kennwort konfigurieren möchten, geben Sie die gewünschte Anzahl von Zeichen in das Feld **minimale Kennwortlänge** ein.

> **Hinweis:** Diese Einstellungen werden beim Aktivieren von BitLocker erzwungen, nicht beim Entsperren eines Laufwerks. BitLocker ermöglicht das Entsperren eines Laufwerks mit einem der auf dem Laufwerk verfügbaren Schutzvorrichtungen.

Damit die Komplexitäts Anforderungs Einstellung effektiv ist, muss die Gruppenrichtlinieneinstellung **Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy\Password den Komplexitätsanforderungen entsprechen** , ebenfalls aktiviert sein. Diese Richtlinieneinstellung wird pro Computer konfiguriert. Dies bedeutet, dass Sie für lokale Benutzerkonten und Domänenbenutzerkonten gilt. Da sich der Kennwortfilter, der zur Überprüfung der Kennwortkomplexität verwendet wird, auf den

Domänencontrollern befindet, können lokale Benutzerkonten nicht auf den Kennwortfilter zugreifen, da Sie für den Domänenzugriff nicht authentifiziert sind. Wenn diese Richtlinieneinstellung aktiviert ist, wenn Sie sich mit einem lokalen Benutzerkonto anmelden und versuchen, ein Laufwerk zu verschlüsseln oder ein Kennwort auf einem vorhandenen BitLocker-geschützten Laufwerk zu ändern, wird die Fehlermeldung "Zugriff verweigert" angezeigt. In diesem Fall kann die Kennwortschlüssel-Schutzfolie dem Laufwerk nicht hinzugefügt werden.

Wenn Sie diese Richtlinieneinstellung aktivieren, muss die Verbindung zu einer Domäne hergestellt werden, bevor ein Kennwortschlüssel Schutz zu einem mit BitLocker geschützten Laufwerk hinzugefügt wird. Benutzer, die Remote arbeiten und Zeiträume haben, in denen Sie keine Verbindung mit der Domäne herstellen können, sollten auf diese Anforderung hingewiesen werden, damit Sie einen Zeitpunkt planen können, zu dem Sie mit der Domäne verbunden sind, um BitLocker zu aktivieren oder ein Kennwort für ein BitLocker-Protect zu ändern. Ed-Datenlaufwerk.

> **Wichtig:** Kennwörter können nicht verwendet werden, wenn die FIPS-Konformität aktiviert ist. Die **System Kryptografie: Verwenden von FIPS-kompatiblen Algorithmen für Verschlüsselung, Hashing und Signatur** Richtlinieneinstellung in **Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Optionen** gibt an, ob die FIPS-Konformität aktiviert ist.

Konfigurieren der Verwendung von Smartcards auf wechselbaren Datenlaufwerken

Diese Richtlinieneinstellung wird verwendet, um die Verwendung von Smartcards mit Wechseldatenträgern zu erzwingen, zu genehmigen oder abzulehnen.

Richtlinienbeschreibung	Mit dieser Richtlinieneinstellung können Sie angeben, ob Smartcards zum Authentifizieren des Benutzerzugriffs auf von BitLocker geschützte Wechseldaten Laufwerke auf einem Computer verwendet werden können.
Eingeführt	Windows Server 2008 R2 und Windows 7
Laufwerktyp	Austauschbare Datenlaufwerke
Richtlinienpfad	Computer Configuration\Administrative Vorlagen\Windows-Komponenten\Internet BitLocker-Laufwerkverschlüsselung Drive Encryption\Removable Datenlaufwerke
Konflikte	Um Smartcards mit BitLocker verwenden zu können, müssen Sie möglicherweise auch die Einstellung Objekt-**ID in der Configuration\Administrative Templates\BitLocker Drive Encryption\Validate Smartcard-Zertifikat Nutzungs** Regel-Kompatibilitätsrichtlinien Einstellung so ändern, dass Sie der Objekt-ID Ihrer Smartcard-Zertifikate entspricht.
Wenn aktiviert	Smartcards können verwendet werden, um den Benutzer Zugriff auf das Laufwerk zu authentifizieren. Sie können Smartcard-Authentifizierung anfordern, indem Sie **das** Kontrollkästchen Verwenden von Smartcards auf Wechseldatenträgern anfordern aktivieren.

Wenn deaktiviert oder nicht konfiguriert	Benutzer dürfen keine Smartcards verwenden, um Ihren Zugriff auf von BitLocker geschützte Wechseldaten Laufwerke zu authentifizieren.
Wenn nicht konfiguriert	Smartcards stehen zur Authentifizierung des Benutzerzugriffs auf ein von BitLocker geschütztes Wechseldaten Laufwerk zur Verfügung.

Referenz

> **Hinweis:** Diese Einstellungen werden beim Aktivieren von BitLocker erzwungen, nicht beim Entsperren eines Laufwerks. BitLocker ermöglicht das Entsperren eines Laufwerks mit einem der auf dem Laufwerk verfügbaren Schutzvorrichtungen.

Konfigurieren der Verwendung von Kennwörtern auf austauschbaren Datenlaufwerken

Diese Richtlinieneinstellung wird verwendet, um die Verwendung von Kennwörtern mit Wechseldatenträgern zu erzwingen, zu genehmigen oder abzulehnen.

Richtlinienbeschreibung	Mit dieser Richtlinieneinstellung können Sie angeben, ob ein Kennwort zum Entsperren von BitLocker-geschützten Wechseldaten Laufwerken erforderlich ist.
Eingeführt	Windows Server 2008 R2 und Windows 7
Laufwerktyp	Austauschbare Datenlaufwerke
Richtlinienpfad	Computer Configuration\Administrative Vorlagen\Windows-Komponenten\Internet BitLocker-Laufwerkverschlüsselung Drive Encryption\Removable Datenlaufwerke
Konflikte	Um die Kennwortkomplexität zu **verwenden, muss das Kennwort** die Richtlinieneinstellung Komplexitätsanforderungen erfüllen **, die sich auf Computer Computerkonfiguration\Windows-Einstellungen** befindet Richtlinien\Zuweisen Settings\Account Policies\Password Richtlinie muss ebenfalls aktiviert sein.
Wenn aktiviert	Benutzer können ein Kennwort konfigurieren, das die von Ihnen definierten Anforderungen erfüllt. Um die Verwendung eines Kennworts zu erzwingen, **wählen Sie Kennwort für Wechseldatenträger anfordern**aus. Um die Komplexitätsanforderungen für das Kennwort zu **erzwingen,**wählen Sie Komplexität anfordern aus.
Wenn deaktiviert	Dem Benutzer ist es nicht gestattet, ein Kennwort zu verwenden.

Wenn nicht konfiguriert	Kennwörter werden mit den Standardeinstellungen unterstützt, die keine Anforderungen an die Kennwortkomplexität enthalten und nur 8 Zeichen erfordern.

Referenz

Wenn Sie die Verwendung eines Kennworts zulassen möchten, können Sie die Verwendung eines Kennworts anfordern, Komplexitätsanforderungen erzwingen und eine minimale Länge konfigurieren. Damit die Komplexitäts Anforderungs Einstellung effektiv ist, muss das Kennwort für die Gruppenrichtlinieneinstellung den **Komplexitätsanforderungen entsprechen**, die sich auf **Computer Configuration\Windows befinden Settings\Security Settings\Account Policies\Password Richtlinie** muss ebenfalls aktiviert sein.

> **Hinweis:** Diese Einstellungen werden beim Aktivieren von BitLocker erzwungen, nicht beim Entsperren eines Laufwerks. BitLocker ermöglicht das Entsperren eines Laufwerks mit einem der auf dem Laufwerk verfügbaren Schutzvorrichtungen.

Kennwörter müssen aus mindestens 8 Zeichen bestehen. Wenn Sie eine größere Mindestlänge für das Kennwort konfigurieren möchten, geben Sie die gewünschte Anzahl von Zeichen in das Feld **minimale Kennwortlänge** ein.

Wenn die Option " **Komplexität erforderlich**" lautet, ist eine Verbindung mit einem Domänencontroller erforderlich, wenn BitLocker aktiviert ist, um die Komplexität des Kennworts zu überprüfen.

Wenn Sie auf **Komplexität zulassen**festzulegen, wird versucht, eine Verbindung mit einem Domänencontroller zu überprüfen, ob die Komplexität den von der Richtlinie festgelegten Regeln entspricht. Wenn jedoch keine Domänencontroller gefunden werden, wird das Kennwort unabhängig von der tatsächlichen Kennwortkomplexität weiterhin akzeptiert, und das Laufwerk wird mithilfe dieses Kennworts als Beschützer verschlüsselt.

Wenn die Einstellung auf **Komplexität nicht zulassen**eingestellt ist, wird keine Überprüfung der Kennwortkomplexität durchgeführt.

> **Hinweis:** Kennwörter können nicht verwendet werden, wenn die FIPS-Konformität aktiviert ist. Die **System Kryptografie: Verwenden von FIPS-kompatiblen Algorithmen für Verschlüsselung, Hashing und Signatur** Richtlinieneinstellung in **Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Optionen** gibt an, ob die FIPS-Konformität aktiviert ist.

Informationen zu dieser Einstellung finden Sie unter System Kryptografie: Verwenden von FIPS-kompatiblen Algorithmen für Verschlüsselung, Hashing und Signierung.

Überprüfen der Kompatibilität von Smartcard-Zertifikat Nutzungsregeln

Diese Richtlinieneinstellung wird verwendet, um zu ermitteln, welches Zertifikat für BitLocker verwendet werden soll.

Richtlinienbeschreibung	Mit dieser Richtlinieneinstellung können Sie einen Objektbezeichner aus einem Smartcard-Zertifikat einem mit BitLocker geschützten Laufwerk zuordnen.
Eingeführt	Windows Server 2008 R2 und Windows 7

Laufwerktyp	Fest-und Wechseldaten Laufwerke
Richtlinienpfad	Computer Configuration\Administrative Vorlagen\Windows-Komponenten\Internet BitLocker-Laufwerkverschlüsselung Drive Encryption
Konflikte	Keine
Wenn aktiviert	Der Objektbezeichner, der in der **Objekt-ID** -Einstellung angegeben ist, muss mit der Objekt-ID im Smartcard-Zertifikat übereinstimmen.
Wenn deaktiviert oder nicht konfiguriert	Die Standardobjekt-ID wird verwendet.

Referenz

Diese Richtlinieneinstellung wird angewendet, wenn Sie BitLocker aktivieren.

Der Objektbezeichner wird in der erweiterten Schlüsselverwendung eines Zertifikats angegeben. BitLocker kann ermitteln, welche Zertifikate zur Authentifizierung eines Benutzerzertifikats für ein mit BitLocker geschütztes Laufwerk verwendet werden können, indem Sie die Objekt-ID im Zertifikat mit der Objekt-ID vergleichen, die durch diese Richtlinieneinstellung definiert ist.

Die Standardobjekt-ID lautet 1.3.6.1.4.1.311.67.1.1.

> **Hinweis:** Für BitLocker ist es nicht erforderlich, dass ein Zertifikat ein EKU-Attribut aufweist. Wenn jedoch eine für das Zertifikat konfiguriert ist, muss Sie auf eine Objekt-ID festgelegt werden, die dem für BitLocker konfigurierten Objektbezeichner entspricht.

Aktivieren der Verwendung der BitLocker-Authentifizierung, die eine Vorstart Tastatureingabe auf Schiefer erfordert

Diese Richtlinieneinstellung ermöglicht Benutzern das Aktivieren von Authentifizierungsoptionen, bei denen Benutzereingaben aus der Preboot-Umgebung erforderlich sind, selbst wenn die Plattform einen Mangel an Preboot-Eingabefunktionen angibt.

Richtlinienbeschreibung	Mit dieser Richtlinieneinstellung können Sie es Benutzern ermöglichen, Authentifizierungsoptionen zu aktivieren, die Benutzereingaben aus der Preboot-Umgebung erfordern, selbst wenn die Plattform einen Mangel an Vorstart-Eingabefunktionen angibt.
Eingeführt	Windows Server 2012 und Windows 8
Laufwerktyp	Betriebssystemlaufwerk
Richtlinienpfad	Computer Configuration\Administrative Vorlagen\Windows-Komponenten\Internet BitLocker-Laufwerkverschlüsselung Drive Encryption\Operating-System Laufwerk

Konflikte	Keine
Wenn aktiviert	Geräte müssen über eine alternative Möglichkeit zur vorboot Eingabe verfügen (beispielsweise eine USB-Tastatur).
Wenn deaktiviert oder nicht konfiguriert	Die Windows-Wiederherstellungsumgebung muss auf Tablets aktiviert sein, damit Sie das BitLocker-Wiederherstellungskennwort eingeben können.

Referenz

Die Windows-Bildschirmtastatur (wie Sie von Tablets verwendet wird) steht in der Preboot-Umgebung nicht zur Verfügung, in der BitLocker zusätzliche Informationen wie eine PIN oder ein Kennwort benötigt.

Es wird empfohlen, dass Administratoren diese Richtlinie nur für Geräte aktivieren, die überprüft werden, dass Sie über eine alternative Möglichkeit zur vorboots Eingabe verfügen, beispielsweise das Anschließen einer USB-Tastatur.

Wenn die Windows-Wiederherstellungsumgebung nicht aktiviert ist und diese Richtlinie nicht aktiviert ist, können Sie BitLocker auf einem Gerät, auf dem die Windows-Bildschirmtastatur verwendet wird, nicht aktivieren.

Wenn Sie diese Richtlinieneinstellung nicht aktivieren, stehen die folgenden Optionen in der Richtlinie **zusätzliche Authentifizierung beim Start erfordern** möglicherweise nicht zur Verfügung:

- Konfigurieren der TPM-Start-PIN: erforderlich und zulässig
- Konfigurieren des TPM-Startschlüssels und der PIN: erforderlich und zulässig
- Konfigurieren der Verwendung von Kennwörtern für Betriebssystemlaufwerke

Schreibzugriff auf Festplattenlaufwerke verweigern, die nicht durch BitLocker geschützt sind

Diese Richtlinieneinstellung wird verwendet, um vor dem Gewähren von Schreibzugriff die Verschlüsselung fester Laufwerke vorzuschreiben.

Richtlinienbeschreibung	Mit dieser Richtlinieneinstellung können Sie festlegen, ob der BitLocker-Schutz erforderlich ist, damit feste Datenlaufwerke auf einem Computer beschreibbar sind.
Eingeführt	Windows Server 2008 R2 und Windows 7
Laufwerktyp	Feste Datenlaufwerke
Richtlinienpfad	Computer Configuration\Administrative Vorlagen\Windows-Komponenten\Internet BitLocker-Laufwerkverschlüsselung Drive Encryption\Fixed Datenlaufwerke
Konflikte	Eine Beschreibung der Konflikte finden Sie im Abschnitt "Referenz".

Wenn aktiviert	Alle festen Datenlaufwerke, die nicht mit BitLocker geschützt sind, werden schreibgeschützt bereitgestellt. Wenn das Laufwerk von BitLocker geschützt ist, wird es mit Lese-und Schreibzugriff bereitgestellt.
Wenn deaktiviert oder nicht konfiguriert	Alle festen Datenlaufwerke auf dem Computer sind mit Lese-und Schreibzugriff bereitgestellt.

Referenz

Diese Richtlinieneinstellung wird angewendet, wenn Sie BitLocker aktivieren.

Zu den Konflikt Überlegungen gehören:

1. Wenn diese Richtlinieneinstellung aktiviert ist, erhalten die Benutzer die Fehlermeldung "Zugriff verweigert", wenn Sie versuchen, Daten auf nicht verschlüsselten festen Datenlaufwerken zu speichern. Weitere Konflikte finden Sie im Abschnitt "Referenz".
2. Wenn BdeHdCfg. exe auf einem Computer ausgeführt wird, wenn diese Richtlinieneinstellung aktiviert ist, können die folgenden Probleme auftreten:
   - Wenn Sie versucht haben, das Laufwerk zu verkleinern und das Systemlaufwerk zu erstellen, wird die Laufwerksgröße erfolgreich reduziert und eine RAW-Partition erstellt. Die RAW-Partition ist jedoch nicht formatiert. Die folgende Fehlermeldung wird angezeigt: "das neue aktive Laufwerk kann nicht formatiert werden. Möglicherweise müssen Sie Ihr Laufwerk für BitLocker manuell vorbereiten. "
   - Wenn Sie versuchen, nicht zugewiesenen Speicherplatz zum Erstellen des Systemlaufwerks zu verwenden, wird eine RAW-Partition erstellt. Die RAW-Partition wird jedoch nicht formatiert. Die folgende Fehlermeldung wird angezeigt: "das neue aktive Laufwerk kann nicht formatiert werden. Möglicherweise müssen Sie Ihr Laufwerk für BitLocker manuell vorbereiten. "
   - Wenn Sie versuchen, ein vorhandenes Laufwerk mit dem Systemlaufwerk zusammenzuführen, kann das Tool die erforderliche Startdatei nicht auf das Ziellaufwerk kopieren, um das Systemlaufwerk zu erstellen. Die folgende Fehlermeldung wird angezeigt: Fehler beim Kopieren von Startdateien durch das BitLocker-Setup. Möglicherweise müssen Sie Ihr Laufwerk für BitLocker manuell vorbereiten. "
3. Wenn diese Richtlinieneinstellung erzwungen wird, kann eine Festplatte nicht neu partitioniert werden, da das Laufwerk geschützt ist. Wenn Sie Computer in Ihrer Organisation von einer früheren Version von Windows aktualisieren und diese Computer mit einer einzelnen Partition konfiguriert wurden, sollten Sie die erforderliche BitLocker-Systempartition erstellen, bevor Sie diese Richtlinieneinstellung auf die Computer anwenden.

Schreibzugriff auf Wechseldatenträger verweigern, die nicht durch BitLocker geschützt sind

Mit dieser Richtlinieneinstellung muss festgelegt werden, dass Wechseldatenträger vor dem Erteilen von Schreibzugriff verschlüsselt werden, und um zu steuern, ob mit BitLocker geschützte Wechseldatenträger, die in einer anderen Organisation konfiguriert wurden, mit Schreibzugriff geöffnet werden können.

Richtlinienbeschreibung	Mit dieser Richtlinieneinstellung können Sie konfigurieren, ob der BitLocker-Schutz erforderlich ist, damit ein Computer Daten auf ein Wechsellaufwerk schreiben kann.
Eingeführt	Windows Server 2008 R2 und Windows 7
Laufwerktyp	Austauschbare Datenlaufwerke

Richtlinienpfad	Computer Configuration\Administrative Vorlagen\Windows-Komponenten\Internet BitLocker-Laufwerkverschlüsselung Drive Encryption\Removable Datenlaufwerke
Konflikte	Eine Beschreibung der Konflikte finden Sie im Abschnitt "Referenz".
Wenn aktiviert	Alle Wechseldatenträger, die nicht mit BitLocker geschützt sind, werden schreibgeschützt bereitgestellt. Wenn das Laufwerk von BitLocker geschützt ist, wird es mit Lese-und Schreibzugriff bereitgestellt.
Wenn deaktiviert oder nicht konfiguriert	Alle auf dem Computer entfernbaren Datenlaufwerke sind mit Lese-und Schreibzugriff bereitgestellt.

Referenz

Wenn das Kontrollkästchen **Schreibzugriff auf Geräte verweigern, die in einer anderen Organisation konfiguriert** sind aktiviert ist, werden nur Laufwerke mit Identifikations Feldern, die den ID-Feldern des Computers entsprechen, Schreibzugriff erhalten. Wenn auf ein Wechsellaufwerk zugegriffen wird, wird es auf ein gültiges Identifikationsfeld und zulässige Identifikations Felder überprüft. Diese Felder werden durch die Richtlinieneinstellung **eindeutige IDs für Ihre Organisation bereitstellen** definiert.

> **Hinweis:** Sie können diese Richtlinieneinstellung mit den Richtlinieneinstellungen unter **Benutzer Configuration\Administrative Templates\System\Removable Speicherzugriff**außer Kraft setzen. Wenn die Richtlinie für den **Wechsel von Datenträgern: Richtlinieneinstellung "Schreibzugriff verweigern** " aktiviert ist, wird diese Richtlinieneinstellung ignoriert.

Zu den Konflikt Überlegungen gehören:

1. Die Verwendung von BitLocker mit dem TPM sowie einem Startschlüssel oder mit dem TPM sowie einer PIN und einem Starttaste muss nicht zulässig sein, wenn die Einstellung **Schreibzugriff auf Wechsellaufwerke, die nicht durch BitLocker geschützt sind,** aktiviert ist.
2. Die Verwendung von Wiederherstellungsschlüsseln muss nicht zugelassen werden, wenn die Einstellung **Schreibzugriff auf Wechseldatenträger, die nicht durch BitLocker** -Richtlinien geschützt sind, aktiviert ist.
3. Sie müssen die Richtlinieneinstellung **die eindeutigen IDs für Ihre Organisation bereitstellen** aktivieren, wenn Sie den Schreibzugriff auf Laufwerke verweigern möchten, die in einer anderen Organisation konfiguriert wurden.

Steuern der Verwendung von BitLocker auf Wechseldatenträgern

Diese Richtlinieneinstellung wird verwendet, um zu verhindern, dass Benutzer BitLocker auf Wechseldatenträgern aktivieren oder deaktivieren.

Richtlinienbeschreibung	Mit dieser Richtlinieneinstellung können Sie die Verwendung von BitLocker auf wechselbaren Datenlaufwerken steuern.
Eingeführt	Windows Server 2008 R2 und Windows 7

Laufwerktyp	Austauschbare Datenlaufwerke
Richtlinienpfad	Computer Configuration\Administrative Vorlagen\Windows-Komponenten\Internet BitLocker-Laufwerkverschlüsselung Drive Encryption\Removable Datenlaufwerke
Konflikte	Keine
Wenn aktiviert	Sie können Eigenschaftseinstellungen auswählen, die Steuern, wie Benutzer BitLocker konfigurieren können.
Wenn deaktiviert	Benutzer können BitLocker nicht auf Wechseldaten Laufwerken verwenden.
Wenn nicht konfiguriert	Benutzer können BitLocker auf Wechseldaten Laufwerken verwenden.

Referenz

Diese Richtlinieneinstellung wird angewendet, wenn Sie BitLocker aktivieren.

Informationen zum Anhalten des BitLocker-Schutzes finden Sie unter BitLocker-grundlegende Bereitstellung.

Die Optionen für die Auswahl von Eigenschafteneinstellungen, die Steuern, wie Benutzer BitLocker konfigurieren können, sind:

- **Zulassen, dass Benutzer den BitLocker-Schutz auf Wechseldatenträgern anwenden** Ermöglicht es dem Benutzer, den BitLocker-Setup-Assistenten auf einem Wechseldaten Laufwerk auszuführen.
- **Zulassen, dass Benutzer BitLocker auf wechselbaren Datenlaufwerken anhalten und entschlüsseln** Ermöglicht es dem Benutzer, BitLocker vom Laufwerk zu entfernen oder die Verschlüsselung während der Ausführung der Wartung zu unterbrechen.

Wählen Sie Laufwerk Verschlüsselungsmethode und Verschlüsselungsstärke aus.

Diese Richtlinieneinstellung wird verwendet, um die Verschlüsselungsmethode und die Verschlüsselungsstärke zu steuern.

Richtlinienbeschreibung	Mit dieser Richtlinieneinstellung können Sie die Verschlüsselungsmethode und die Stärke für Laufwerke steuern.
Eingeführt	Windows Server 2012 und Windows 8
Laufwerktyp	Alle Laufwerke
Richtlinienpfad	Computer Configuration\Administrative Vorlagen\Windows-Komponenten\Internet BitLocker-Laufwerkverschlüsselung Drive Encryption

Konflikte	Keine
Wenn aktiviert	Sie können einen Verschlüsselungsalgorithmus und eine Schlüssel Verschlüsselungsstärke für BitLocker auswählen, um Laufwerke zu verschlüsseln.
Wenn deaktiviert oder nicht konfiguriert	Ab Windows 10, Version 1511, verwendet BitLocker die Standardverschlüsselungsmethode von XTS-AES 128-Bit oder die vom Setupskript angegebene Verschlüsselungsmethode. Windows phone unterstützt XTS nicht; Standardmäßig wird AES-CBC 128-Bit verwendet und AES-CBC 256-Bit nach Richtlinie unterstützt.

Referenz

Die Werte dieser Richtlinie bestimmen die Stärke der Chiffre, die von BitLocker für die Verschlüsselung verwendet wird. Unternehmen möchten möglicherweise die Verschlüsselungsstufe für erhöhte Sicherheit Steuern (AES-256 ist stärker als AES-128).

Wenn Sie diese Einstellung aktivieren, können Sie einen Verschlüsselungsalgorithmus und eine Schlüssel Verschlüsselungsstärke für feste Datenlaufwerke, Betriebssystemlaufwerke und Wechseldatenträger einzeln konfigurieren. Für fest-und Betriebssystemlaufwerke empfiehlt es sich, den XTS-AES-Algorithmus zu verwenden. Für Wechseldatenträger sollten Sie AES-CBC 128-Bit oder AES-CBC 256-Bit verwenden, wenn das Laufwerk auf anderen Geräten verwendet wird, auf denen nicht Windows 10, Version 1511 oder höher ausgeführt wird.

Das Ändern der Verschlüsselungsmethode hat keine Auswirkungen, wenn das Laufwerk bereits verschlüsselt ist oder wenn die Verschlüsselung durchgeführt wird. In diesen Fällen wird diese Richtlinieneinstellung ignoriert.

> **Warnung:** Diese Richtlinie gilt nicht für verschlüsselte Laufwerke. Verschlüsselte Laufwerke verwenden ihren eigenen Algorithmus, der während der Partitionierung vom Laufwerk festgesetzt wird.

Wenn diese Richtlinieneinstellung deaktiviert oder nicht konfiguriert ist, verwendet BitLocker die Standardverschlüsselungsmethode von XTS-AES 128-Bit oder die im Setupskript angegebene Verschlüsselungsmethode.

Konfigurieren der Verwendung von hardwarebasierter Verschlüsselung für fest Netzlaufwerke

Diese Richtlinie steuert, wie BitLocker auf Systeme reagiert, die mit verschlüsselten Laufwerken ausgestattet sind, wenn Sie als festes Datenvolumen verwendet werden. Die Verwendung von hardwarebasierter Verschlüsselung kann die Leistung von Laufwerks Vorgängen verbessern, die häufiges lesen oder Schreiben von Daten auf das Laufwerk beinhalten.

Richtlinienbeschreibung	Mit dieser Richtlinieneinstellung können Sie die Verwendung der hardwarebasierten Verschlüsselung von BitLocker auf festen Datenlaufwerken verwalten und angeben, welche Verschlüsselungsalgorithmen BitLocker für die hardwarebasierte Verschlüsselung verwenden kann.
Eingeführt	Windows Server 2012 und Windows 8

Laufwerktyp	Feste Datenlaufwerke
Richtlinienpfad	Computer Configuration\Administrative Vorlagen\Windows-Komponenten\Internet BitLocker-Laufwerkverschlüsselung Drive Encryption\Fixed Datenlaufwerke
Konflikte	Keine
Wenn aktiviert	Sie können zusätzliche Optionen angeben, die Steuern, ob die BitLocker-softwarebasierte Verschlüsselung anstelle der hardwarebasierten Verschlüsselung auf Computern verwendet wird, die keine hardwarebasierte Verschlüsselung unterstützen. Sie können auch angeben, ob Sie die Verschlüsselungsalgorithmen und Verschlüsselungs Pakete einschränken möchten, die mit hardwarebasierter Verschlüsselung verwendet werden.
Wenn deaktiviert	BitLocker kann keine hardwarebasierte Verschlüsselung mit festen Datenlaufwerken verwenden, und die BitLocker-softwarebasierte Verschlüsselung wird standardmäßig verwendet, wenn das Laufwerk verschlüsselt ist.
Wenn nicht konfiguriert	Die softwarebasierte BitLocker-Verschlüsselung wird unabhängig von der hardwarebasierten Verschlüsselungs Fähigkeit verwendet.

Referenz

> **Hinweis:** Die Richtlinieneinstellung **Drive-Verschlüsselungsmethode und Verschlüsselungsstärke auswählen** gilt nicht für hardwarebasierte Verschlüsselung.

Der Verschlüsselungsalgorithmus, der von hardwarebasierter Verschlüsselung verwendet wird, wird bei der Partitionierung des Laufwerks festgesetzt. Standardmäßig verwendet BitLocker den für das Laufwerk konfigurierten Algorithmus, um das Laufwerk zu verschlüsseln. Mit der Option **Verschlüsselungsalgorithmen und Verschlüsselungs Pakete einschränken für hardwarebasierte Verschlüsselung** dieser Einstellung können Sie die Verschlüsselungsalgorithmen einschränken, die BitLocker für die Hardwareverschlüsselung verwenden kann. Wenn der für das Laufwerk festgelegte Algorithmus nicht verfügbar ist, deaktiviert BitLocker die Verwendung von hardwarebasierter Verschlüsselung. Verschlüsselungsalgorithmen werden durch Objektbezeichner (OID) angegeben, beispielsweise:

- Erweiterter Verschlüsselungs Standard (AES) 128 im Verschlüsselungs Block verketten (CBC)-Modus OID: 2.16.840.1.101.3.4.1.2
- AES 256 im CBC-Modus OID: 2.16.840.1.101.3.4.1.42

Konfigurieren der Verwendung von hardwarebasierter Verschlüsselung für Betriebssystemlaufwerke

Diese Richtlinie steuert, wie BitLocker reagiert, wenn verschlüsselte Laufwerke als Betriebssystemlaufwerke verwendet werden. Die Verwendung von hardwarebasierter Verschlüsselung kann die Leistung von Laufwerks Vorgängen verbessern, die häufiges lesen oder Schreiben von Daten auf das Laufwerk beinhalten.

Richtlinienbeschreibung	Mit dieser Richtlinieneinstellung können Sie die Verwendung der hardwarebasierten Verschlüsselung auf Betriebssystemlaufwerken durch BitLocker verwalten und angeben, welche Verschlüsselungsalgorithmen für die hardwarebasierte Verschlüsselung verwendet werden können.
Eingeführt	Windows Server 2012 und Windows 8
Laufwerktyp	Betriebssystemlaufwerke
Richtlinienpfad	Computer Configuration\Administrative Vorlagen\Windows-Komponenten\Internet BitLocker-Laufwerkverschlüsselung Drive Encryption\Operating System Laufwerke
Konflikte	Keine
Wenn aktiviert	Sie können zusätzliche Optionen angeben, die Steuern, ob die BitLocker-softwarebasierte Verschlüsselung anstelle der hardwarebasierten Verschlüsselung auf Computern verwendet wird, die keine hardwarebasierte Verschlüsselung unterstützen. Sie können auch angeben, ob Sie die Verschlüsselungsalgorithmen und Verschlüsselungs Pakete einschränken möchten, die mit hardwarebasierter Verschlüsselung verwendet werden.
Wenn deaktiviert	BitLocker kann keine hardwarebasierte Verschlüsselung mit Betriebssystemlaufwerken verwenden, und die BitLocker-softwarebasierte Verschlüsselung wird standardmäßig verwendet, wenn das Laufwerk verschlüsselt ist.
Wenn nicht konfiguriert	Die softwarebasierte BitLocker-Verschlüsselung wird unabhängig von der hardwarebasierten Verschlüsselungs Fähigkeit verwendet.

Referenz

Wenn keine hardwarebasierte Verschlüsselung verfügbar ist, wird stattdessen die BitLocker-softwarebasierte Verschlüsselung verwendet.

> **Hinweis:** Die Richtlinieneinstellung **Drive-Verschlüsselungsmethode und Verschlüsselungsstärke auswählen** gilt nicht für hardwarebasierte Verschlüsselung.

Der Verschlüsselungsalgorithmus, der von hardwarebasierter Verschlüsselung verwendet wird, wird bei der Partitionierung des Laufwerks festgesetzt. Standardmäßig verwendet BitLocker den für das Laufwerk konfigurierten Algorithmus, um das Laufwerk zu verschlüsseln. Mit der Option **Verschlüsselungsalgorithmen und Verschlüsselungs Pakete einschränken für hardwarebasierte Verschlüsselung** dieser Einstellung können Sie die Verschlüsselungsalgorithmen einschränken, die BitLocker für die Hardwareverschlüsselung verwenden kann. Wenn der für das Laufwerk festgelegte Algorithmus nicht verfügbar ist, deaktiviert BitLocker

die Verwendung von hardwarebasierter Verschlüsselung. Verschlüsselungsalgorithmen werden durch Objektbezeichner (OID) angegeben, beispielsweise:

- Erweiterter Verschlüsselungs Standard (AES) 128 im Verschlüsselungs Block verketten (CBC)-Modus OID: 2.16.840.1.101.3.4.1.2
- AES 256 im CBC-Modus OID: 2.16.840.1.101.3.4.1.42

Konfigurieren der Verwendung von hardwarebasierter Verschlüsselung für Wechseldaten Laufwerke

Diese Richtlinie steuert, wie BitLocker auf verschlüsselte Laufwerke reagiert, wenn Sie als Wechseldatenträger verwendet werden. Die Verwendung von hardwarebasierter Verschlüsselung kann die Leistung von Laufwerks Vorgängen verbessern, die häufiges lesen oder Schreiben von Daten auf das Laufwerk beinhalten.

Richtlinienbeschreibung	Mit dieser Richtlinieneinstellung können Sie die Verwendung der hardwarebasierten Verschlüsselung auf Wechseldatenträgern durch BitLocker verwalten und angeben, welche Verschlüsselungsalgorithmen mit hardwarebasierter Verschlüsselung verwendet werden können.
Eingeführt	Windows Server 2012 und Windows 8
Laufwerktyp	Wechseldaten Laufwerk
Richtlinienpfad	Computer Configuration\Administrative Vorlagen\Windows-Komponenten\Internet BitLocker-Laufwerkverschlüsselung Drive Encryption\Removable Datenlaufwerke
Konflikte	Keine
Wenn aktiviert	Sie können zusätzliche Optionen angeben, die Steuern, ob die BitLocker-softwarebasierte Verschlüsselung anstelle der hardwarebasierten Verschlüsselung auf Computern verwendet wird, die keine hardwarebasierte Verschlüsselung unterstützen. Sie können auch angeben, ob Sie die Verschlüsselungsalgorithmen und Verschlüsselungs Pakete einschränken möchten, die mit hardwarebasierter Verschlüsselung verwendet werden.
Wenn deaktiviert	BitLocker kann keine hardwarebasierte Verschlüsselung mit Wechseldatenträgern verwenden, und die BitLocker-softwarebasierte Verschlüsselung wird standardmäßig verwendet, wenn das Laufwerk verschlüsselt ist.
Wenn nicht konfiguriert	Die softwarebasierte BitLocker-Verschlüsselung wird unabhängig von der hardwarebasierten Verschlüsselungs Fähigkeit verwendet.

Referenz

Wenn keine hardwarebasierte Verschlüsselung verfügbar ist, wird stattdessen die BitLocker-softwarebasierte Verschlüsselung verwendet.

> **Hinweis:** Die Richtlinieneinstellung **Drive-Verschlüsselungsmethode und Verschlüsselungsstärke auswählen** gilt nicht für hardwarebasierte Verschlüsselung.

Der Verschlüsselungsalgorithmus, der von hardwarebasierter Verschlüsselung verwendet wird, wird bei der Partitionierung des Laufwerks festgesetzt. Standardmäßig verwendet BitLocker den für das Laufwerk konfigurierten Algorithmus, um das Laufwerk zu verschlüsseln. Mit der Option **Verschlüsselungsalgorithmen und Verschlüsselungs Pakete einschränken für hardwarebasierte Verschlüsselung** dieser Einstellung können Sie die Verschlüsselungsalgorithmen einschränken, die BitLocker für die Hardwareverschlüsselung verwenden kann. Wenn der für das Laufwerk festgelegte Algorithmus nicht verfügbar ist, deaktiviert BitLocker die Verwendung von hardwarebasierter Verschlüsselung. Verschlüsselungsalgorithmen werden durch Objektbezeichner (OID) angegeben, beispielsweise:

- Erweiterter Verschlüsselungs Standard (AES) 128 im Verschlüsselungs Block verketten (CBC)-Modus OID: 2.16.840.1.101.3.4.1.2
- AES 256 im CBC-Modus OID: 2.16.840.1.101.3.4.1.42

Erzwingen des Laufwerk Verschlüsselungstyps auf festen Datenlaufwerken

Diese Richtlinie steuert, ob feste Datenlaufwerke nur verschlüsselte Speicherplatz Verschlüsselung oder voll Verschlüsselung verwenden. Das Festlegen dieser Richtlinie bewirkt auch, dass der BitLocker-Setup-Assistent die Seite mit den Verschlüsselungsoptionen überspringt, damit keine Verschlüsselungs Auswahl für den Benutzer angezeigt wird.

Richtlinienbeschreibung	Mit dieser Richtlinieneinstellung können Sie den von BitLocker verwendeten Verschlüsselungstyp konfigurieren.
Eingeführt	Windows Server 2012 und Windows 8
Laufwerktyp	Festes Datenlaufwerk
Richtlinienpfad	Computer Configuration\Administrative Vorlagen\Windows-Komponenten\Internet BitLocker-Laufwerkverschlüsselung Drive Encryption\Fixed Datenlaufwerke
Konflikte	Keine
Wenn aktiviert	Diese Richtlinie definiert den Verschlüsselungstyp, den BitLocker zum Verschlüsseln von Laufwerken verwendet, und die Option Verschlüsselungstyp wird im BitLocker-Setup-Assistenten nicht angezeigt.
Wenn deaktiviert oder nicht konfiguriert	Der BitLocker-Setup-Assistent fordert den Benutzer auf, den Verschlüsselungstyp auszuwählen, bevor BitLocker aktiviert wird.

Referenz

Diese Richtlinieneinstellung wird angewendet, wenn Sie BitLocker aktivieren. Das Ändern des Verschlüsselungstyps hat keine Auswirkungen, wenn das Laufwerk bereits verschlüsselt ist oder wenn die

Verschlüsselung durchgeführt wird. Wählen Sie vollständige Verschlüsselung aus, um die Verschlüsselung des gesamten Laufwerks zu erzwingen, wenn BitLocker aktiviert ist. Wählen Sie verwendeter Speicherplatz nur Verschlüsselung aus, um zu erzwingen, dass nur der Teil des Laufwerks, der zum Speichern von Daten verwendet wird, verschlüsselt ist, wenn BitLocker aktiviert ist.

> **Hinweis:** Diese Richtlinie wird ignoriert, wenn Sie ein Volume verkleinern oder erweitern, und der BitLocker-Treiber verwendet die aktuelle Verschlüsselungsmethode. Wenn beispielsweise ein Laufwerk, auf dem nur gebrauchte Speicherplatz Verschlüsselung verwendet wird, erweitert wird, wird der neue freie Speicherplatz nicht so gelöscht, wie es bei einem Laufwerk mit vollständiger Verschlüsselung der Fall wäre. Der Benutzer kann den freien Speicherplatz auf einem verwendeten Speicherplatz nur mithilfe des folgenden Befehls löschen: **manage-bde-w**. Wenn die Lautstärke geschrumpft ist, wird für den neuen freien Speicherplatz keine Aktion ausgeführt.

Weitere Informationen zum Tool zum Verwalten von BitLocker finden Sie unter Verwalten von BDE.

Erzwingen des Laufwerk Verschlüsselungstyps auf Betriebssystemlaufwerken

Diese Richtlinie steuert, ob Betriebssystemlaufwerke die vollständige Verschlüsselung oder nur die gebrauchte Speicherplatz Verschlüsselung verwenden. Das Festlegen dieser Richtlinie bewirkt auch, dass der BitLocker-Setup-Assistent die Seite mit den Verschlüsselungsoptionen überspringt, sodass keine Verschlüsselungs Auswahl für den Benutzer angezeigt wird.

Richtlinienbeschreibung	Mit dieser Richtlinieneinstellung können Sie den von BitLocker verwendeten Verschlüsselungstyp konfigurieren.
Eingeführt	Windows Server 2012 und Windows 8
Laufwerktyp	Betriebssystemlaufwerk
Richtlinienpfad	Computer Configuration\Administrative Vorlagen\Windows-Komponenten\Internet BitLocker-Laufwerkverschlüsselung Drive Encryption\Operating System Laufwerke
Konflikte	Keine
Wenn aktiviert	Der Verschlüsselungstyp, den BitLocker zum Verschlüsseln von Laufwerken verwendet, wird durch diese Richtlinie definiert, und die Option Verschlüsselungstyp wird im BitLocker-Setup-Assistenten nicht angezeigt.
Wenn deaktiviert oder nicht konfiguriert	Der BitLocker-Setup-Assistent fordert den Benutzer auf, den Verschlüsselungstyp auszuwählen, bevor BitLocker aktiviert wird.

Referenz

Diese Richtlinieneinstellung wird angewendet, wenn Sie BitLocker aktivieren. Das Ändern des Verschlüsselungstyps hat keine Auswirkungen, wenn das Laufwerk bereits verschlüsselt ist oder wenn die Verschlüsselung durchgeführt wird. Wählen Sie vollständige Verschlüsselung aus, um die Verschlüsselung des

gesamten Laufwerks zu erzwingen, wenn BitLocker aktiviert ist. Wählen Sie verwendeter Speicherplatz nur Verschlüsselung aus, um zu erzwingen, dass nur der Teil des Laufwerks, der zum Speichern von Daten verwendet wird, verschlüsselt ist, wenn BitLocker aktiviert ist.

> **Hinweis:** Diese Richtlinie wird beim Verkleinern oder Erweitern eines Volumes ignoriert, und der BitLocker-Treiber verwendet die aktuelle Verschlüsselungsmethode. Wenn beispielsweise ein Laufwerk, auf dem nur gebrauchte Speicherplatz Verschlüsselung verwendet wird, erweitert wird, wird der neue freie Speicherplatz nicht so gelöscht, wie es bei einem Laufwerk mit vollständiger Verschlüsselung der Fall wäre. Der Benutzer kann den freien Speicherplatz auf einem verwendeten Speicherplatz nur mithilfe des folgenden Befehls löschen: **manage-bde-w**. Wenn die Lautstärke geschrumpft ist, wird für den neuen freien Speicherplatz keine Aktion ausgeführt.

Weitere Informationen zum Tool zum Verwalten von BitLocker finden Sie unter Verwalten von BDE.

Erzwingen des Laufwerk Verschlüsselungstyps auf Wechseldatenträgern

Diese Richtlinie steuert, ob feste Datenlaufwerke die vollständige Verschlüsselung oder nur die gebrauchte Speicherplatz Verschlüsselung verwenden. Das Festlegen dieser Richtlinie bewirkt auch, dass der BitLocker-Setup-Assistent die Seite mit den Verschlüsselungsoptionen überspringt, sodass keine Verschlüsselungs Auswahl für den Benutzer angezeigt wird.

Richtlinienbeschreibung	Mit dieser Richtlinieneinstellung können Sie den von BitLocker verwendeten Verschlüsselungstyp konfigurieren.
Eingeführt	Windows Server 2012 und Windows 8
Laufwerktyp	Wechseldaten Laufwerk
Richtlinienpfad	Computer Configuration\Administrative Vorlagen\Windows-Komponenten\Internet BitLocker-Laufwerkverschlüsselung Drive Encryption\Removable Datenlaufwerke
Konflikte	Keine
Wenn aktiviert	Der Verschlüsselungstyp, den BitLocker zum Verschlüsseln von Laufwerken verwendet, wird durch diese Richtlinie definiert, und die Option Verschlüsselungstyp wird im BitLocker-Setup-Assistenten nicht angezeigt.
Wenn deaktiviert oder nicht konfiguriert	Der BitLocker-Setup-Assistent fordert den Benutzer auf, den Verschlüsselungstyp auszuwählen, bevor BitLocker aktiviert wird.

Referenz

Diese Richtlinieneinstellung wird angewendet, wenn Sie BitLocker aktivieren. Das Ändern des Verschlüsselungstyps hat keine Auswirkungen, wenn das Laufwerk bereits verschlüsselt ist oder wenn die Verschlüsselung durchgeführt wird. Wählen Sie vollständige Verschlüsselung aus, um die Verschlüsselung des gesamten Laufwerks zu erzwingen, wenn BitLocker aktiviert ist. Wählen Sie verwendeter Speicherplatz nur

Verschlüsselung aus, um zu erzwingen, dass nur der Teil des Laufwerks, der zum Speichern von Daten verwendet wird, verschlüsselt ist, wenn BitLocker aktiviert ist.

> **Hinweis:** Diese Richtlinie wird beim Verkleinern oder Erweitern eines Volumes ignoriert, und der BitLocker-Treiber verwendet die aktuelle Verschlüsselungsmethode. Wenn beispielsweise ein Laufwerk, auf dem nur gebrauchte Speicherplatz Verschlüsselung verwendet wird, erweitert wird, wird der neue freie Speicherplatz nicht so gelöscht, wie es bei einem Laufwerk mit vollständiger Verschlüsselung der Fall wäre. Der Benutzer kann den freien Speicherplatz auf einem verwendeten Speicherplatz nur mithilfe des folgenden Befehls löschen: **manage-bde-w**. Wenn die Lautstärke geschrumpft ist, wird für den neuen freien Speicherplatz keine Aktion ausgeführt.

Weitere Informationen zum Tool zum Verwalten von BitLocker finden Sie unter Verwalten von BDE.

Auswählen, wie BitLocker-geschützte Betriebssystemlaufwerke wiederhergestellt werden können

Diese Richtlinieneinstellung wird verwendet, um Wiederherstellungsmethoden für Betriebssystemlaufwerke zu konfigurieren.

Richtlinienbeschreibung	Mit dieser Richtlinieneinstellung können Sie steuern, wie BitLocker-geschützte Betriebssystemlaufwerke wiederhergestellt werden, ohne dass die erforderlichen Startschlüssel Informationen vorhanden sind.
Eingeführt	Windows Server 2008 R2 und Windows 7
Laufwerktyp	Betriebssystemlaufwerke
Richtlinienpfad	Computer Configuration\Administrative Vorlagen\Windows-Komponenten\Internet BitLocker-Laufwerkverschlüsselung Drive Encryption\Operating System Laufwerke
Konflikte	Sie müssen die Verwendung von Wiederherstellungsschlüsseln **verweigern, wenn die Einstellung Schreibzugriff auf Wechseldatenträger,** die nicht von der BitLocker-Richtlinie geschützt werden, aktiviert ist. Wenn Sie Daten Wiederherstellungs-Agents verwenden, **müssen Sie die Richtlinieneinstellung die eindeutigen** IDs für Ihre Organisation bereitstellen aktivieren.
Wenn aktiviert	Sie können die Methoden steuern, die Benutzern zur Wiederherstellung von Daten aus von BitLocker geschützten Betriebssystemlaufwerken zur Verfügung stehen.

Wenn deaktiviert oder nicht konfiguriert	Die Standardwiederherstellungsoptionen werden für die BitLocker-Wiederherstellung unterstützt. Standardmäßig ist ein Daten Wiederherstellungs-Agent zulässig, die Wiederherstellungsoptionen können vom Benutzer festgelegt werden (einschließlich des Wiederherstellungskennworts und des Wiederherstellungsschlüssels), und Wiederherstellungsinformationen werden nicht in AD DS gesichert.

Referenz

Diese Richtlinieneinstellung wird angewendet, wenn Sie BitLocker aktivieren.

Das Kontrollkästchen **Daten Wiederherstellungs-Agent zulassen** wird verwendet, um anzugeben, ob ein Daten Wiederherstellungs-Agent mit mit BitLocker geschützten Betriebssystemlaufwerken verwendet werden kann. Bevor ein Daten Wiederherstellungs-Agent verwendet werden kann, muss er aus **Richtlinien für öffentliche Schlüssel**hinzugefügt werden, die sich in der Gruppenrichtlinien-Verwaltungskonsole (Group Policy Management Console, GPMC) oder im Editor für lokale Gruppenrichtlinien befinden.

Weitere Informationen zum Hinzufügen von Daten Wiederherstellungs-Agents finden Sie unter BitLocker Basic Deployment.

Wählen Sie unter **Konfigurieren des Benutzerspeichers von BitLocker-Wiederherstellungsinformationen**aus, ob Benutzer zulässig, erforderlich oder nicht berechtigt sind, ein 48-stelliges Wiederherstellungskennwort zu generieren.

Wählen Sie **im BitLocker-Setup-Assistenten die Option Wiederherstellungsoptionen auslassen** aus, um zu verhindern, dass Benutzer Wiederherstellungsoptionen angeben, wenn Sie BitLocker auf einem Laufwerk aktivieren Das bedeutet, dass Sie nicht angeben können, welche Wiederherstellungsoption beim Aktivieren von BitLocker verwendet werden soll. Stattdessen werden die BitLocker-Wiederherstellungsoptionen für das Laufwerk durch die Richtlinieneinstellung bestimmt.

Wählen Sie unter **BitLocker-Wiederherstellungsinformationen in Active Directory-Domänendienste speichern**die BitLocker-Wiederherstellungsinformationen aus, die in Active Directory-Domänendiensten (AD DS) für Betriebssystemlaufwerke gespeichert werden sollen. Wenn Sie " **Wiederherstellungskennwort und Schlüsselpakete speichern**" auswählen, werden das BitLocker-Wiederherstellungskennwort und das Schlüsselpaket in AD DS gespeichert. Das Speichern des Schlüsselpakets unterstützt das erneute Herstellen von Daten von einem physisch beschädigten Laufwerk. Wenn Sie **nur Wiederherstellungskennwort speichern**auswählen, wird nur das Wiederherstellungskennwort in AD DS gespeichert.

Aktivieren Sie das Kontrollkästchen **BitLocker bis Wiederherstellungsinformationen in AD DS für Betriebssystemlaufwerke nicht aktivieren** , wenn Sie verhindern möchten, dass Benutzer BitLocker aktivieren können, es sei denn, der Computer ist mit der Domäne verbunden, und die Sicherung der BitLocker-Wiederherstellungsinformationen in AD DS ist erfolgreich.

> **Hinweis:** Wenn das Kontrollkästchen **BitLocker-bis-Wiederherstellungsinformationen nicht in AD DS für Betriebssystemlaufwerke speichern** aktiviert ist, wird automatisch ein Wiederherstellungskennwort generiert.

Auswählen, wie Benutzer BitLocker-geschützte Laufwerke wiederherstellen können (Windows Server 2008 und Windows Vista)

Diese Richtlinieneinstellung wird verwendet, um Wiederherstellungsmethoden für BitLocker-geschützte Laufwerke auf Computern mit Windows Server 2008 oder Windows Vista zu konfigurieren.

Richtlinienbeschreibung	Mit dieser Richtlinieneinstellung können Sie steuern, ob der BitLocker-Setup-Assistent BitLocker-Wiederherstellungsoptionen anzeigen und angeben kann.
Eingeführt	Windows Server 2008 und Windows Vista
Laufwerktyp	Betriebssystemlaufwerke und fest Netzlaufwerke auf Computern unter Windows Server 2008 und Windows Vista
Richtlinienpfad	Computer Configuration\Administrative Vorlagen\Windows-Komponenten\Internet BitLocker-Laufwerkverschlüsselung Drive Encryption
Konflikte	Diese Richtlinieneinstellung stellt eine administrative Methode zum Zurücksetzen von Daten bereit, die von BitLocker verschlüsselt werden, um Datenverluste aufgrund fehlender Schlüsselinformationen zu verhindern. Wenn Sie **die Option nicht** zulassen für beide Wiederherstellungsoptionen für Benutzer auswählen, müssen Sie **die Richtlinieneinstellung BitLocker-Wiederherstellungsinformationen in Active Directory-Domänendiensten (Windows** Server 2008 und Windows Vista) speichern, um einen Richtlinienfehler zu verhindern.
Wenn aktiviert	Sie können die Optionen konfigurieren, die der BitLocker-Setup-Assistent Benutzern für das erneute Herstellen von BitLocker-verschlüsselten Daten anzeigt.
Wenn deaktiviert oder nicht konfiguriert	Der BitLocker-Setup-Assistent bietet Benutzern die Möglichkeit, Wiederherstellungsoptionen zu speichern.

Referenz

Diese Richtlinie gilt nur für Computer mit Windows Server 2008 oder Windows Vista. Diese Richtlinieneinstellung wird angewendet, wenn Sie BitLocker aktivieren.

Zwei Wiederherstellungsoptionen können verwendet werden, um BitLocker-verschlüsselte Daten zu entsperren, wenn keine erforderlichen Startschlüssel Informationen vorhanden sind. Benutzer können ein 48-stelliges Kennwort für die numerische Wiederherstellung eingeben, oder Sie können ein USB-Laufwerk einfügen, das einen 256-Bit-Wiederherstellungsschlüssel enthält.

Wenn Sie das Wiederherstellungskennwort auf einem USB-Laufwerk speichern, wird das 48-stellige Wiederherstellungskennwort als Textdatei und der 256-Bit-Wiederherstellungsschlüssel als versteckte Datei gespeichert. Beim Speichern in einem Ordner wird das 48-stellige Wiederherstellungskennwort als Textdatei gespeichert. Beim Drucken wird das 48-stellige Wiederherstellungskennwort an den Standarddrucker gesendet. Wenn Sie beispielsweise das 48-stellige Wiederherstellungskennwort nicht zulassen, wird verhindert, dass Benutzer die Wiederherstellungsinformationen in einem Ordner drucken oder speichern.

> **Wichtig:** Wenn die TPM-Initialisierung während des BitLocker-Setups durchgeführt wird, werden TPM-Besitzerinformationen mit den BitLocker-Wiederherstellungsinformationen gespeichert oder gedruckt. Das

48-stellige Wiederherstellungskennwort steht im FIPS-Konformitäts Modus nicht zur Verfügung.

Wichtig: Um Datenverluste zu vermeiden, müssen Sie eine Möglichkeit zum Wiederherstellen von BitLocker-Verschlüsselungsschlüsseln haben. Wenn Sie nicht beide Wiederherstellungsoptionen zulassen, müssen Sie die Sicherung der BitLocker-Wiederherstellungsinformationen in AD DS aktivieren. Andernfalls tritt ein Richtlinienfehler auf.

Speichern von BitLocker-Wiederherstellungsinformationen in den Active Directory-Domänendiensten (Windows Server 2008 und Windows Vista)

Diese Richtlinieneinstellung wird verwendet, um die Speicherung von BitLocker-Wiederherstellungsinformationen in AD DS zu konfigurieren. Dies stellt eine administrative Methode zur Verfügung, die von BitLocker verschlüsselte Daten zurückgibt, um Datenverluste aufgrund fehlender Schlüsselinformationen zu verhindern.

Richtlinienbeschreibung	Mit dieser Richtlinieneinstellung können Sie die AD DS-Sicherung der Wiederherstellungsinformationen für BitLocker-Laufwerksverschlüsselung verwalten.
Eingeführt	Windows Server 2008 und Windows Vista
Laufwerktyp	Betriebssystemlaufwerke und fest Netzlaufwerke auf Computern unter Windows Server 2008 und Windows Vista.
Richtlinienpfad	Computer Configuration\Administrative Vorlagen\Windows-Komponenten\Internet BitLocker-Laufwerkverschlüsselung Drive Encryption
Konflikte	Keine
Wenn aktiviert	BitLocker-Wiederherstellungsinformationen werden automatisch und lautlos in AD DS gesichert, wenn BitLocker für einen Computer aktiviert ist.
Wenn deaktiviert oder nicht konfiguriert	BitLocker-Wiederherstellungsinformationen werden nicht in AD DS gesichert.

Referenz

Diese Richtlinie gilt nur für Computer mit Windows Server 2008 oder Windows Vista.

Diese Richtlinieneinstellung wird angewendet, wenn Sie BitLocker aktivieren.

Zu den BitLocker-Wiederherstellungsinformationen gehören das Wiederherstellungskennwort und eindeutige bezeichnerdaten. Sie können auch ein Paket einbeziehen, das einen Verschlüsselungsschlüssel für ein mit BitLocker geschütztes Laufwerk enthält. Dieses Schlüsselpaket wird durch ein oder mehrere Wiederherstellungskennwörter gesichert, und es kann helfen, eine spezielle Wiederherstellung durchzuführen, wenn der Datenträger beschädigt oder beschädigt ist.

Wenn Sie **BitLocker-Sicherung für AD DS anfordern**auswählen, kann BitLocker nicht aktiviert werden, es sei denn, der Computer ist mit der Domäne verbunden, und die Sicherung der BitLocker-Wiederherstellungsinformationen für AD DS ist erfolgreich. Diese Option ist standardmäßig aktiviert, um

sicherzustellen, dass die BitLocker-Wiederherstellung möglich ist.

Ein Wiederherstellungskennwort ist eine 48-stellige Zahl, die den Zugriff auf ein mit BitLocker geschütztes Laufwerk aufhebt. Ein Schlüsselpaket enthält den BitLocker-Verschlüsselungsschlüssel eines Laufwerks, der durch ein oder mehrere Wiederherstellungskennwörter gesichert wird. Schlüsselpakete können dazu beitragen, eine spezielle Wiederherstellung durchzuführen, wenn der Datenträger beschädigt oder beschädigt ist.

Wenn die Option **BitLocker-Sicherung in AD DS anfordern** nicht aktiviert ist, wird die AD DS-Sicherung versucht, aber Netzwerk-oder andere Sicherungsfehler verhindern nicht das BitLocker-Setup. Der Sicherungsvorgang wird nicht automatisch wiederholt, und das Wiederherstellungskennwort wird während des BitLocker-Setups möglicherweise nicht in AD DS gespeichert. Die TPM-Initialisierung ist möglicherweise während des BitLocker-Setups erforderlich. Aktivieren Sie die Richtlinieneinstellung **TPM-Sicherung in Active Directory-Domänendienste** aktivieren in **Computer Configuration\Administrative Templates\System\Trusted Platform Module Services** , um sicherzustellen, dass auch TPM-Informationen gesichert werden.

Weitere Informationen zu dieser Einstellung finden Sie unter TPM-Gruppenrichtlinieneinstellungen.

Standardordner für Wiederherstellungskennwort auswählen

Diese Richtlinieneinstellung wird verwendet, um den Standardordner für Wiederherstellungskennwörter zu konfigurieren.

Richtlinienbeschreibung	Mit dieser Richtlinieneinstellung können Sie den Standardpfad angeben, der angezeigt wird, wenn der BitLocker-Setup-Assistent den Benutzer auffordert, den Speicherort eines Ordners einzugeben, in dem das Wiederherstellungskennwort gespeichert werden soll.
Eingeführt	Windows Vista
Laufwerktyp	Alle Laufwerke
Richtlinienpfad	Computer Configuration\Administrative Vorlagen\Windows-Komponenten\Internet BitLocker-Laufwerkverschlüsselung Drive Encryption
Konflikte	Keine
Wenn aktiviert	Sie können den Pfad angeben, der als Standardspeicherort für den Ordner verwendet werden soll, wenn der Benutzer die Option zum Speichern des Wiederherstellungskennworts in einem Ordner auswählt. Sie können einen vollqualifizierten Pfad angeben oder die Umgebungsvariablen des Zielcomputers's in den Pfad einbeziehen. Wenn der Pfad ungültig ist, zeigt der BitLocker-Setup-Assistent die Ordneransicht auf oberster Ebene des Computers'an.
Wenn deaktiviert oder nicht konfiguriert	Der BitLocker-Setup-Assistent zeigt die Ordneransicht der obersten Ebene des Computers'an, wenn der Benutzer die Option zum Speichern des Wiederherstellungskennworts in einem Ordner auswählt.

Referenz

Diese Richtlinieneinstellung wird angewendet, wenn Sie BitLocker aktivieren.

> **Hinweis:** Diese Richtlinieneinstellung verhindert nicht, dass der Benutzer das Wiederherstellungskennwort in einem anderen Ordner speichert.

Auswählen, wie BitLocker-geschützte Festplatten wiederhergestellt werden können

Diese Richtlinieneinstellung wird verwendet, um Wiederherstellungsmethoden für feste Datenlaufwerke zu konfigurieren.

Richtlinienbeschreibung	Mit dieser Richtlinieneinstellung können Sie steuern, wie BitLocker-geschützte fest Netzlaufwerke wiederhergestellt werden, ohne dass die erforderlichen Anmeldeinformationen vorhanden sind.
Eingeführt	Windows Server 2008 R2 und Windows 7
Laufwerktyp	Feste Datenlaufwerke
Richtlinienpfad	Computer Configuration\Administrative Vorlagen\Windows-Komponenten\Internet BitLocker-Laufwerkverschlüsselung Drive Encryption\Fixed Datenlaufwerke
Konflikte	Sie müssen die Verwendung von Wiederherstellungsschlüsseln **verweigern, wenn die Einstellung Schreibzugriff auf Wechseldatenträger,** die nicht von der BitLocker-Richtlinie geschützt werden, aktiviert ist. Wenn Sie Daten Wiederherstellungs-Agents verwenden, müssen Sie **die Richtlinieneinstellung die eindeutigen IDs für** Ihre Organisation bereitstellen aktivieren und konfigurieren.
Wenn aktiviert	Sie können die Methoden steuern, die Benutzern zur Wiederherstellung von Daten aus durch BitLocker geschützten festen Datenlaufwerken zur Verfügung stehen.
Wenn deaktiviert oder nicht konfiguriert	Die Standardwiederherstellungsoptionen werden für die BitLocker-Wiederherstellung unterstützt. Standardmäßig ist ein Daten Wiederherstellungs-Agent zulässig, die Wiederherstellungsoptionen können vom Benutzer festgelegt werden (einschließlich des Wiederherstellungskennworts und des Wiederherstellungsschlüssels), und Wiederherstellungsinformationen werden nicht in AD DS gesichert.

Referenz

Diese Richtlinieneinstellung wird angewendet, wenn Sie BitLocker aktivieren.

Das Kontrollkästchen **Daten Wiederherstellungs-Agent zulassen** wird verwendet, um anzugeben, ob ein Daten Wiederherstellungs-Agent mit mit BitLocker geschützten festen Datenlaufwerken verwendet werden kann. Bevor ein Daten Wiederherstellungs-Agent verwendet werden kann, muss er aus **Richtlinien für öffentliche Schlüssel**hinzugefügt werden, die sich in der Gruppenrichtlinien-Verwaltungskonsole (Group Policy Management Console, GPMC) oder im Editor für lokale Gruppenrichtlinien befinden.

Wählen Sie unter **Konfigurieren des Benutzerspeichers von BitLocker-Wiederherstellungsinformationen**aus, ob Benutzer zulässig, erforderlich oder nicht berechtigt sind, ein 48-stelliges Wiederherstellungskennwort oder einen 256-Bit-Wiederherstellungsschlüssel zu generieren.

Wählen Sie **im BitLocker-Setup-Assistenten die Option Wiederherstellungsoptionen auslassen** aus, um zu verhindern, dass Benutzer Wiederherstellungsoptionen angeben, wenn Sie BitLocker auf einem Laufwerk aktivieren Das bedeutet, dass Sie bei der Aktivierung von BitLocker nicht angeben können, welche Wiederherstellungsoption verwendet werden soll. Stattdessen werden die BitLocker-Wiederherstellungsoptionen für das Laufwerk durch die Richtlinieneinstellung bestimmt.

Wählen Sie unter **BitLocker-Wiederherstellungsinformationen in Active Directory-Domänendienste speichern**die BitLocker-Wiederherstellungsinformationen aus, die in AD DS für feste Datenlaufwerke gespeichert werden sollen. Wenn Sie das **Kennwort für die Sicherungswiederherstellung und das Schlüsselpaket**auswählen, werden das BitLocker-Wiederherstellungskennwort und das Schlüsselpaket in AD DS gespeichert. Das Speichern des Schlüsselpakets unterstützt das erneute Herstellen von Daten von einem physisch beschädigten Laufwerk. Zum Wiederherstellen dieser Daten können Sie das Befehlszeilentool **Repair-bde** verwenden. Wenn Sie **nur Backup-Wiederherstellungskennwort**auswählen, wird nur das Wiederherstellungskennwort in AD DS gespeichert.

Weitere Informationen zum BitLocker-Reparaturtool finden Sie unter Repair-bde.

Aktivieren Sie das Kontrollkästchen **BitLocker bis Wiederherstellungsinformationen in AD DS für feste Datenlaufwerke nicht aktivieren** , wenn Sie verhindern möchten, dass Benutzer BitLocker aktivieren können, es sei denn, der Computer ist mit der Domäne verbunden, und die Sicherung der BitLocker-Wiederherstellungsinformationen in AD DS ist erfolgreich.

> **Hinweis:** Wenn das Kontrollkästchen **BitLocker-bis-Wiederherstellungsinformationen nicht in AD DS für feste Datenlaufwerke speichern** aktiviert ist, wird automatisch ein Wiederherstellungskennwort generiert.

Auswählen, wie BitLocker-geschützte Wechsellaufwerke wiederhergestellt werden können

Diese Richtlinieneinstellung wird verwendet, um Wiederherstellungsmethoden für Wechseldaten Laufwerke zu konfigurieren.

Richtlinienbeschreibung	Mit dieser Richtlinieneinstellung können Sie steuern, wie BitLocker-geschützte Wechseldaten Laufwerke wiederhergestellt werden, ohne dass die erforderlichen Anmeldeinformationen vorhanden sind.
Eingeführt	Windows Server 2008 R2 und Windows 7
Laufwerktyp	Austauschbare Datenlaufwerke

Richtlinienpfad	Computer Configuration\Administrative Vorlagen\Windows-Komponenten\Internet BitLocker-Laufwerkverschlüsselung Drive Encryption\Removable Datenlaufwerke
Konflikte	Sie müssen die Verwendung von Wiederherstellungsschlüsseln **verweigern, wenn die Einstellung Schreibzugriff auf Wechseldatenträger,** die nicht von der BitLocker-Richtlinie geschützt werden, aktiviert ist. Wenn Sie Daten Wiederherstellungs-Agents verwenden, müssen Sie **die Richtlinieneinstellung die eindeutigen IDs für** Ihre Organisation bereitstellen aktivieren und konfigurieren.
Wenn aktiviert	Sie können die Methoden steuern, die für Benutzer verfügbar sind, um Daten aus von BitLocker geschützten Wechseldaten Laufwerken wiederherzustellen.
Wenn deaktiviert oder nicht konfiguriert	Die Standardwiederherstellungsoptionen werden für die BitLocker-Wiederherstellung unterstützt. Standardmäßig ist ein Daten Wiederherstellungs-Agent zulässig, die Wiederherstellungsoptionen können vom Benutzer festgelegt werden (einschließlich des Wiederherstellungskennworts und des Wiederherstellungsschlüssels), und Wiederherstellungsinformationen werden nicht in AD DS gesichert.

Referenz

Diese Richtlinieneinstellung wird angewendet, wenn Sie BitLocker aktivieren.

Das Kontrollkästchen **Daten Wiederherstellungs-Agent zulassen** wird verwendet, um anzugeben, ob ein Daten Wiederherstellungs-Agent mit von BitLocker geschützten Wechseldaten Laufwerken verwendet werden kann. Bevor ein Daten Wiederherstellungs-Agent verwendet werden kann, muss er aus **Richtlinien für öffentliche Schlüssel** hinzugefügt werden, auf die über die GPMC oder den Editor für lokale Gruppenrichtlinien zugegriffen wird.

Wählen Sie unter **Konfigurieren des Benutzerspeichers von BitLocker-Wiederherstellungsinformationen**aus, ob Benutzer zulässig, erforderlich oder nicht berechtigt sind, ein 48-stelliges Wiederherstellungskennwort zu generieren.

Wählen Sie **im BitLocker-Setup-Assistenten die Option Wiederherstellungsoptionen auslassen** aus, um zu verhindern, dass Benutzer Wiederherstellungsoptionen angeben, wenn Sie BitLocker auf einem Laufwerk aktivieren Das bedeutet, dass Sie bei der Aktivierung von BitLocker nicht angeben können, welche Wiederherstellungsoption verwendet werden soll. Stattdessen werden die BitLocker-Wiederherstellungsoptionen für das Laufwerk durch die Richtlinieneinstellung bestimmt.

Wählen Sie unter **BitLocker-Wiederherstellungsinformationen in Active Directory-Domänendienste speichern**die BitLocker-Wiederherstellungsinformationen aus, die in AD DS für Wechseldaten Laufwerke gespeichert werden sollen. Wenn Sie das **Kennwort für die Sicherungswiederherstellung und das Schlüsselpaket**auswählen, werden das BitLocker-Wiederherstellungskennwort und das Schlüsselpaket in AD DS gespeichert. Wenn Sie **nur Backup-Wiederherstellungskennwort**auswählen, wird nur das Wiederherstellungskennwort in AD DS gespeichert.

Aktivieren Sie das Kontrollkästchen **BitLocker bis Wiederherstellungsinformationen in AD DS für Wechseldatenträger nicht aktivieren** , wenn Sie verhindern möchten, dass Benutzer BitLocker aktivieren, wenn der Computer mit der Domäne verbunden ist und die Sicherung der BitLocker-Wiederherstellungsinformationen für AD DS erfolgreich ist.

> **Hinweis:** Wenn das Kontrollkästchen **BitLocker-bis-Wiederherstellungsinformationen nicht in AD DS für feste Datenlaufwerke speichern** aktiviert ist, wird automatisch ein Wiederherstellungskennwort generiert.

Konfigurieren der Nachricht und der URL für die Pre-Boot-Wiederherstellung

Diese Richtlinieneinstellung wird verwendet, um die gesamte Wiederherstellungs Nachricht zu konfigurieren und die vorhandene URL zu ersetzen, die beim Sperren des Betriebssystemlaufwerks auf dem Bildschirm "Pre-Boot-Wiederherstellung" angezeigt wird.

Richtlinienbeschreibung	Mit dieser Richtlinieneinstellung können Sie den BitLocker-Wiederherstellungsbildschirm so konfigurieren, dass eine benutzerdefinierte Nachricht und eine angepasste URL angezeigt werden.
Eingeführt	Windows 10
Laufwerktyp	Betriebssystemlaufwerke
Richtlinienpfad	Computer Konfiguration \ administrative Vorlagen \ Windows-Komponenten \ BitLocker-Laufwerkverschlüsselung \ Betriebs System Laufwerke \ Konfigurieren der vor-Start-Wiederherstellungs Nachricht und-URL
Konflikte	Keine
Wenn aktiviert	Die angepasste Nachricht und die URL werden auf dem Bildschirm "Pre-Boot Recovery" angezeigt. Wenn Sie zuvor eine benutzerdefinierte Wiederherstellungs Nachricht und-URL aktiviert haben und die Standardnachricht und-URL wiederherstellen möchten, müssen Sie die Richtlinieneinstellung aktiviert **lassen und die Option Standard Wiederherstellungs Nachricht und-URL** verwenden auswählen.
Wenn deaktiviert oder nicht konfiguriert	Wenn die Einstellung zuvor nicht aktiviert wurde, wird der standardmäßige Pre-Boot-Wiederherstellungsbildschirm für die BitLocker-Wiederherstellung angezeigt. Wenn die Einstellung zuvor aktiviert und anschließend deaktiviert wurde, wird die letzte Nachricht in Startkonfigurationsdaten (Start Configuration Data, BCD) angezeigt, ob es sich um die standardmäßige Wiederherstellungs Nachricht oder die benutzerdefinierte Nachricht handelt.

Referenz

Wenn Sie die Einstellungen für die **Konfiguration der Wiederherstellungs Nachricht und der URL-** Richtlinie konfigurieren aktivieren, können Sie die Standardnachricht für den Wiederherstellungsbildschirm und die URL anpassen, um Kunden bei der Wiederherstellung Ihres Schlüssels zu unterstützen.

Nachdem Sie die Einstellung aktiviert haben, gibt es drei Optionen:

- Wenn Sie die Option **Standard Wiederherstellungs Nachricht und-URL verwenden** auswählen, werden die standardmäßige BitLocker-Wiederherstellungs Nachricht und die URL auf dem Bildschirm "Pre-Boot Recovery" angezeigt.
- Wenn Sie die Option **benutzerdefinierte Wiederherstellungs Nachricht verwenden** aktivieren, geben Sie die benutzerdefinierte Meldung in das Textfeld **benutzerdefinierte Wiederherstellungs Nachricht** ein. Die Nachricht, die Sie in das Textfeld **benutzerdefinierte Wiederherstellungs Nachricht** eingeben, wird auf dem Bildschirm "Pre-Boot Recovery" angezeigt. Wenn eine Wiederherstellungs-URL verfügbar ist, fügen Sie Sie in die Nachricht ein.
- Wenn Sie die Option **benutzerdefinierte Wiederherstellungs-URL verwenden** auswählen, geben Sie die benutzerdefinierte Nachrichten-URL in das Textfeld **benutzerdefinierte Wiederherstellungs-URL** ein. Die URL, die Sie im Textfeld **benutzerdefinierte Wiederherstellungs-URL** eingeben, ersetzt die Standard-URL in der standardmäßigen Wiederherstellungs Nachricht, die auf dem Bildschirm "Pre-Boot Recovery" angezeigt wird.

> **Wichtig:** Nicht alle Zeichen und Sprachen werden in der Pre-Boot-Umgebung unterstützt. Wir empfehlen dringend, dass Sie die richtige Darstellung der Zeichen überprüfen, die Sie für die benutzerdefinierte Nachricht und die URL auf dem Bildschirm "Pre-Boot Recovery" verwenden.
>
> **Wichtig:** Da Sie die bcdedit-Befehle manuell ändern können, bevor Sie Gruppenrichtlinieneinstellungen festgelegt haben, können Sie die Richtlinieneinstellung nicht auf die Standardeinstellung zurücksetzen, indem Sie die Option **nicht konfiguriert** auswählen, nachdem Sie diese Richtlinieneinstellung konfiguriert haben. Um zum standardmäßigen Pre-Boot-Wiederherstellungsbildschirm zurückzukehren, lassen Sie die Richtlinieneinstellung aktiviert, und wählen Sie im Dropdown-Listenfeld **Wählen Sie eine Option für die Option " Standardnachrichten verwenden** " aus.

Sicheren Start für Integritätsüberprüfung zulassen

Diese Richtlinie steuert, wie BitLocker-fähige Systemdatenträger in Verbindung mit dem Secure Boot-Feature verarbeitet werden. Durch Aktivieren dieses Features wird die sichere Start Überprüfung während des Startvorgangs erzwungen, und die Einstellungen für die Startkonfigurationsdaten (BCD) werden gemäß der sicheren Startrichtlinie überprüft.

Richtlinienbeschreibung	Mit dieser Richtlinieneinstellung können Sie konfigurieren, ob der sichere Start als Platt Form Integritäts Anbieter für BitLocker-Betriebssystemlaufwerke zulässig ist.
Eingeführt	Windows Server 2012 und Windows 8
Laufwerktyp	Alle Laufwerke
Richtlinienpfad	Computer Configuration\Administrative Vorlagen\Windows-Komponenten\Internet BitLocker-Laufwerkverschlüsselung Drive Encryption\Operating System Laufwerke

Konflikte	Wenn Sie die **Option sicheren Start für die Integritätsprüfung**zulassen aktivieren **, stellen Sie sicher, dass die Gruppenrichtlinieneinstellung** TPM-plattformüberprüfung für die systemeigene UEFI-Firmware-Konfiguration nicht aktiviert ist oder PCR 7 enthält, um BitLocker die Verwendung von Secure Boot für Platform-oder BCD-Integritätsüberprüfung zu ermöglichen. Weitere Informationen zu PCR 7 finden Sie unter Platform Configuration Register (PCR) in diesem Thema.
Wenn aktiviert oder nicht konfiguriert	BitLocker verwendet den sicheren Start für die Plattformintegrität, wenn die Plattform eine sichere Start basierte Integritätsüberprüfung durchlaufen kann.
Wenn deaktiviert	BitLocker verwendet die Überprüfung der Legacy-Plattformintegrität, sogar auf Systemen, die eine sichere Boot basierte Integritätsüberprüfung aufweisen können.

Referenz

Beim sicheren Start wird sichergestellt, dass die Preboot-Umgebung des Computers nur die Firmware lädt, die von autorisierten Softwareherausgebern digital signiert wurde. Der sichere Start bietet außerdem mehr Flexibilität bei der Verwaltung von Preboot-Konfigurationen als bei BitLocker-Integritätsprüfungen vor Windows Server 2012 und Windows 8. Wenn diese Richtlinie aktiviert ist und die Hardware in der Lage ist, Secure Boot für BitLocker-Szenarien zu verwenden, wird die Gruppenrichtlinieneinstellung **use Enhanced Boot Configuration Data Validation profile** ignoriert, und Secure Boot überprüft die BCD-Einstellungen gemäß der Einstellung für sichere Start Richtlinien, die separat von BitLocker konfiguriert ist.

> **Warnung:** Das Aktivieren dieser Richtlinie kann zur BitLocker-Wiederherstellung führen, wenn herstellerspezifische Firmware aktualisiert wird. Wenn Sie diese Richtlinie deaktivieren, Sperren Sie BitLocker vor dem Anwenden von Firmware-Updates.

Bereitstellen der eindeutigen Bezeichner für Ihre Organisation

Diese Richtlinieneinstellung wird verwendet, um einen Bezeichner festzulegen, der auf alle Laufwerke angewendet wird, die in Ihrer Organisation verschlüsselt sind.

Richtlinienbeschreibung	Mit dieser Richtlinieneinstellung können Sie einem neuen Laufwerk, das mit BitLocker aktiviert ist, eindeutige Organisations-IDs zuordnen.
Eingeführt	Windows Server 2008 R2 und Windows 7
Laufwerktyp	Alle Laufwerke
Richtlinienpfad	Computer Configuration\Administrative Vorlagen\Windows-Komponenten\Internet BitLocker-Laufwerkverschlüsselung Drive Encryption

Konflikte	Für die Verwaltung zertifikatbasierter Daten Wiederherstellungs-Agents auf durch BitLocker geschützten Laufwerken sind Identifikations Felder erforderlich. BitLocker verwaltet und aktualisiert zertifikatbasierte Daten Wiederherstellungs-Agents nur, wenn das ID-Feld auf einem Laufwerk vorhanden ist und identisch mit dem auf dem Computer konfigurierten Wert ist.
Wenn aktiviert	Sie können das Feld "Identifikation" auf dem mit BitLocker geschützten Laufwerk und alle zulässigen Identifikations Felder konfigurieren, die von Ihrer Organisation verwendet werden.
Wenn deaktiviert oder nicht konfiguriert	Das Feld "Identifikation" ist nicht erforderlich.

Referenz

Diese Bezeichner werden als Identifikationsfeld und das Feld zulässige Identifikation gespeichert. Das Feld "Identifikation" ermöglicht es Ihnen, BitLocker-geschützten Laufwerken eine eindeutige Organisations-ID zuzuordnen. Dieser Bezeichner wird automatisch zu neuen durch BitLocker geschützten Laufwerken hinzugefügt und kann mithilfe des Befehlszeilentools manage-bde auf vorhandenen BitLocker-geschützten Laufwerken aktualisiert werden.

Zum Verwalten von zertifikatbasierten Daten Wiederherstellungs-Agents auf von BitLocker geschützten Laufwerken und für potenzielle Updates des BitLocker To Go-Readers ist ein Identifikationsfeld erforderlich. BitLocker verwaltet und aktualisiert Daten Wiederherstellungs-Agents nur, wenn das Identifikationsfeld auf dem Laufwerk mit dem Wert übereinstimmt, der im Feldidentifizierung konfiguriert ist. Auf ähnliche Weise aktualisiert BitLocker den BitLocker To Go-Reader nur, wenn das ID-Feld auf dem Laufwerk dem Wert entspricht, der für das ID-Feld konfiguriert ist.

Weitere Informationen zum Tool zum Verwalten von BitLocker finden Sie unter Verwalten von BDE.

Das Feld zulässige Identifikation wird in Kombination mit der Einstellung **Schreibzugriff auf Wechseldatenträger, die nicht von der BitLocker** -Richtlinie geschützt werden, verwendet, um die Verwendung von Wechseldatenträgern in Ihrer Organisation zu steuern. Hierbei handelt es sich um eine durch trennzeichengetrennte Liste der Identifizierungs Felder in Ihrer Organisation oder in externen Organisationen.

Sie können die Identifikations Felder auf vorhandenen Laufwerken mithilfe des Befehlszeilentools manage-bde konfigurieren.

Wenn ein von BitLocker geschütztes Laufwerk auf einem anderen BitLocker-fähigen Computer bereitgestellt wird, werden das Feld "ID" und das Feld "zulässige Identifikation" verwendet, um zu ermitteln, ob das Laufwerk von einer externen Organisation stammt.

Mehrere durch Kommas getrennte Werte können in die Felder Identifikation und zulässige Identifikation eingegeben werden. Das Feld "ID" kann ein beliebiger Wert bis zu 260 Zeichen sein.

Verhindern, dass beim Neustart Speicher überschrieben wird

Diese Richtlinieneinstellung wird verwendet, um zu steuern, ob der Arbeitsspeicher des Computers beim nächsten Neustart des Computers überschrieben wird.

Richtlinienbeschreibung	Mit dieser Richtlinieneinstellung können Sie die Leistung des Computerstarts steuern, um BitLocker-Geheimnisse verfügbar zu machen.
Eingeführt	Windows Vista
Laufwerktyp	Alle Laufwerke
Richtlinienpfad	Computer Configuration\Administrative Vorlagen\Windows-Komponenten\Internet BitLocker-Laufwerkverschlüsselung Drive Encryption
Konflikte	Keine
Wenn aktiviert	Beim Neustart des Computers wird der Arbeitsspeicher nicht überschrieben. Das verhindern von Speicherüberschreibungen kann die Neustart Leistung verbessern, erhöht aber das Risiko, BitLocker-Geheimnisse verfügbar zu machen.
Wenn deaktiviert oder nicht konfiguriert	BitLocker-Geheimnisse werden beim Neustart des Computers aus dem Arbeitsspeicher entfernt.

Referenz

Diese Richtlinieneinstellung wird angewendet, wenn Sie BitLocker aktivieren. Zu den BitLocker-Geheimnissen gehören Schlüsselmaterialien, die zum Verschlüsseln von Daten verwendet werden. Diese Richtlinieneinstellung gilt nur, wenn der BitLocker-Schutz aktiviert ist.

Konfigurieren des TPM-Platt Form Überprüfungsprofils für BIOS-basierte Firmware-Konfigurationen

Diese Richtlinieneinstellung bestimmt, welche Werte das TPM misst, wenn es frühe Startkomponenten überprüft, bevor es ein Betriebssystemlaufwerk auf einem Computer mit einer BIOS-Konfiguration oder mit UEFI-Firmware aufhebt, die das Compatibility Support Module (CSM) aktiviert hat.

Richtlinienbeschreibung	Mit dieser Richtlinieneinstellung können Sie konfigurieren, wie die TPM-Sicherheitshardware des Computers'den BitLocker-Verschlüsselungsschlüssel sichert.
Eingeführt	Windows Server 2012 und Windows 8
Laufwerktyp	Betriebssystemlaufwerke
Richtlinienpfad	Computer Configuration\Administrative Vorlagen\Windows-Komponenten\Internet BitLocker-Laufwerkverschlüsselung Drive Encryption\Operating System Laufwerke

Konflikte	Keine
Wenn aktiviert	Sie können die Startkomponenten konfigurieren, die das TPM überprüft, bevor der Zugriff auf das BitLocker-verschlüsselte Betriebssystemlaufwerk aufgehoben wird. Wenn sich eine dieser Komponenten ändert, während der BitLocker-Schutz aktiviert ist, gibt das TPM den Verschlüsselungsschlüssel zum Entsperren des Laufwerks nicht frei. Stattdessen zeigt der Computer die BitLocker-Wiederherstellungskonsole an und setzt voraus, dass das Wiederherstellungskennwort oder der Wiederherstellungsschlüssel zum Entsperren des Laufwerks bereitgestellt wird.
Wenn deaktiviert oder nicht konfiguriert	Das TPM verwendet das Standardprofil für die plattformüberprüfung oder das Platt Form Überprüfungsprofil, das vom Setupskript angegeben wird.

Referenz

Diese Richtlinieneinstellung trifft nicht zu, wenn der Computer nicht über ein kompatibles TPM verfügt oder wenn BitLocker bereits mit TPM-Schutz aktiviert wurde.

> **Wichtig:** Diese Gruppenrichtlinieneinstellung gilt nur für Computer mit BIOS-Konfigurationen oder für Computer mit UEFI-Firmware, wobei CSM aktiviert ist. Computer, die eine systemeigene UEFI-Firmware-Konfiguration verwenden, speichern unterschiedliche Werte in den Platform Configuration Registers (PCRs). Verwenden Sie das **TPM-Platt Form Überprüfungsprofil für systemeigene UEFI-Firmware-Konfigurationen konfigurieren** , um das TPM-PCR-Profil für Computer zu konfigurieren, die die systemeigene UEFI-Firmware verwenden.

Ein Platt Form Überprüfungsprofil besteht aus einer Reihe von PCR-Indizes, die zwischen 0 und 23 liegen. Das Standardprofil der plattformüberprüfung sichert den Verschlüsselungsschlüssel vor Änderungen an den folgenden:

- Core Root of Trust of measurement (CRTM), BIOS und Plattformerweiterungen (PCR 0)
- Option ROM-Code (PCR 2)
- Master Boot Record (MBR)-Code (PCR 4)
- NTFS-Boot Sektor (PCR 8)
- NTFS-Start Block (PCR 9)
- Boot-Manager (PCR 10)
- BitLocker-Zugriffssteuerung (PCR 11)

> **Hinweis:** Das Ändern des standardmäßigen Platt Form Überprüfungsprofils wirkt sich auf die Sicherheit und Verwaltbarkeit Ihres Computers aus. Die Vertraulichkeit von BitLocker für Plattformänderungen (böswillig oder autorisiert) wird je nach Inklusion oder Ausschluss (beziehungsweise) des PCRs erhöht oder verringert.

In der folgenden Liste sind alle verfügbaren PCRs aufgeführt:

- PCR 0: Core Root-of-Trust für Measurement-, BIOS-und Platform-Erweiterungen
- PCR 1: Konfiguration von Plattformen und Motherboards und Daten.
- PCR 2: Option ROM-Code

- PCR 3: Option ROM-Daten und-Konfiguration
- PCR 4: Master Boot Record (MBR)-Code
- PCR 5: Partitionstabelle für Master Boot Record (MBR)
- PCR 6: Zustandsübergangs-und Aktivierungsereignisse
- PCR 7: Computer herstellerspezifisch
- PCR 8: NTFS-Bootsektor
- PCR 9: NTFS-Startblock
- PCR 10: Start-Manager
- PCR 11: BitLocker-Zugriffssteuerung
- PCR 12-23: reserviert für zukünftige Verwendung

Konfigurieren des TPM-Platt Form Überprüfungsprofils (Windows Vista, Windows Server 2008, Windows 7, Windows Server 2008 R2)

Diese Richtlinieneinstellung bestimmt, welche Werte das TPM misst, wenn es frühe Startkomponenten überprüft, bevor ein Laufwerk auf einem Computer unter Windows Vista, Windows Server 2008 oder Windows 7 aufgehoben wird.

Richtlinienbeschreibung	Mit dieser Richtlinieneinstellung können Sie konfigurieren, wie die TPM-Sicherheitshardware des Computers'den BitLocker-Verschlüsselungsschlüssel sichert.
Eingeführt	Windows Server 2008 und Windows Vista
Laufwerktyp	Betriebssystemlaufwerke
Richtlinienpfad	Computer Configuration\Administrative Vorlagen\Windows-Komponenten\Internet BitLocker-Laufwerkverschlüsselung Drive Encryption\Operating System Laufwerke
Konflikte	Keine
Wenn aktiviert	Sie können die Startkomponenten konfigurieren, die das TPM überprüft, bevor der Zugriff auf das BitLocker-verschlüsselte Betriebssystemlaufwerk aufgehoben wird. Wenn sich eine dieser Komponenten ändert, während der BitLocker-Schutz aktiviert ist, gibt das TPM den Verschlüsselungsschlüssel zum Entsperren des Laufwerks nicht frei. Stattdessen zeigt der Computer die BitLocker-Wiederherstellungskonsole an und setzt voraus, dass das Wiederherstellungskennwort oder der Wiederherstellungsschlüssel zum Entsperren des Laufwerks bereitgestellt wird.
Wenn deaktiviert oder nicht konfiguriert	Das TPM verwendet das Standardprofil für die plattformüberprüfung oder das Platt Form Überprüfungsprofil, das vom Setupskript angegeben wird.

Referenz

Diese Richtlinieneinstellung trifft nicht zu, wenn der Computer nicht über ein kompatibles TPM verfügt oder wenn BitLocker bereits mit TPM-Schutz aktiviert ist.

Ein Platt Form Überprüfungsprofil besteht aus einer Reihe von PCR-Indizes, die zwischen 0 und 23 liegen. Das Standardprofil der plattformüberprüfung sichert den Verschlüsselungsschlüssel vor Änderungen an den folgenden:

- Core Root of Trust of measurement (CRTM), BIOS und Plattformerweiterungen (PCR 0)
- Option ROM-Code (PCR 2)
- Master Boot Record (MBR)-Code (PCR 4)
- NTFS-Boot Sektor (PCR 8)
- NTFS-Start Block (PCR 9)
- Boot-Manager (PCR 10)
- BitLocker-Zugriffssteuerung (PCR 11)

> **Hinweis:** Die standardmäßigen TPM-Validierungs Profil-PCR-Einstellungen für Computer, die eine erweiterbare Firmware-Schnittstelle (EFI) verwenden, sind nur die PCRS 0, 2, 4 und 11.

In der folgenden Liste sind alle verfügbaren PCRs aufgeführt:

- PCR 0: Core-Trust für Messung, EFI-Start-und Laufzeitdienste, EFI-Treiber, die in System-ROM eingebettet sind, statische ACPI-Tabellen, eingebetteter SMM-Code und BIOS-Code
- PCR 1: Konfiguration von Plattformen und Motherboards und Daten. Hand-Off-Tabellen und EFI-Variablen, die sich auf die Systemkonfiguration auswirken
- PCR 2: Option ROM-Code
- PCR 3: Option ROM-Daten und-Konfiguration
- PCR 4: Master Boot Record (MBR)-Code oder Code von anderen Startgeräten
- PCR 5: Partitionstabelle für Master Boot Record (MBR). Verschiedene EFI-Variablen und die GPT-Tabelle
- PCR 6: Zustandsübergangs-und Aktivierungsereignisse
- PCR 7: Computer herstellerspezifisch
- PCR 8: NTFS-Bootsektor
- PCR 9: NTFS-Startblock
- PCR 10: Start-Manager
- PCR 11: BitLocker-Zugriffssteuerung
- PCR 12-23: reserviert für zukünftige Verwendung

> **Warnung:** Das Ändern des standardmäßigen Platt Form Überprüfungsprofils wirkt sich auf die Sicherheit und Verwaltbarkeit Ihres Computers aus. Die Vertraulichkeit von BitLocker für Plattformänderungen (böswillig oder autorisiert) wird je nach Inklusion oder Ausschluss (beziehungsweise) des PCRs erhöht oder verringert.

Konfigurieren des TPM-Platt Form Prüfungs Profils für systemeigene UEFI-Firmware-Konfigurationen

Diese Richtlinieneinstellung bestimmt, welche Werte das TPM misst, wenn es frühe Startkomponenten überprüft, bevor ein Betriebssystemlaufwerk auf einem Computer mit systemeigenen UEFI-Firmware-Konfigurationen aufgehoben wird.

Richtlinienbeschreibung	Mit dieser Richtlinieneinstellung können Sie konfigurieren, wie die TPM-Sicherheitshardware (Trusted Platform Module) des Computers'den BitLocker-Verschlüsselungsschlüssel sichert.

Eingeführt	Windows Server 2012 und Windows 8
Laufwerktyp	Betriebssystemlaufwerke
Richtlinienpfad	Computer Configuration\Administrative Vorlagen\Windows-Komponenten\Internet BitLocker-Laufwerkverschlüsselung Drive Encryption\Operating System Laufwerke
Konflikte	Wenn diese Richtlinie mit PCR 7 nicht mehr fest **gelegt wird, wird die Gruppen** Richtlinieneinstellung Secure-Boot für Integritätsüberprüfung zulassen überschrieben, und es wird verhindert, dass BitLocker Secure Boot für die Integritätsprüfung von Plattformen oder Startkonfigurationsdaten (BCD) verwendet. Wenn Ihre Umgebungen TPM und Secure Boot für Platt Form Integritätsprüfungen verwenden, sollte diese Richtlinie nicht konfiguriert werden. Weitere Informationen zu PCR 7 finden Sie unter Platform Configuration Register (PCR) in diesem Thema.
Wenn aktiviert	Bevor Sie BitLocker aktivieren, können Sie die Startkomponenten konfigurieren, die vom TPM überprüft werden, bevor der Zugriff auf das BitLocker-verschlüsselte Betriebssystemlaufwerk aufgehoben wird. Wenn sich eine dieser Komponenten ändert, während der BitLocker-Schutz aktiviert ist, gibt das TPM den Verschlüsselungsschlüssel zum Entsperren des Laufwerks nicht frei. Stattdessen zeigt der Computer die BitLocker-Wiederherstellungskonsole an und setzt voraus, dass das Wiederherstellungskennwort oder der Wiederherstellungsschlüssel zum Entsperren des Laufwerks bereitgestellt wird.
Wenn deaktiviert oder nicht konfiguriert	BitLocker verwendet das Standardprofil für die plattformüberprüfung oder das Platt Form Überprüfungsprofil, das vom Setupskript angegeben wird.

Referenz

Diese Richtlinieneinstellung trifft nicht zu, wenn der Computer nicht über ein kompatibles TPM verfügt oder wenn BitLocker bereits mit TPM-Schutz aktiviert ist.

> **Wichtig:** Diese Gruppenrichtlinieneinstellung gilt nur für Computer mit einer systemeigenen UEFI-Firmware-Konfiguration. Computer mit BIOS-oder UEFI-Firmware mit aktiviertem Kompatibilitäts Support Modul (CSM) speichern unterschiedliche Werte in den Plattformkonfigurationsregistern (PCRs). Verwenden Sie die Gruppenrichtlinieneinstellung für die Konfiguration der **TPM-Platt Form Überprüfungsprofile für BIOS-basierte Firmware-Konfigurationen** , um das TPM-PCR-Profil für Computer mit BIOS-Konfigurationen oder für Computer mit UEFI-Firmware mit aktiviertem CSM zu konfigurieren.

Ein Platt Form Überprüfungsprofil besteht aus einer Reihe von PCR-Indizes (Platform Configuration Register), die von 0 bis 23 reichen. Das Standardprofil der plattformüberprüfung sichert den Verschlüsselungsschlüssel vor

Änderungen des ausführbaren Codes der Kernsystem-Firmware (PCR 0), des erweiterten oder steckbaren ausführbaren Codes (PCR 2), des Start-Managers (PCR 4) und der BitLocker-Zugriffssteuerung (PCR 11).

In der folgenden Liste sind alle verfügbaren PCRs aufgeführt:

- PCR 0: ausführbarer Code der Kern System-Firmware
- PCR 1: Core System Firmware-Daten
- PCR 2: erweiterter oder steckbarer ausführbarer Code
- PCR 3: Erweiterte oder steckbare Firmware-Daten
- PCR 4: Start-Manager
- PCR 5: GPT/Partitionstabelle
- PCR 6: fortsetzen von S4-und S5-Energiezustands Ereignissen
- PCR 7: sicherer Startzustand

  Weitere Informationen zu diesem PCR finden Sie unter Platform Configuration Register (PCR) in diesem Thema.

- PCR 8: initialisiert zu 0 ohne extends (reserviert für zukünftige Verwendung)
- PCR 9: initialisiert zu 0 ohne extends (reserviert für zukünftige Verwendung)
- PCR 10: initialisiert zu 0 ohne extends (reserviert für zukünftige Verwendung)
- PCR 11: BitLocker-Zugriffssteuerung
- PCR 12: Daten Ereignisse und stark flüchtige Ereignisse
- PCR 13: Startmodul Details
- PCR 14: Start Autoritäten
- PCR 15 – 23: reserviert für zukünftige Verwendung

> **Warnung:** Das Ändern des standardmäßigen Platt Form Überprüfungsprofils wirkt sich auf die Sicherheit und Verwaltbarkeit Ihres Computers aus. Die Vertraulichkeit von BitLocker für Plattformänderungen (böswillig oder autorisiert) wird je nach Inklusion oder Ausschluss (beziehungsweise) des PCRs erhöht oder verringert.

Zurücksetzen von Platt Form Überprüfungsdaten nach BitLocker-Wiederherstellung

Diese Richtlinieneinstellung bestimmt, ob Platt Form Überprüfungsdaten aktualisiert werden sollen, wenn Windows nach einer BitLocker-Wiederherstellung gestartet wird. Ein Platt Form Überprüfungsdaten Profil besteht aus den Werten in einer Reihe von PCR-Indizes (Platform Configuration Register), die zwischen 0 und 23 liegen.

Richtlinienbeschreibung	Mit dieser Richtlinieneinstellung können Sie steuern, ob Platt Form Überprüfungsdaten aktualisiert werden, wenn Windows nach einer BitLocker-Wiederherstellung gestartet wird.
Eingeführt	Windows Server 2012 und Windows 8
Laufwerktyp	Betriebssystemlaufwerke
Richtlinienpfad	Computer Configuration\Administrative Vorlagen\Windows-Komponenten\Internet BitLocker-Laufwerkverschlüsselung Drive Encryption\Operating System Laufwerke

Konflikte	Keine
Wenn aktiviert	Platt Form Überprüfungsdaten werden aktualisiert, wenn Windows nach einer BitLocker-Wiederherstellung gestartet wird.
Wenn deaktiviert	Platt Form Überprüfungsdaten werden nicht aktualisiert, wenn Windows nach einer BitLocker-Wiederherstellung gestartet wird.
Wenn nicht konfiguriert	Platt Form Überprüfungsdaten werden aktualisiert, wenn Windows nach einer BitLocker-Wiederherstellung gestartet wird.

Referenz

Weitere Informationen zum Wiederherstellungsprozess finden Sie im BitLocker-Wiederherstellungs Handbuch.

Verwenden des erweiterten Startkonfigurationsdaten Überprüfungsprofils

Diese Richtlinieneinstellung bestimmt bestimmte Startkonfigurationsdaten Einstellungen, die während der plattformüberprüfung überprüft werden sollen. Eine plattformüberprüfung verwendet die Daten im Platt Form Überprüfungsprofil, das aus einer Reihe von PCR-Indizes (Platform Configuration Register) besteht, die zwischen 0 und 23 liegen.

Richtlinienbeschreibung	Mit dieser Richtlinieneinstellung können Sie Startkonfigurationsdaten (BCD)-Einstellungen angeben, die während der plattformüberprüfung überprüft werden sollen.
Eingeführt	Windows Server 2012 und Windows 8
Laufwerktyp	Betriebssystemlaufwerke
Richtlinienpfad	Computer Configuration\Administrative Vorlagen\Windows-Komponenten\Internet BitLocker-Laufwerkverschlüsselung Drive Encryption\Operating System Laufwerke
Konflikte	Wenn BitLocker Secure Boot für die Überprüfung der Datenintegrität für die Platt Form- **und Startkonfiguration verwendet, wird die** Gruppenrichtlinieneinstellung use Enhanced Boot Configuration Data Validation **profile ignoriert (wie in der** Gruppenrichtlinieneinstellung Secure Boot für Integritätsüberprüfung zulassen definiert).

Wenn aktiviert	Sie können zusätzliche BCD-Einstellungen hinzufügen, die von Ihnen angegebenen BCD-Einstellungen ausschließen oder Inklusions-und Ausschlusslisten kombinieren, um ein benutzerdefiniertes BCD-Validierungs Profil zu erstellen, das Ihnen die Möglichkeit gibt, diese BCD-Einstellungen zu überprüfen.
Wenn deaktiviert	Der Computer kehrt auf eine BCD-Profilüberprüfung zurück, die dem standardmäßigen BCD-Profil entspricht, das von Windows 7 verwendet wird.
Wenn nicht konfiguriert	Der Computer überprüft die standardmäßigen BCD-Einstellungen in Windows.

Referenz

> **Hinweis:** Die Einstellung zum Steuern des Start Debuggens (0x16000010) wird immer überprüft und hat keine Auswirkungen, wenn Sie in der Inklusions-oder Ausschlussliste enthalten ist.

Gewähren des Zugriffs auf von BitLocker geschützte fest Netzlaufwerke aus früheren Versionen von Windows

Diese Richtlinieneinstellung wird verwendet, um zu steuern, ob der Zugriff auf Laufwerke mithilfe des BitLocker To Go-Readers zulässig ist und ob die Anwendung auf dem Laufwerk installiert ist.

Richtlinienbeschreibung	Mit dieser Richtlinieneinstellung können Sie konfigurieren, ob feste Datenlaufwerke, die mit dem FAT-Dateisystem formatiert sind, freigegeben und auf Computern unter Windows Vista, Windows XP mit Service Pack 3 (SP3) oder Windows XP mit Service Pack 2 (SP2) angezeigt werden können.
Eingeführt	Windows Server 2008 R2 und Windows 7
Laufwerktyp	Feste Datenlaufwerke
Richtlinienpfad	Computer Configuration\Administrative Vorlagen\Windows-Komponenten\Internet BitLocker-Laufwerkverschlüsselung Drive Encryption\Fixed Datenlaufwerke
Konflikte	Keine
Wenn diese Option **aktiviert und nicht konfiguriert ist**	Feste Datenlaufwerke, die mit dem FAT-Dateisystem formatiert sind, können auf Computern, auf denen Windows Server 2008, Windows Vista, Windows XP mit SP3 oder Windows XP mit SP2 ausgeführt wird, freigegeben werden, und deren Inhalt kann angezeigt werden. Diese Betriebssysteme verfügen über schreibgeschützten Zugriff auf von BitLocker geschützte Laufwerke.

Wenn deaktiviert	Feste Datenlaufwerke, die mit dem FAT-Dateisystem formatiert sind und BitLocker-geschützt sind, können auf Computern unter Windows Vista, Windows XP mit SP3 oder Windows XP mit SP2 nicht entsperrt werden. Der BitLocker To Go-Reader (bitlockertogo. exe) ist nicht installiert.

Referenz

> **Hinweis:** Diese Richtlinieneinstellung gilt nicht für Laufwerke, die mit dem NTFS-Dateisystem formatiert sind.

Wenn diese Richtlinieneinstellung aktiviert ist, aktivieren Sie das Kontrollkästchen **BitLocker To Go-Reader auf FAT-formatierten Festplatten nicht installieren** , um zu verhindern, dass Benutzer BitLocker To Go-Reader auf Ihren Festplatten ausführen können. Wenn der BitLocker To Go-Reader (bitlockertogo. exe) auf einem Laufwerk vorhanden ist, auf dem kein Identifizierungs Feld angegeben ist, oder wenn das Laufwerk über das gleiche Identifikationsfeld verfügt, wie es in der Richtlinieneinstellung **eindeutige IDs für Ihre Organisation bereitstellen** angegeben ist, wird der Benutzer aufgefordert, BitLocker zu aktualisieren, und der BitLocker To Go-Reader wird vom Laufwerk gelöscht. In diesem Fall muss der BitLocker To Go-Reader auf dem Computer installiert sein, damit das festgelegte Laufwerk auf Computern unter Windows Vista, Windows XP mit SP3 oder Windows XP mit SP2 gesperrt wird. Wenn dieses Kontrollkästchen nicht aktiviert ist, wird der BitLocker To Go-Reader auf dem festgelegten Laufwerk installiert, damit Benutzer das Laufwerk auf Computern unter Windows Vista, Windows XP mit SP3 oder Windows XP mit SP2 entsperren können.

Gewähren des Zugriffs auf von BitLocker geschützte Wechseldaten Laufwerke aus früheren Versionen von Windows

Diese Richtlinieneinstellung steuert den Zugriff auf Wechseldatenträger, die den BitLocker To Go-Reader verwenden, und ob der BitLocker To Go-Reader auf dem Laufwerk installiert werden kann.

Richtlinienbeschreibung	Mit dieser Richtlinieneinstellung können Sie konfigurieren, ob wechselbare Datenlaufwerke, die mit dem FAT-Dateisystem formatiert sind, freigegeben und auf Computern unter Windows Vista, Windows XP mit SP3 oder Windows XP mit SP2 angezeigt werden können.
Eingeführt	Windows Server 2008 R2 und Windows 7
Laufwerktyp	Austauschbare Datenlaufwerke
Richtlinienpfad	Computer Configuration\Administrative Vorlagen\Windows-Komponenten\Internet BitLocker-Laufwerkverschlüsselung Drive Encryption\Removable Datenlaufwerke
Konflikte	Keine

Wenn diese Option **aktiviert und nicht konfiguriert ist**	Wechseldatenträger, die mit dem FAT-Dateisystem formatiert sind, können auf Computern, auf denen Windows Vista, Windows XP mit SP3 oder Windows XP mit SP2 ausgeführt wird, freigegeben werden, und deren Inhalte können angezeigt werden. Diese Betriebssysteme verfügen über schreibgeschützten Zugriff auf von BitLocker geschützte Laufwerke.
Wenn deaktiviert	Wechseldatenträger, die mit dem FAT-Dateisystem formatiert sind, die mit BitLocker geschützt sind, können auf Computern unter Windows Vista, Windows XP mit SP3 oder Windows XP mit SP2 nicht freigegeben werden. Der BitLocker To Go-Reader (bitlockertogo. exe) ist nicht installiert.

Referenz

> **Hinweis:** Diese Richtlinieneinstellung gilt nicht für Laufwerke, die mit dem NTFS-Dateisystem formatiert sind.

Wenn diese Richtlinieneinstellung aktiviert ist, aktivieren Sie das Kontrollkästchen **BitLocker To Go-Reader auf FAT-formatierten Wechseldatenträgern nicht installieren** , um zu verhindern, dass Benutzer BitLocker To Go-Reader auf Ihren Wechseldatenträgern ausführen können. Wenn der BitLocker To Go-Reader (bitlockertogo. exe) auf einem Laufwerk vorhanden ist, auf dem kein Identifizierungs Feld angegeben ist, oder wenn das Laufwerk über das gleiche Identifikationsfeld verfügt, wie es in der Richtlinieneinstellung **eindeutige IDs für Ihre Organisation bereitstellen** angegeben ist, wird der Benutzer aufgefordert, BitLocker zu aktualisieren, und der BitLocker To Go-Reader wird vom Laufwerk gelöscht. In diesem Fall muss der BitLocker To Go-Reader auf dem Computer installiert sein, damit das Wechsellaufwerk auf Computern unter Windows Vista, Windows XP mit SP3 oder Windows XP mit SP2 gesperrt wird. Wenn dieses Kontrollkästchen nicht aktiviert ist, wird der BitLocker To Go-Reader auf dem Wechseldatenträger installiert, damit Benutzer das Laufwerk auf Computern unter Windows Vista, Windows XP mit SP3 oder Windows XP mit SP2 entsperren können, auf denen der BitLocker To Go-Reader nicht installiert ist.

FIPS-Einstellung

Sie können die FIPS-Einstellung (Federal Information Processing Standard) für die FIPS-Konformität konfigurieren. Als Folge der FIPS-Konformität können Benutzer kein BitLocker-Kennwort für die Wiederherstellung oder als Schlüsselschutz erstellen oder speichern. Die Verwendung eines Wiederherstellungsschlüssels ist zulässig.

Richtlinienbeschreibung	Anmerkungen
Eingeführt	Windows Server 2003 mit SP1
Laufwerktyp	Systemübergreifend
Richtlinienpfad	Lokale Richtlinien\Sicherheitsoptionen-Options\System-Kryptografie **: Verwenden von FIPS-kompatiblen Algorithmen für Verschlüsselung, Hashing und Signierung**

Konflikte	Einige Anwendungen wie Terminal Dienste unterstützen FIPS-140 nicht auf allen Betriebssystemen.
Wenn aktiviert	Benutzer können ein Wiederherstellungskennwort nicht an einem beliebigen Speicherort speichern. Dazu gehören AD DS-und Netzwerkordner. Darüber hinaus können Sie keine WMI oder den Setup-Assistenten für die BitLocker-Laufwerkverschlüsselung verwenden, um ein Wiederherstellungskennwort zu erstellen.
Wenn deaktiviert oder nicht konfiguriert	Es wird kein BitLocker-Verschlüsselungsschlüssel generiert

Referenz

Diese Richtlinie muss aktiviert sein, bevor ein Verschlüsselungsschlüssel für BitLocker generiert wird. Beachten Sie, dass BitLocker, wenn diese Richtlinie aktiviert ist, das Erstellen oder Verwenden von Wiederherstellungskennwörtern verhindert, sodass stattdessen Wiederherstellungsschlüssel verwendet werden sollten.

Sie können den optionalen Wiederherstellungsschlüssel auf einem USB-Laufwerk speichern. Da Wiederherstellungskennwörter nicht in AD DS gespeichert werden können, wenn FIPS aktiviert ist, wird ein Fehler verursacht, wenn die AD DS-Sicherung für Gruppenrichtlinien erforderlich ist.

Sie können die FIPS-Einstellung mit dem Sicherheitsrichtlinien-Editor (secpol. msc) oder durch Bearbeiten der Windows-Registrierung bearbeiten. Sie müssen ein Administrator sein, um diese Verfahren ausführen zu können.

Weitere Informationen zum Festlegen dieser Richtlinie finden Sie unter System Kryptografie: Verwenden von FIPS-kompatiblen Algorithmen für Verschlüsselung, Hashing und Signierung.

Energie Verwaltungsgruppen Richtlinieneinstellungen: Ruhezustand und Ruhezustand

Die standardmäßigen Energieeinstellungen für einen Computer führen dazu, dass der Computer häufig in den Ruhezustand wechselt, um im Leerlauf Energie zu sparen und die Akkulebensdauer des Systems zu verlängern. Wenn ein Computer in den Ruhezustand wechselt, werden die geöffneten Programme und Dokumente im Arbeitsspeicher gespeichert. Wenn ein Computer aus dem Ruhezustand fortgesetzt wird, müssen die Benutzer sich nicht erneut mit einem PIN-oder USB-Startschlüssel authentifizieren, um auf verschlüsselte Daten zugreifen zu können. Dies kann zu Bedingungen führen, bei denen die Datensicherheit beeinträchtigt wird.

Wenn jedoch ein Computer über den Ruhezustand des Laufwerks gesperrt ist und es aus dem Ruhezustand fortgesetzt wird, wird das Laufwerk entsperrt, was bedeutet, dass Benutzer eine PIN oder einen Startschlüssel angeben müssen, wenn Sie die mehrstufige Authentifizierung mit BitLocker verwenden. Daher möchten Organisationen, die BitLocker verwenden, den Ruhezustand anstelle des Ruhezustands verwenden, um die Sicherheit zu verbessern. Diese Einstellung hat keinen Einfluss auf den TPM-Modus, da Sie beim Start und beim fortsetzen aus dem Ruhezustand eine transparente Benutzeroberfläche bietet.

Sie können die folgenden Gruppenrichtlinieneinstellungen deaktivieren, die sich in **Computer Configuration\Administrative Templates\System\Power-Verwaltung** befinden, um alle verfügbaren Ruhezustandseinstellungen zu deaktivieren:

- Standby-Status (S1-S3) beim schlafen zulassen (angeschlossen)
- Standby-Status (S1-S3) beim schlafen zulassen (Akku)

Informationen zum Platform Configuration Register (PCR)

Ein Platt Form Überprüfungsprofil besteht aus einer Reihe von PCR-Indizes, die zwischen 0 und 23 liegen. Der Bereich der Werte kann für die Version des Betriebssystems spezifisch sein.

Das Ändern des standardmäßigen Platt Form Überprüfungsprofils wirkt sich auf die Sicherheit und Verwaltbarkeit Ihres Computers aus. Die Vertraulichkeit von BitLocker für Plattformänderungen (böswillig oder autorisiert) wird je nach Inklusion oder Ausschluss (beziehungsweise) des PCRs erhöht oder verringert.

Informationen zu PCR 7

PCR 7 misst den Zustand des sicheren Starts. Mit PCR 7 kann BitLocker das sichere Booten für die Integritätsüberprüfung nutzen. Beim sicheren Start wird sichergestellt, dass die Preboot-Umgebung des Computers nur die Firmware lädt, die von autorisierten Softwareherausgebern digital signiert wurde. PCR 7-Messungen geben an, ob ein sicheres Booten aktiviert ist und welche Schlüssel auf der Plattform als vertrauenswürdig eingestuft werden. Wenn Secure Boot aktiviert ist und die Firmware PCR 7 gemäß der UEFI-Spezifikation richtig misst, kann BitLocker eine Bindung an diese Informationen statt an PCRs 0, 2 und 4 vornehmen, die die Abmessungen der exakten Firmware-und Startdatei-Bilder geladen haben. Dadurch wird die Wahrscheinlichkeit verringert, dass BitLocker aufgrund von Firmware-und Image-Updates im Wiederherstellungsmodus gestartet wird, und es bietet Ihnen eine größere Flexibilität beim Verwalten der Preboot-Konfiguration.

PCR 7-Messungen müssen den Anleitungen entsprechen, die in Anhang A Trusted Execution Environment EFI-Protokollbeschrieben sind.

Bei PCR 7-Messungen handelt es sich um eine obligatorische Logo-Anforderung für Systeme, die modernen Standby-Modus (auch bekannt als Always-Always-Connected-PCs) unterstützen, beispielsweise Microsoft Surface RT. Bei solchen Systemen bindet BitLocker standardmäßig an PCR 7 und PCR 11, wenn das TPM mit PCR 7-Messung und Secure-Boot korrekt konfiguriert ist.

Weitere Informationen

- Trusted Platform Module
- Gruppenrichtlinieneinstellungen für TPM-Dienste
- Häufig gestellte Fragen (Frequently Asked Questions, FAQ) zu BitLocker
- Übersicht über BitLocker
- Vorbereiten Ihrer Organisation auf BitLocker: Planung und Richtlinien

BCD-Einstellungen und BitLocker

27.10.2019 • 6 minutes to read

Betrifft

- Windows 10

Dieses Thema für IT-Experten beschreibt die BCD-Einstellungen, die von BitLocker verwendet werden.

Beim Schutz von Daten auf einem Betriebssystemvolume während des Startvorgangs überprüft BitLocker, ob die Einstellungen für die sicherheitssensitiven Startkonfigurationsdaten (Boot Configuration Data, BCD) seit dem letzten aktivieren, fortsetzen oder Wiederherstellen von BitLocker geändert wurden.

BitLocker-und BCD-Einstellungen

In Windows 7 und Windows Server 2008 R2 hat BitLocker nahezu alle BCD-Einstellungen mit den Präfixen Winload, winresume und Memtest überprüft. Dieses hohe Maß an Validierung hat jedoch dazu geführt, dass BitLocker in den Wiederherstellungsmodus für gutartige Einstellungsänderungen wechselt, beispielsweise beim Anwenden eines Sprachpakets, das BitLocker in die Wiederherstellung eingibt.

In Windows 8, Windows Server 2012 und neueren Betriebssystemen verengt BitLocker den Satz von BCD-Einstellungen, die überprüft werden, um die Wahrscheinlichkeit von gutartigen Änderungen zu verringern, die ein BCD-überprüfungsproblem verursachen. Wenn Sie der Meinung sind, dass eine bestimmte BCD-Einstellung aus dem Überprüfungsprofil ausgeschlossen werden kann, können Sie die BCD-Gültigkeitsprüfung entsprechend ihren Validierungseinstellungen erhöhen. Wenn eine standardmäßige BCD-Einstellung die Wiederherstellung für gutartige Änderungen dauerhaft auslöst, können Sie diese BCD-Einstellung aus dem Validierungs Profil ausschließen.

Wenn sicheres Booten aktiviert ist

Computer mit UEFI-Firmware können mithilfe des Secure-Boot-Vorgangs eine verbesserte Boot-Sicherheit bieten. Wenn BitLocker die Secure-Boot-Funktion für die Platt Form-und BCD-Integritätsüberprüfung verwenden kann, wie es die Gruppenrichtlinieneinstellung " **sichere Start für Integritätsüberprüfung zulassen** " definiert hat, wird die Gruppe " **Erweiterte Startkonfigurationsdaten Überprüfung" verwenden** ignoriert.

Einer der Vorteile der Verwendung eines sicheren Starts besteht darin, dass die BCD-Einstellungen während des Starts korrigiert werden können, ohne dass Wiederherstellungsereignisse ausgelöst werden. Der sichere Start erzwingt die gleichen BCD-Einstellungen wie BitLocker. Die sichere Start-BCD-Erzwingung kann nicht innerhalb des Betriebssystems konfiguriert werden.

Anpassen von BCD-Überprüfungseinstellungen

So ändern Sie die BCD-Einstellungen BitLocker überprüft, ob der IT-Manager BCD-Einstellungen aus dem Platt Form Überprüfungsprofil hinzufügen oder ausschließen soll, indem die Gruppenrichtlinieneinstellung **Erweiterte Startkonfigurationsdaten Überprüfungsprofil verwenden** aktiviert und konfiguriert wird.

Zum Zweck der BitLocker-Validierung sind BCD-Einstellungen einem bestimmten Satz von Microsoft-Startanwendungen zugeordnet. BCD-Einstellungen sind entweder mit einer bestimmten Startanwendung verknüpft oder können für alle Startanwendungen gelten, indem Sie der in der Gruppenrichtlinieneinstellung eingegebenen BCD-Einstellung ein Präfix zuordnen. Zu den Präfix Werten gehören:

- Winload
- winresume

- Memtest
- Alle

Alle BCD-Einstellungen werden durch Kombinieren des Präfix Werts mit einem Hexadezimalwert (Hex) oder einem "Anzeigenamen" angegeben.

Der BCD-Einstellung-Hex-Wert wird gemeldet, wenn BitLocker in den Wiederherstellungsmodus wechselt und im Ereignisprotokoll gespeichert wird (Ereignis-ID 523). Der Hex-Wert gibt eindeutig an, welche BCD-Einstellung das Wiederherstellungsereignis verursacht hat.

Mit dem Befehl "`bcdedit.exe /enum all`" können Sie schnell den Anzeigenamen für die BCD-Einstellungen auf Ihrem Computer abrufen.

Nicht alle BCD-Einstellungen weisen Anzeigenamen auf, für diese Einstellungen ist der Hex-Wert die einzige Möglichkeit zum Konfigurieren einer Ausschlussrichtlinie.

Verwenden Sie bei der Angabe von BCD-Werten in der Gruppenrichtlinieneinstellung **Enhanced Boot Configuration Data Validation profile** die folgende Syntax:

- Präfix für die Einstellung mit dem Start Anwendungs Präfix
- Anhängen eines Doppelpunkts ":"
- Anfügen des Hex-Werts oder des Anzeigenamens
- Wenn Sie mehr als eine BCD-Einstellung eingeben, müssen Sie die einzelnen BCD-Einstellungen in einer neuen Zeile eingeben.

Beispielsweise geben entweder "`winload:hypervisordebugport`" oder "`winload:0x250000f4`" denselben Wert zurück.

Einstellungen, die für alle Startanwendungen gelten, werden möglicherweise nur auf eine einzelne Anwendung angewendet, allerdings ist das Gegenteil nicht der Fall. So kann beispielsweise Folgendes angegeben werden: "`all:locale`" oder "`winresume:locale`", aber da die BCD-Einstellung `win-pe`"" nicht für alle Startanwendungen gilt, `winload:winpe`"" ist gültig, aber "`all:winpe`" ist ungültig. Die Einstellung zum Steuern des Start Debuggens `bootdebug`("" oder 0x16000010) wird immer überprüft und hat keine Auswirkungen, wenn Sie in den bereitgestellten Feldern enthalten ist.

> **Hinweis:** achten Sie beim Konfigurieren von BCD-Einträgen in der Gruppenrichtlinieneinstellung. Der Editor für lokale Gruppenrichtlinien überprüft nicht die Richtigkeit des BCD-Eintrags. BitLocker kann nicht aktiviert werden, wenn die angegebene Gruppenrichtlinieneinstellung ungültig ist.

Standardmäßiges BCD-Validierungs Profil

Die folgende Tabelle enthält das standardmäßige BCD-Validierungs Profil, das von BitLocker in Windows 8, Windows Server 2012 und höheren Betriebssystemen verwendet wird:

HEX-WERT	PRÄFIX	ANZEIGE NAME
0x11000001	Alle	Gerät
0x12000002	Alle	path
0x12000030	Alle	LoadOptions
0x16000010	Alle	bootdebug
0x16000040	Alle	Erweiterte Optionen

HEX-WERT	PRÄFIX	ANZEIGE NAME
0x16000041	Alle	EinstellungenBearbeiten
0x16000048	Alle	nointegritychecks
0x16000049	Alle	testsigning
0x16000060	Alle	isolatedcontext
0x1600007b	Alle	forcefipscrypto
0x22000002	Winload	systemroot
0x22000011	Winload	Kernel
0x22000012	Winload	Hal
0x22000053	Winload	evstore
0x25000020	Winload	NX
0x25000052	Winload	restrictapiccluster
0x26000022	Winload	WinPE
0x26000025	Winload	LastKnownGood
0x26000081	Winload	safebootalternateshell
0x260000a0	Winload	debuggen
0x260000f2	Winload	hypervisordebug
0x26000116	Winload	hypervisorusevapic
0x21000001	winresume	FILEDEVICE
0x22000002	winresume	FilePath
0x26000006	winresume	debugoptionenabled

Vollständige Liste der angezeigten Namen für ignorierte BCD-Einstellungen

Im folgenden finden Sie eine vollständige Liste der BCD-Einstellungen mit angezeigten Namen, die standardmäßig ignoriert werden. Diese Einstellungen sind nicht Teil des standardmäßigen BitLocker-Überprüfungsprofils, können aber hinzugefügt werden, wenn eine Überprüfung dieser Einstellungen erforderlich ist, bevor ein von BitLocker geschütztes Betriebssystemlaufwerk freigegeben werden kann.

> **Hinweis:** es sind zusätzliche BCD-Einstellungen vorhanden, die Hex-Werte haben, aber keine Anzeigenamen aufweisen. Diese Einstellungen sind nicht in dieser Liste enthalten.

HEX-WERT	PRÄFIX	ANZEIGE NAME
0x12000004	Alle	description
0x12000005	Alle	locale
0x12000016	Alle	TargetName
0x12000019	Alle	busparams
0x1200001d	Alle	key
0x1200004a	Alle	FontPath
0x14000006	Alle	Erben
0x14000008	Alle	recoverysequence
0x15000007	Alle	Truncatememory
0x1500000c	Alle	firstmegabytepolicy
0x1500000d	Alle	relocatephysical
0x1500000e	Alle	avoidlowmemory
0x15000011	Alle	DebugType
0x15000012	Alle	debugaddress
0x15000013	Alle	Debugport
0x15000014	Alle	Baudrate
0x15000015	Alle	Kanal
0x15000018	Alle	debuggendebugging starten
0x1500001a	Alle	HostIP
0x1500001b	Alle	Anschluss
0x15000022	Alle	emsport
0x15000023	Alle	emsbaudrate
0x15000042	Alle	keyringaddress
0x15000047	Alle	configaccesspolicy
0x1500004b	Alle	integrityservices

HEX-WERT	PRÄFIX	ANZEIGE NAME
0x1500004c	Alle	volumebandid
0x15000051	Alle	initialconsoleinput
0x15000052	Alle	graphicsresolution
0x15000065	Alle	Display Message
0x15000066	Alle	displaymessageoverride
0x15000081	Alle	logcontrol
0x16000009	Alle	recoveryenabled
0x1600000b	Alle	badmemoryaccess
0x1600000f	Alle	traditionalkseg
0x16000017	Alle	noumex
0x1600001c	Alle	DHCP
0x1600001e	Alle	VM
0x16000020	Alle	bootems
0x16000046	Alle	graphicsmodedisabled
0x16000050	Alle	extendedinput
0x16000053	Alle	restartonfailure
0x16000054	Alle	highestmode
0x1600006c	Alle	bootuxdisabled
0x16000072	Alle	nokeyboard
0x16000074	Alle	bootshutdowndisabled
0x1700000a	Alle	badmemorylist
0x17000077	Alle	allowedinmemorysettings
0x22000040	Alle	fverecoveryurl
0x22000041	Alle	fverecoverymessage
0x31000003	Alle	ramdisksdidevice

HEX-WERT	PRÄFIX	ANZEIGE NAME
0x32000004	Alle	ramdisksdipath
0x35000001	Alle	ramdiskimageoffset
0x35000002	Alle	ramdisktftpclientport
0x35000005	Alle	ramdiskimagelength
0x35000007	Alle	ramdisktftpblocksize
0x35000008	Alle	ramdisktftpwindowsize
0x36000006	Alle	exportascd
0x36000009	Alle	ramdiskmcenabled
0x3600000a	Alle	ramdiskmctftpfallback
0x3600000b	Alle	ramdisktftpvarwindow
0x21000001	Winload	osdevice
0x22000013	Winload	dbgtransport
0x220000f9	Winload	hypervisorbusparams
0x22000110	Winload	hypervisorusekey
0x23000003	Winload	RESUMEOBJECT
0x25000021	Winload	PAE
0x25000031	Winload	removememory
0x25000032	Winload	increaseuserva
0x25000033	Winload	perfmem
0x25000050	Winload	clustermodeaddressing
0x25000055	Winload	x2apicpolicy
0x25000061	Winload	numproc
0x25000063	Winload	configflags
0x25000066	Winload	Gruppierung
0x25000071	Winload	MSI

HEX-WERT	PRÄFIX	ANZEIGE NAME
0x25000072	Winload	PCIExpress
0x25000080	Winload	SafeBoot
0x250000a6	Winload	tscsyncpolicy
0x250000c1	Winload	driverloadfailurepolicy
0x250000c2	Winload	bootmenupolicy
0x250000e0	Winload	bootstatuspolicy
0x250000f0	Winload	hypervisorlaunchtype
0x250000f3	Winload	hypervisordebugtype
0x250000f4	Winload	hypervisordebugport
0x250000f5	Winload	hypervisorbaudrate
0x250000f6	Winload	hypervisorchannel
0x250000f7	Winload	bootux
0x250000fa	Winload	hypervisornumproc
0x250000fb	Winload	hypervisorrootprocpernode
0x250000fd	Winload	hypervisorhostip
0x250000fe	Winload	hypervisorhostport
0x25000100	Winload	tpmbootentropy
0x25000113	Winload	hypervisorrootproc
0x25000115	Winload	hypervisoriommupolicy
0x25000120	Winload	xsavepolicy
0x25000121	Winload	xsaveaddfeature0
0x25000122	Winload	xsaveaddfeature1
0x25000123	Winload	xsaveaddfeature2
0x25000124	Winload	xsaveaddfeature3
0x25000125	Winload	xsaveaddfeature4

HEX-WERT	PRÄFIX	ANZEIGE NAME
0x25000126	Winload	xsaveaddfeature5
0x25000127	Winload	xsaveaddfeature6
0x25000128	Winload	xsaveaddfeature7
0x25000129	Winload	xsaveremovefeature
0x2500012a	Winload	xsaveprocessorsmask
0x2500012b	Winload	xsavedisable
0x25000130	Winload	claimedtpmcounter
0x26000004	Winload	stampdisks
0x26000010	Winload	detecthal
0x26000024	Winload	nocrashautoreboot
0x26000030	Winload	nolowmem
0x26000040	Winload	VGA
0x26000041	Winload	quietboot
0x26000042	Winload	novesa
0x26000043	Winload	novga
0x26000051	Winload	usephysicaldestination
0x26000054	Winload	uselegacyapicmode
0x26000060	Winload	onecpu
0x26000062	Winload	maxproc
0x26000064	Winload	maxgroup
0x26000065	Winload	groupaware
0x26000070	Winload	usefirmwarepcisettings
0x26000090	Winload	bootlog
0x26000091	Winload	SOS
0x260000a1	Winload	halbreakpoint

HEX-WERT	PRÄFIX	ANZEIGE NAME
0x260000a2	Winload	useplatformclock
0x260000a3	Winload	forcelegacyplatform
0x260000a4	Winload	useplatformtick
0x260000a5	Winload	disabledynamictick
0x260000b0	Winload	EMS
0x260000c3	Winload	onetimeadvancedoptions
0x260000c4	Winload	onetimeoptionsedit
0x260000e1	Winload	disableelamdrivers
0x260000f8	Winload	hypervisordisableslat
0x260000fc	Winload	hypervisoruselargevtlb
0x26000114	Winload	hypervisordhcp
0x21000005	winresume	associatedosdevice
0x25000007	winresume	bootux
0x25000008	winresume	bootmenupolicy
0x26000003	winresume	CustomSettings
0x26000004	winresume	PAE
0x25000001	Memtest	PASSCOUNT
0x25000002	Memtest	testmix
0x25000005	Memtest	stridefailcount
0x25000006	Memtest	invcfailcount
0x25000007	Memtest	matsfailcount
0x25000008	Memtest	randfailcount
0x25000009	Memtest	chckrfailcount
0x26000003	Memtest	cacheenable
0x26000004	Memtest	failuresenabled

BitLocker-Wiederherstellungs Handbuch

27.10.2019 • 30 minutes to read

Betrifft

- Windows 10

In diesem Thema für IT-Experten wird beschrieben, wie BitLocker-Schlüssel aus AD DS wiederhergestellt werden.

Organisationen können BitLocker-Wiederherstellungsinformationen verwenden, die in den Active Directory-Domänendiensten (Adds) gespeichert sind, um auf BitLocker-geschützte Daten zuzugreifen. Es wird empfohlen, ein Wiederherstellungsmodell für BitLocker zu erstellen, während Sie Ihre BitLocker-Bereitstellung planen.

In diesem Artikel wird davon ausgegangen, dass Sie wissen, wie Sie das Hinzufügen zum automatischen Sichern von BitLocker-Wiederherstellungsinformationen und welche Typen von Wiederherstellungsinformationen in "hinzufügen" gespeichert werden.

In diesem Artikel wird nicht ausführlich erläutert, wie Sie zum Speichern der BitLocker-Wiederherstellungsinformationen hinzufügen konfigurieren.

Was ist die BitLocker-Wiederherstellung?

Die BitLocker-Wiederherstellung ist der Vorgang, mit dem Sie den Zugriff auf ein mit BitLocker geschütztes Laufwerk wiederherstellen können, falls Sie das Laufwerk nicht normal entsperren können. In einem Wiederherstellungsszenario stehen Ihnen die folgenden Optionen zum Wiederherstellen des Zugriffs auf das Laufwerk zur Verfügung:

- Der Benutzer kann das Wiederherstellungskennwort angeben. Wenn Ihre Organisation Benutzern das Drucken oder Speichern von Wiederherstellungskennwörtern ermöglicht, kann der Benutzer das 48-stellige Wiederherstellungskennwort eingeben, das auf einem USB-Laufwerk oder mit Ihrem Microsoft-Konto online gedruckt oder gespeichert wurde. (Das Speichern eines Wiederherstellungskennworts mit Ihrem Microsoft-Konto ist online nur möglich, wenn BitLocker auf einem PC verwendet wird, der kein Mitglied einer Domäne ist).
- Ein Daten Wiederherstellungs-Agent kann Ihre Anmeldeinformationen verwenden, um das Laufwerk zu entsperren. Wenn es sich bei dem Laufwerk um ein Betriebssystemlaufwerk handelt, muss das Laufwerk als Datenlaufwerk auf einem anderen Computer bereitgestellt werden, damit der Daten Wiederherstellungs-Agent die Sperre aufheben kann.
- Ein Domänenadministrator kann das Wiederherstellungskennwort von AD DS abrufen und zum Entsperren des Laufwerks verwenden. Das Speichern von Wiederherstellungskennwörtern in AD DS wird empfohlen, um IT-Experten die Möglichkeit zu bieten, bei Bedarf Wiederherstellungskennwörter für Laufwerke in Ihrer Organisation abzurufen. Diese Methode setzt voraus, dass Sie diese Wiederherstellungsmethode in der BitLocker-Gruppenrichtlinieneinstellung aktiviert haben, **Wählen Sie aus, wie BitLocker-geschützte Betriebssystemlaufwerke wiederhergestellt werden können** , die sich auf **Computer Configuration\Administrative befinden Templates\ Windows Components\BitLocker Drive Encryption\Operating System Laufwerke** im Editor für lokale Gruppenrichtlinien. Weitere Informationen finden Sie unter BitLocker-Gruppenrichtlinieneinstellungen.

Was ist die Ursache für die BitLocker-Wiederherstellung?

In der folgenden Liste finden Sie Beispiele für bestimmte Ereignisse, die dazu führen, dass BitLocker beim Versuch, das Betriebssystemlaufwerk zu starten, den Wiederherstellungsmodus aktiviert:

- Auf PCs, die die BitLocker-Laufwerkverschlüsselung verwenden, oder auf Geräten wie Tablets oder

Smartphones, die nur die BitLocker-Geräteverschlüsselung verwenden, wird das Gerät beim Erkennen eines Angriffs sofort neu gestartet und in den BitLocker-Wiederherstellungsmodus versetzt. Um diese Funktion zu nutzen, können Administratoren die Gruppenrichtlinieneinstellung für die **interaktive Anmeldung: Computerkonto Sperrungs Schwellenwert** in **\Computer Configuration\Windows Settings\Security Settings\Local Policies\ Sicherheitsoptionen** im Editor für lokale Gruppenrichtlinien oder verwenden Sie die **MaxFailedPasswordAttempts** -Richtlinie von Exchange ActiveSync (auch konfigurierbar über Windows InTune), um die Anzahl fehlerhafter Kennwortversuche zu begrenzen, bevor die Gerät wechselt in die Gerätesperrung.

- Auf Geräten mit TPM 1,2 bewirkt die Änderung der BIOS-oder Firmware-Startgerätereihenfolge eine BitLocker-Wiederherstellung. Bei Geräten mit TPM 2,0 wird in diesem Fall die BitLocker-Wiederherstellung jedoch nicht gestartet. TPM 2,0 berücksichtigt keine Änderung der Boot-Device-Reihenfolge als Sicherheitsrisiko, da der Betriebssystem-Bootloader nicht beeinträchtigt wird.
- Wenn Sie das CD-oder DVD-Laufwerk vor der Festplatte in der BIOS-Startreihenfolge haben und dann eine CD oder DVD einfügen oder entfernen.
- Fehler beim Booten von einem Netzlaufwerk, bevor Sie von der Festplatte booten.
- Andocken oder Abdocken eines tragbaren Computers In einigen Fällen (je nach Computerhersteller und BIOS) ist die Docking-Bedingung des tragbaren Computers Teil der Systemmessung und muss konsistent sein, um den Systemstatus zu überprüfen und BitLocker zu entsperren. Wenn ein tragbarer Computer mit der Docking-Station verbunden ist, wenn BitLocker aktiviert ist, müssen Sie möglicherweise auch mit der Docking-Station verbunden sein, wenn die Sperre aufgehoben wird. Wenn ein tragbarer Computer jedoch nicht mit seiner Docking-Station verbunden ist, wenn BitLocker aktiviert ist, muss er möglicherweise von der Dockingstation getrennt werden, wenn er entriegelt ist.
- Änderungen an der NTFS-Partitionstabelle auf dem Datenträger, einschließlich erstellen, löschen oder Ändern der Größe einer primären Partition.
- Die persönliche Identifikationsnummer (PIN) wird zu oft falsch eingegeben, damit die Anti-Hämmer-Logik des TPM aktiviert wird. Die Anti-Hämmer-Logik ist Software-oder Hardware Methoden, die den Schwierigkeitsgrad und die Kosten eines Brute-Force-Angriffs auf eine PIN erhöhen, indem Sie die PIN-Einträge erst nach einer bestimmten Zeitspanne akzeptieren.
- Deaktivieren Sie die Unterstützung für das Lesen des USB-Geräts in der Pre-Boot-Umgebung vom BIOS oder der UEFI-Firmware, wenn Sie USB-basierte Schlüssel anstelle eines TPMs verwenden.
- Deaktivieren, deaktivieren, deaktivieren oder Löschen des TPMs
- Aktualisieren kritischer Frühstartkomponenten wie ein BIOS-oder UEFI-Firmware-Upgrade, wodurch sich die zugehörigen Start Messungen ändern.
- Vergessen Sie die PIN, wenn die PIN-Authentifizierung aktiviert wurde.
- Aktualisieren der Option ROM-Firmware
- Aktualisieren der TPM-Firmware
- Hinzufügen oder Entfernen von Hardware; So können Sie beispielsweise eine neue Karte auf dem Computer einfügen, einschließlich einiger PCMIA-WLAN-Karten.
- Entfernen, Einsetzen oder vollständiges Leeren der Ladung eines Smart-Akkus in einem tragbaren Computer.
- Änderungen am Master Boot Record auf dem Datenträger.
- Änderungen am Start-Manager auf dem Datenträger.
- Ausblenden des TPMs aus dem Betriebssystem. Einige BIOS-oder UEFI-Einstellungen können verwendet werden, um die Enumeration des TPMs für das Betriebssystem zu verhindern. Bei der Implementierung kann diese Option das TPM aus dem Betriebssystem verdeckt machen. Wenn das TPM ausgeblendet ist, werden BIOS und UEFI Secure Startup deaktiviert, und das TPM reagiert nicht auf Befehle aus einer Software.
- Verwenden einer anderen Tastatur, die nicht ordnungsgemäß in die PIN eingegeben wird oder deren Tastaturzuordnung nicht mit der Tastaturzuordnung übereinstimmt, die von der Pre-Boot-Umgebung angenommen wurde. Dadurch kann die Eingabe von erweiterten Pins verhindert werden.
- Ändern der vom TPM-Validierungs Profil verwendeten Plattformkonfigurationsregister (Platform Configuration Registers, PCRs) Wenn beispielsweise **PCR \ [1]** dazu führt, dass BitLocker die meisten

Änderungen an den BIOS-Einstellungen misst, verursacht BitLocker den Wiederherstellungsmodus, auch wenn sich die Einstellungen für nicht-Start kritische BIOS-Einstellungen ändern.

> **Hinweis:** einige Computer verfügen über BIOS-Einstellungen, die Messungen an bestimmte PCRs überspringen, wie etwa **PCR \ [2]**. Das Ändern dieser Einstellung im BIOS würde dazu führen, dass BitLocker in den Wiederherstellungsmodus wechselt, weil die PCR-Messung anders ist.

- Verschieben des BitLocker-geschützten Laufwerks in einen neuen Computer
- Aktualisieren Sie die Hauptplatine auf eine neue mit einem neuen TPM.
- Verlust des USB-Sticks, der den Startschlüssel enthält, wenn die Schlüsselauthentifizierung für den Start aktiviert wurde.
- Fehler beim TPM-Selbsttest.
- Sie verfügen über ein BIOS, eine UEFI-Firmware oder eine Option ROM-Komponente, die nicht mit den relevanten Trusted Computing Group-Standards für einen Clientcomputer kompatibel ist. So kann beispielsweise eine nicht kompatible Implementierung in den TPM-Messungen flüchtige Daten (wie Zeit) aufzeichnen, die bei jedem Start unterschiedliche Maße verursachen und dazu führen, dass BitLocker im Wiederherstellungsmodus gestartet wird.
- Das Ändern der Verwendungsberechtigung für den Speicherstammschlüssel des TPM auf einen Wert ungleich NULL.

> **Hinweis:** der BitLocker-TPM-Initialisierungsprozess legt den Wert für die Nutzungsautorisierung auf NULL fest, sodass ein anderer Benutzer oder Prozess diesen Wert explizit geändert haben muss.

- Deaktivieren der Code Integritätsprüfung oder Aktivieren der Testsignierung im Windows-Start-Manager
- Drücken der Taste F8 oder F10 während des Startvorgangs
- Hinzufügen oder Entfernen von Add-in-Karten (wie Video-oder Netzwerkkarten) oder Aktualisieren der Firmware auf Add-in-Karten.
- Verwenden einer BIOS-Hotkey-Taste während des Startvorgangs, um die Startreihenfolge auf eine andere Festplatte zu ändern.

> **Hinweis:** bevor Sie mit der Wiederherstellung beginnen, empfehlen wir, die Ursache für die Wiederherstellung zu ermitteln. Dies kann dazu beitragen, dass das Problem in Zukunft nicht mehr auftritt. Wenn Sie beispielsweise feststellen, dass ein Angreifer Ihren Computer durch Abrufen von physischem Zugriff geändert hat, können Sie neue Sicherheitsrichtlinien für die Nachverfolgung von Personen erstellen, die physisch anwesend sind. Nachdem das Wiederherstellungskennwort zum Wiederherstellen des Zugriffs auf den PC verwendet wurde, versiegelt BitLocker den Verschlüsselungsschlüssel erneut auf die aktuellen Werte der gemessenen Komponenten.

Für geplante Szenarien, wie etwa bekannte Hardware-oder Firmware-Upgrades, können Sie das Initiieren der Wiederherstellung vermeiden, indem Sie den BitLocker-Schutz vorübergehend anhalten. Da BitLocker durch Anhalten des Laufwerks vollständig verschlüsselt bleibt, kann der Administrator den BitLocker-Schutz nach Abschluss der geplanten Aufgabe schnell wieder aufnehmen. Durch Verwenden von anhalten und fortsetzen wird auch der Verschlüsselungsschlüssel wieder versiegelt, ohne dass die Eingabe des Wiederherstellungsschlüssels erforderlich ist.

> **Hinweis:** wenn BitLocker angehalten wird, wird der Schutz beim Neustart des PCs automatisch fortgesetzt, es sei denn, die Anzahl der Neustarts wird über das Befehlszeilentool manage-bde angegeben.

Wenn der Computer durch Softwarewartung neu gestartet werden muss und Sie die zweistufige Authentifizierung verwenden, können Sie die BitLocker-Netzwerksperrung so aktivieren, dass der sekundäre

Authentifizierungs Faktor bereitgestellt wird, wenn die Computer keinen lokalen Benutzer besitzen, um die zusätzliche Authentifizierungsmethode.

Die Wiederherstellung wurde im Kontext des ungeplanten oder unerwünschten Verhaltens beschrieben, aber Sie können auch die Wiederherstellung als beabsichtigtes Produktionsszenario auslösen, um die Zugriffssteuerung zu verwalten. Wenn Sie beispielsweise Desktop-oder Laptop Computer für andere Abteilungen oder Mitarbeiter in Ihrem Unternehmen erneut bereitstellen, können Sie BitLocker in die Wiederherstellung zwingen, bevor der Computer einem neuen Benutzer zugewiesen wird.

Testen der Wiederherstellung

Bevor Sie einen gründlichen BitLocker-Wiederherstellungsprozess erstellen, empfehlen wir, die Funktionsweise des Wiederherstellungsprozesses sowohl für Endbenutzer (Personen, die Ihren Helpdesk für das Wiederherstellungskennwort anrufen) als auch für Administratoren (Personen, die dem Endbenutzer helfen, das Wiederherstellungskennwort abzurufen) zu testen. . Der Befehl – forcerecovery von manage-bde bietet Ihnen eine einfache Möglichkeit, den Wiederherstellungsprozess zu durchlaufen, bevor die Benutzer eine Wiederherstellungs Situation erleben.

So erzwingen Sie eine Wiederherstellung für den lokalen Computer

1. Klicken Sie auf die Schaltfläche **Start** , geben Sie im Feld **Suche starten** den **Befehl cmd** ein, klicken Sie mit der rechten Maustaste auf **cmd. exe**, und klicken Sie dann auf **als Administrator ausführen**.
2. Geben Sie an der Eingabeaufforderung den folgenden Befehl ein, und drücken Sie dann die EINGABETASTE: `manage-bde -forcerecovery <BitLockerVolume>`

So erzwingen Sie die Wiederherstellung für einen Remotecomputer

1. Geben Sie im Start Bildschirm**cmd. exe**ein, und klicken Sie dann auf **als Administrator ausführen**.
2. Geben Sie an der Eingabeaufforderung den folgenden Befehl ein, und drücken Sie dann die EINGABETASTE: `manage-bde. -ComputerName <RemoteComputerName> -forcerecovery <BitLockerVolume>`

> **Hinweis:** die von `-forcerecovery` der Wiederherstellung ausgelöste Wiederherstellung wird für mehrere Neustarts fortgesetzt, bis eine TPM-Schutzkomponente hinzugefügt oder der Schutz des Benutzers angehalten wurde. Bei Verwendung von modernen Standby-Geräten (wie Surface-Geräten) `-forcerecovery` wird die Option nicht empfohlen, da BitLocker manuell aus der WinRE-Umgebung entsperrt und deaktiviert werden muss, bevor das Betriebssystem erneut booten kann. Weitere Informationen finden Sie unter BitLocker-Problembehandlung: Continuous Reboot-Schleife mit BitLocker-Wiederherstellung auf einem Slate-Gerät.

Planen des Wiederherstellungsprozesses

Wenn Sie den BitLocker-Wiederherstellungsprozess planen, konsultieren Sie zunächst die bewährten Methoden zur Wiederherstellung vertraulicher Informationen in Ihrer Organisation. Beispiel: wie behandelt Ihr Unternehmen verlorene Windows-Kennwörter? Wie führt Ihr Unternehmen Smartcard-PIN-zurücksetzen durch? Sie können diese bewährten Methoden und zugehörigen Ressourcen (Personen und Tools) verwenden, um ein BitLocker-Wiederherstellungsmodell zu formulieren.

Organisationen, die sich auf die BitLocker-Laufwerkverschlüsselung und BitLocker To Go stützen, um Daten auf einer Vielzahl von Computern und Wechseldatenträgern zu schützen, auf denen die Betriebssysteme Windows10, Windows 8 oder Windows 7 und Windows to go ausgeführt werden, sollten die Verwendung von Microsoft BitLocker-Verwaltungs-und-Überwachungs Tool (MBAM), Version 2,0, das im Microsoft Desktop Optimization Pack (MDOP) für Microsoft Software Assurance enthalten ist. MBAM vereinfacht die Bereitstellung und Verwaltung von BitLocker-Implementierungen und ermöglicht Administratoren die Bereitstellung und Überwachung der Verschlüsselung für Betriebssystem-und Festplatten. MBAM fordert den Benutzer auf, die Festplatten zu verschlüsseln. MBAM verwaltet auch Wiederherstellungsschlüssel für fest-und

Wechseldatenträger, wodurch die Wiederherstellung einfacher zu verwalten ist. MBAM kann als Teil einer Microsoft System Center-Bereitstellung oder als eigenständige Lösung verwendet werden. Weitere Informationen finden Sie unter Microsoft BitLocker-Verwaltung und-Überwachung.

Nachdem eine BitLocker-Wiederherstellung initiiert wurde, können Benutzer ein Wiederherstellungskennwort verwenden, um den Zugriff auf verschlüsselte Daten aufzuheben. Sie müssen sowohl Self-Recovery-als auch Wiederherstellungs-Kennwortabfrage Methoden für Ihre Organisation in Frage stellen.

Wenn Sie den Wiederherstellungsprozess ermitteln, sollten Sie Folgendes tun:

- Lernen Sie, wie Sie das Wiederherstellungskennwort abrufen können. Siehe:
  - Self-Recovery
  - Wiederherstellung des Kenn Wort Abrufs
- Ermitteln Sie eine Reihe von Schritten für die nach der Wiederherstellung, einschließlich der Analyse, warum die Wiederherstellung stattgefunden hat, und Zurücksetzen des Wiederherstellungskennworts. Siehe:
  - Analyse nach der Wiederherstellung

Self-Recovery

In einigen Fällen verfügen Benutzer möglicherweise über das Wiederherstellungskennwort in einem Ausdruck oder einem USB-Flashlaufwerk und können eine Selbstwiederherstellung durchführen. Wir empfehlen, dass Ihre Organisation eine Richtlinie für die Selbstwiederherstellung erstellt. Wenn die Self-Recovery-Anwendung ein Kennwort oder einen Wiederherstellungsschlüssel enthält, die auf einem USB-Stick gespeichert sind, sollten die Benutzer gewarnt werden, den USB-Stick nicht an der gleichen Stelle wie der PC zu speichern, insbesondere während des Reisens, beispielsweise wenn sich sowohl der PC als auch die Wiederherstellungselemente im gleichen Beutel befinden Es wäre sehr einfach, wenn ein unbefugter Nutzer auf den PC zugreifen kann. Eine andere zu berücksichtigende Richtlinie besteht darin, dass Benutzer den Helpdesk vor oder nach der Durchführung der Selbstwiederherstellung kontaktieren, damit die Ursache identifiziert werden kann.

Wiederherstellung des Kenn Wort Abrufs

Wenn der Benutzer kein Wiederherstellungskennwort auf einem Ausdruck oder auf einem USB-Stick hat, muss der Benutzer das Wiederherstellungskennwort aus einer Onlinequelle abrufen können. Wenn der PC Mitglied einer Domäne ist, kann das Wiederherstellungskennwort in AD DS gesichert werden. Dies geschieht jedoch standardmäßig nicht, Sie müssen die entsprechenden Gruppenrichtlinieneinstellungen konfiguriert haben, bevor BitLocker auf dem PC aktiviert wurde. BitLocker-Gruppenrichtlinieneinstellungen befinden sich im Editor für lokale Gruppenrichtlinien oder in der Gruppenrichtlinien-Verwaltungskonsole (Group Policy Management Console, GPMC) unter **Computer Configuration\Administrative Templates\Windows Components\BitLocker-Laufwerkverschlüsselung**. Die folgenden Richtlinieneinstellungen definieren die Wiederherstellungsmethoden, die zum Wiederherstellen des Zugriffs auf ein mit BitLocker geschütztes Laufwerk verwendet werden können, wenn eine Authentifizierungsmethode fehlschlägt oder nicht verwendet werden kann.

- **Auswählen, wie BitLocker-geschützte Betriebssystemlaufwerke wiederhergestellt werden können**
- **Auswählen, wie BitLocker-geschützte Festplatten wiederhergestellt werden können**
- **Auswählen, wie BitLocker-geschützte Wechsellaufwerke wiederhergestellt werden können** Wählen Sie in den einzelnen Richtlinien die Option **BitLocker-Wiederherstellungsinformationen in Active Directory-Domänendiensten speichern** aus, und wählen Sie dann die BitLocker-Wiederherstellungsinformationen aus, die in den Active Directory-Domänendiensten gespeichert werden sollen. Aktivieren Sie das Kontrollkästchen **BitLocker bis Wiederherstellungsinformationen werden nicht in AD DS gespeichert** , wenn Sie verhindern möchten, dass Benutzer BitLocker aktivieren können, es sei denn, der Computer ist mit der Domäne verbunden, und die BitLocker-Wiederherstellungsinformationen für das Laufwerk werden gesichert. Fügt erfolgreich hinzu.

> **Hinweis:** wenn die PCs zu einer Arbeitsgruppe gehören, sollten Benutzer darauf hingewiesen werden, Ihr

> BitLocker-Wiederherstellungskennwort mit Ihrem Microsoft-Konto online zu speichern. Es wird empfohlen, eine Onlinekopie Ihres BitLocker-Wiederherstellungskennworts zu erhalten, um sicherzustellen, dass der Zugriff auf Ihre Daten nicht verloren geht, falls eine Wiederherstellung erforderlich ist.

Das BitLocker-Wiederherstellungskennwort-Viewer-Tool für Active Directory-Benutzer und-Computer ermöglicht es Domänenadministratoren, BitLocker-Wiederherstellungskennwörter für bestimmte Computerobjekte in Active Directory anzuzeigen.

Sie können die folgende Liste als Vorlage zum Erstellen eines eigenen Wiederherstellungsprozesses für die Wiederherstellung des Kenn Wort Abrufs verwenden. In diesem Beispielprozess wird der BitLocker-Wiederherstellungskennwort-Viewer für Active Directory-Benutzer und-Computer verwendet.

- Aufzeichnen des Namens des Computers des Benutzers
- Überprüfen der Identität des Benutzers
- Suchen des Wiederherstellungskennworts in Adds
- Sammeln von Informationen, um zu ermitteln, warum eine Wiederherstellung erfolgt ist
- Dem Benutzer das Wiederherstellungskennwort zuweisen

Aufzeichnen des Namens des Computers des Benutzers

Sie können den Namen des Computers des Benutzers verwenden, um das Wiederherstellungskennwort in Adds zu finden. Wenn der Benutzer den Namen des Computers nicht kennt, bitten Sie den Benutzer, das erste Wort der **Laufwerk Beschriftung** auf der Benutzeroberfläche des **BitLocker Drive Encryption-Kennworteintrags** zu lesen. Hierbei handelt es sich um den Computernamen, wenn BitLocker aktiviert wurde und wahrscheinlich der aktuelle Name des Computers ist.

Überprüfen der Identität des Benutzers

Vergewissern Sie sich, dass die Person, die das Wiederherstellungskennwort auffordert, wirklich der autorisierte Benutzer dieses Computers ist. Sie können auch sicherstellen, dass der Computer mit dem vom Benutzer angegebenen Namen dem Nutzer gehört.

Suchen des Wiederherstellungskennworts in Adds

Suchen Sie das Computer Objekt mit dem übereinstimmenden Namen in Adds. Da Computer Objektnamen im globalen Katalog hinzugefügt aufgeführt werden, sollten Sie das Objekt auch dann finden können, wenn Sie über eine Gesamtstruktur mit mehreren Domänen verfügen.

Mehrere Wiederherstellungskennwörter

Wenn mehrere Wiederherstellungskennwörter unter einem Computerobjekt in Adds gespeichert sind, enthält der Name des BitLocker-Wiederherstellungs Informationsobjekts das Datum, an dem das Kennwort erstellt wurde.

Wenn Sie sich nicht sicher sind, welches Kennwort Sie angeben sollen, oder wenn Sie der Meinung sind, dass Sie möglicherweise das falsche Kennwort angeben, bitten Sie den Benutzer, die Kennwort-ID mit acht Zeichen zu lesen, die in der Wiederherstellungskonsole angezeigt wird.

Da es sich bei der Kenn Wort Kennung um einen eindeutigen Wert handelt, der jedem in Adds gespeicherten Wiederherstellungskennwort zugeordnet ist, wird durch Ausführen einer Abfrage mithilfe dieser ID das richtige Kennwort zum Entsperren des verschlüsselten Volumes gefunden.

Sammeln von Informationen, um zu ermitteln, warum eine Wiederherstellung erfolgt ist

Bevor Sie dem Benutzer das Wiederherstellungskennwort zuweisen, sollten Sie alle Informationen sammeln, anhand derer Sie ermitteln können, warum die Wiederherstellung erforderlich war, um die Ursache während der Analyse nach der Wiederherstellung zu analysieren. Weitere Informationen zur Analyse nach der Wiederherstellung finden Sie unter Analyse nach der Wiederherstellung.

Dem Benutzer das Wiederherstellungskennwort zuweisen

Da das Wiederherstellungskennwort 48 Ziffern lang ist, muss der Benutzer möglicherweise das Kennwort aufzeichnen, indem Sie es notieren oder auf einem anderen Computer eingeben. Wenn Sie MBAM verwenden, wird das Wiederherstellungskennwort erneut generiert, nachdem es aus der MBAM-Datenbank wiederhergestellt wurde, um die Sicherheitsrisiken zu vermeiden, die mit einem unkontrollierten Kennwort verbunden sind.

> **Hinweis:** da das 48-stellige Wiederherstellungskennwort lang ist und eine Kombination aus Ziffern enthält, kann es vorkommen, dass der Benutzer das Kennwort verhört oder versagt. Die Start Zeit Wiederherstellungskonsole verwendet integrierte Prüfsummen Nummern, um Eingabefehler in jedem sechsstelligen Block des 48-stelligen Wiederherstellungskennworts zu erkennen, und bietet dem Benutzer die Möglichkeit, derartige Fehler zu beheben.

Analyse nach der Wiederherstellung

Wenn ein Volume mithilfe eines Wiederherstellungskennworts freigegeben wird, wird ein Ereignis in das Ereignisprotokoll geschrieben, und die Platt Form Überprüfungs Messungen werden im TPM zurückgesetzt, um der aktuellen Konfiguration zu entsprechen. Das Entsperren des Volumes bedeutet, dass der Verschlüsselungsschlüssel freigegeben wurde und für die on-the-fly-Verschlüsselung bereit ist, wenn Daten auf das Volume geschrieben werden, und die Entschlüsselung erfolgt, wenn Daten vom Volume gelesen werden. Nach dem Entsperren des Volumes verhält sich BitLocker unabhängig davon, wie der Zugriff gewährt wurde, auf die gleiche Weise.

Wenn Sie feststellen, dass ein Computer wiederholte Wiederherstellungskennwort-Sperrungen aufweist, möchten Sie möglicherweise einen Administrator nach der Wiederherstellung durchführen, um die Ursache der Wiederherstellung zu ermitteln und die BitLocker-plattformüberprüfung zu aktualisieren, damit der Benutzer nicht mehr jedes Mal, wenn der Computer gestartet wird, muss ein Wiederherstellungskennwort eingegeben werden. Siehe:

- Ermitteln der Hauptursache der Wiederherstellung
- Aktualisieren des BitLocker-Schutzes

Ermitteln der Hauptursache der Wiederherstellung

Wenn ein Benutzer das Laufwerk wiederherstellen musste, ist es wichtig, die Ursache zu ermitteln, die die Wiederherstellung so schnell wie möglich initiiert hat. Durch eine ordnungsgemäße Analyse des Zustands des Computers und das Erkennen von Manipulationen können Bedrohungen auftreten, die umfassendere Auswirkungen auf die Unternehmenssicherheit haben.

Während ein Administrator die Ursache für die Wiederherstellung in einigen Fällen Remote untersuchen kann, muss der Endbenutzer möglicherweise den Computer, auf dem das wiederhergestellte Laufwerk enthalten ist, auf der Website bereitstellen, um die Ursachen weiter zu analysieren.

Überprüfen und beantworten Sie die folgenden Fragen für Ihre Organisation:

1. Welcher BitLocker-Schutzmodus ist aktiviert (TPM, TPM + PIN, TPM + Startschlüssel, nur Startschlüssel)? Welches PCR-Profil wird auf dem PC verwendet?
2. Hat der Benutzer lediglich die PIN vergessen oder den Startschlüssel verloren? Wenn ein Token verloren ging, wo kann das Token sein?
3. Wenn der TPM-Modus aktiviert war, wurde die Wiederherstellung durch eine Boot Dateiänderung verursacht?
4. Wenn die Wiederherstellung durch eine Boot Dateiänderung verursacht wurde, liegt dies an einer beabsichtigten Benutzeraktion (beispielsweise BIOS-Aktualisierung) oder an bösartiger Software?
5. Wann war der Benutzer zuletzt in der Lage, den Computer erfolgreich zu starten, und was ist seither möglicherweise mit dem Computer geschehen?
6. Kann der Benutzer bösartige Software gefunden haben oder den Computer seit dem letzten erfolgreichen Start unbeaufsichtigt lassen?

Wenn Sie diese Fragen beantworten möchten, verwenden Sie das BitLocker-Befehlszeilentool, um den aktuellen

Konfigurations-und Schutzmodus anzuzeigen (beispielsweise **manage-bde-Status**). Überprüfen Sie das Ereignisprotokoll, um Ereignisse zu finden, die angeben, warum die Wiederherstellung initiiert wurde (beispielsweise, wenn die Boot Dateiänderung aufgetreten ist). Beide Funktionen können Remote ausgeführt werden.

Beheben der Ursache

Nachdem Sie festgestellt haben, was die Wiederherstellung verursacht hat, können Sie den BitLocker-Schutz zurücksetzen und die Wiederherstellung bei jedem Start verhindern.

Die Details dieses Zurücksetzens können je nach der Hauptursache der Wiederherstellung variieren. Wenn Sie die Ursache nicht ermitteln können, oder wenn Schadsoftware oder ein Rootkit den Computer infiziert haben, sollte Helpdesk bewährte Viren Richtlinien anwenden, um entsprechend reagieren zu können.

> **Hinweis:** Sie können ein BitLocker-Validierungs Profil zurücksetzen, indem Sie BitLocker anhalten und fortsetzen.

- Unbekannte PIN
- Startschlüssel verloren
- Änderungen an Startdateien ### Unbekannte PIN

Wenn ein Benutzer die PIN vergessen hat, müssen Sie die PIN zurücksetzen, während Sie bei dem Computer angemeldet sind, um zu verhindern, dass BitLocker beim Neustart des Computers eine Wiederherstellung initiiert.

So verhindern Sie die fortlaufende Wiederherstellung aufgrund einer unbekannten PIN

1. Entsperren Sie den Computer mit dem Wiederherstellungskennwort.
2. Zurücksetzen der PIN:
   a. Klicken Sie mit der rechten Maustaste auf das Laufwerk, und klicken Sie dann auf **PIN ändern**
   b. Klicken Sie im Dialogfeld BitLocker-Laufwerkverschlüsselung auf **vergessene Pins zurücksetzen**. Wenn Sie nicht mit einem Administratorkonto angemeldet sind, müssen Sie zu diesem Zeitpunkt Administratoranmeldeinformationen angeben.
   c. Geben Sie im Dialogfeld Pin-Reset die zu verwendende neue PIN ein, und bestätigen Sie Sie, und klicken Sie dann auf **Fertig stellen**.
3. Sie werden die neue PIN verwenden, wenn Sie das Laufwerk das nächste Mal entsperren.

Startschlüssel verloren

Wenn Sie das USB-Flashlaufwerk verloren haben, das den Startschlüssel enthält, müssen Sie das Laufwerk mit dem Wiederherstellungsschlüssel entsperren und dann einen neuen Startschlüssel erstellen.

So verhindern Sie die fortlaufende Wiederherstellung aufgrund eines verlorenen Startschlüssels

1. Melden Sie sich als Administrator auf dem Computer an, auf dem sich der Schlüssel "verloren" befindet.
2. Öffnen Sie BitLocker verwalten.
3. Klicken Sie auf **doppelte Start Taste**, fügen Sie das saubere USB-Laufwerk ein, auf dem Sie den Schlüssel schreiben möchten, und klicken Sie dann auf **Speichern**.

Änderungen an Startdateien

Dieser Fehler kann auftreten, wenn Sie die Firmware aktualisiert haben. Als bewährte Methode sollten Sie BitLocker anhalten, bevor Sie die Firmware ändern und dann den Schutz fortsetzen, nachdem die Aktualisierung abgeschlossen ist. Dadurch wird verhindert, dass der Computer in den Wiederherstellungsmodus wechselt. Wenn jedoch Änderungen vorgenommen wurden, als der BitLocker-Schutz aktiviert war, können Sie sich einfach mit dem Wiederherstellungskennwort beim Computer anmelden, und das Platt Form Überprüfungsprofil wird aktualisiert, damit die Wiederherstellung nicht beim nächsten Mal stattfindet.

Windows RE-und BitLocker-Geräteverschlüsselung

Die Windows-Wiederherstellungsumgebung (Re) kann verwendet werden, um den Zugriff auf ein Laufwerk wiederherzustellen, das durch die BitLocker-Geräteverschlüsselunggeschützt ist. Wenn ein PC nach zwei Fehlern nicht gestartet werden kann, wird die Startreparatur automatisch gestartet. Wenn die Startreparatur aufgrund von Startfehlern automatisch gestartet wird, werden nur Betriebssystem-und Treiberdatei Reparaturen ausgeführt, vorausgesetzt, dass die Start Protokolle oder ein verfügbares Absturzspeicherabbild auf eine bestimmte beschädigte Datei verweisen. In Windows 8,1 und höher können Geräte, die eine Firmware zur Unterstützung spezifischer TPM-Messungen für PCR \ [7] enthalten, das TPM überprüfen, ob Windows RE eine vertrauenswürdige Betriebsumgebung ist, und alle von BitLocker geschützten Laufwerke entsperren, wenn Windows RE nicht geändert wurde. Wenn die Windows RE-Umgebung geändert wurde, beispielsweise wenn das TPM deaktiviert wurde, bleiben die Laufwerke so lange gesperrt, bis der BitLocker-Wiederherstellungsschlüssel bereitgestellt wird. Wenn die Startreparatur nicht automatisch vom PC ausgeführt werden kann und stattdessen Windows RE manuell von einem Reparatur Datenträger gestartet wird, muss der BitLocker-Wiederherstellungsschlüssel bereitgestellt werden, um die BitLocker-geschützten Laufwerke zu entsperren.

Verwenden zusätzlicher Wiederherstellungsinformationen

Neben dem 48-stelligen BitLocker-Wiederherstellungskennwort werden andere Arten von Wiederherstellungsinformationen in Active Directory gespeichert. In diesem Abschnitt wird beschrieben, wie diese zusätzlichen Informationen verwendet werden können.

BitLocker-Schlüsselpaket

Wenn die zuvor in diesem Dokument erörterten Wiederherstellungsmethoden die Lautstärke nicht entsperren, können Sie das BitLocker-Reparaturtool verwenden, um die Lautstärke auf Blockebene zu entschlüsseln. Das Tool verwendet das BitLocker-Schlüsselpaket, um verschlüsselte Daten von schwer beschädigten Laufwerken wiederherzustellen. Sie können diese wiederhergestellten Daten dann verwenden, um verschlüsselte Daten zu retten, auch wenn das richtige Wiederherstellungskennwort das beschädigte Volume nicht entsperren konnte. Wir empfehlen, das Wiederherstellungskennwort weiterhin zu speichern. Ein Schlüsselpaket kann nicht ohne das entsprechende Wiederherstellungskennwort verwendet werden.

> **Hinweis:** Sie müssen das BitLocker-Reparaturtool **Repair-bde** verwenden, um das BitLocker-Schlüsselpaket zu verwenden.

Das BitLocker-Schlüsselpaket wird nicht standardmäßig gespeichert. Wenn Sie das Paket zusammen mit dem Wiederherstellungskennwort in AD DS speichern möchten, müssen Sie in den Gruppenrichtlinieneinstellungen, mit denen die Wiederherstellungsmethode gesteuert wird, die Option Kennwort für die **Sicherungswiederherstellung und das Schlüsselpaket** auswählen. Sie können das Schlüsselpaket auch aus einem Arbeitsvolume exportieren. Weitere Informationen zum Exportieren von Schlüsselpaketen finden Sie unter Abrufen des BitLocker-Schlüsselpakets.

Zurücksetzen von Wiederherstellungskennwörtern

Sie sollten ein Wiederherstellungskennwort ungültig machen, nachdem es bereitgestellt und verwendet wurde. Dies sollte auch erfolgen, wenn Sie aus irgendeinem Grund absichtlich ein vorhandenes Wiederherstellungskennwort ungültig machen möchten.

Sie können das Wiederherstellungskennwort auf zwei Arten zurücksetzen:

- **Verwenden von manage-bde** Sie können manage-bde verwenden, um das alte Wiederherstellungskennwort zu entfernen und ein neues Wiederherstellungskennwort hinzuzufügen. Die Prozedur identifiziert den Befehl und die Syntax für diese Methode.
- **Ausführen eines Skripts** Sie können ein Skript ausführen, um das Kennwort zurückzusetzen, ohne die

Lautstärke zu entschlüsseln. Das Beispielskript in der Prozedur veranschaulicht diese Funktionalität. Das Beispielskript erstellt ein neues Wiederherstellungskennwort und macht alle anderen Kennwörter ungültig.

So setzen Sie ein Wiederherstellungskennwort mithilfe von manage-bde zurück

1. Entfernen des vorherigen Wiederherstellungskennworts

```
Manage-bde –protectors –delete C: –type RecoveryPassword
```

2. Hinzufügen des neuen Wiederherstellungskennworts

```
Manage-bde –protectors –add C: -RecoveryPassword
```

3. Rufen Sie die ID des neuen Wiederherstellungskennworts ab. Kopieren Sie auf dem Bildschirm die ID des Wiederherstellungskennworts.

```
Manage-bde –protectors –get C: -Type RecoveryPassword
```

4. Sichern des neuen Wiederherstellungskennworts in AD DS

```
Manage-bde –protectors –adbackup C: -id {EXAMPLE6-5507-4924-AA9E-AFB2EB003692}
```

> **Warnung:** Sie müssen die geschweiften Klammern in die ID-Zeichenfolge einbeziehen.

So führen Sie das Beispielkennwort für die Wiederherstellung aus

1. Speichern Sie das folgende Beispielskript in einer VBScript-Datei. Beispiel: ResetPassword. vbs.
2. Geben Sie an der Eingabeaufforderung einen Befehl ähnlich der folgenden ein:

   cscript ResetPassword. vbs

> **Wichtig:** Dieses Beispielskript ist so konfiguriert, dass es nur für das C-Volume funktioniert. Sie müssen das Skript so anpassen, dass es dem Volume entspricht, auf dem Sie die Kennwortzurücksetzung testen möchten.
>
> **Hinweis:** Wenn Sie einen Remotecomputer verwalten möchten, können Sie den Namen des Remotecomputers und nicht den Namen des lokalen Computers angeben.

Mit dem folgenden Beispielskript können Sie eine VBScript-Datei erstellen, um die Wiederherstellungskennwörter zurückzusetzen.

```
' Target drive letter
strDriveLetter = "c:"
' Target computer name
' Use "." to connect to the local computer
strComputerName = "."
' ---------------------------------------------------------------------------
' Connect to the BitLocker WMI provider class
' ---------------------------------------------------------------------------
strConnectionStr = "winmgmts:" _
                 & "{impersonationLevel=impersonate,authenticationLevel=pktPrivacy}!\\" _
                 & strComputerName _
                 & "\root\cimv2\Security\MicrosoftVolumeEncryption"


On Error Resume Next 'handle permission errors
Set objWMIService = GetObject(strConnectionStr)
```

```
Set objWMIService = GetObject(strConnectionStr)
If Err.Number <> 0 Then
     WScript.Echo "Failed to connect to the BitLocker interface (Error 0x" & Hex(Err.Number) & ")."
     Wscript.Echo "Ensure that you are running with administrative privileges."
     WScript.Quit -1
End If
On Error GoTo 0
strQuery = "Select * from Win32_EncryptableVolume where DriveLetter='" & strDriveLetter & "'"
Set colTargetVolumes = objWMIService.ExecQuery(strQuery)
If colTargetVolumes.Count = 0 Then
    WScript.Echo "FAILURE: Unable to find BitLocker-capable drive " &  strDriveLetter & " on computer " &
strComputerName & "."
    WScript.Quit -1
End If
' there should only be one volume found
For Each objFoundVolume in colTargetVolumes
    set objVolume = objFoundVolume
Next
' objVolume is now our found BitLocker-capable disk volume
' ---------------------------------------------------------------------------
' Perform BitLocker WMI provider functionality
' ---------------------------------------------------------------------------
' Add a new recovery password, keeping the ID around so it doesn't get deleted later
' ---------------------------------------------------------------------------
nRC = objVolume.ProtectKeyWithNumericalPassword("Recovery Password Refreshed By Script", , sNewKeyProtectorID)
If nRC <> 0 Then
WScript.Echo "FAILURE: ProtectKeyWithNumericalPassword failed with return code 0x" & Hex(nRC)
WScript.Quit -1
End If
' Removes the other, "stale", recovery passwords
' ---------------------------------------------------------------------------
nKeyProtectorTypeIn = 3 ' type associated with "Numerical Password" protector
nRC = objVolume.GetKeyProtectors(nKeyProtectorTypeIn, aKeyProtectorIDs)
If nRC <> 0 Then
WScript.Echo "FAILURE: GetKeyProtectors failed with return code 0x" & Hex(nRC)
WScript.Quit -1
End If
' Delete those key protectors other than the one we just added.
For Each sKeyProtectorID In aKeyProtectorIDs
If sKeyProtectorID <> sNewKeyProtectorID Then
nRC = objVolume.DeleteKeyProtector(sKeyProtectorID)
If nRC <> 0 Then
WScript.Echo "FAILURE: DeleteKeyProtector on ID " & sKeyProtectorID & " failed with return code 0x" & Hex(nRC)
WScript.Quit -1
Else
' no output
'WScript.Echo "SUCCESS: Key protector with ID " & sKeyProtectorID & " deleted"
End If
End If
Next
WScript.Echo "A new recovery password has been added. Old passwords have been removed."
' - some advanced output (hidden)
'WScript.Echo ""
'WScript.Echo "Type ""manage-bde -protectors -get " & strDriveLetter & " -type recoverypassword"" to view
existing passwords."
```

Abrufen des BitLocker-Schlüsselpakets

Sie können zwei Methoden verwenden, um das Schlüsselpaket abzurufen, wie unter Verwenden zusätzlicher Wiederherstellungsinformationenbeschrieben:

- **Exportieren eines zuvor gespeicherten Schlüsselpakets aus Adds.** Sie müssen über Lesezugriff auf Kennwörter für BitLocker-Wiederherstellung verfügen, die in Adds gespeichert sind.
- **Exportieren eines neuen Schlüsselpakets aus einem nicht gesperrten, mit BitLocker geschützten Volume** Sie benötigen lokalen Administratorzugriff auf das Arbeitsvolumen, bevor ein Schaden eingetreten

ist.

Im folgenden Beispielskript werden alle zuvor gespeicherten Schlüsselpakete von Adds exportiert.

So führen Sie das Skript zum Abrufen von Schlüsselpaketen aus

1. Speichern Sie das folgende Beispielskript in einer VBScript-Datei. Beispiel: GetBitLockerKeyPackageADDS.vbs.
2. Geben Sie an der Eingabeaufforderung einen Befehl ähnlich der folgenden ein:

   cscript GetBitLockerKeyPackageADDS. vbs-?

Mit dem folgenden Beispielskript können Sie eine VBScript-Datei erstellen, um das BitLocker-Schlüsselpaket von Adds abzurufen.

```
' ---------------------------------------------------------------------------
' Usage
' ---------------------------------------------------------------------------
Sub ShowUsage
   Wscript.Echo "USAGE: GetBitLockerKeyPackageADDS [Path To Save Key Package] [Optional Computer Name]"
   Wscript.Echo "If no computer name is specified, the local computer is assumed."
   Wscript.Echo
   Wscript.Echo "Example: GetBitLockerKeyPackageADDS E:\bitlocker-ad-key-package mycomputer"
   WScript.Quit
End Sub
' ---------------------------------------------------------------------------
' Parse Arguments
' ---------------------------------------------------------------------------
Set args = WScript.Arguments
Select Case args.Count
  Case 1
    If args(0) = "/?" Or args(0) = "-?" Then
    ShowUsage
    Else
      strFilePath = args(0)
      ' Get the name of the local computer
      Set objNetwork = CreateObject("WScript.Network")
      strComputerName = objNetwork.ComputerName
    End If

  Case 2
    If args(0) = "/?" Or args(0) = "-?" Then
      ShowUsage
    Else
      strFilePath = args(0)
      strComputerName = args(1)
    End If
  Case Else
    ShowUsage
End Select
' ---------------------------------------------------------------------------
' Get path to Active Directory computer object associated with the computer name
' ---------------------------------------------------------------------------
Function GetStrPathToComputer(strComputerName)
    ' Uses the global catalog to find the computer in the forest
    ' Search also includes deleted computers in the tombstone
    Set objRootLDAP = GetObject("LDAP://rootDSE")
    namingContext = objRootLDAP.Get("defaultNamingContext") ' e.g. string dc=fabrikam,dc=com
    strBase = "<GC://" & namingContext & ">"

    Set objConnection = CreateObject("ADODB.Connection")
    Set objCommand = CreateObject("ADODB.Command")
    objConnection.Provider = "ADsDSOOBject"
    objConnection.Open "Active Directory Provider"
    Set objCommand.ActiveConnection = objConnection
    strFilter = "(&(objectCategory=Computer)(cn=" &  strComputerName & "))"
```

```
    strQuery = strBase & ";" & strFilter  & ";distinguishedName;subtree"
    objCommand.CommandText = strQuery
    objCommand.Properties("Page Size") = 100
    objCommand.Properties("Timeout") = 100
    objCommand.Properties("Cache Results") = False
    ' Enumerate all objects found.
    Set objRecordSet = objCommand.Execute
    If objRecordSet.EOF Then
      WScript.echo "The computer name '" &  strComputerName & "' cannot be found."
      WScript.Quit 1
    End If
    ' Found object matching name
    Do Until objRecordSet.EOF
      dnFound = objRecordSet.Fields("distinguishedName")
      GetStrPathToComputer = "LDAP://" & dnFound
      objRecordSet.MoveNext
    Loop
    ' Clean up.
    Set objConnection = Nothing
    Set objCommand = Nothing
    Set objRecordSet = Nothing
End Function
' ---------------------------------------------------------------------------
' Securely access the Active Directory computer object using Kerberos
' ---------------------------------------------------------------------------
Set objDSO = GetObject("LDAP:")
strPathToComputer = GetStrPathToComputer(strComputerName)
WScript.Echo "Accessing object: " + strPathToComputer
Const ADS_SECURE_AUTHENTICATION = 1
Const ADS_USE_SEALING = 64 '0x40
Const ADS_USE_SIGNING = 128 '0x80
' ---------------------------------------------------------------------------
' Get all BitLocker recovery information from the Active Directory computer object
' ---------------------------------------------------------------------------
' Get all the recovery information child objects of the computer object
Set objFveInfos = objDSO.OpenDSObject(strPathToComputer, vbNullString, vbNullString, _
                                  ADS_SECURE_AUTHENTICATION + ADS_USE_SEALING + ADS_USE_SIGNING)
objFveInfos.Filter = Array("msFVE-RecoveryInformation")
' Iterate through each recovery information object and saves any existing key packages
nCount = 1
strFilePathCurrent = strFilePath & nCount
For Each objFveInfo in objFveInfos
   strName = objFveInfo.Get("name")
   strRecoveryPassword = objFveInfo.Get("msFVE-RecoveryPassword")
   strKeyPackage = objFveInfo.Get("msFVE-KeyPackage")
   WScript.echo
   WScript.echo "Recovery Object Name: " + strName
   WScript.echo "Recovery Password: " + strRecoveryPassword
   ' Validate file path
   Set fso = CreateObject("Scripting.FileSystemObject")
   If (fso.FileExists(strFilePathCurrent)) Then
 WScript.Echo "The file " & strFilePathCurrent & " already exists. Please use a different path."
WScript.Quit -1
   End If
   ' Save binary data to the file
   SaveBinaryDataText strFilePathCurrent, strKeyPackage

   WScript.echo "Related key package successfully saved to " + strFilePathCurrent
   ' Update next file path using base name
   nCount = nCount + 1
   strFilePathCurrent = strFilePath & nCount
Next
'-----------------------------------------------------------------------------------------
' Utility functions to save binary data
'-----------------------------------------------------------------------------------------
Function SaveBinaryDataText(FileName, ByteArray)
  'Create FileSystemObject object
  Dim FS: Set FS = CreateObject("Scripting.FileSystemObject")
```

```
  'Create text stream object
  Dim TextStream
  Set TextStream = FS.CreateTextFile(FileName)

  'Convert binary data To text And write them To the file
  TextStream.Write BinaryToString(ByteArray)
End Function
Function BinaryToString(Binary)
  Dim I, S
  For I = 1 To LenB(Binary)
    S = S & Chr(AscB(MidB(Binary, I, 1)))
  Next
  BinaryToString = S
End Function
WScript.Quit
```

Im folgenden Beispielskript wird ein neues Schlüsselpaket aus einem nicht gesperrten, verschlüsselten Volume exportiert.

So führen Sie das Skript zum Abrufen von Schlüsselpaketen aus

1. Speichern Sie das folgende Beispielskript in einer VBScript-Datei. Beispiel: GetBitLockerKeyPackage. vbs
2. Öffnen Sie eine Eingabeaufforderung des Administrators, und geben Sie einen Befehl ähnlich der folgenden ein:

   cscript GetBitLockerKeyPackage. vbs-?

```
' ---------------------------------------------------------------------------
' Usage
' ---------------------------------------------------------------------------
Sub ShowUsage
   Wscript.Echo "USAGE: GetBitLockerKeyPackage [VolumeLetter/DriveLetter:] [Path To Save Key Package]"
   Wscript.Echo
   Wscript.Echo "Example: GetBitLockerKeyPackage C: E:\bitlocker-backup-key-package"
   WScript.Quit
End Sub
' ---------------------------------------------------------------------------
' Parse Arguments
' ---------------------------------------------------------------------------
Set args = WScript.Arguments
Select Case args.Count
  Case 2
    If args(0) = "/?" Or args(0) = "-?" Then
      ShowUsage
    Else
      strDriveLetter = args(0)
      strFilePath = args(1)
    End If
  Case Else
    ShowUsage
End Select
' ---------------------------------------------------------------------------
' Other Inputs
' ---------------------------------------------------------------------------
' Target computer name
' Use "." to connect to the local computer
strComputerName = "."
' Default key protector ID to use. Specify "" to let the script choose.
strDefaultKeyProtectorID = ""
' strDefaultKeyProtectorID = "{001298E0-870E-4BA0-A2FF-FC74758D5720}"  ' sample
' ---------------------------------------------------------------------------
' Connect to the BitLocker WMI provider class
' ---------------------------------------------------------------------------
strConnectionStr = "winmgmts:" _
                 & "{impersonationLevel=impersonate,authenticationLevel=pktPrivacy}!\\" _
                 & strComputerName
```

```
                    & strComputerName _
                    & "\root\cimv2\Security\MicrosoftVolumeEncryption"


On Error Resume Next 'handle permission errors
Set objWMIService = GetObject(strConnectionStr)
If Err.Number <> 0 Then
     WScript.Echo "Failed to connect to the BitLocker interface (Error 0x" & Hex(Err.Number) & ")."
     Wscript.Echo "Ensure that you are running with administrative privileges."
     WScript.Quit -1
End If
On Error GoTo 0
strQuery = "Select * from Win32_EncryptableVolume where DriveLetter='" & strDriveLetter & "'"
Set colTargetVolumes = objWMIService.ExecQuery(strQuery)
If colTargetVolumes.Count = 0 Then
    WScript.Echo "FAILURE: Unable to find BitLocker-capable drive " &  strDriveLetter & " on computer " &
strComputerName & "."
    WScript.Quit -1
End If
' there should only be one volume found
For Each objFoundVolume in colTargetVolumes
    set objVolume = objFoundVolume
Next
' objVolume is now our found BitLocker-capable disk volume
' ---------------------------------------------------------------------------
' Perform BitLocker WMI provider functionality
' ---------------------------------------------------------------------------
' Collect all possible valid key protector ID's that can be used to get the package
' ----------------------------------------------------------------------------
nNumericalKeyProtectorType = 3 ' type associated with "Numerical Password" protector
nRC = objVolume.GetKeyProtectors(nNumericalKeyProtectorType, aNumericalKeyProtectorIDs)
If nRC <> 0 Then
WScript.Echo "FAILURE: GetKeyProtectors failed with return code 0x" & Hex(nRC)
WScript.Quit -1
End If
nExternalKeyProtectorType = 2 ' type associated with "External Key" protector
nRC = objVolume.GetKeyProtectors(nExternalKeyProtectorType, aExternalKeyProtectorIDs)
If nRC <> 0 Then
WScript.Echo "FAILURE: GetKeyProtectors failed with return code 0x" & Hex(nRC)
WScript.Quit -1
End If
' Get first key protector of the type "Numerical Password" or "External Key", if any
' ----------------------------------------------------------------------------
if strDefaultKeyProtectorID = "" Then
' Save first numerical password, if exists
If UBound(aNumericalKeyProtectorIDs) <> -1 Then
strDefaultKeyProtectorID = aNumericalKeyProtectorIDs(0)
End If
' No numerical passwords exist, save the first external key
If strDefaultKeyProtectorID = "" and UBound(aExternalKeyProtectorIDs) <> -1 Then
strDefaultKeyProtectorID = aExternalKeyProtectorIDs(0)
End If
' Fail case: no recovery key protectors exist.
If strDefaultKeyProtectorID = "" Then
WScript.Echo "FAILURE: Cannot create backup key package because no recovery passwords or recovery keys exist.
Check that BitLocker protection is on for this drive."
WScript.Echo "For help adding recovery passwords or recovery keys, type ""manage-bde -protectors -add -?""."
WScript.Quit -1
End If
End If
' Get some information about the chosen key protector ID
' ----------------------------------------------------------------------------
' is the type valid?
nRC = objVolume.GetKeyProtectorType(strDefaultKeyProtectorID, nDefaultKeyProtectorType)
If Hex(nRC) = "80070057" Then
WScript.Echo "The key protector ID " & strDefaultKeyProtectorID & " is not valid."
WScript.Echo "This ID value may have been provided by the script writer."
ElseIf nRC <> 0 Then
WScript.Echo "FAILURE: GetKeyProtectorType failed with return code 0x" & Hex(nRC)
WScript.Quit -1
```

```
WScript.Quit -1
End If
' what's a string that can be used to describe it?
strDefaultKeyProtectorType = ""
Select Case nDefaultKeyProtectorType
  Case nNumericalKeyProtectorType
      strDefaultKeyProtectorType = "recovery password"
  Case nExternalKeyProtectorType
      strDefaultKeyProtectorType = "recovery key"
  Case Else
      WScript.Echo "The key protector ID " & strDefaultKeyProtectorID & " does not refer to a valid recovery
password or recovery key."
      WScript.Echo "This ID value may have been provided by the script writer."
End Select
' Save the backup key package using the chosen key protector ID
' ------------------------------------------------------------------------------
nRC = objVolume.GetKeyPackage(strDefaultKeyProtectorID, oKeyPackage)
If nRC <> 0 Then
WScript.Echo "FAILURE: GetKeyPackage failed with return code 0x" & Hex(nRC)
WScript.Quit -1
End If
' Validate file path
Set fso = CreateObject("Scripting.FileSystemObject")
If (fso.FileExists(strFilePath)) Then
WScript.Echo "The file " & strFilePath & " already exists. Please use a different path."
WScript.Quit -1
End If
Dim oKeyPackageByte, bKeyPackage
For Each oKeyPackageByte in oKeyPackage
  'WScript.echo "key package byte: " & oKeyPackageByte
  bKeyPackage = bKeyPackage & ChrB(oKeyPackageByte)
Next
' Save binary data to the file
SaveBinaryDataText strFilePath, bKeyPackage
' Display helpful information
' ------------------------------------------------------------------------------
WScript.Echo "The backup key package has been saved to " & strFilePath & "."
WScript.Echo "IMPORTANT: To use this key package, the " & strDefaultKeyProtectorType & " must also be saved."
' Display the recovery password or a note about saving the recovery key file
If nDefaultKeyProtectorType = nNumericalKeyProtectorType Then
nRC = objVolume.GetKeyProtectorNumericalPassword(strDefaultKeyProtectorID, sNumericalPassword)
If nRC <> 0 Then
WScript.Echo "FAILURE: GetKeyProtectorNumericalPassword failed with return code 0x" & Hex(nRC)
WScript.Quit -1
End If
WScript.Echo "Save this recovery password: " & sNumericalPassword
ElseIf nDefaultKeyProtectorType = nExternalKeyProtectorType Then
WScript.Echo "The saved key file is named " & strDefaultKeyProtectorID & ".BEK"
WScript.Echo "For help re-saving this external key file, type ""manage-bde -protectors -get -?"""
End If
'-----------------------------------------------------------------------------------
' Utility functions to save binary data
'-----------------------------------------------------------------------------------
Function SaveBinaryDataText(FileName, ByteArray)
  'Create FileSystemObject object
  Dim FS: Set FS = CreateObject("Scripting.FileSystemObject")

  'Create text stream object
  Dim TextStream
  Set TextStream = FS.CreateTextFile(FileName)

  'Convert binary data To text And write them To the file
  TextStream.Write BinaryToString(ByteArray)
End Function
Function BinaryToString(Binary)
  Dim I, S
  For I = 1 To LenB(Binary)
    S = S & Chr(AscB(MidB(Binary, I, 1)))
  Next
```

```
    BinaryToString = S
  End Function
```

Weitere Informationen

- Übersicht über BitLocker

BitLocker-Gegenmaßnahmen

27.10.2019 • 9 minutes to read

Betrifft

- Windows 10

Windows verwendet Technologien wie TPM (Trusted Platform Module), sicheres Booten und gemessener Start, um BitLocker-Verschlüsselungsschlüssel vor Angriffen zu schützen. BitLocker ist Teil eines strategischen Ansatzes zum Sichern von Daten vor Offlineangriffen mithilfe von Verschlüsselungstechnologien. Daten auf einem verloren gegangenen oder gestohlenen Computer sind verwundbar. So kann beispielsweise ein unbefugter Zugriff erfolgen, entweder durch Ausführen eines Software-Angriffstools oder durch übertragen der Festplatte des Computers auf einen anderen Computer.

BitLocker hilft, den unbefugten Datenzugriff auf verloren gegangenen oder gestohlenen Computern zu verringern, bevor das autorisierte Betriebssystem gestartet wird:

- **Verschlüsseln von Volumes auf Ihrem Computer.** So können Sie beispielsweise BitLocker für Ihr Betriebssystemvolume oder ein Volume auf einem festen oder Wechseldatenträger (wie einem USB-Stick, einer SD-Karte usw.) aktivieren. Wenn Sie BitLocker für Ihr Betriebssystemvolume aktivieren, werden alle Systemdateien auf dem Datenträger verschlüsselt, einschließlich der Auslagerungsdateien und Ruhezustandsdateien. Die einzige Ausnahme ist die System Partition, die den Windows-Start-Manager und minimale Start Sicherheiten enthält, die für die Entschlüsselung des Betriebs System Datenträgers erforderlich sind, nachdem der Schlüssel entsiegelt wurde.
- **Sicherstellen der Integrität von frühen Startkomponenten und Startkonfigurationsdaten** Auf Geräten mit einer TPM-Version 1,2 oder höher verwendet BitLocker die erweiterten Sicherheitsfunktionen des TPM, um Daten nur dann zugänglich zu machen, wenn der BIOS-Firmwarecode und die Konfiguration des Computers, die ursprüngliche Startsequenz, die Startkomponenten und die BCD-Konfiguration alle wird unverändert angezeigt, und der verschlüsselte Datenträger befindet sich auf dem ursprünglichen Computer. Auf Systemen, die TPM-PCR nutzen [7], sind BCD-Einstellungen, die als sicher eingestuft werden, zur Verbesserung der Benutzerfreundlichkeit zugelassen.

In den nächsten Abschnitten finden Sie weitere Informationen dazu, wie Windows vor verschiedenen Angriffen auf die BitLocker-Verschlüsselungsschlüssel in Windows 10, Windows 8,1 und Windows 8 schützt.

Weitere Informationen dazu, wie Sie die beste Gesamt Sicherheitskonfiguration für Geräte aktivieren, die mit Windows 10, Version 1803, beginnen, finden Sie unter Standards für ein hochsicheres Windows 10-Gerät.

Schutz vor dem Start

Bevor Windows gestartet wird, müssen Sie sich auf Sicherheitsfeatures verlassen, die als Teil der Gerätehardware und-Firmware implementiert sind, einschließlich TPM und Secure Boot. Glücklicherweise verfügen viele moderne Computer über ein TPM und einen sicheren Start.

Trusted Platform Module

Bei einem TPM handelt es sich um einen Mikrochip, der grundlegende sicherheitsrelevante Funktionen bereitstellen soll, hauptsächlich mit Verschlüsselungsschlüsseln. Auf einigen Plattformen kann TPM auch als Teil der sicheren Firmware implementiert werden. BitLocker bindet Verschlüsselungsschlüssel an das TPM, um sicherzustellen, dass ein Computer nicht manipuliert wurde, während das System offline war. Weitere Informationen zu TPM finden Sie unter Trusted Platform Module.

UEFI und sicheres Booten

Unified Extensible Firmware Interface (UEFI) ist eine programmierbare Boot-Umgebung, die Geräte initialisiert und den Bootloader des Betriebssystems startet.

Die UEFI-Spezifikation definiert einen Firmware-Ausführungs Authentifizierungsprozess mit dem Namen Secure Boot. Secure Boot blockiert nicht vertrauenswürdige Firmware und Bootloader (signiert oder nicht signiert), damit Sie nicht auf dem System gestartet werden können.

Standardmäßig bietet BitLocker Integritätsschutz für sicheres Booten durch Verwendung der TPM-PCR [7]-Messung. Eine nicht autorisierte EFI-Firmware, EFI-Startanwendung oder ein Bootloader kann nicht ausgeführt werden und den BitLocker-Schlüssel abrufen.

BitLocker-und Reset-Angriffe

Zur Abwehr von böswilligen Zurücksetzungs Angriffen nutzt BitLocker die Abwehr des TCG-Zurücksetzungs Angriffs, die auch als Mor-Bit (Memory overwrite Request) bezeichnet wird, bevor Schlüssel in den Arbeitsspeicher extrahiert werden.

> **NOTE**
> Dies schützt nicht vor physischen Angriffen, bei denen ein Angreifer den Fall öffnet und die Hardware angreift.

Sicherheitsrichtlinien

In den nächsten Abschnitten werden Pre-Boot-Authentifizierungs-und DMA-Richtlinien behandelt, die zusätzlichen Schutz für BitLocker bieten.

Pre-Boot-Authentifizierung

Bei der Pre-Boot-Authentifizierung mit BitLocker handelt es sich um eine Richtlinieneinstellung, die die Verwendung von Benutzereingaben wie einer PIN, einem Startschlüssel oder beide zur Authentifizierung erfordert, bevor Sie den Inhalt des Systemlaufwerks barrierefrei machen. Die Gruppenrichtlinieneinstellung erfordert beim Start eine zusätzliche Authentifizierung , und die entsprechende Einstellung im BitLocker-Kryptografiedienstanbieter lautet SystemDrivesRequireStartupAuthentication.

BitLocker greift und speichert die Verschlüsselungsschlüssel nur im Arbeitsspeicher, nachdem die Pre-Boot-Authentifizierung abgeschlossen ist. Wenn Windows nicht auf die Verschlüsselungsschlüssel zugreifen kann, kann das Gerät die Dateien auf dem Systemlaufwerk nicht lesen oder bearbeiten. Die einzige Option zum Umgehen der Pre-Boot-Authentifizierung ist die Eingabe des Wiederherstellungsschlüssels.

Die Pre-Boot-Authentifizierung soll verhindern, dass die Verschlüsselungsschlüssel in den Systemspeicher geladen werden, ohne dass der vertrauenswürdige Benutzer einen anderen Authentifizierungs Faktor wie eine PIN oder einen Startschlüssel bereitstellt. Auf diese Weise können DMA-und Speicher Remanenz-Angriffe verringert werden.

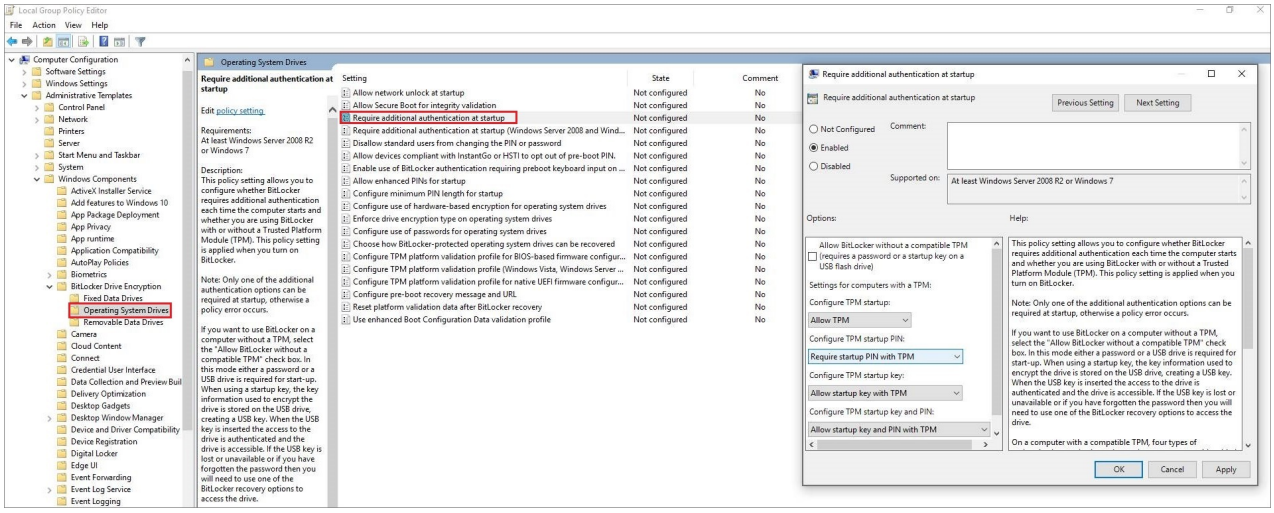
Auf Computern mit einem kompatiblen TPM können Betriebssystemlaufwerke, die mit BitLocker geschützt sind, auf vier Arten freigegeben werden:

- **Nur TPM.** Bei Verwendung der nur-TPM-Validierung ist keine Interaktion mit dem Benutzer erforderlich, um die Sperre aufzuheben und den Zugriff auf das Laufwerk zu ermöglichen. Wenn die TPM-Überprüfung erfolgreich ist, ist die Benutzeranmelde Erfahrung mit einer Standardanmeldung identisch. Wenn das TPM fehlt oder geändert wird oder wenn BitLocker Änderungen am BIOS oder UEFI-Code oder der Konfiguration, kritischen Betriebssystem-Startdateien oder der Startkonfiguration erkennt, wechselt BitLocker in den Wiederherstellungsmodus, und der Benutzer muss ein Wiederherstellungskennwort eingeben, um wieder Zugriff zu erhalten. zu den Daten. Diese Option ist für die Anmeldung günstiger, aber weniger sicher als die anderen Optionen, die einen zusätzlichen Authentifizierungs Faktor erfordern.
- **TPM mit dem Startschlüssel** Neben dem Schutz, den das TPM nur bietet, wird ein Teil des Verschlüsselungsschlüssels auf einem USB-Flashlaufwerk gespeichert, das als Startschlüssel bezeichnet wird.

Auf Daten auf dem verschlüsselten Volume kann ohne den Startschlüssel nicht zugegriffen werden.

- **TPM mit PIN.** Neben dem vom TPM bereitgestellten Schutz erfordert BitLocker, dass der Benutzer eine PIN eingeben muss. Auf Daten auf dem verschlüsselten Volume kann nicht zugegriffen werden, ohne die PIN einzugeben. TPMs verfügt auch über einen antihämmerschutz , der zum Verhindern von Brute-Force-Attacken dient, die versuchen, die PIN zu ermitteln.
- **TPM mit Startschlüssel und PIN.** Neben dem zentralen Komponentenschutz, den das TPM nur bereitstellt, wird ein Teil des Verschlüsselungsschlüssels auf einem USB-Flashlaufwerk gespeichert, und eine PIN ist erforderlich, um den Benutzer für das TPM zu authentifizieren. Diese Konfiguration bietet eine mehrstufige Authentifizierung, sodass Sie, wenn der USB-Stick verloren geht oder gestohlen wird, nicht für den Zugriff auf das Laufwerk verwendet werden kann, da die richtige PIN ebenfalls erforderlich ist.

Im folgenden Gruppenrichtlinien Beispiel ist TPM + PIN zum Entsperren eines Betriebssystemlaufwerks erforderlich:



Die Pre-Boot-Authentifizierung mit einer PIN kann einen Angriffsvektor für Geräte mildern, die eine startbare edrive verwenden, da ein verfügbar gemachter edrive-Bus einem Angreifer die Erfassung des BitLocker-Verschlüsselungsschlüssels während des Starts gestatten kann. Durch die Pre-Boot-Authentifizierung mit einer PIN können auch DMA-Port Angriffe während des Zeitfensters verringert werden, zwischen dem BitLocker die Sperre des Laufwerks aufhebt, und Windows bootet so, dass Windows alle konfigurierten Port bezogenen Richtlinien einrichten kann.

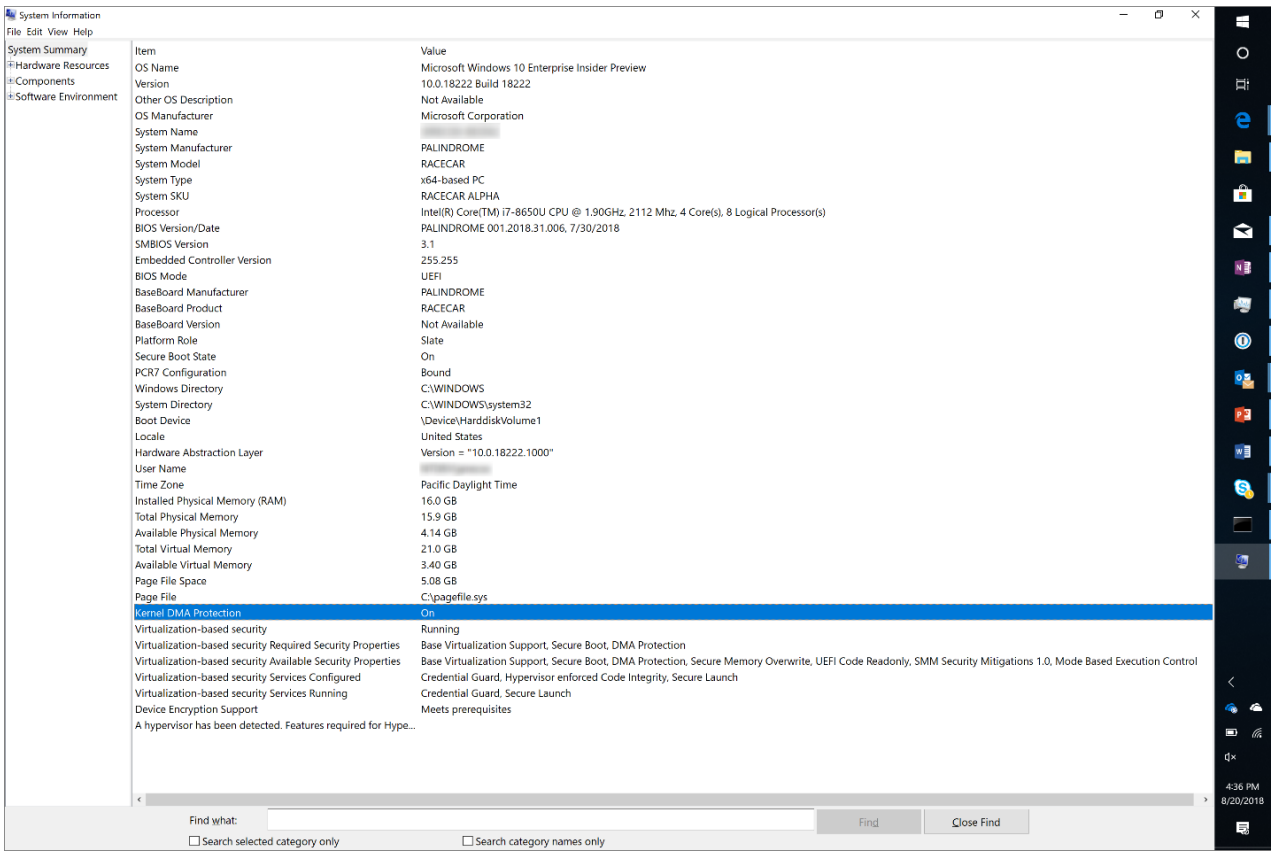
Auf der anderen Seite können die Eingabeaufforderungen zur Vorabstart Authentifizierung für Benutzer unbequem sein. Darüber hinaus wird Benutzern, die Ihre PIN vergessen oder deren Startschlüssel verloren gehen, der Zugriff auf Ihre Daten verweigert, bis Sie sich an das Support Team Ihrer Organisation wenden können, um einen Wiederherstellungsschlüssel zu erhalten. Die Pre-Boot-Authentifizierung kann es auch erschweren, unbeaufsichtigte Desktops und Remote verwaltete Server zu aktualisieren, da eine PIN eingegeben werden muss, wenn ein Computer neu startet oder aus dem Ruhezustand fortgesetzt wird.

Zur Behebung dieser Probleme können Sie die BitLocker-Netzwerksperrungbereitstellen. Mit der Netzwerksperrung können Systeme innerhalb des physischen Unternehmens Sicherheitsperimeters, die die Hardwareanforderungen erfüllen, und BitLocker mit TPM + PIN aktiviert werden, um ohne Benutzereingriff in Windows zu starten. Sie erfordert direkte Ethernet-Konnektivität zu einem Enterprise Windows Deployment Services (WDS)-Server.

Schützen von Thunderbolt und anderen DMA-Ports

Es gibt einige verschiedene Optionen zum Schützen von DMA-Ports wie Thunderbolt™ 3. Ab Windows 10, Version 1803, verfügen neue Intel-basierte Geräte über einen Kernel Schutz vor DMA-Attacken über Thunderbolt™ 3 Ports, die standardmäßig aktiviert sind. Dieser Kernel-DMA-Schutz ist nur für neue Systeme verfügbar, die mit Windows 10, Version 1803, verwendet werden, da Änderungen in der System-Firmware und/oder dem BIOS erforderlich sind.

Sie können die System Information Desktop-App (Msinfo32) verwenden, um zu überprüfen, ob ein Gerät den Kernel-DMA-Schutz aktiviert hat:



Wenn der Kernel-DMA-Schutz *nicht* aktiviert ist, führen Sie die folgenden Schritte aus, um Thunderbolt™ 3-fähige Ports zu schützen:

1. Anfordern eines Kennworts für BIOS-Änderungen
2. Intel Thunderbolt-Sicherheit muss in den BIOS-Einstellungen auf Benutzerautorisierung eingestellt sein. Weitere Informationen finden Sie unter Intel Thunderbolt™ 3 und Sicherheit unter Microsoft Windows® 10-Betriebs System Dokumentation
3. Zusätzliche DMA-Sicherheit kann durch Bereitstellen der Richtlinie (ab Windows 10, Version 1607) hinzugefügt werden:
   - MDM: Daten Schutz-AllowDirectMemoryAccess- Richtlinie
   - Gruppenrichtlinie: neue DMA-Geräte deaktivieren, wenn dieser Computer gesperrt ist (diese Einstellung ist standardmäßig nicht konfiguriert.)

Für Thunderbolt v1 und v2 (DisplayPort-Connector) finden Sie im Abschnitt "Thunderbolt-Minderung" in KB 2516445. Für SBP-2 und 1394 (a.k.a. FireWire) finden Sie im Abschnitt "SBP-2-Milderung" in KB 2516445.

Angriffs Gegenmaßnahmen

In diesem Abschnitt werden die Gegenmaßnahmen für Angriffe bestimmter Typen behandelt.

Bootkits und Rootkits

Ein physisch anwesender Angreifer versucht möglicherweise, eine bootkit-oder Rootkit-ähnliche Software in die bootkette zu installieren, um die BitLocker-Schlüssel zu stehlen. Das TPM sollte diese Installation über PCR-Messungen beobachten, und der BitLocker-Schlüssel wird nicht freigegeben. Dies ist die Standardkonfiguration.

Ein BIOS-Kennwort wird für die Tiefenverteidigung empfohlen, falls ein BIOS Einstellungen verfügbar macht, die möglicherweise das BitLocker-Sicherheitsversprechen Schwächen. Intel Boot Guard und AMD Hardware verifiziertes Booten unterstützen stärkere Implementierungen von Secure Boot, die zusätzliche

Widerstandsfähigkeit gegen Malware und physische Angriffe bieten. Intel Boot Guard und AMD Hardware-geprüfter Start sind Teil der Plattformstart-Verifizierungs Standards für ein hochsicheres Windows 10-Gerät.

Brute-Force-Angriffe auf eine PIN

TPM + PIN für den Schutz gegen hämmern erforderlich.

DMA-Angriffe

Weitere Informationen finden Sie unter Schützen von Thunderbolt-und anderen DMA-Anschlüssen weiter oben in diesem Thema.

Auslagerungsdatei, Absturzspeicherabbild und Hyberfil. sys-Angriffe

Diese Dateien werden standardmäßig auf einem verschlüsselten Volume gesichert, wenn BitLocker auf Betriebssystem-Laufwerken aktiviert ist. Sie blockiert auch automatische oder manuelle Versuche, die Auslagerungsdatei zu verschieben.

Speicher Remanenz

Aktivieren Sie sicheres Booten, und fordern Sie ein Kennwort zum Ändern der BIOS-Einstellungen an. Für Kunden, die Schutz vor diesen erweiterten Angriffen benötigen, konfigurieren Sie eine TPM + PIN-Schutzfunktion, deaktivieren Sie die Standby-Energieverwaltung, und beenden oder Überwintern Sie das Gerät, bevor es die Kontrolle über einen autorisierten Benutzer verlässt.

Gegenmaßnahmen gegen Angriffe

In den folgenden Abschnitten werden Schutzmaßnahmen für verschiedene Typen von Angreifern behandelt.

Angreifer ohne viel Geschick oder eingeschränkter physischer Zugriff

Physischer Zugriff kann durch einen Formfaktor, der keine Busse und Arbeitsspeicher verfügbar macht, limitiert sein. Beispielsweise gibt es keine externen DMA-fähigen Anschlüsse, keine exponierten Schrauben, um das Chassis zu öffnen, und der Speicher wird an das Mainboard gelötet. Dieser Angreifer von Opportunity verwendet keine zerstörerischen Methoden oder ausgeklügelte forensische Hardware/Software.

Entschärfungs

- Pre-Boot-Authentifizierung nur auf TPM (Standardeinstellung)

Angreifer mit Geschick und langwierigem physischem Zugriff

Gezielte Attacke mit viel Zeit; dieser Angreifer wird den Fall öffnen, wird Löten und wird eine ausgeklügelte Hardware oder Software verwenden.

Entschärfungs

- Pre-Boot-Authentifizierung auf TPM mit einer PIN-Beschützer (mit einer ausgeklügelten alphanumerischen Pin zur Unterstützung des TPM-Abschwächungs Schutzes).

  Und

- Deaktivieren Sie die Standby-Energieverwaltung, und beenden oder Überwintern Sie das Gerät, bevor es die Kontrolle über einen autorisierten Benutzer verlässt. Dies kann mithilfe von Gruppenrichtlinien eingestellt werden:
  - Computer Konfiguration | Richtlinien | Administrative Vorlagen | Windows-Komponenten | Datei-Explorer | "Ruhezustand anzeigen" im Menü "Energieoptionen"
  - Computer Konfiguration | Richtlinien | Administrative Vorlagen | System | Energieverwaltung | Einstellungen für den Ruhezustand | Standby-Status (S1-S3) beim schlafen zulassen (angeschlossen)
  - Computer Konfiguration | Richtlinien | Administrative Vorlagen | System | Energieverwaltung | Einstellungen für den Ruhezustand | Standby-Status (S1-S3) beim schlafen zulassen (auf Akku)

Diese Einstellungen sind standardmäßig **nicht konfiguriert** .

Bei einigen Systemen ist es möglich, dass das umgehen von TPM-nur das Öffnen des Falls erfordert und möglicherweise löten erfordert, aber möglicherweise zu vertretbaren Kosten durchgeführt wird. Wenn Sie ein TPM mit einer PIN-Schutzvorrichtung umgehen, würde dies viel teurer sein, und die PIN muss durch Brute erzwungen werden. Mit einer ausgeklügelten, verbesserten PIN kann es nahezu unmöglich sein. Die Gruppenrichtlinieneinstellung für die Erweiterte Pin lautet wie folgt:

Computer Konfiguration | Administrative Vorlagen | Windows-Komponenten | BitLocker-Laufwerkverschlüsselung | Betriebs System Laufwerke | Erweiterte Pins für den Start zulassen

Diese Einstellung ist standardmäßig **nicht konfiguriert** .

Für sichere administrative Workstations empfiehlt Microsoft TPM mit PIN Protector und die Standby-Energieverwaltung zu deaktivieren und das Gerät herunterzufahren oder in den Ruhezustand zu versetzen.

Weitere Informationen

- Blockieren des SBP-2-Treibers und des Thunderbolt-Controllers, um 1394-DMA-und Thunderbolt-DMA-Bedrohungen für BitLocker zu verringern
- BitLocker-Gruppenrichtlinieneinstellungen
- BitLocker-Konfigurationsdienstanbieter

Schützen von freigegebenen Clustervolumes und Storage Area Networks mit BitLocker

27.10.2019 • 8 minutes to read

Betrifft

- Windows Server 2016

In diesem Thema für IT-Experten wird beschrieben, wie der Schutz von CSVs (Cluster Shared Volumes, freigegebene Clustervolumes) und SANs mit BitLocker erfolgt.

BitLocker kann sowohl physische Datenträgerressourcen als auch freigegebene Clustervolumes, Version 2,0 (CSV 2.0), schützen. BitLocker auf gruppierten Volumes bietet eine zusätzliche Schutzebene für Administratoren, die vertrauliche, hoch verfügbare Daten schützen möchten. Durch Hinzufügen zusätzlicher Schutzvorrichtungen zum Clusterdatenträger können Administratoren auch eine zusätzliche Sicherheitsbarriere für Ressourcen innerhalb einer Organisation hinzufügen, indem Sie nur bestimmten Benutzerkonten Zugriff auf die Sperrung des BitLocker-Volumes gewähren.

Konfigurieren von BitLocker für freigegebene Clustervolumes

Verwenden von BitLocker mit gruppierten Volumes

BitLocker für Volumes innerhalb eines Clusters werden basierend darauf verwaltet, wie der Clusterdienst das zu schützende Volume "anzeigt". Das Volume kann eine physikalische Datenträgerressource sein, beispielsweise eine LUN (Logical Unit Number) in einem SAN (Storage Area Network) oder NAS (Network Attached Storage).

> **Wichtige**Sans, die für BitLocker verwendet werden, müssen die Windows-Hardware Zertifizierung erhalten haben. Weitere Informationen finden Sie unter Windows Hardware Lab Kit.

Das Volume kann auch ein freigegebenes Clustervolume sein, ein freigegebener Namespace innerhalb des Clusters. Windows Server 2012 erweiterte die CSV-Architektur, die jetzt als CSV 2.0 bekannt ist, um die Unterstützung für BitLocker zu aktivieren. Bei Verwendung von BitLocker mit Volumes, die für einen Cluster vorgesehen sind, muss das Volume BitLocker aktivieren, bevor es dem Speicherpool in Cluster hinzugefügt wird, oder die Ressource in den Wartungsmodus versetzen, bevor BitLocker-Vorgänge abgeschlossen werden.

Windows PowerShell oder die Befehlszeilenschnittstelle manage-bde ist die bevorzugte Methode zum Verwalten von BitLocker auf CSV 2.0-Volumes. Dies wird für das Element "BitLocker-Systemsteuerung" empfohlen, da CSV 2.0-Volumes Bereitstellungspunkte sind. Bereitstellungspunkte sind ein NTFS-Objekt, das verwendet wird, um einen Einstiegspunkt für andere Volumes bereitzustellen. Bereitstellungspunkte erfordern keine Verwendung eines Laufwerkbuchstabens. Volumes, die keine Laufwerkbuchstaben aufweisen, werden nicht im Element der BitLocker-Systemsteuerung angezeigt. Darüber hinaus ist die neue Active Directory-basierte Protector-Option für die Cluster-Datenträgerressource oder für CSV 2.0-Ressourcen im Element Control Panel nicht verfügbar.

> **Hinweis:** Bereitstellungspunkte können verwendet werden, um Remote Bereitstellungspunkte auf SMB-basierten Netzwerkfreigaben zu unterstützen. Diese Art von Freigabe wird für die BitLocker-Verschlüsselung nicht unterstützt.

Bei einem Thin bereitgestellten Speicher, beispielsweise einer dynamischen virtuellen Festplatte (VHD), wird BitLocker nur im Verschlüsselungsmodus verwendeter Speicherplatz ausgeführt. Sie können den Befehl **manage-bde-WipeFreeSpace** nicht verwenden, um die Lautstärke auf die vollständige Lautstärke Verschlüsselung auf

diesen Volumentypen umzustellen. Dies wird blockiert, um zu vermeiden, dass Thin-bereitgestellte Volumes so erweitert werden, dass Sie den gesamten Sicherungsspeicher belegen, während Sie den unbesetzten (freien) Speicherplatz abwischen.

Active Directory-basierter Schutz

Sie können auch einen Active Directory-Domänendienste (AD DS)-Schutz verwenden, um in Ihrer AD DS-Infrastruktur gehaltene Clusterdatenträger zu schützen. Der **ADAccountOrGroup** -Beschützer ist ein sid-basierter Schutz (Domain Security Identifier), der an ein Benutzerkonto, ein Computerkonto oder eine Gruppe gebunden werden kann. Wenn für ein geschütztes Volume eine Unlock-Anforderung erfolgt, unterbricht der BitLocker-Dienst die Anforderung und verwendet die BitLocker Protect/Unprotect-APIs, um die Anforderung zu entsperren oder abzulehnen. BitLocker schaltet geschützte Volumes ohne Benutzereingriff frei, indem es in der folgenden Reihenfolge versucht, den Schutz zu verwenden:

1. Clear-Taste
2. Treiberbasierte automatische Freigabetaste
3. ADAccountOrGroup-Schutz
   a. Dienstkontext Schutz
   b. Benutzer Schutz
4. Registrierungsbasierter Schlüssel zur automatischen Sperrung

> **Hinweis:** ein Windows Server 2012-oder höher-Domänencontroller ist erforderlich, damit dieses Feature ordnungsgemäß funktioniert.

Aktivieren von BitLocker vor dem Hinzufügen von Datenträgern zu einem Cluster mithilfe von Windows PowerShell

Die BitLocker-Verschlüsselung steht für Datenträger vor oder nach dem Hinzufügen zu einem Clusterspeicher Pool zur Verfügung. Der Vorteil des Verschlüsselns von Volumes vor dem Hinzufügen zu einem Cluster besteht darin, dass für die Datenträgerressource keine Unterbrechungen der Ressource erforderlich sind, um den Vorgang abzuschließen. Gehen Sie wie folgt vor, um BitLocker für einen Datenträger zu aktivieren, bevor Sie es zu einem Cluster hinzufügen:

1. Installieren Sie das BitLocker-Laufwerk Verschlüsselungsfeature, wenn es noch nicht installiert ist.
2. Stellen Sie sicher, dass der Datenträger mit NTFS formatiert ist und ihm ein Laufwerkbuchstabe zugewiesen ist.
3. Ermitteln Sie den Namen des Clusters mit Windows PowerShell.

   ```
   Get-Cluster
   ```

4. Aktivieren Sie BitLocker auf dem Volume Ihrer Wahl mit einem **ADAccountOrGroup** -Beschützer unter Verwendung des Clusternamens. Verwenden Sie beispielsweise einen Befehl wie:

   ```
   Enable-BitLocker E: -ADAccountOrGroupProtector -ADAccountOrGroup CLUSTER$
   ```

   > **Warnung:** Sie müssen einen **ADAccountOrGroup** -Protector mithilfe des Cluster-CNO für ein BitLocker-fähiges Volume konfigurieren, um entweder in einem freigegebenen Clustervolume freigegeben zu werden oder um in einem herkömmlichen Failovercluster ordnungsgemäß zu funktionieren.

5. Wiederholen Sie die vorherigen Schritte für jeden Datenträger im Cluster.

6. Fügen Sie dem Cluster die Volumes (n) hinzu.

Aktivieren von BitLocker für einen gruppierten Datenträger mithilfe von Windows PowerShell

Wenn der Clusterdienst bereits eine Datenträgerressource besitzt, muss er in den Wartungsmodus versetzt werden, bevor BitLocker aktiviert werden kann. Führen Sie die folgenden Schritte aus, um BitLocker für einen gruppierten Datenträger zu aktivieren:

1. Installieren Sie das BitLocker-Laufwerk Verschlüsselungsfeature, wenn es noch nicht installiert ist.
2. Überprüfen Sie den Status des Clusterdatenträgers mithilfe von Windows PowerShell.

   ```
   Get-ClusterResource "Cluster Disk 1"
   ```

3. Setzen Sie die physikalische Datenträgerressource mithilfe von Windows PowerShell in den Wartungsmodus.

   ```
   Get-ClusterResource "Cluster Disk 1" | Suspend-ClusterResource
   ```

4. Ermitteln Sie den Namen des Clusters mit Windows PowerShell.

   ```
   Get-Cluster
   ```

5. Aktivieren Sie BitLocker auf dem Volume Ihrer Wahl mit einem **ADAccountOrGroup** -Beschützer unter Verwendung des Clusternamens. Verwenden Sie beispielsweise einen Befehl wie:

   ```
   Enable-BitLocker E: -ADAccountOrGroupProtector -ADAccountOrGroup CLUSTER$
   ```

   > **Warnung:** Sie müssen einen **ADAccountOrGroup** -Protector mithilfe des Cluster-CNO für ein BitLocker-fähiges Volume konfigurieren, um entweder in einem freigegebenen Clustervolume freigegeben zu werden oder um in einem herkömmlichen Failovercluster ordnungsgemäß zu funktionieren.

6. Verwenden Sie **Resume-ClusterResource** , um die physikalische Datenträgerressource wieder in den Wartungsmodus zu versetzen:

   ```
   Get-ClusterResource "Cluster Disk 1" | Resume-ClusterResource
   ```

7. Wiederholen Sie die vorherigen Schritte für jeden Datenträger im Cluster.

Hinzufügen von BitLocker-verschlüsselten Volumes zu einem Cluster mithilfe von manage-bde

Sie können auch manage-bde verwenden, um BitLocker auf gruppierten Volumes zu aktivieren. Die Schritte, die zum Hinzufügen einer physikalischen Datenträgerressource oder eines CSV 2.0-Volumes zu einem vorhandenen Cluster erforderlich sind, umfassen Folgendes:

1. Überprüfen Sie, ob das BitLocker-Laufwerk Verschlüsselungsfeature auf dem Computer installiert ist.
2. Stellen Sie sicher, dass neuer Speicher als NTFS formatiert ist.
3. Verschlüsseln Sie den Datenträger, fügen Sie einen Wiederherstellungsschlüssel hinzu, und fügen Sie den Cluster Administrator mithilfe der Befehlszeilenschnittstelle manage-bde als Schutzschlüssel hinzu (siehe Beispiel):

   - `Manage-bde -on -used <drive letter> -RP -sid domain\CNO$ -sync`

     a. BitLocker überprüft, ob der Datenträger bereits Teil eines Clusters ist. Wenn dies der Fall ist, können Administratoren auf einen harten Block stoßen. Andernfalls wird die Verschlüsselung

fortgesetzt.

   b. Die Verwendung des-Sync-Parameters ist optional. Durch die Verwendung wird sichergestellt, dass der Befehl wartet, bis die Verschlüsselung für das Volume abgeschlossen ist, bevor das Volume zur Verwendung im Clusterspeicher Pool freigegeben wird.

4. Öffnen des Failovercluster-Manager-Snap-Ins oder von Cluster-PowerShell-Cmdlets zum Aktivieren des Datenträgers in einem Cluster

   - Sobald der Datenträger gruppiert ist, kann er auch für die CSV-Datei aktiviert werden.

5. Während des Ressourcen Onlinevorgangs überprüft Cluster, ob es sich bei dem Datenträger um BitLocker-Verschlüsselung handelt.

   a. Wenn das Volume nicht mit BitLocker aktiviert ist, treten herkömmliche Cluster Onlinevorgänge auf.
   b. Wenn für das Volume BitLocker aktiviert ist, tritt die folgende Überprüfung auf:

      - Wenn Lautstärke **gesperrt**ist, wird BitLocker die CNO und die Lautstärke mit dem CNO-Schutz aufheben. Wenn dieser Vorgang fehlschlägt, wird ein Ereignis protokolliert, das das Volume nicht entsperrt und der Online-Vorgang fehlschlägt.

6. Sobald die Festplatte im Speicherpool Online ist, kann Sie einer CSV-Datei hinzugefügt werden, indem Sie mit der rechten Maustaste auf die Datenträgerressource klickt und "**zu freigegebenen Clustervolumes hinzufügen**" auswählen. CSVs kann sowohl verschlüsselte als auch unverschlüsselte Volumes umfassen. Zum Überprüfen des Status eines bestimmten Volumes für die BitLocker-Verschlüsselung können Administratoren den Befehl manage-bde-Status mit einem Pfad zu dem Volume innerhalb des CSV-Namespaces verwenden, wie in der folgenden Beispiel Befehlszeile zu sehen ist.

```
manage-bde -status "C:\ClusterStorage\volume1"
```

Physikalische Datenträgerressourcen

Im Gegensatz zu CSV 2.0-Volumes kann nur jeweils ein Clusterknoten auf physische Datenträgerressourcen zugreifen. Das bedeutet, dass Vorgänge, wie das Verschlüsseln, entschlüsseln, sperren oder Entsperren von Volumes, den Kontext erfüllen müssen. So können Sie beispielsweise keine physische Datenträgerressource entsperren oder entschlüsseln, wenn Sie nicht den Clusterknoten verwalten, der Besitzer der Datenträgerressource ist, da die Datenträgerressource nicht verfügbar ist.

Einschränkungen für BitLocker-Aktionen mit Cluster-Volumes

Die folgende Tabelle enthält Informationen zu physikalischen Datenträgerressourcen (also herkömmlicher Failovercluster-Volumes) und freigegebenen Clustervolumes (Shared Volumes) sowie zu den Aktionen, die von BitLocker in den jeweiligen Situationen zugelassen sind.

Aktion	Auf dem Besitzer Knoten des Failover-Volumes	Auf dem Metadaten-Server (MDS) von CSV	Auf (Daten Server) DS von CSV	Wartungsmodus
Manage-bde – ein	Blockiert	Blockiert	Blockiert	Allowed
Manage-bde – aus	Blockiert	Blockiert	Blockiert	Allowed

Verwalten – BDE anhalten/fortsetzen	Blockiert	Blockiert	Blockiert	Allowed
Manage-bde – Sperren	Blockiert	Blockiert	Blockiert	Allowed
manage-bde – wischen	Blockiert	Blockiert	Blockiert	Allowed
Entsperrung	Automatisch per Clusterdienst	Automatisch per Clusterdienst	Automatisch per Clusterdienst	Allowed
manage-bde – Protector – hinzufügen	Allowed	Allowed	Blockiert	Allowed
manage-bde-Protector-DELETE	Allowed	Allowed	Blockiert	Allowed
manage-bde – autounlock	Zulässig (nicht empfohlen)	Zulässig (nicht empfohlen)	Blockiert	Zulässig (nicht empfohlen)
Manage-bde-Upgrade	Allowed	Allowed	Blockiert	Allowed
Verkleinern	Allowed	Allowed	Blockiert	Allowed
Erweitern	Allowed	Allowed	Blockiert	Allowed

>Hinweis: * * Obwohl der Befehl "manage-bde-Pause" in Clustern blockiert ist, setzt der Clusterdienst automatisch eine angehaltene Verschlüsselung oder Entschlüsselung vom MDS-Knoten fort.

In dem Fall, in dem eine physikalische Datenträgerressource während der Konvertierung ein Failover-Ereignis erlebt, erkennt der neue Besitzer Knoten, dass die Konvertierung nicht abgeschlossen ist, und führt den Konvertierungsprozess aus.

Weitere Überlegungen bei der Verwendung von BitLocker auf CSV 2.0

Einige weitere Überlegungen, die für BitLocker in einem Clusterspeicher berücksichtigt werden sollten, sind die folgenden:

- BitLocker-Volumes müssen initialisiert werden und die Verschlüsselung beginnen, bevor Sie einem CSV 2.0-Volume hinzugefügt werden können.
- Wenn ein Administrator ein CSV-Volume entschlüsseln muss, entfernen Sie das Volume aus dem Cluster, oder setzen Sie den Datenträger Wartungsmodus. Sie können die CSV-Datei dem Cluster wieder hinzufügen, während Sie darauf warten, dass die Entschlüsselung abgeschlossen ist.
- Wenn ein Administrator mit dem Verschlüsseln eines CSV-Volumes beginnen muss, entfernen Sie das Volume aus dem Cluster, oder setzen Sie es in den Wartungsmodus.

- Wenn die Konvertierung mit der laufenden Verschlüsselung angehalten wird und das CSV-Volume Offline aus dem Cluster ist, wird der Cluster Thread (Integritätsprüfung) die Konvertierung automatisch fortsetzen, wenn das Volume online auf dem Cluster ist.
- Wenn die Konvertierung mit der laufenden Verschlüsselung angehalten wird und ein physisches Datenträger-Ressourcen Volume aus dem Cluster offline ist, wird der BitLocker-Treiber die Konvertierung automatisch fortsetzen, wenn das Volume online auf dem Cluster ist.
- Wenn die Konvertierung mit der laufenden Verschlüsselung angehalten wird, während sich das CSV-Volume im Wartungsmodus befindet, wird der Cluster Thread (Integritätsprüfung) automatisch die Konvertierung fortsetzen, wenn die Lautstärke wieder aus der Wartung verschoben wird.
- Wenn die Konvertierung mit der laufenden Verschlüsselung angehalten wird, während sich das Datenträgerressourcen Volumen im Wartungsmodus befindet, wird der BitLocker-Treiber die Konvertierung automatisch fortsetzen, wenn das Volume aus dem Wartungsmodus zurück verschoben wird.

Richtlinien für die Problembehandlung bei BitLocker

03.12.2019 • 4 minutes to read

In diesem Artikel werden häufige Probleme in BitLocker behandelt, und es werden Richtlinien für die Behandlung dieser Probleme bereitgestellt. Dieser Artikel enthält auch Verweise auf den Beginn des Problembehandlungsprozesses, einschließlich der zu erfassenden Daten und der zu überprüfenden Einstellungen, um den Speicherort zu verkleinern, in dem diese Probleme auftreten.

Überprüfen der Ereignisprotokolle

Öffnen Sie die Ereignisanzeige, und überprüfen Sie die folgenden Protokolle unter Anwendungen und Dienste logs\Microsoft\Windows:

- **BitLocker-API**. Überprüfen Sie das Verwaltungsprotokoll, das operative Protokoll und alle anderen Protokolle, die in diesem Ordner generiert werden. Die Standardprotokolle weisen die folgenden eindeutigen Namen auf:
  - Microsoft-Windows-BitLocker/BitLocker betriebsbereit
  - Microsoft-Windows-BitLocker/BitLocker-Verwaltung
- **BitLocker-DrivePreparationTool**. Überprüfen Sie das Administratorprotokoll, das * *-Betriebsprotokoll und alle anderen Protokolle, die in diesem Ordner generiert werden. Die Standardprotokolle weisen die folgenden eindeutigen Namen auf:
  - Microsoft-Windows-BitLocker-DrivePreparationTool/betriebsbereit
  - Microsoft-Windows-BitLocker-DrivePreparationTool/Administrator

Überprüfen Sie außerdem das Windows logs\System-Protokoll auf Ereignisse, die von den TCM-und TCM-WMI-Ereignisquellen erstellt wurden.

Zum Filtern und anzeigen oder Exportieren von Protokollen können Sie das Befehlszeilentool " wevtutil. exe " oder das Cmdlet " Get-WinEvent " verwenden.

Wenn Sie beispielsweise wevtutil verwenden möchten, um den Inhalt des operativen Protokolls aus dem BitLocker-API-Ordner in eine Textdatei mit dem Namen "BitLockerAPIOpsLog. txt" zu exportieren, öffnen Sie ein Eingabeaufforderungsfenster, und führen Sie einen Befehl aus, der wie folgt aussieht:

```
wevtutil qe "Microsoft-Windows-BitLocker/BitLocker Operational" /f:text > BitLockerAPIOpsLog.txt
```

Wenn Sie das Cmdlet **Get-WinEvent** verwenden möchten, um dasselbe Protokoll in eine durch trennzeichengetrennte Textdatei zu exportieren, öffnen Sie ein Windows PowerShell-Fenster, und führen Sie einen Befehl aus, der wie folgt aussieht:

```
Get-WinEvent -logname "Microsoft-Windows-BitLocker/BitLocker Operational"  | Export-Csv -Path Bitlocker-
Operational.csv
```

Sie können Get-WinEvent in einem erhöhten PowerShell-Fenster verwenden, um gefilterte Informationen aus dem System-oder Anwendungsprotokoll mithilfe einer Syntax anzuzeigen, die wie folgt aussieht:

- So zeigen Sie BitLocker-bezogene Informationen an:

```
Get-WinEvent -FilterHashtable @{LogName='System'} | Where-Object -Property Message -Match 'BitLocker' |
fl
```

Die Ausgabe eines solchen Befehls ähnelt wie folgt.

```
PS C:\> Get-WinEvent -FilterHashtable @{LogName='System'} | Where-Object -Property Message -Match 'Bitlocker' |fl


TimeCreated  : 9/22/2019 8:44:00 PM
ProviderName : Microsoft-Windows-BitLocker-Driver
Id           : 24667
Message      : BitLocker finalization sweep completed for volume H:.

TimeCreated  : 9/22/2019 8:44:00 PM
ProviderName : Microsoft-Windows-BitLocker-Driver
Id           : 24665
Message      : BitLocker finalization sweep paused for volume H:.
```

- So exportieren Sie BitLocker-bezogene Informationen:

```
Get-WinEvent -FilterHashtable @{LogName='System'} | Where-Object -Property Message -Match 'BitLocker' |
Export-Csv -Path System-BitLocker.csv
```

- So zeigen Sie TPM-bezogene Informationen an:

```
Get-WinEvent -FilterHashtable @{LogName='System'} | Where-Object -Property Message -Match 'TPM' | fl
```

- So exportieren Sie TPM-bezogene Informationen:

```
Get-WinEvent -FilterHashtable @{LogName='System'} | Where-Object -Property Message -Match 'TPM' |
Export-Csv -Path System-TPM.csv
```

Die Ausgabe eines solchen Befehls ähnelt wie folgt.

```
PS C:\> Get-WinEvent -FilterHashtable @{LogName='System'} | Where-Object -Property Message -Match 'TPM' | fl


TimeCreated  : 10/12/2019 3:17:47 PM
ProviderName : Microsoft-Windows-TPM-WMI
Id           : 1025
Message      : The TPM was successfully provisioned and is now ready for use.

TimeCreated  : 10/12/2019 3:17:44 PM
ProviderName : Microsoft-Windows-TPM-WMI
Id           : 1025
Message      : The TPM was successfully provisioned and is now ready for use.
```

NOTE

Wenn Sie beabsichtigen, sich an den Microsoft-Support zu wenden, empfehlen wir, die in diesem Abschnitt aufgelisteten Protokolle zu exportieren.

Sammeln von Statusinformationen aus den BitLocker-Technologien

Öffnen Sie ein erweitertes Windows PowerShell-Fenster, und führen Sie die folgenden Befehle aus.

BEFEHL	ANMERKUNGEN

BEFEHL	ANMERKUNGEN
Get-TPM \ #a0 C:\TPM.txt	Exportiert Informationen über das Trusted Platform Module (TPM) des lokalen Computers. Dieses Cmdlet zeigt abhängig davon, ob der TPM-Chip Version 1,2 oder 2,0 ist, verschiedene Werte an. Dieses Cmdlet wird in Windows 7 nicht unterstützt.
manage-bde – Status \ > C:\BDEStatus.txt	Exportiert Informationen zum allgemeinen Verschlüsselungsstatus aller Laufwerke auf dem Computer.
manage-bde c: -Protektoren-Get \ > C:\Protectors	Exportiert Informationen zu den Schutzmethoden, die für den BitLocker-Verschlüsselungsschlüssel verwendet werden.
REAgentC >/Info C:\reagent.txt	Exportiert Informationen zu einem Online-oder Offlineabbild über den aktuellen Status der Windows-Wiederherstellungsumgebung (WindowsRE) und eines verfügbaren Wiederherstellungsabbilds.
[**Get-BitLockerVolume \	FL**] (https://docs.microsoft.com/powershell/module/bitlocker/get-bitlockervolume?view=win10-ps)

Überprüfen der Konfigurationsinformationen

1. Öffnen Sie ein Eingabeaufforderungsfenster mit erhöhten Rechten, und führen Sie die folgenden Befehle aus.

BEFEHL	ANMERKUNGEN
**gpresult/h **	Exportiert den resultierenden Satz von Richtlinieninformationen und speichert die Informationen als HTML-Datei.
**msinfo/Report \ /Computer **	Exportiert umfassende Informationen zu Hardware, Systemkomponenten und Softwareumgebung auf dem lokalen Computer. Mit der Option **/Report** werden die Informationen als txt-Datei gespeichert.

2. Öffnen Sie den Registrierungs-Editor, und exportieren Sie die Einträge in den folgenden Unterschlüsseln:

   - **HKLM\SOFTWARE\Policies\Microsoft\FVE**
   - **HKLM\SYSTEM\CurrentControlSet\Services\TPM**

Überprüfen der BitLocker-Voraussetzungen

Zu den allgemeinen Einstellungen, die zu Problemen bei BitLocker führen können, gehören die folgenden:

- Das TPM muss freigegeben werden. Sie können die Ausgabe des Befehls **Get-TPM** für den Status des TPM überprüfen.
- Windows RE muss aktiviert sein. Sie können die Ausgabe des Befehls **REAgentC** für den Status von WindowsRE überprüfen.
- Die für das System reservierte Partition muss das richtige Format verwenden.
  - Auf Unified Extensible Firmware Interface (UEFI)-Computern muss die System reservierte Partition als FAT32 formatiert sein.
  - Auf Legacy Computern muss die System reservierte Partition als NTFS formatiert sein.

- Wenn es sich bei dem Gerät, das Sie zur Problembehandlung verwenden, https://gpsearch.azurewebsites.net/#8153 um einen Schiefer-oder Tablet PC handelt, überprüfen Sie den Status der Option **Verwendung der BitLocker-Authentifizierung aktivieren, die eine Vorstart Tastatureingabe auf Slates erfordert** .

Weitere Informationen zu den BitLocker-Voraussetzungen finden Sie unter BitLocker-grundlegende Bereitstellung: Verwenden von BitLocker zum Verschlüsseln von Volumes

Nächste Schritte

Wenn die Informationen, die Sie bisher geprüft haben, auf ein bestimmtes Problem hindeuten (beispielsweise ist WindowsRE nicht aktiviert), kann das Problem eine einfache Lösung sein.

Das Beheben von Problemen, die nicht offensichtliche Ursachen haben, hängt davon ab, welche Komponenten betroffen sind und welches Verhalten Sie sehen. Mithilfe der gesammelten Informationen können Sie die zu untersuchenden Bereiche einschränken.

- Wenn Sie an einem Gerät arbeiten, das von Microsoft InTune verwaltet wird, lesen Sie Erzwingen von BitLocker-Richtlinien mithilfe von InTune: bekannte Probleme.
- Wenn BitLocker nicht gestartet wird oder kein Laufwerk verschlüsseln kann und Sie Fehler oder Ereignisse bemerken, die sich auf das TPM beziehen, lesen Sie BitLocker kann ein Laufwerk nicht verschlüsseln: bekannte TPM-Probleme.
- Wenn BitLocker ein Laufwerk nicht startet oder nicht verschlüsseln kann, lesen Sie BitLocker kann ein Laufwerk nicht verschlüsseln: bekannte Probleme.
- Wenn sich die BitLocker-Netzwerksperrung nicht wie erwartet verhält, lesen Sie BitLocker-Netzwerksperre: bekannte Probleme.
- Wenn sich BitLocker beim Wiederherstellen eines verschlüsselten Laufwerks nicht erwartungsgemäß verhält oder wenn Sie nicht erwartet haben, dass BitLocker das Laufwerk wiederhergestellt hat, lesen Sie BitLocker-Wiederherstellung: bekannte Probleme.
- Wenn sich BitLocker nicht wie erwartet verhält oder sich das verschlüsselte Laufwerk nicht erwartungsgemäß verhält und Sie Fehler oder Ereignisse bemerken, die sich auf das TPM beziehen, lesen Sie BitLocker und TPM: Weitere bekannte Probleme.
- Wenn sich BitLocker nicht wie erwartet verhält oder sich das verschlüsselte Laufwerk nicht erwartungsgemäß verhält, lesen Sie BitLocker-Konfiguration: bekannte Probleme.

Wir empfehlen, dass Sie die von Ihnen gesammelten Informationen für den Fall behalten, dass Sie den Microsoft-Support kontaktieren, um Hilfe bei der Lösung Ihres Problems zu erhalten.

BitLocker kann ein Laufwerk nicht verschlüsseln: bekannte Probleme

03.12.2019 • 2 minutes to read

In diesem Artikel werden häufige Probleme beschrieben, die verhindern, dass BitLocker ein Laufwerk verschlüsseln kann. Dieser Artikel enthält auch Anleitungen zur Behebung dieser Probleme.

> **NOTE**
>
> Wenn Sie festgestellt haben, dass Ihr BitLocker-Problem mit dem Trusted Platform Module (TPM) verbunden ist, lesen Sie BitLocker kann ein Laufwerk nicht verschlüsseln: bekannte TPM-Probleme.

Fehler 0x80310059: die BitLocker-Laufwerkverschlüsselung führt bereits einen Vorgang auf diesem Laufwerk durch.

Wenn Sie die BitLocker-Laufwerkverschlüsselung auf einem Computer mit Windows 10 Professional aktivieren, wird eine Meldung angezeigt, die der folgenden ähnelt:

> **Fehler:** Es ist ein Fehler aufgetreten (Code 0x80310059): die BitLocker-Laufwerkverschlüsselung führt bereits einen Vorgang auf diesem Laufwerk durch. Bitte schließen Sie alle Vorgänge ab, bevor Sie fortfahren. Hinweis: Wenn der Schalter "-on" Fehler beim Hinzufügen von Schlüssel Beschützern oder beim Starten der Verschlüsselung hat, müssen Sie möglicherweise "manage-bde-Off" aufrufen, bevor Sie erneut versuchen.

Ursache

Dieses Problem kann durch Einstellungen verursacht werden, die von Gruppenrichtlinienobjekten (Group Policy Objects, GPOs) gesteuert werden.

Auflösung

> **IMPORTANT**
>
> Führen Sie die Schritte in diesem Abschnitt sorgfältig aus. Wird die Registrierung falsch angepasst, können schwerwiegende Probleme auftreten. Bevor Sie ihn ändern, Sichern Sie die Registrierung für die Wiederherstellung , falls Probleme auftreten.

Führen Sie die folgenden Schritte aus, um dieses Problem zu beheben:

1. Starten Sie den Registrierungs-Editor, und navigieren Sie zum folgenden Unterschlüssel: **HKEY _LOCAL _MACHINE \software\policies\microsoft\fve**
2. Löschen Sie die folgenden Einträge:
   - **OSPlatformValidation _BIOS**
   - **OSPlatformValidation _UEFI**
   - **PlatformValidation**
3. Beenden Sie den Registrierungs-Editor, und aktivieren Sie die BitLocker-Laufwerkverschlüsselung erneut.

Meldung "Zugriff verweigert", wenn Sie versuchen, Wechseldatenträger zu verschlüsseln

Sie verfügen über einen Computer, auf dem Windows 10, Version 1709 oder Version 1607 ausgeführt wird. Sie versuchen, ein USB-Laufwerk zu verschlüsseln, indem Sie die folgenden Schritte ausführen:

1. Klicken Sie im Windows-Explorer mit der rechten Maustaste auf das USB-Laufwerk, und wählen Sie **BitLocker aktivieren**aus.
2. Wählen Sie auf der Seite Wählen Sie aus, **wie Sie das Laufwerk entsperren möchten die Option Kennwort verwenden aus, um das Laufwerk zu entsperren**.
3. Folgen Sie den Anweisungen auf der Seite, um Ihr Kennwort einzugeben.
4. Wählen Sie auf der Seite **sind Sie bereit, dieses Laufwerk zu verschlüsseln?** die Option **Verschlüsselung starten**aus.
5. Auf der Seite " **Verschlüsselung wird gestartet** " wird die Meldung "Zugriff verweigert" angezeigt.

Sie erhalten diese Meldung auf jedem Computer, auf dem Windows 10, Version 1709 oder Version 1607, ausgeführt wird, wenn Sie ein beliebiges USB-Laufwerk verwenden.

Ursache

Die Sicherheitsbeschreibung des BitLocker Drive Encryption Service (BDESvc) hat einen falschen Eintrag. Anstelle von NT Autorität \ authentifizierte-Benutzern verwendet die Sicherheitsbeschreibung NT-AUTHORITY\INTERACTIVE.

Führen Sie die folgenden Schritte aus, um zu überprüfen, ob dieses Problem aufgetreten ist:

1. Öffnen Sie auf einem betroffenen Computer ein Eingabeaufforderungsfenster mit erhöhten Rechten und ein erweitertes PowerShell-Fenster.

2. Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

   ```
   C:\>sc sdshow bdesvc
   ```

   Die Ausgabe dieses Befehls sieht wie folgt aus:

   ```
   D: (a;; CCDCLCSWRPWPDTLORCWDWO;;; SY) (A;; CCDCLCSWRPWPDTLORCWDWO;;; BA) (A;; CCLCSWRPLORC;;; BU) (A;; CCLCSWRPLORC;;; Au) S: (au; FA; CCDCLCSWRPWPDTLOSDRCWDWO;;; WD
   ```

3. Kopieren Sie diese Ausgabe, und verwenden Sie Sie wie folgt als Teil des Befehls **ConvertFrom-SDDL-** Befehl im PowerShell-Fenster.

```
PS C:\WINDOWS\system32> ConvertFrom-SddlString -Sddl "D:(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)
(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SY)(A;;CCLCSWLOCRRC;;;IU)S:
(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)" -Type ActiveDirectoryRights

Owner            :
Group            :
DiscretionaryAcl : {

NT AUTHORITY\INTERACTIVE :        AccessAllowed (CreateChild, ExtendedRight, GenericExecute,
ListChildren, ListObject, Read, ReadControl, Self),
NT AUTHORITY\SYSTEM:             AccessAllowed (CreateChild, Delete, DeleteChild,
DeleteTree, ExecuteKey, ExtendedRight, FullControl, GenericAll, GenericExecute, GenericRead,
GenericWrite, ListChildren, ListObject, Modify, Read, ReadAndExecute, ReadControl,
ReadProperty, Self, Write, WriteDacl, WriteKey, WriteOwner, WriteProperty),
BUILTIN\Administrators:          AccessAllowed (CreateChild, Delete, DeleteChild,
DeleteTree, ExecuteKey, ExtendedRight, FullControl, GenericAll, GenericExecute, GenericRead,
GenericWrite, ListChildren, ListObject, Modify, Read, ReadAndExecute, ReadControl,
ReadProperty, Self, Write, WriteDacl, WriteKey, WriteOwner, WriteProperty)}

SystemAcl        : {Everyone: SystemAudit FailedAccess (CreateChild, Delete, DeleteChild,
DeleteTree, ExecuteKey, ExtendedRight, FullControl, GenericAll, GenericExecute, GenericRead,
GenericWrite, ListChildren, ListObject, Modify, Read, ReadAndExecute, ReadControl,
ReadProperty, Self, Write, WriteDacl, WriteKey, WriteOwner, WriteProperty)}
RawDescriptor    : System.Security.AccessControl.CommonSecurityDescriptor
```

Wenn NT AUTHORITY\INTERACTIVE (als hervorgehoben) angezeigt wird, ist dies in der Ausgabe dieses Befehls die Ursache des Problems. Unter typischen Bedingungen sollte die Ausgabe wie folgt aussehen:

```
PS C:\WINDOWS\system32> ConvertFrom-SddlString -Sddl "D:(A;;CCDCLCSWRPWPDTLORCWDWO;;;SY)
(A;;CCDCLCSWRPWPDTLORCWDWO;;;BA)(A;;CCLCSWRPLORC;;;BU)(A;;CCLCSWRPLORC;;;AU)S:
(AU;FA;CCDCLCSWRPWPDTLOSDRCWDWO;;;WD)" -Type ActiveDirectoryRights

Owner            :
Group            :
DiscretionaryAcl : {

NT AUTHORITY\Authenticated Users :        AccessAllowed (CreateChild, ExecuteKey,
GenericExecute, GenericRead, ListChildren, ListObject, Read, ReadControl, ReadProperty,
Self),
NT AUTHORITY\SYSTEM:                     AccessAllowed (CreateChild, DeleteChild,
DeleteTree, ExecuteKey, GenericExecute, GenericRead, GenericWrite, ListChildren, ListObject,
Read, ReadAndExecute, ReadControl, ReadProperty, Self, WriteDacl, WriteKey, WriteOwner,
WriteProperty),
BUILTIN\Administrators:                  AccessAllowed (CreateChild, DeleteChild,
DeleteTree, ExecuteKey, GenericExecute, GenericRead, GenericWrite, ListChildren, ListObject,
Read, ReadAndExecute, ReadControl, ReadProperty, Self, WriteDacl, WriteKey, WriteOwner,
WriteProperty), BUILTIN\Users: AccessAllowed (CreateChild, ExecuteKey, GenericExecute,
GenericRead, ListChildren, ListObject, Read, ReadControl, ReadProperty, Self)}

SystemAcl        : {Everyone: SystemAudit FailedAccess (CreateChild, Delete, DeleteChild,
DeleteTree, ExecuteKey, FullControl, GenericExecute, GenericRead, GenericWrite,
ListChildren, ListObject, Read, ReadAndExecute, ReadControl, ReadProperty, Self, WriteDacl,
WriteKey, WriteOwner, WriteProperty)}
RawDescriptor    : System.Security.AccessControl.CommonSecurityDescriptor
```

NOTE

GPOs, die die Sicherheitsbeschreibungen von Diensten ändern, haben dieses Problem bekanntermaßen verursacht.

Auflösung

1. Wenn Sie die Sicherheitsbeschreibung von BDESvc reparieren möchten, öffnen Sie ein erweitertes PowerShell-Fenster, und geben Sie den folgenden Befehl ein:

```
sc sdset bdesvc D:(A;;CCDCLCSWRPWPDTLORCWDWO;;;SY)(A;;CCDCLCSWRPWPDTLORCWDWO;;;BA)(A;;CCLCSWRPLORC;;;BU)
(A;;CCLCSWRPLORC;;;AU)S:(AU;FA;CCDCLCSWRPWPDTLOSDRCWDWO;;;WD)
```

2. Starten Sie den Computer neu.

Das Problem sollte jetzt behoben sein.

Erzwingen von BitLocker-Richtlinien mithilfe von Intune: bekannte Probleme

11.02.2020 • 10 minutes to read

Dieser Artikel unterstützt Sie bei der Behandlung von Problemen, die auftreten können, wenn Sie die Microsoft InTune-Richtlinie zum Verwalten der unbeaufsichtigten BitLocker-Verschlüsselung auf Geräten verwenden. Das InTune-Portal gibt an, ob BitLocker ein oder mehrere verwaltete Geräte nicht verschlüsseln konnte.

BitLockerFixedDrivesRecoveryOptions	Succeeded	
Warning for other disk encryption	Succeeded	
Encrypt devices	Error	-2016281112 (Remediation failed)
Allow standard users to enable encryption during Azure A...	Succeeded	
BitLockerFixedDrivesRequireEncryption	Succeeded	

Wenn Sie die Ursache des Problems einschränken möchten, überprüfen Sie die Ereignisprotokolle wie unter Problembehandlung bei BitLockerbeschrieben. Konzentrieren Sie sich auf die Verwaltungs-und Vorgangsprotokolle im Ordner **Applications and Services logs\Microsoft\Windows\BitLocker-API** . In den folgenden Abschnitten finden Sie weitere Informationen dazu, wie die angegebenen Ereignisse und Fehlermeldungen aufgelöst werden können:

- Ereignis-ID 853: Fehler: ein kompatibles TPM-Sicherheitsgerät (Trusted Platform Module) wurde auf diesem Computer nicht gefunden.
- Ereignis-ID 853: Fehler: die BitLocker-Laufwerkverschlüsselung hat startbare Medien (CD oder DVD) auf dem Computer erkannt
- Ereignis-ID 854: WinRE ist nicht konfiguriert
- Ereignis-ID 851: Kontakt Hersteller für BIOS-Upgrade
- Fehlermeldung: die UEFI-Variable "SecureBoot" konnte nicht gelesen werden
- Ereignis-ID 846, 778 und 851: Fehler 0x80072f9a
- Fehlermeldung: in Konflikt stehende Gruppenrichtlinieneinstellungen für Wiederherstellungsoptionen auf Betriebssystemlaufwerken

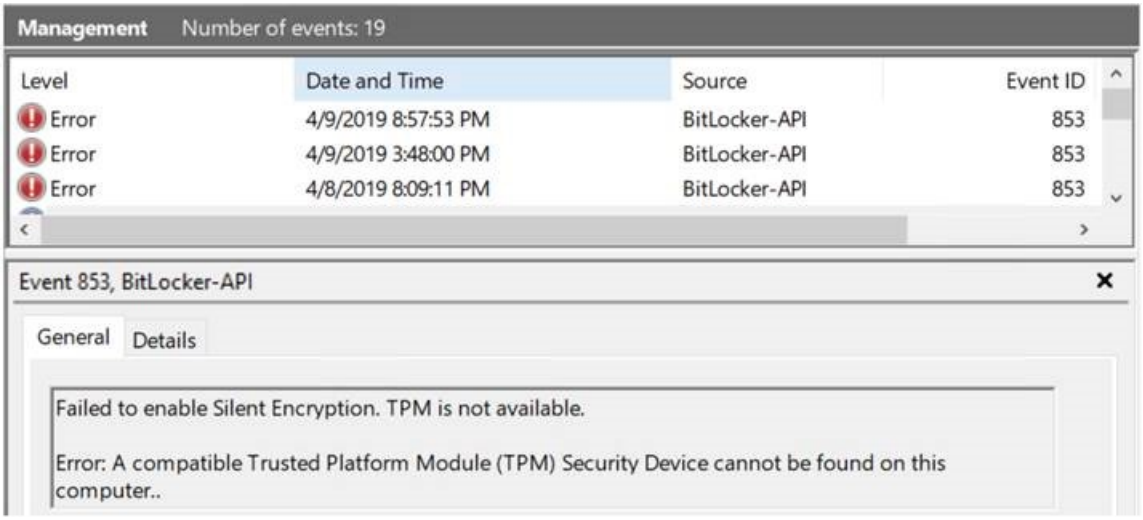
Wenn Sie nicht über eine eindeutige Spur von Ereignissen oder Fehlermeldungen verfügen, die Sie folgen sollten, gehören die folgenden zu untersuchenden Bereiche:

- Überprüfen der Hardwareanforderungen für die Verwendung von InTune zum Verwalten von BitLocker auf Geräten
- Überprüfen der BitLocker-Richtlinienkonfiguration

Informationen dazu, wie Sie überprüfen können, ob InTune-Richtlinien BitLocker ordnungsgemäß erzwingen, finden Sie unter überprüfen, ob BitLocker ordnungsgemäßfunktioniert.

Ereignis-ID 853: Fehler: ein kompatibles TPM-Sicherheitsgerät (Trusted Platform Module) wurde auf diesem Computer nicht gefunden.

Ereignis-ID 853 kann je nach Kontext unterschiedliche Fehlermeldungen aufweisen. In diesem Fall zeigt die Fehlermeldung "Ereignis-ID 853" an, dass auf dem Gerät kein TPM zu sehen ist. Die Ereignisinformationen ähneln den folgenden:



Ursache

Das Gerät, das Sie zu sichern versuchen, hat möglicherweise keinen TPM-Chip, oder das Geräte-BIOS ist möglicherweise so konfiguriert, dass das TPM deaktiviert wird.

Lösung

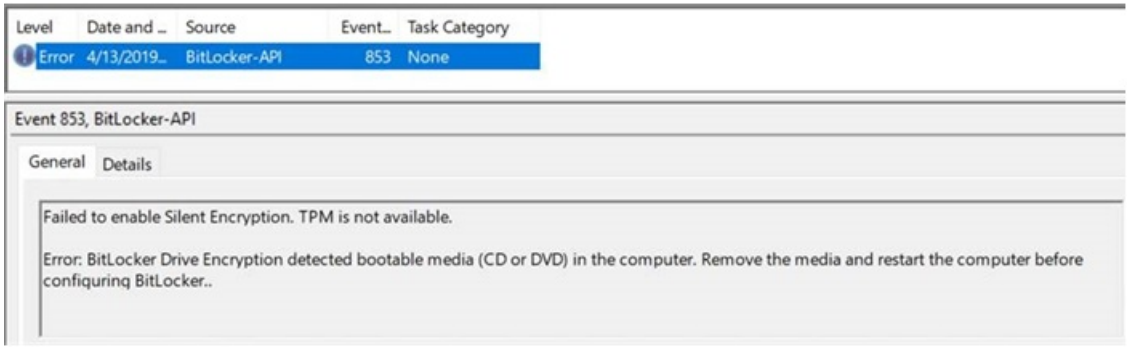
Um dieses Problem zu beheben, überprüfen Sie Folgendes:

- Das TPM ist im Geräte-BIOS aktiviert.
- Der TPM-Status in der TPM-Verwaltungskonsole sieht wie folgt aus:
  - Bereit (TPM 2,0)
  - Initialisiert (TPM 1,2)

Weitere Informationen finden Sie unter Problembehandlung für das TPM.

Ereignis-ID 853: Fehler: die BitLocker-Laufwerkverschlüsselung hat startbare Medien (CD oder DVD) auf dem Computer erkannt

In diesem Fall wird die Ereignis-ID 853 angezeigt, und die Fehlermeldung im Ereignis zeigt an, dass startfähige Medien für das Gerät verfügbar sind. Die Ereignisinformationen ähneln den folgenden.



Ursache

Während des Bereitstellungsprozesses zeichnet die BitLocker-Laufwerkverschlüsselung die Konfiguration des Geräts auf, um einen Basisplan einzurichten. Wenn sich die Gerätekonfiguration später ändert (wenn Sie beispielsweise das Medium entfernen), wird der BitLocker-Wiederherstellungsmodus automatisch gestartet.

Um dieses Problem zu vermeiden, wird der Bereitstellungsprozess angehalten, wenn er wechselbare startfähige Medien erkennt.

Lösung

Entfernen Sie die startbaren Medien, und starten Sie das Gerät neu. Überprüfen Sie nach dem Neustart des Geräts

den Verschlüsselungsstatus.

Ereignis-ID 854: WinRE ist nicht konfiguriert

Die Ereignisinformationen ähneln den folgenden:

> Fehler beim Aktivieren der automatischen Verschlüsselung. WinRe ist nicht konfiguriert.
>
> Fehler: dieser PC kann die Geräteverschlüsselung nicht unterstützen, da WinRE nicht ordnungsgemäß konfiguriert ist.

Ursache

Windows-Wiederherstellungsumgebung (WinRE) ist ein minimales Windows-Betriebssystem, das auf der Windows-Vorinstallationsumgebung (Windows PE) basiert. WinRE enthält mehrere Tools, die ein Administrator zum Wiederherstellen oder Zurücksetzen von Windows sowie zum Diagnostizieren von Windows-Problemen verwenden kann. Wenn ein Gerät das reguläre Windows-Betriebssystem nicht starten kann, versucht das Gerät, WinRE zu starten.

Der Bereitstellungsprozess ermöglicht die BitLocker-Laufwerkverschlüsselung auf dem Betriebssystemlaufwerk während der Windows PE-Phase der Bereitstellung. Diese Aktion stellt sicher, dass das Laufwerk geschützt ist, bevor das vollständige Betriebssystem installiert ist. Der Bereitstellungsprozess erstellt auch eine Systempartition, die WinRE verwenden soll, wenn das System abstürzt.

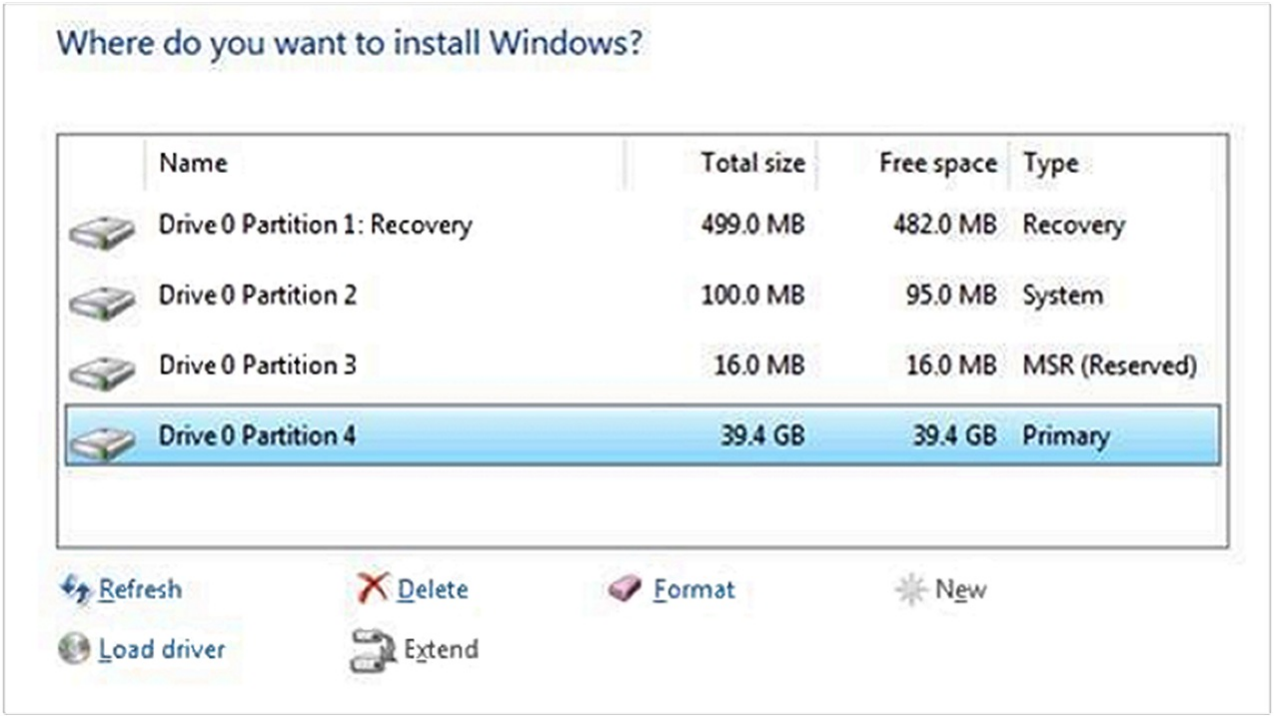
Wenn WinRE auf dem Gerät nicht verfügbar ist, wird die Bereitstellung angehalten.

Lösung

Sie können dieses Problem beheben, indem Sie die Konfiguration der Datenträgerpartitionen, den Status von WinRE und die Konfiguration des Windows-Bootloaders überprüfen. Führen Sie dazu die folgenden Schritte aus.

Schritt 1: Überprüfen der Konfiguration der Datenträgerpartitionen

Die in diesem Abschnitt beschriebenen Verfahren hängen von den standardmäßigen Datenträgerpartitionen ab, die von Windows während der Installation konfiguriert werden. Windows 10 erstellt automatisch eine Wiederherstellungspartition, die die WinRE. WIM-Datei enthält. Die Partitionskonfiguration ähnelt wie folgt.

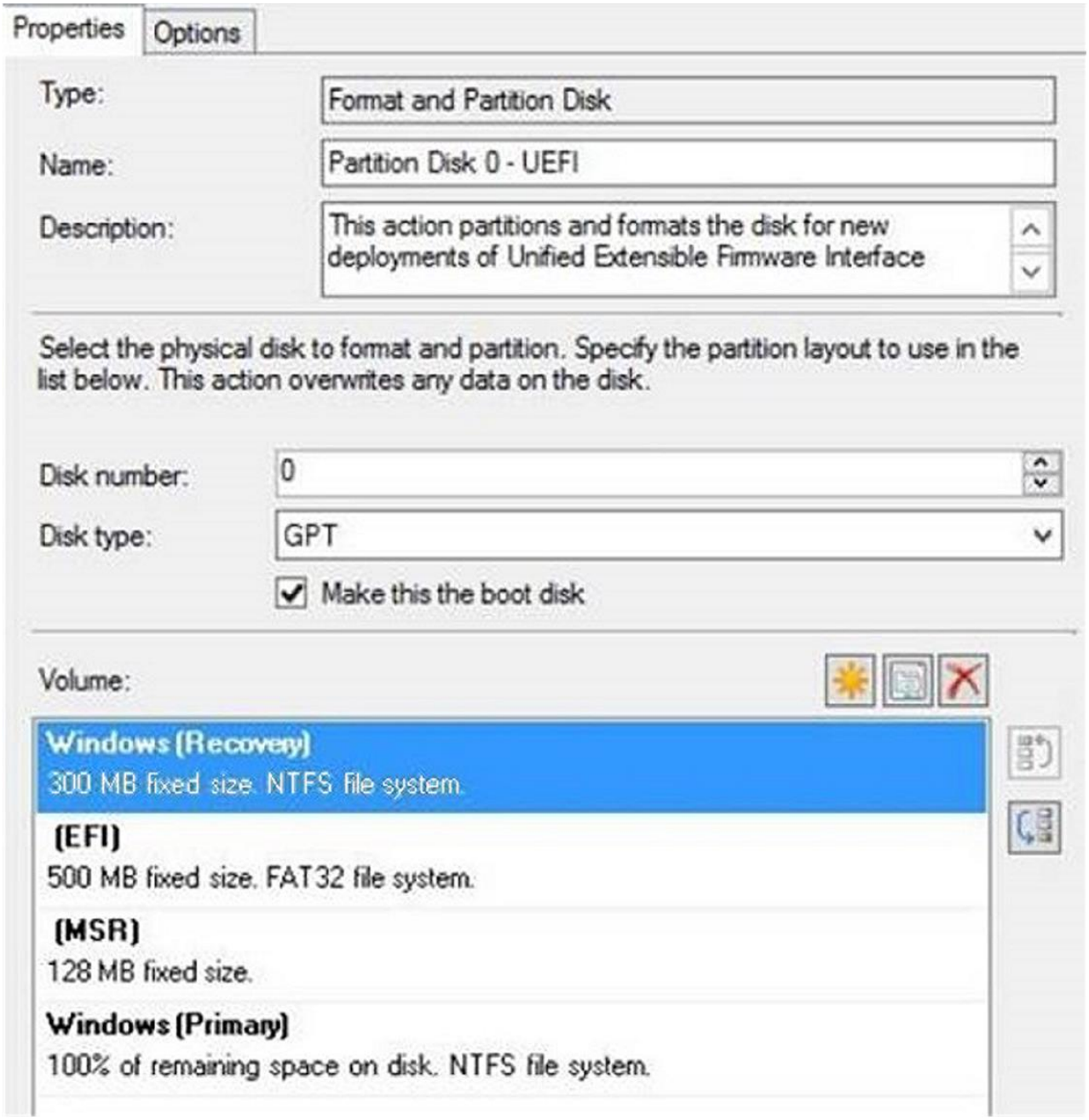


Um die Konfiguration der Datenträgerpartitionen zu überprüfen, öffnen Sie ein Eingabeaufforderungsfenster mit erhöhten Rechten, und führen Sie die folgenden Befehle aus:

```
diskpart
list volume
```

```
C:\WINDOWS\system32>diskpart

Microsoft DiskPart version 10.0.17763.1

Copyright (C) Microsoft Corporation.
On computer: MININT-8L1MASA

DISKPART> list vol

  Volume ###  Ltr  Label        Fs     Type        Size     Status     Info
  ----------  ---  -----------  -----  ----------  -------  ---------  --------
  Volume 0     E                       DVD-ROM         0 B  No Media
  Volume 1         System       NTFS   Partition    499 MB  Healthy    System
  Volume 2     C   OSDisk       NTFS   Partition    216 GB  Healthy    Boot
  Volume 3     D   New Volume   NTFS   Partition    248 GB  Healthy
```

Wenn der Status eines Volumes nicht fehlerfrei ist oder die Wiederherstellungspartition nicht vorhanden ist, müssen Sie möglicherweise Windows erneut installieren. Bevor Sie dies tun, überprüfen Sie die Konfiguration des Windows-Abbilds, das Sie für die Bereitstellung verwenden. Stellen Sie sicher, dass das Bild die richtige Datenträgerkonfiguration verwendet. Die Bild Konfiguration sollte wie folgt aussehen (dieses Beispiel beruht auf dem Microsoft Endpoint Configuration Manager).



Schritt 2: Überprüfen des Status von WinRE

Um den Status von WinRE auf dem Gerät zu überprüfen, öffnen Sie ein Eingabeaufforderungsfenster mit erhöhten Rechten, und führen Sie den folgenden Befehl aus:

```
reagentc /info
```

Die Ausgabe dieses Befehls ähnelt wie folgt.

```
C:\>reagentc /info
Windows Recovery Environment (Windows RE) and system reset configuration
Information:

    Windows RE status:         Enabled
    Windows RE location:       \\?\GLOBALROOT\device\harddisk0\partition3\Recovery\WindowsRE
    Boot Configuration Data (BCD) identifier: 795594e5-c7d0-11e8-b0ac-af33c6ecd1ec
    Recovery image location:
    Recovery image index:      0
    Custom image location:
    Custom image index:        0

REAGENTC.EXE: Operation Successful.
```

Wenn der **Windows RE-Status** nicht **aktiviert**ist, führen Sie den folgenden Befehl aus, um ihn zu aktivieren:

```
reagentc /enable
```

Schritt 3: Überprüfen der Konfiguration des Windows-Startladeprogramms

Wenn der Partitionsstatus fehlerfrei ist, der Befehl **REAgentC/enable** aber zu einem Fehler führt, überprüfen Sie, ob der Windows-Startladeprogramm die GUID der Wiederherstellungssequenz enthält. Führen Sie dazu den folgenden Befehl in einem Eingabeaufforderungsfenster mit erhöhten Rechten aus:

```
bcdedit /enum all
```

Die Ausgabe dieses Befehls ähnelt wie folgt.

```
C:\WINDOWS\system32>bcdedit /enum all

Windows Boot Manager
--------------------
identifier              {bootmgr}
device                  partition=\Device\HarddiskVolume1
description             Windows Boot Manager
locale                  en-US
inherit                 {globalsettings}
fverecoverymessage      To retrieve this key, go to https://aka.ms/bitlockerrecovery from another device with access to
the corporate network, or to https://bitlockerrecovery.microsoft.com for registered, non-domain joined machines.
default                 {current}
resumeobject            {4b2bb885-8418-11e8-b279-001f29044af6}
displayorder            {current}
toolsdisplayorder       {memdiag}
timeout                 30

Windows Boot Loader
-------------------
identifier              {current}
device                  partition=C:
path                    \WINDOWS\system32\winload.exe
description             Windows 10
locale                  en-US
inherit                 {bootloadersettings}
recoverysequence        {795594e5-c7d0-11e8-b0ac-af33c6ecd1ec}
displaymessageoverride  Recovery
recoveryenabled         Yes
allowedinmemorysettings 0x15000075
osdevice                partition=C:
systemroot              \WINDOWS
resumeobject            {4b2bb885-8418-11e8-b279-001f29044af6}
nx                      OptIn
bootmenupolicy          Standard
hypervisorlaunchtype    Auto
```

Suchen Sie in der Ausgabe den **Windows-Bootloader** -Abschnitt, der den Zeilen **Bezeichner = {Current}** enthält. Suchen Sie in diesem Abschnitt das **recoverysequence**-Attribut. Der Wert dieses Attributs sollte ein GUID-Wert und nicht eine Zeichenfolge von Nullen sein.

Ereignis-ID 851: wenden Sie sich an den Hersteller für BIOS-Upgrade-Anweisungen.

Die Ereignisinformationen ähneln den folgenden:

> Fehler beim Aktivieren der automatischen Verschlüsselung.
>
> Fehler: die BitLocker-Laufwerkverschlüsselung kann auf dem Betriebssystemlaufwerk nicht aktiviert werden. Wenden Sie sich an den Computerhersteller, um BIOS-Aktualisierungsanweisungen zu erhalten.

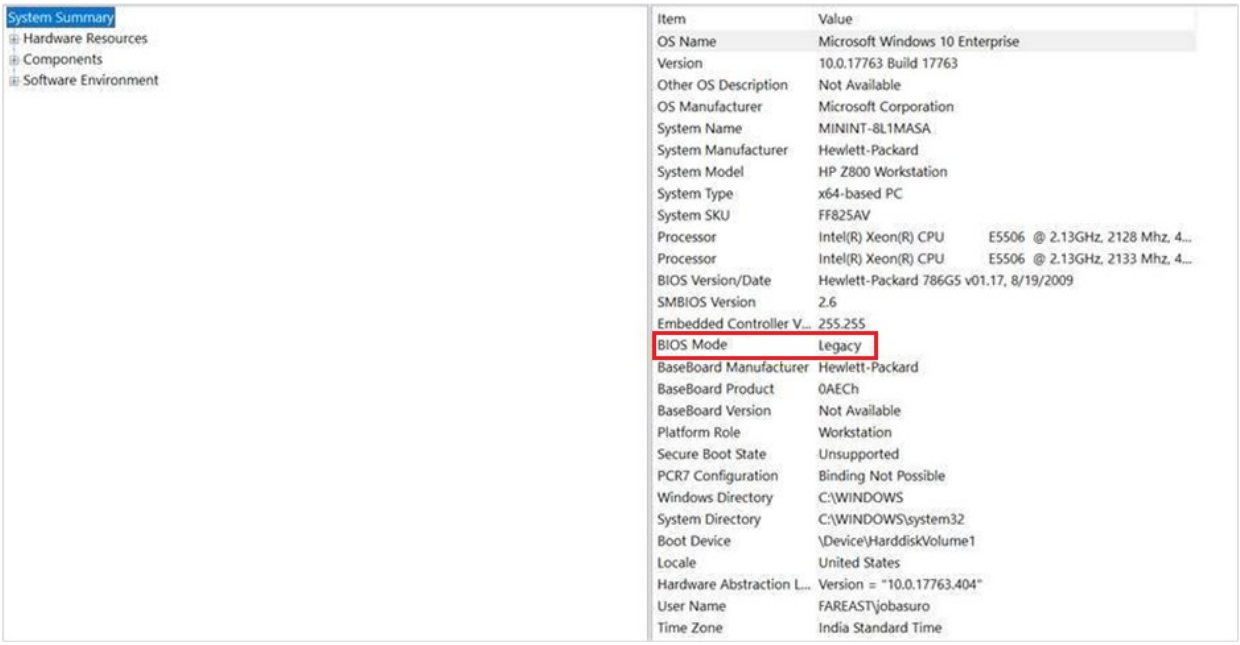
Ursache

Das Gerät muss das Unified Extensible Firmware Interface (UEFI)-BIOS aufweisen. Die Silent BitLocker-Laufwerkverschlüsselung unterstützt kein Legacy-BIOS.

Lösung

Verwenden Sie die System Informations-APP, um den BIOS-Modus zu überprüfen. Gehen Sie hierzu folgendermaßen vor:

1. Wählen Sie **Start**aus, und geben Sie **msinfo32** in das **Suchfeld** ein.
2. Stellen Sie sicher, dass die Einstellung für den **BIOS-Modus UEFI** und nicht **Legacy**ist.



3. Wenn die **BIOS-Modus** -Einstellung **Legacy**ist, müssen Sie das BIOS in den **UEFI** -oder **EFI** -Modus umschalten. Die dazu erforderlichen Schritte gelten speziell für das Gerät. > [!NOTE] > Wenn das Gerät nur den Legacy Modus unterstützt, können Sie mit InTune keine BitLocker-Geräteverschlüsselung auf dem Gerät verwalten.

Fehlermeldung: die UEFI-Variable "SecureBoot" konnte nicht gelesen werden

Sie erhalten eine Fehlermeldung, die wie folgt aussieht:

> **Fehler:** BitLocker kann Secure Boot nicht für Integrität verwenden, weil die UEFI-Variable "SecureBoot" nicht gelesen werden konnte. Ein erforderliches Privileg wird nicht vom Client gehalten.

Ursache

Bei einem Platform Configuration Register (PCR) handelt es sich um einen Speicherplatz im TPM. Insbesondere misst PCR 7 den Zustand des sicheren Starts. Für die automatische BitLocker-Laufwerkverschlüsselung muss der sichere Start aktiviert sein.

Lösung

Sie können dieses Problem beheben, indem Sie das PCR-Validierungs Profil des TPM und den sicheren Startzustand überprüfen. Gehen Sie hierzu folgendermaßen vor:

Schritt 1: Überprüfen des PCR-Validierungs Profils des TPM

Um zu überprüfen, ob PCR 7 verwendet wird, öffnen Sie ein Eingabeaufforderungsfenster mit erhöhten Rechten, und führen Sie den folgenden Befehl aus:

```
Manage-bde -protectors -get %systemdrive%
```

Überprüfen Sie im TPM-Abschnitt der Ausgabe dieses Befehls, ob die Einstellung für das **PCR-Validierungs Profil** wie folgt **7**umfasst.

```
C:\windows\system32>manage-bde -protectors -get %systemdrive%
BitLocker Drive Encryption: Configuration Tool version 10.0.17763
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

Volume C: [OSDisk]
All Key Protectors

    Numerical Password:
      ID: {DFBA5848-A9B1-4D5E-AAC5-011DEF09F705}
      Password:


    TPM:
      ID: {1B527682-77DA-475F-A2A7-EB81B73D1A88}
      PCR Validation Profile:
        7, 11
        (Uses Secure Boot for integrity validation)
```

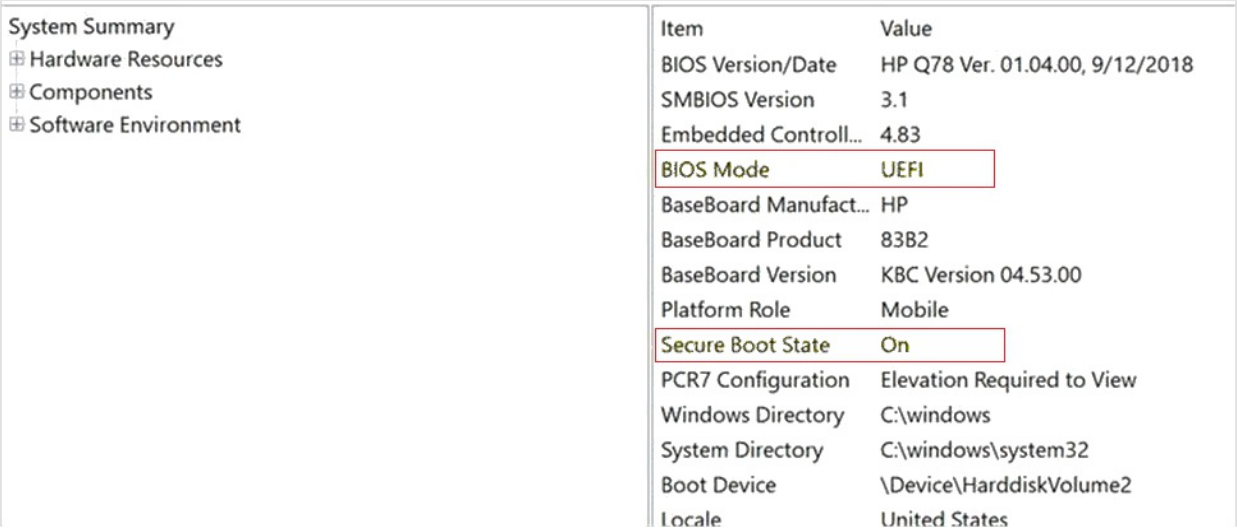
Wenn das **PCR-Validierungs Profil** nicht **7** enthält (beispielsweise sind die Werte **0**, **2**, **4**und **11**, aber nicht **7**), ist der sichere Start nicht aktiviert.

```
C:\WINDOWS\system32>manage-bde -protectors -get %systemdrive%
BitLocker Drive Encryption: Configuration Tool version 10.0.17763
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

Volume C: [OSDisk]
All Key Protectors

    Numerical Password:
      ID: {4856F8A7-2751-4668-89F8-BDF0D519AD4D}
      Password:


    TPM:
      ID: {90A0BB72-ABA6-4F08-AC89-84C4884491BD}
      PCR Validation Profile:
        0, 2, 4, 8, 9, 10, 11
```

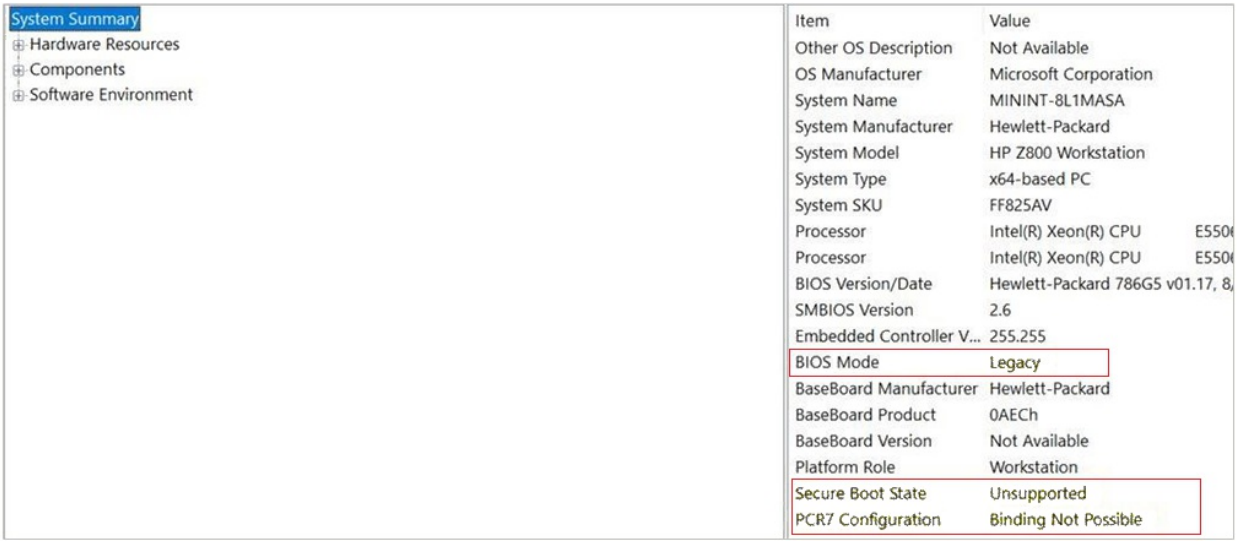
2. Überprüfen des sicheren Startzustands

Verwenden Sie die System Informations-APP, um den sicheren Startzustand zu überprüfen. Gehen Sie hierzu folgendermaßen vor:

1. Wählen Sie **Start**aus, und geben Sie **msinfo32** in das **Suchfeld** ein.
2. Überprüfen Sie, ob die Einstellung für den **sicheren Startzustand** wie folgt **aktiviert**ist:



3. Wenn die Einstellung für den **sicheren Startzustand** nicht **unterstützt**wird, können Sie auf diesem Gerät keine Silent BitLocker-Verschlüsselung verwenden.



NOTE

Sie können auch das Cmdlet Confirm-SecureBootUEFI verwenden, um den sicheren Startzustand zu überprüfen. Öffnen Sie dazu ein erweitertes PowerShell-Fenster, und führen Sie den folgenden Befehl aus:

```
PS C:\> Confirm-SecureBootUEFI
```

Wenn der Computer den sicheren Start unterstützt und der sichere Start aktiviert ist, gibt dieses Cmdlet "true" zurück.

Wenn der Computer den sicheren Start unterstützt und der sichere Start deaktiviert ist, gibt dieses Cmdlet "false" zurück.

Wenn der Computer keinen sicheren Start unterstützt oder ein BIOS-Computer (ohne UEFI) ist, gibt dieses Cmdlet "Cmdlet, das auf dieser Plattform nicht unterstützt wird" zurück.

Ereignis-ID 846, 778 und 851: Fehler 0x80072f9a

In diesem Fall stellen Sie die Intune-Richtlinie bereit, um ein Windows 10-, Version 1809-Gerät zu verschlüsseln und das Wiederherstellungskennwort in Azure Active Directory (Azure AD) zu speichern. Im Rahmen der Richtlinienkonfiguration haben Sie die Option **Standardbenutzer können Verschlüsselung während Azure AD-Joins aktivieren** aktiviert.

Die Richtlinienbereitstellung schlägt fehl und generiert die folgenden Ereignisse (sichtbar in der Ereignisanzeige im **Logs\Microsoft\Windows\BitLocker-API-Ordner "Anwendungen und Dienste** "):

> Ereignis-ID: 846
>
> Ereignis: Fehler beim Sichern der Wiederherstellungsinformationen für die BitLocker-Laufwerkverschlüsselung für Volume C: zu ihrer Azure AD.
>
> Ablaufverfolgungs-Nr: {cbac2b6f-1434-4faa-a9c3-597b17c1dfa3} Fehler: Unbekannter HRESULT-Fehlercode: 0x80072f9a
>
> Ereignis-ID: 778
>
> Ereignis: das BitLocker-Volume C: wurde in einen ungeschützten Zustand zurückgesetzt.
>
> Ereignis-ID: 851
>
> Ereignis: Fehler beim Aktivieren der automatischen Verschlüsselung.
>
> Fehler: Unbekannter HRESULT-Fehlercode: 0x80072f9a.

Diese Ereignisse beziehen sich auf den Fehlercode 0x80072f9a.

Ursache

Diese Ereignisse deuten darauf hin, dass der angemeldete Benutzer nicht über die Berechtigung zum Lesen des privaten Schlüssels für das Zertifikat verfügt, das im Rahmen des Bereitstellungs-und Registrierungsprozesses generiert wird. Daher schlägt die Aktualisierung der BitLocker-MDM-Richtlinie fehl.

Das Problem betrifft Windows 10, Version 1809.

Lösung

Um dieses Problem zu beheben, installieren Sie das Update vom Mai 21, 2019 .

Fehlermeldung: in Konflikt stehende Gruppenrichtlinieneinstellungen für Wiederherstellungsoptionen auf Betriebssystemlaufwerken

Es wird eine Meldung angezeigt, die der folgenden ähnelt:

> **Fehler:** Die BitLocker-Laufwerkverschlüsselung kann auf dieses Laufwerk nicht angewendet werden, da es in Konflikt stehende Gruppenrichtlinieneinstellungen für Wiederherstellungsoptionen auf Betriebssystemlaufwerken gibt. Das Speichern von Wiederherstellungsinformationen in Active Directory-Domänendiensten kann nicht erforderlich sein, wenn die Generierung von Wiederherstellungskennwörtern nicht zulässig ist. Bitten Sie Ihren System Administrator, diese Richtlinienkonflikte zu beheben, bevor Sie versuchen, BitLocker zu aktivieren...

Lösung

Um dieses Problem zu beheben, überprüfen Sie die Einstellungen für das Gruppenrichtlinienobjekt (GPO) für Konflikte. Weitere Anleitungen finden Sie im nächsten Abschnitt Überprüfen der BitLocker-Richtlinienkonfiguration.

Weitere Informationen zu GPOs und BitLocker finden Sie unter BitLocker-Gruppenrichtlinien Referenz.

Überprüfen der BitLocker-Richtlinienkonfiguration

Informationen dazu, wie Sie die Richtlinie zusammen mit BitLocker und InTune verwenden, finden Sie in den folgenden Ressourcen:

- BitLocker-Verwaltung für Unternehmen: Verwalten von Geräten, die mit Azure Active Directory verbunden sind
- BitLocker-Gruppenrichtlinieneinstellungen

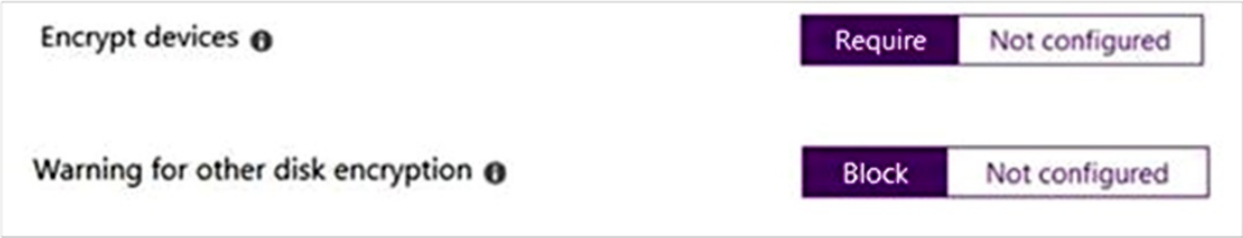
- Referenz zum Konfigurationsdienstanbieter
- Richtlinien- – CSP BitLocker
- BitLocker-Konfigurationsdienstanbieter
- Aktivieren von ADMX-Backup-Richtlinien in MDM
- gpresult

InTune bietet die folgenden Erzwingungstypen für BitLocker:

- **Automatisch** (erzwungen, wenn das Gerät während des Bereitstellungsprozesses zu Azure AD wechselt. Diese Option steht in Windows 10, Version 1703 und höher, zur Verfügung.)
- **Silent** (Endpunktschutz Richtlinie. Diese Option steht in Windows 10, Version 1803 und höher, zur Verfügung.)
- **Interaktiv** (Endpunkt Richtlinie für Windows-Versionen, die älter als Windows 10, Version 1803, sind.)

Wenn auf Ihrem Gerät Windows 10, Version 1703 oder höher, unterstützt wird, unterstützt modern Standby (auch bekannt als Instant Go) und ist HSTI-kompatibel, das Gerät mit Azure AD zu verknüpfen, löst die automatische Geräteverschlüsselung aus. Eine separate Endpunktschutz Richtlinie ist nicht erforderlich, um die Geräteverschlüsselung durchzusetzen.

Wenn Ihr Gerät HSTI-kompatibel ist, aber den modernen Standbymodus nicht unterstützt, müssen Sie eine Endpunktschutz Richtlinie konfigurieren, um die automatische BitLocker-Laufwerkverschlüsselung zu erzwingen. Die Einstellungen für diese Richtlinie sollten wie folgt aussehen:



Die Oma-URI-Verweise für diese Einstellungen lauten wie folgt:

- Oma-URI: **./Device/Vendor/MSFT/BitLocker/RequireDeviceEncryption**
  Werttyp: **Ganzzahl**
  Wert: **1** (1 = require; 0 = nicht konfiguriert)

- Oma-URI: **./Device/Vendor/MSFT/BitLocker/AllowWarningForOtherDiskEncryption**
  Werttyp: **Ganzzahl**
  Wert: **0** (0 = blockiert; 1 = zulässig)

> **NOTE**
> Aufgrund eines Updates für den BitLocker-Richtlinien Kryptografiedienstanbieter können Sie bei Verwendung von Windows 10, Version 1809 oder höher, eine Endpunktschutz Richtlinie verwenden, um die automatische BitLocker-Geräteverschlüsselung zu erzwingen, auch wenn das Gerät nicht HSTI-kompatibel ist.

> **NOTE**
> Wenn die Einstellung **Warnung für andere Datenträgerverschlüsselung** auf **nicht konfiguriert**festgelegt ist, müssen Sie den BitLocker-Laufwerk Verschlüsselungs-Assistenten manuell starten.

Wenn das Gerät den modernen Standbymodus nicht unterstützt, aber HSTI-kompatibel ist und eine Version von Windows verwendet, die älter als Windows 10, Version 1803, ist, stellt eine Endpunktschutz Richtlinie mit den in diesem Artikel beschriebenen Einstellungen die Richtlinie bereit. Konfiguration für das Gerät. Windows benachrichtigt den Benutzer jedoch, die BitLocker-Laufwerkverschlüsselung manuell zu aktivieren. Dazu wählt der

Benutzer die Benachrichtigung aus. Mit dieser Aktion wird der BitLocker Drive Encryption-Assistent gestartet.

Die Version InTune 1901 enthält Einstellungen, die Sie zum Konfigurieren der automatischen Geräteverschlüsselung für Autopilot-Geräte für Standardbenutzer verwenden können. Jedes Gerät muss die folgenden Voraussetzungen erfüllen:

- HSTI-kompatibel sein
- Unterstützen des modernen Standbymodus
- Verwenden von Windows 10, Version 1803 oder höher

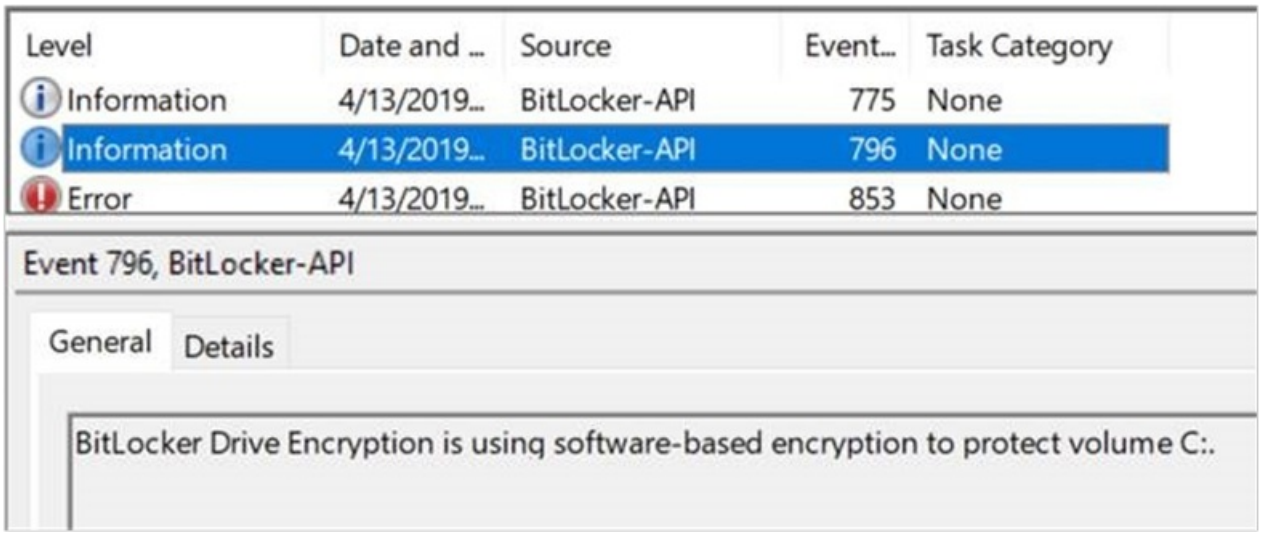
Die Oma-URI-Verweise für diese Einstellungen lauten wie folgt:

- Oma-URI: **./Device/Vendor/MSFT/BitLocker/AllowStandardUserEncryption**
  Werttyp: **ganzzahliger** Wert: **1**

> **NOTE**
> Dieser Knoten funktioniert zusammen mit den **RequireDeviceEncryption** -und **AllowWarningForOtherDiskEncryption** -Knoten. Aus diesem Grund wird beim Setzen von **RequireDeviceEncryption** auf **1**, **AllowStandardUserEncryption** auf **1**und **AllowWarningForOtherDiskEncryption** auf **0**gesetzt. InTune kann die Silent BitLocker-Verschlüsselung für Autopilot-Geräte erzwingen, die Standardbenutzer Profile aufweisen.

Überprüfen, ob BitLocker ordnungsgemäß funktioniert

Während regulärer Vorgänge generiert die BitLocker-Laufwerkverschlüsselung Ereignisse wie Ereignis-ID 796 und Ereignis-ID 845.



Level	Date and ...	Source	Event...	Task Category
Information	4/13/2019...	BitLocker-API	845	None
Information	4/13/2019...	BitLocker-API	775	None
Information	4/13/2019...	BitLocker-API	796	None

Event 845, BitLocker-API

General Details

BitLocker Drive Encryption recovery information for volume C: was backed up successfully to your Azure AD.
Protector GUID: {dda4f062-803e-4efb-bd1e-5f46e0c52a24}.
TraceId: {e3c6b9f3-dc9b-4bc9-9ace-0c98e818db69}

Sie können auch feststellen, ob das BitLocker-Wiederherstellungskennwort in Azure AD hochgeladen wurde, indem Sie im Abschnitt Azure AD Devices die Gerätedetails überprüfen.

BITLOCKER KEY ID	BITLOCKER RECOVERY KEY	DRIVE TYPE
dda4f062-803e-4efb-bd1e-...	003289-619993-483340-53...	Operating system drive

Überprüfen Sie auf dem Gerät den Registrierungs-Editor, um die Richtlinieneinstellungen auf dem Gerät zu überprüfen. Überprüfen Sie die Einträge unter den folgenden Unterschlüsseln:

- **HKEY \ _LOCAL \ _MACHINE \software\microsoft\policymanager\current\device\bitlocker**
- **HKEY \ _LOCAL \ _MACHINE \software\microsoft\policymanager\current\device**

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\PolicyManager\current\device\BitLocker

OnlineProviders
Outlook Express
Palm
Phone
Photos
Pim
PLA
PlayToReceiver
PointOfService
Policies
PolicyManager
current
device
BitLocker
DataProtection

Name	Type	Data
(Default)	REG_SZ	(value not set)
AllowStandardUserEncryption	REG_DWORD	0x00000001 (1)
AllowStandardUserEncryption_ProviderSet	REG_DWORD	0x00000001 (1)
AllowWarningForOtherDiskEncryption	REG_DWORD	0x00000000 (0)
AllowWarningForOtherDiskEncryption_ProviderSet	REG_DWORD	0x00000001 (1)
EncryptionMethodByDriveType_ADMXInstanceData	REG_SZ	Software\Microsoft\PolicyManager\providers\6F3C...
EncryptionMethodByDriveType_ProviderSet	REG_DWORD	0x00000001 (1)
FixedDrivesRecoveryOptions_ADMXInstanceData	REG_SZ	Software\Microsoft\PolicyManager\providers\6F3C...
FixedDrivesRecoveryOptions_ProviderSet	REG_DWORD	0x00000001 (1)
FixedDrivesRequireEncryption_ADMXInstanceData	REG_SZ	Software\Microsoft\PolicyManager\providers\6F3C...
FixedDrivesRequireEncryption_ProviderSet	REG_DWORD	0x00000001 (1)
RequireDeviceEncryption	REG_DWORD	0x00000001 (1)
RequireDeviceEncryption_ProviderSet	REG_DWORD	0x00000001 (1)

BitLocker-Netzwerksperre: bekannte Probleme

03.12.2019 • 3 minutes to read

Mithilfe des BitLocker-Features für die Netzwerksperrung können Sie Computer remote verwalten, ohne eine BitLocker-PIN eingeben zu müssen, wenn die einzelnen Computer gestartet werden. Dazu müssen Sie Ihre Umgebung so konfigurieren, dass die folgenden Anforderungen erfüllt sind:

- Jeder Computer gehört zu einer Domäne
- Jeder Computer verfügt über eine kabelgebundene Verbindung mit dem Unternehmensnetzwerk.
- Das Unternehmensnetzwerk verwendet DHCP zum Verwalten von IP-Adressen
- Jeder Computer verfügt über einen DHCP-Treiber, der in seiner Unified Extensible Firmware Interface (UEFI)-Firmware implementiert ist.

Allgemeine Richtlinien zur Problembehandlung bei der Netzwerksperrung finden Sie unter Aktivieren der Netzwerksperrung : Problembehandlung bei der Netzwerksperrung.

In diesem Artikel werden verschiedene bekannte Probleme beschrieben, die bei Verwendung der Netzwerksperrung auftreten können, und es werden Anleitungen zur Behebung dieser Probleme bereitgestellt.

Tipp: ermitteln, ob die BitLocker-Netzwerksperrung auf einem bestimmten Computer aktiviert ist

Auf Computern mit x64-oder x32-UEFI-Systemen können Sie die folgenden Schritte ausführen. Sie können diese Befehle auch Skripten erstellen.

1. Öffnen Sie ein Eingabeaufforderungsfenster mit erhöhten Rechten, und führen Sie den folgenden Befehl aus:

   ```
   manage-bde protectors get <Drive>
   ```

   Dabei ist \ <*Laufwerks*> der Laufwerkbuchstabe, gefolgt von einem Doppelpunkt (:) des startbaren Laufwerks). Wenn die Ausgabe dieses Befehls einen Schlüssel Beschützer des Typs **TpmCertificate (9)** enthält, ist die Konfiguration für die BitLocker-Netzwerksperrung korrekt.

2. Starten Sie den Registrierungs-Editor, und überprüfen Sie die folgenden Einstellungen:

   - Entry **HKEY \ _LOCAL \ _MACHINE \software\policies\microsoft\fve: OSManageNKP** ist auf **1** eingestellt.
   - Subkey **HKEY \ _LOCAL \ _MACHINE \software\policies\microsoft\systemcertificates\fve\ _NKP \certificates** einen Eintrag enthält, dessen Name mit dem Namen des Fingerabdrucks des Zertifikats des Netzwerksperre-Schlüsselschutzes übereinstimmt, den Sie in Schritt 1 gefunden haben.

Auf einem Surface pro 4-Gerät funktioniert die BitLocker-Netzwerksperre nicht, da der UEFI-Netzwerkstapel falsch konfiguriert ist.

Sie haben die BitLocker-Netzwerksperrung konfiguriert, wie unter BitLocker: Aktivieren der Netzwerksperrungbeschrieben. Sie haben das UEFI des Geräts für die Verwendung von DHCP konfiguriert. Wenn Sie das Gerät neu starten, werden Sie jedoch weiterhin zur BitLocker-PIN aufgefordert.

Sie testen ein anderes Gerät, beispielsweise einen anderen Typ von Tablet oder Laptop-PC, das für die Verwendung der gleichen Infrastruktur konfiguriert ist. Das Gerät wird wie erwartet neu gestartet, ohne die BitLocker-PIN einzugeben. Sie schließen die ordnungsgemäße Konfiguration der Infrastruktur ab, und das Problem ist für das Gerät spezifisch.

Ursache

Der UEFI-Netzwerkstapel auf dem Geräte wasincorrectly konfiguriert.

Auflösung

Wenn Sie den UEFI-Netzwerkstapel von Surface pro 4 ordnungsgemäß konfigurieren möchten, müssen Sie den Microsoft Surface Enterprise Management-Modus (Semm) verwenden. Informationen zu Semm finden Sie unter registrieren und Konfigurieren von Surface-Geräten mit Semm.

> **NOTE**
>
> Wenn Sie Semm nicht verwenden können, können Sie möglicherweise die Oberfläche pro 4 so konfigurieren, dass die BitLocker-Netzwerksperre verwendet wird, indem Sie das Gerät so konfigurieren, dass es das Netzwerk als erste Startoption verwendet.

BitLocker-Netzwerk Sperrungs Funktion kann auf einem Windows-Clientcomputer nicht verwendet werden

Sie haben die BitLocker-Netzwerksperrung konfiguriert, wie unter BitLocker: Aktivieren der Netzwerksperrungbeschrieben. Sie verfügen über einen Windows 8-basierten Clientcomputer, der über ein Ethernet-Kabel mit dem Unternehmensnetzwerk verbunden ist. Wenn Sie den Computer neu starten, werden Sie jedoch weiterhin zur BitLocker-PIN aufgefordert.

Ursache

Ein Windows 8-basierter oder Windows Server 2012-basierter Clientcomputer empfängt oder verwendet manchmal nicht das Netzwerk-Unlock Protector, je nachdem, ob der Client nicht verknüpfte BOOTP-Antworten von einem DHCP-Server oder einem WDS-Server empfängt.

DHCP-Server senden möglicherweise DHCP-Optionen an einen BOOTP-Client, wie dies von den DHCP-Optionen und den BOOTP-Lieferanten Erweiterungen zugelassen ist. Das bedeutet, dass der DHCP-Server auf BOOTP-Anforderungen antwortet, da ein DHCP-Server BOOTP-Clients unterstützt.

Die Art und Weise, in der ein DHCP-Server eine eingehende Nachricht verarbeitet, hängt teilweise davon ab, ob die Nachricht die Option Nachrichtentyp verwendet:

- Die ersten beiden Nachrichten, die vom BitLocker-Netzwerkclient freigegeben werden, sind DHCP-DISCOVER\REQUEST-Nachrichten. Sie verwenden die Option Nachrichtentyp, sodass Sie vom DHCP-Server als DHCP-Nachrichten behandelt werden.
- Die dritte Nachricht, die vom BitLocker-Netzwerk entsperren-Client gesendet wird, verfügt nicht über die Option Nachrichtentyp. Der DHCP-Server behandelt die Nachricht als BOOTP-Anforderung.

Ein DHCP-Server, der BOOTP-Clients unterstützt, muss mit diesen Clients entsprechend dem BOOTP-Protokoll interagieren. Der Server muss eine BOOTP-BOOTREPLY-Nachricht anstelle einer DHCP-DHCPOFFER-Nachricht erstellen. (Anders ausgedrückt: der Server darf den Typ der DHCP-Nachrichten Option nicht enthalten und darf die Größenbeschränkung für BOOTREPLY-Nachrichten nicht überschreiten.) Nachdem der Server die BOOTP-BOOTREPLY-Nachricht gesendet hat, kennzeichnet der Server eine Bindung für einen BOOTP-Client als gebunden. Ein nicht-DHCP-Client sendet weder eine DHCPREQUEST-Nachricht noch erwartet dieser Client eine DHCPAck-Nachricht.

Wenn ein DHCP-Server, der nicht für die Unterstützung von BOOTP-Clients konfiguriert ist, eine

BOOTREQUEST-Nachricht von einem BOOTP-Client empfängt, verwirft dieser Server die BOOTREQUEST-Nachricht automatisch.

Weitere Informationen zu DHCP und zur BitLocker-Netzwerksperrung finden Sie unter BitLocker: Aktivieren der Netzwerksperrung: Netzwerk Sperrungs Sequenz

Auflösung

Um dieses Problem zu beheben, ändern Sie die Konfiguration des DHCP-Servers, indem Sie die **DHCP** -Option von **DHCP und BOOTP** in **DHCP**ändern.

BitLocker-Wiederherstellung: bekannte Probleme

03.12.2019 • 11 minutes to read

In diesem Artikel werden häufige Probleme beschrieben, die möglicherweise verhindern, dass sich BitLocker beim Wiederherstellen eines Laufwerks wie erwartet verhält, oder dass BitLocker die Wiederherstellung unerwartet starten kann. Dieser Artikel enthält Anleitungen zur Behebung dieser Probleme.

> **NOTE**
>
> In diesem Artikel bezieht sich "Wiederherstellungskennwort" auf das 48-stellige Wiederherstellungskennwort, und "Wiederherstellungsschlüssel" bezieht sich auf den Wiederherstellungsschlüssel 32-stellig. Weitere Informationen finden Sie unter BitLocker-Schlüsselschutz.

Windows 10 fordert zur Eingabe eines nicht vorhandenen BitLocker-Wiederherstellungskennworts auf

In Windows 10 werden Sie aufgefordert, ein BitLocker-Wiederherstellungskennwort einzugeben. Sie haben jedoch kein BitLocker-Wiederherstellungskennwort konfiguriert.

Auflösung

Die FAQ für BitLocker-und Active Directory-Domänendienste (AD DS) bezieht sich auf Situationen, in denen dieses Symptom auftreten kann, und enthält Informationen zur Behebung des Problems:

- Was geschieht, wenn BitLocker auf einem Computer aktiviert ist, bevor der Computer der Domäne beigetreten ist?
- Was geschieht, wenn die Sicherung anfänglich fehlschlägt? Wird die Sicherung von BitLocker wiederholt?

Das Wiederherstellungskennwort für einen Laptop wurde nicht gesichert, und der Laptop ist gesperrt.

Sie verfügen über einen Windows 10 Home-Based-Laptop und müssen die Festplatte wiederherstellen. Der Datenträger wurde mithilfe der BitLocker-Treiber Verschlüsselung verschlüsselt. Das BitLocker-Wiederherstellungskennwort wurde jedoch nicht gesichert, und der übliche Benutzer des Laptops steht nicht zur Verfügung, um das Kennwort bereitzustellen.

Auflösung

Mit einer der folgenden Methoden können Sie die vorhandenen Wiederherstellungsinformationen eines Online-Clients manuell sichern oder synchronisieren:

- Erstellen Sie ein WMI-Skript (Windows Management Instrumentation), mit dem die Informationen gesichert werden. Weitere Informationen finden Sie unter BitLocker-Laufwerk Verschlüsselungsanbieter.
- Verwenden Sie in einem Eingabeaufforderungsfenster mit erhöhten Rechten den Befehl manage-bde , um die Informationen zu sichern.

  Wenn Sie beispielsweise alle Wiederherstellungsinformationen für das Laufwerk C: auf Hinzufügen sichern möchten, öffnen Sie ein Eingabeaufforderungsfenster mit erhöhten Rechten, und führen Sie den folgenden Befehl aus:

```
manage-bde -protectors -adbackup C:
```

> **NOTE**
>
> Dieser Sicherungsvorgang wird von BitLocker nicht automatisch verwaltet.

Tablet-Geräte unterstützen nicht die Verwendung von manage-bde-forcerecovery zum Testen des Wiederherstellungsmodus

Sie verfügen über ein Tablet-oder Slate-Gerät, und Sie versuchen, die BitLocker-Wiederherstellung zu testen, indem Sie den folgenden Befehl ausführen:

```
Manage-bde -forcerecovery
```

Nachdem Sie das Wiederherstellungskennwort eingegeben haben, kann das Gerät jedoch nicht gestartet werden.

Ursache

> **IMPORTANT**
>
> Tablet-Geräte unterstützen den Befehl **manage-bde-forcerecovery**nicht.

Dieses Problem tritt auf, weil der Windows-Start-Manager die Fingereingabe während der Pre-Boot-Phase des Startvorgangs nicht verarbeiten kann. Wenn der Start-Manager erkennt, dass es sich bei dem Gerät um ein Tablet handelt, leitet es den Startvorgang an die Windows-Wiederherstellungsumgebung (WinRE) weiter, die die Fingereingabe verarbeiten kann.

Wenn WindowsRE die TPM-Schutzfunktion auf der Festplatte erkennt, wird eine PCR-erneute Versiegelung durchgestellt. Der Befehl **manage-bde-forcerecovery**löscht jedoch die TPM-Beschützer auf der Festplatte. Daher kann WinRE die PCRS nicht erneut versiegeln. Dieser Fehler löst einen unendlichen BitLocker-Wiederherstellungs Zyklus aus und verhindert, dass Windows gestartet wird.

Dieses Verhalten ist beabsichtigt für alle Windows-Versionen.

Problemumgehung

Führen Sie die folgenden Schritte aus, um die Neustartschleife zu beheben:

1. Wählen Sie auf dem Bildschirm BitLocker-Wiederherstellung die Option **dieses Laufwerk überspringen**aus.
2. Wählen Sie die**EingabeaufforderungErweiterte Optionen** > **behandeln** > aus.
3. Führen Sie im Eingabeaufforderungsfenster die folgenden Befehle aus:
   ```
   cmd manage-bde –unlock C: -rp <48-digit BitLocker recovery password> manage-bde -protectors -disable C:
   ```
4. Schließen Sie das Eingabeaufforderungsfenster.
5. Schalten Sie das Gerät aus.
6. Starten Sie das Gerät. Windows sollte wie gewohnt beginnen.

Nachdem Sie UEFI-oder TPM-Firmware-Updates auf Surface installiert haben, fordert BitLocker zur Eingabe des Wiederherstellungskennworts auf.

Sie verfügen über ein Surface-Gerät, auf dem die BitLocker-Laufwerkverschlüsselung aktiviert ist. Sie aktualisieren die Firmware des TPM-Geräts oder installieren ein Update, mit dem die Signatur der System-Firmware geändert

wird. Beispielsweise installieren Sie das Surface TPM-Update (IFX).

Auf dem Surface-Gerät treten eines oder mehrere der folgenden Symptome auf:

- Beim Start werden Sie aufgefordert, Ihr BitLocker-Wiederherstellungskennwort einzugeben. Sie geben das richtige Wiederherstellungskennwort ein, aber Windows wird nicht gestartet.
- Der Start Fortschritt erfolgt direkt in die UEFI-Einstellungen (Extensible Firmware Interface) von SurfaceUnified.
- Das Surface-Gerät befindet sich anscheinend in einer Endlosschleife für den Neustart.

Ursache

Dieses Problem tritt auf, wenn das TPM des Surface-Geräts so konfiguriert ist, dass es andere PCR-Werte (Platform Configuration Register) als die Standardwerte von PCR 7 und PCR 11 verwendet. So können Sie beispielsweise die folgenden Einstellungen für das TPM konfigurieren:

- Sicheres Booten ist deaktiviert.
- PCR-Werte wurden explizit definiert, beispielsweisedurch Gruppenrichtlinien.

Geräte, die den verbundenen Standby-Modus (auch bekannt als " *InstantGO* " oder " *Always on", immer angeschlossene PCs*) unterstützen, einschließlich Surface Devices, müssen PCR 7 des TPM verwenden. In der Standardkonfiguration auf solchen Systemen bindet BitLocker an PCR 7 und PCR 11, wenn PCR 7 und sicheres Booten richtig konfiguriert sind. Weitere Informationen finden Sie unter "Informationen zum Platform Configuration Register (PCR)" unter BitLocker-Gruppenrichtlinieneinstellungen.

Auflösung

Um die auf einem Gerät verwendeten PCR-Werte zu überprüfen, öffnen Sie das Eingabeaufforderungsfenster, und führen Sie den folgenden Befehl aus:

```
manage-bde.exe -protectors -get <OSDriveLetter>:
```

In diesem Befehl <stellt *OSDriveLetter* > den Laufwerkbuchstaben des Betriebssystemlaufwerks dar.

Führen Sie die folgenden Schritte aus, um dieses Problem zu beheben und das Gerät zu reparieren.

Schritt 1: Deaktivieren der TPM-Beschützer auf dem Startlaufwerk

Wenn Sie ein TPM-oder UEFI-Update installiert haben und Ihr Gerät nicht gestartet werden kann, auch wenn Sie das richtige BitLocker-Wiederherstellungskennwort eingeben, können Sie die Möglichkeit wiederherstellen, mit dem BitLocker-Wiederherstellungskennwort und einem DGM-Wiederherstellungsabbild zu beginnen, um die TPM-Beschützer zu entfernen. vom Startlaufwerk aus.

Gehen Sie hierzu folgendermaßen vor:

1. Besorgen Sie sich Ihr BitLocker-Wiederherstellungskennwort über Ihr Microsoft.com-Konto. Wenn BitLocker von einer anderen Methode wie Microsoft BitLocker-Verwaltung und-Überwachung (MBAM) verwaltet wird, wenden Sie sich an Ihren Administrator, um Hilfe zu erhalten.
2. Verwenden Sie einen anderen Computer zum Herunterladen des Surface-Wiederherstellungs Bilds aus Herunterladen eines Wiederherstellungs Bilds für Ihre Oberfläche. Verwenden Sie das heruntergeladene Bild zum Erstellen eines USB-Wiederherstellungs Laufwerks.
3. Legen Sie das USB Surface Recovery-Bild Laufwerk in das Surface-Gerät ein, und starten Sie das Gerät.
4. Wenn Sie dazu aufgefordert werden, wählen Sie die folgenden Elemente aus:
   a. Die Sprache Ihres Betriebssystems.
   b. Ihr Tastaturlayout
5. Wählen Sie die**EingabeaufforderungErweiterte Optionen** > **behandeln** > aus.
6. Führen Sie im Eingabeaufforderungsfenster die folgenden Befehle aus:

```
cmd manage-bde -unlock -recoverypassword <Password> <DriveLetter>: manage-bde -protectors -disable
<DriveLetter>:
```

In diesen Befehlen \ <*Kennwort*\ #a1 das BitLocker-Wiederherstellungskennwort, das Sie in Schritt 1 abgerufen haben, und \ <*DriveLetter*> ist der Laufwerkbuchstabe, der Ihrem Betriebssystemlaufwerk zugewiesen ist.
> [!NOTE] > Weitere Informationen zur Verwendung dieses Befehls finden Sie unter Verwalten-BDE: entsperren.

7. Starten Sie den Computer neu.
8. Wenn Sie dazu aufgefordert werden, geben Sie das BitLocker-Wiederherstellungskennwort ein, das Sie in Schritt 1 abgerufen haben.

> **NOTE**
> Nachdem Sie die TPM-Schutzvorrichtungen deaktiviert haben, schützt die BitLocker-Laufwerkverschlüsselung Ihr Gerät nicht mehr. Um die BitLocker-Laufwerkverschlüsselung erneut zu aktivieren, wählen Sie **Start**aus, geben Sie **Manage BitLocker**ein, und drücken Sie dann die EINGABETASTE. Führen Sie die Schritte zum Verschlüsseln des Laufwerks aus.

Schritt 2: Verwenden von Surface-gu zum Wiederherstellen von Daten und Zurücksetzen des Geräts

So stellen Sie Daten von Ihrem Surface-Gerät wieder her wenn Sie Windows nicht starten können, führen Sie die Schritte 1 bis 5 von Schritt 1 aus, um zum Eingabeaufforderungsfenster zurückzukehren, und führen Sie dann die folgenden Schritte aus:

1. Führen Sie an der Eingabeaufforderung den folgenden Befehl aus:
   `cmd manage-bde -unlock -recoverypassword <Password> <DriveLetter>:` In diesem Befehl \ <*Kennwort*\ #a1 das BitLocker-Wiederherstellungskennwort, das Sie in Schritt 1 von Schritt 1abgerufen haben, und \ <*DriveLetter*> ist der Laufwerkbuchstabe, der Ihrem Betriebssystemlaufwerk zugewiesen ist.
2. Verwenden Sie nach dem Entsperren des Laufwerks den Befehl **Kopieren** oder **xcopy** , um die Benutzerdaten auf ein anderes Laufwerk zu kopieren.

   > **NOTE**
   > Weitere Informationen zum thesecommands finden Sie in denWindows-Befehlen.

3. Wenn Sie Ihr Gerät mithilfe eines Surface-Wiederherstellungs Bilds zurücksetzen möchten, folgen Sie den Anweisungen im Abschnitt "Zurücksetzen des Surface mithilfe Ihres USB-Wiederherstellungs Laufwerks" unter Erstellen und Verwenden eines USB-Wiederherstellungs Laufwerks.

Schritt 3: Wiederherstellen der standardmäßigen PCR-Werte

Um zu verhindern, dass dieses Problem wiederholt wird, verfolgbare Zustellart wir, dass yourestore die Standardkonfiguration für sicheres Booten und die PCR-Werte enthält.

Führen Sie die folgenden Schritte aus, um den sicheren Start auf einem Surface-Gerät zu aktivieren:

1. Sperren Sie BitLocker. Öffnen Sie dazu ein erweitertes Windows PowerShell-Fenster, und führen Sie das folgende Cmdlet aus: `ps Suspend-BitLocker -MountPoint "<DriveLetter>:" -RebootCount 0` In diesem Befehl ist <*DriveLetter*> der Buchstabe, der Ihrem Laufwerk zugewiesen ist.
2. Starten Sie das Gerät neu, und bearbeiten Sie dann das BIOS, um die Option für **sicheres Booten nur für Microsoft**festzulegen.
3. Starten Sie das Gerät neu.
4. Öffnen Sie ein erweitertes PowerShell-Fenster, und führen Sie das folgende Cmdlet aus:
   `ps Resume-BitLocker -MountPoint "<DriveLetter>:"`

Führen Sie die folgenden Schritte aus, um die PCR-Einstellungen für das TPM zurückzusetzen:

1. Deaktivieren Sie alle Gruppenrichtlinienobjekte, die die PCR-Einstellungen konfigurieren, oder entfernen Sie das Gerät aus allen Gruppen, die solche Richtlinien erzwingen.
   Weitere Informationen finden Sie unter BitLocker-Gruppenrichtlinieneinstellungen.
2. Sperren Sie BitLocker. Öffnen Sie dazu ein erweitertes Windows PowerShell-Fenster, und führen Sie das folgende Cmdlet aus:

   ```
   Suspend-BitLocker -MountPoint "<DriveLetter>:" -RebootCount 0
   ```

   Dabei ist <*DriveLetter*> der Buchstabe, der Ihrem Laufwerk zugewiesen ist.

3. Führen Sie das folgende Cmdlet aus:
   ```ps Resume-BitLocker -MountPoint ":"

#### Step 4: Suspend BitLocker during TPM or UEFI firmware updates

You can avoid this scenario when you install updates to system firmware or TPM firmware by temporarily suspending BitLocker before you apply such updates.

> **IMPORTANT**
>
> TPM and UEFI firmware updates may require multiple restarts while they install. To keep BitLocker suspended during this process, you must use Suspend-BitLocker and set the **Reboot Count** parameter to either of the following values:
>
> - **2** or greater: This value sets the number of times the device can restart before BitLocker Device Encryption resumes.
> - **0**: This value suspends BitLocker Drive Encryption indefinitely, until you use Resume-BitLocker or another mechanism to resume protection.

To suspend BitLocker while you install TPM or UEFI firmware updates:

1. Open an elevated Windows PowerShell window, and run the following cmdlet:
   `ps Suspend-BitLocker -MountPoint "<DriveLetter>:" -RebootCount 0` In diesem Cmdlet <*DriveLetter*> der Buchstabe, der Ihrem Laufwerk zugewiesen ist.
2. Installieren Sie den Surface-Gerätetreiber und die Firmware-Updates.
3. Nachdem Sie die Firmware-Updates installiert haben, starten Sie den Computer neu, öffnen Sie ein erweitertes PowerShell-Fenster, und führen Sie dann das folgende Cmdlet aus:
   `ps Resume-BitLocker -MountPoint "<DriveLetter>:"`

Um die BitLocker-Laufwerkverschlüsselung erneut zu aktivieren, wählen Sie **Start**aus, geben Sie **Manage BitLocker**ein, und drücken Sie dann die EINGABETASTE. Führen Sie die Schritte zum Verschlüsseln des Laufwerks aus.

## Nachdem Sie ein Update auf einem Hyper V-fähigen Computer installiert haben, fragt BitLocker nach dem Wiederherstellungskennwort und gibt Fehler 0xC0210000

Sie verfügen über ein Gerät, auf dem Windows 10, Version 1703, Windows 10, Version 1607 oder Windows Server 2016 ausgeführt wird. Darüber hinaus ist Hyper-V auf dem Gerät aktiviert. Nachdem Sie eine betroffene updateand-Startseite installiert haben, wechselt das Gerät in den BitLocker-Wiederherstellungsmodus, und es wird der Fehlercode 0xC0210000 angezeigt.

### Problemumgehung

Wenn sich Ihr Gerät bereits in diesem Zustand befindet, können Sie Windows erfolgreich starten, nachdem BitLocker in der Windows-Wiederherstellungsumgebung (WinRE) angehalten wurde. Gehen Sie hierzu folgendermaßen vor:
   ```

1. Rufen Sie das 48-stellige BitLocker-Wiederherstellungskennwort für das Betriebssystemlaufwerk aus dem Portal Ihrer Organisation oder von der Stelle ab, an der das Kennwort beim ersten Aktivieren der BitLocker-Laufwerkverschlüsselung gespeichert wurde.
2. Drücken Sie auf dem Bildschirm Wiederherstellung die EINGABETASTE. Wenn Sie dazu aufgefordert werden, geben Sie das Wiederherstellungskennwort ein.
3. Wenn Ihr Gerät im (WinRE) gestartet wird und Sie erneut zur Eingabe des Wiederherstellungskennworts aufgefordert werden, wählen Sie **Laufwerk überspringen**aus.
4. Wählen **Sie erweiterte Optionen** > aus, um die**EingabeaufforderungErweiterte Optionen** > zu**beheben** > .
5. Führen Sie im Eingabeaufforderungsfenster die folgenden Befehle aus:

   ```
   Manage-bde -unlock c: -rp <48 digit numerical recovery password separated by “-“ in 6 digit group>
   Manage-bde -protectors -disable c:
   exit
   ```

   Mit diesen Befehlen wird das Laufwerk freigegeben und BitLocker angehalten, indem die TPM-Schutzvorrichtungen auf dem Laufwerk deaktiviert werden. Der endgültige Befehl schließt das Eingabeaufforderungsfenster.

   > **NOTE**
   > Mit diesen Befehlen wird BitLocker für onerestart des Geräts angehalten. Die Option **-RC 1** funktioniert nur innerhalb des Betriebssystems und funktioniert nicht in der Wiederherstellungsumgebung.

6. Wählen Sie **Weiter** aus. Windows sollte beginnen.
7. Nachdem Windows gestartet wurde, öffnen Sie ein Eingabeaufforderungsfenster mit erhöhten Rechten, und führen Sie den folgenden Befehl aus: `cmd Manage-bde -protectors -enable c:`

> **IMPORTANT**
> Wenn Sie BitLocker nicht anhalten, bevor Sie das Gerät starten, wird dieses Problem erneut behoben.

Um BitLocker vorübergehend auszusetzen, unmittelbar bevor Sie das Gerät neu starten, öffnen Sie ein Eingabeaufforderungsfenster mit erhöhten Rechten, und führen Sie den folgenden Befehl aus:

```
Manage-bde -protectors -disable c: -rc 1
```

Auflösung

Um dieses Problem zu beheben, installieren Sie das entsprechende Update auf dem betroffenen Gerät:

- Für Windows 10, Version 1703: 9. Juli 2019 – KB4507450 (OS Build 15063,1928)
- ForWindows 10, Version 1607 und Windows Server 2016: 9. Juli 2019 – KB4507460 (OS Build 14393,3085)

Credential Guard/Device Guard für TPM 1,2: bei jedem Neustart fordert BitLocker das Wiederherstellungskennwort an und gibt Fehler 0xC0210000

Sie verfügen über ein Gerät, das TPM 1,2 verwendet und Windows 10, Version 1809, ausführt. Darüber hinaus werden auf dem Gerät Virtualisierungs-basierte Sicherheits Funktionen wie Device Guard und Credential Guardverwendet. Jedes Mal, wenn Sie das Gerät starten, wechselt das Gerät in den BitLocker-

Wiederherstellungsmodus, und es werden Fehlercode 0xc0210000 und eine Meldung angezeigt, die der folgenden ähnelt.

> Wiederherstellung
>
> Ihr PC/Gerät muss repariert werden. Auf eine erforderliche Datei konnte nicht zugegriffen werden, da der BitLocker-Schlüssel nicht richtig geladen wurde.
>
> Fehlercode 0xc0210000
>
> Sie müssen die Wiederherstellungstools verwenden. Wenn Sie nicht über ein Installationsmedium (wie einen Datenträger oder ein USB-Gerät) verfügen, wenden Sie sich an Ihren PC-Administrator oder Ihren PC/Gerätehersteller.

Ursache

TPM 1,2 unterstützt keine sichere Startfunktion. Weitere Informationen finden Sie unter Systemschutz – sicheres Starten und SMM-Schutz: Anforderungen, die von System Guard-aktivierten Computern erfüllt werden

Weitere Informationen zu dieser Technologie finden Sie unter Windows Defender-System Schutz: wie ein hardwarebasierter Stamm von Trust Windows 10 schützt

Auflösung

Führen Sie eine der folgenden Aktionen aus, um dieses Problem zu beheben:

- Entfernen Sie jedes Gerät, das TPM 1,2 verwendet, aus einer beliebigen Gruppe, die Gruppenrichtlinienobjekte (Group Policy Objects, GPOs) unterliegt, die eine sichere Einführung erzwingen.
- Bearbeiten Sie das Gruppenrichtlinienobjekt **auf Virtualisierungs-basierte Sicherheit aktivieren** , um die **sichere Startkonfiguration** auf **disabled**festzulegen.

BitLocker-Konfiguration: bekannte Probleme

03.12.2019 • 6 minutes to read

In diesem Artikel werden häufige Probleme beschrieben, die sich auf die BitLocker-Konfiguration und die allgemeine Funktionalität von BitLocker auswirken. Dieser Artikel enthält auch Anleitungen zur Behebung dieser Probleme.

BitLocker-Verschlüsselung ist in Windows 10 langsamer

In Windows 10 und Windows 7 wird BitLocker im Hintergrund ausgeführt, um Laufwerke zu verschlüsseln. In Windows 10 ist BitLocker jedoch nicht so aggressiv beim Anfordern von Ressourcen. Dieses Verhalten reduziert die Wahrscheinlichkeit, dass sich BitLocker auf die Leistung des Computers auswirkt.

Um diese Änderungen zu kompensieren, verwendet BitLocker ein neues Konvertierungs Modell. Dieses Modell (auch als "verschlüsseln-on-Write" bezeichnet) stellt sicher, dass alle neuen Datenträger auf allen Client-SKUs und internen Laufwerken immer verschlüsselt sind, sobald *Sie BitLocker aktivieren*.

> **IMPORTANT**
>
> Um die Abwärtskompatibilität zu gewährleisten, verwendet BitLocker das vorherige Konvertierungs Modell zum Verschlüsseln von austauschbaren Laufwerken.

Vorteile der Verwendung des neuen Konvertierungs Modells

Wenn Sie das vorherige Konvertierungs Modell verwenden, können Sie nicht berücksichtigen, dass ein internes Laufwerk geschützt (und mit Datenschutzstandards kompatibel ist), bis die BitLocker-Konvertierung 100 Prozent abgeschlossen ist. Bevor der Prozess abgeschlossen ist, werden die Daten, die vor der Verschlüsselung—auf dem Laufwerk vorhanden waren, möglicherweise—auch ohne Verschlüsselung gelesen und geschrieben. Daher müssen Sie warten, bis der Verschlüsselungsprozess abgeschlossen ist, bevor Sie vertrauliche Daten auf dem Laufwerk speichern. Je nach Größe des Laufwerks kann diese Verzögerung erheblich sein.

Mithilfe des neuen Konvertierungs Modells können Sie vertrauliche Daten auf dem Laufwerk sicher speichern, sobald Sie BitLocker aktivieren. Sie müssen nicht warten, bis der Verschlüsselungsvorgang abgeschlossen ist, und die Verschlüsselung beeinträchtigt die Leistung nicht. Der Nachteil besteht darin, dass der Verschlüsselungsprozess für bereits vorhandene Daten mehr Zeit in Anspruch nimmt.

Weitere BitLocker-Verbesserungen

Nachdem Windows 7 veröffentlicht wurde, wurden einige andere Bereiche von BitLocker verbessert:

- **Neuer Verschlüsselungsalgorithmus, XTS-AES**. Der neue Algorithmus bietet zusätzlichen Schutz vor einer Klasse von Angriffen auf verschlüsselte Daten, die auf Manipulation von Chiffretext abhängen, um vorhersagbare Änderungen im nur-Text zu verursachen.

  Standardmäßig erfüllt dieser Algorithmus die Federal Information Processing Standards (FIPS). FIPS sind US-Government-Standards, die einen Maßstab für die Implementierung von kryptografischer Software bieten.

- **Verbesserte Verwaltungsfunktionen**. Sie können BitLocker auf PCs oder anderen Geräten mithilfe der folgenden Schnittstellen verwalten:

  - BitLocker-Assistent
  - manage-bde

- Gruppenrichtlinienobjekte (GPOs)
- MDM-Richtlinie (Mobile Device Management)
- Windows PowerShell
- Windows-Verwaltungsoberfläche (WMI)

- **Integration in Azure Active Directory** (Azure AD). BitLocker kann Wiederherstellungsinformationen in Azure AD speichern, um eine einfachere Wiederherstellung zu ermöglichen.

- **DMA-Port Schutz (Direct Memory Access)**. Indem Sie MDM-Richtlinien zum Verwalten von BitLocker verwenden, können Sie die DMA-Ports eines Geräts blockieren und das Gerät während des Starts sichern.

- **BitLocker-Netzwerksperre**. Wenn Ihr BitLocker-fähiger Desktop-oder Server Computer mit einem drahtgebundenen Unternehmensnetzwerk in einer Domänenumgebung verbunden ist, können Sie das Betriebssystemvolume während eines Systemneustarts automatisch entsperren.

- **Unterstützung für verschlüsselte Festplatten**. Verschlüsselte Festplatten sind eine neue Klasse von Festplatten, die sich auf Hardwareebene selbst verschlüsseln und die vollständige Festplatten Hardwareverschlüsselung ermöglichen. Durch die Übernahme dieser Arbeitslast erhöhen verschlüsselte Festplatten die BitLocker-Leistung und verringern die CPU-Auslastung und den Stromverbrauch.

- **Unterstützung für Klassen von Festplatten/SSD-Hybrid Datenträgern** BitLocker kann einen Datenträger verschlüsseln, der eine kleine SSD als nicht flüchtigen Cache vor der Festplatte verwendet, beispielsweise die Intel Rapid Storage-Technologie.

Hyper-V Generation 2 VM: Zugriff auf die Lautstärke nach BitLocker-Verschlüsselung nicht möglich

Stellen Sie sich folgenden Fall vor:

1. Sie aktivieren BitLocker auf einem virtuellen Computer der Generation 2 (VM), der auf Hyper-V ausgeführt wird.
2. Beim Verschlüsseln fügen Sie Daten auf dem Datenträger hinzu.
3. Sie starten den virtuellen Computer neu, und beachten Sie Folgendes:
   - Das System Volume ist nicht verschlüsselt.
   - Auf das verschlüsselte Volume kann nicht zugegriffen werden, und der Computer listet das Dateisystem des Volumes als "unbekannt" auf.
   - Es wird eine Meldung angezeigt, die wie folgt aussieht: "Sie müssen den Datenträger in \ <*x*:> Laufwerk formatieren, bevor Sie es verwenden können."

Ursache

Dieses Problem tritt auf, weil der Drittanbieter-Filtertreiber Stcvsm. sys (von StorageCraft) auf dem virtuellen Computer installiert ist.

Auflösung

Um dieses Problem zu beheben, entfernen Sie die Software von Drittanbietern.

Produktions-Snapshots können für virtualisierte Domänencontroller, die BitLocker-verschlüsselte Datenträger verwenden, nicht verwendet werden

Sie verfügen über einen Windows Server 2019 oder 2016 Hyper-V-Server, der VMS (Gäste) hostet, die als Windows-Domänencontroller konfiguriert sind. BitLocker hat die Datenträger verschlüsselt, in denen die Active Directory-Datenbank und-Protokolldateien gespeichert sind. Wenn Sie einen "Produktions-Schnappschuss" der Domänencontroller-Gäste ausführen, wird die Sicherung durch den Volumen-Snap-Shot-Dienst (VSS) nicht

ordnungsgemäß verarbeitet.

Dieses Problem tritt unabhängig von den folgenden Variationen in der Umgebung auf:

- Wie die Domänencontroller-Volumes freigegeben werden.
- Gibt an, ob die VMs Generation 1 oder Generation 2 sind.
- Gibt an, ob es sich bei dem Gastbetriebssystem um Windows Server 2019, 2016 oder 2012 R2 handelt.

Im Anwendungsprotokoll des Domänencontrollers zeichnet die VSS-Ereignisquelle die Ereignis-ID 8229 auf:

```
ID: 8229
Stufe: Warnung
Quelle: VSS
Meldung: ein VSS-Writer hat ein Ereignis mit Fehler 0x800423f4 abgelehnt, der Writer hat einen nicht flüchtigen Fehler erlebt. Wenn der Sicherungsvorgang wiederholt wird, wird der Fehler wahrscheinlich erneut auftreten.

Änderungen, die der Writer während der Behandlung des Ereignisses an den Writer-Komponenten vorgenommen hat, stehen dem anfordernden nicht zur Verfügung.

Überprüfen Sie das Ereignisprotokoll auf verwandte Ereignisse aus der Anwendung, die den VSS-Writer hostet.

Vorgang
PostSnapshot-Ereignis

Kontext
Ausführungskontext: Writer-Writer-Klassen-ID: {b2014c9e-8711-4c5c-a5a9-3cf384484757}
Name des Writers: NTDS
Writer-Instanz-ID: {d170b355-A523-47ba-a5c8-732244f70e75} Befehlszeile: C:\Windows\system32\lsass.exe

Prozess-ID: 680
```

Im Ereignisprotokoll der Domänencontroller-Verzeichnisdienste wird ein Ereignis angezeigt, das wie folgt aussieht:

```
Fehler Microsoft-Windows-ActiveDirectory \ _DomainService 1168
Interner prozessinterner Fehler: ein Active Directory-Domänendienste-Fehler ist aufgetreten.

 Zusätzliche Daten
 Fehlerwert (dezimal): -1022

Fehlerwert (Hex): fffffc02

Interne ID: 160207d9
```

> **NOTE**
> Die interne ID dieses Ereignisses kann je nach Betriebssystemversion und Pfadebene unterschiedlich sein.

Nachdem dieses Problem auftritt, wenn Sie den Befehl **vssadmin List Writers** ausführen, wird die Ausgabe angezeigt, die für den VSS-Writer (Active Directory Domain Services, NTDS) wie folgt aussieht:

```
Writer-Name: ' NTDS '
  Writer-ID: {b2014c9e-8711-4c5c-a5a9-3cf384484757}
  Writer-Instanz-ID: {08321e53-4032-44dc-9b03-7a1a15ad3eb8}
  Status: \ [11 ] Fehler
```

> Letzter Fehler: nicht Retryable Fehler

Darüber hinaus können Sie die VMs erst sichern, nachdem Sie Sie neu gestartet haben.

Ursache

Nachdem VSS eine Momentaufnahme eines Volumes erstellt hat, übernimmt der VSS-Writer die Aktionen "Post-Schnappschuss". Im Fall eines "Production-Snapshots", den Sie vom Hostserver initiieren, versucht Hyper-V, das snapshotted-Volume bereitzustellen. Es ist jedoch nicht möglich, die Lautstärke für unverschlüsselten Zugriff aufzuheben. BitLocker auf dem Hyper-V-Server erkennt die Lautstärke nicht. Daher schlägt der Zugriffsversuch fehl, und der Snapshot-Vorgang schlägt fehl.

Dieses Verhalten ist entwurfsbedingt.

Problemumgehung

Es gibt eine unterstützte Möglichkeit zum Durchführen der Sicherung und Wiederherstellung eines virtualisierten Domänencontrollers:

- Führen Sie die Windows Server-Sicherung im Gastbetriebssystem aus.

Wenn Sie einen Produktions-Schnappschuss eines virtualisierten Domänencontrollers erstellen müssen, können Sie BitLocker im Gastbetriebssystem anhalten, bevor Sie den Produktions-Schnappschuss starten. Dieser Ansatz wird jedoch nicht empfohlen.

Weitere Informationen und Empfehlungen zum Sichern von virtualisierten Domänencontrollern finden Sie unter Virtualisierung von Domänencontrollern mit Hyper-V: Überlegungen zur Sicherung und Wiederherstellung für virtualisierte Domänencontroller

Weitere Informationen

Wenn der VSS-NTDS-Writer Zugriff auf das verschlüsselte Laufwerk anfordert, generiert der Local Security Authority Subsystem Service (LSASS) einen Fehlereintrag, der wie folgt aussieht:

```
\# for hex 0xc0210000 / decimal -1071579136
 STATUS\_FVE\_LOCKED\_VOLUME ntstatus.h
 \# This volume is locked by BitLocker Drive Encryption.
```

Der Vorgang erzeugt den folgenden Aufruf Stapel:

```
\# Child-SP RetAddr Call Site
 00 00000086\`b357a800 00007ffc\`ea6e7a4c KERNELBASE\!FindFirstFileExW+0x1ba \
[d:\\rs1\\minkernel\\kernelbase\\filefind.c @ 872\]
 01 00000086\`b357abd0 00007ffc\`e824accb KERNELBASE\!FindFirstFileW+0x1c \
[d:\\rs1\\minkernel\\kernelbase\\filefind.c @ 208\]
 02 00000086\`b357ac10 00007ffc\`e824afa1 ESENT\!COSFileFind::ErrInit+0x10b \
[d:\\rs1\\onecore\\ds\\esent\\src\\os\\osfs.cxx @ 2476\]
 03 00000086\`b357b700 00007ffc\`e827bf02 ESENT\!COSFileSystem::ErrFileFind+0xa1 \
[d:\\rs1\\onecore\\ds\\esent\\src\\os\\osfs.cxx @ 1443\]
 04 00000086\`b357b960 00007ffc\`e82882a9 ESENT\!JetGetDatabaseFileInfoEx+0xa2 \
[d:\\rs1\\onecore\\ds\\esent\\src\\ese\\jetapi.cxx @ 11503\]
 05 00000086\`b357c260 00007ffc\`e8288166 ESENT\!JetGetDatabaseFileInfoExA+0x59 \
[d:\\rs1\\onecore\\ds\\esent\\src\\ese\\jetapi.cxx @ 11759\]
 06 00000086\`b357c390 00007ffc\`e84c64fb ESENT\!JetGetDatabaseFileInfoA+0x46 \
[d:\\rs1\\onecore\\ds\\esent\\src\\ese\\jetapi.cxx @ 12076\]
 07 00000086\`b357c3f0 00007ffc\`e84c5f23 ntdsbsrv\!CVssJetWriterLocal::RecoverJetDB+0x12f \
[d:\\rs1\\ds\\ds\\src\\jetback\\snapshot.cxx @ 2009\]
 08 00000086\`b357c710 00007ffc\`e80339e0 ntdsbsrv\!CVssJetWriterLocal::OnPostSnapshot+0x293 \
[d:\\rs1\\ds\\ds\\src\\jetback\\snapshot.cxx @ 2190\]
 09 00000086\`b357cad0 00007ffc\`e801fe6d VSSAPI\!CVssIJetWriter::OnPostSnapshot+0x300 \
[d:\\rs1\\base\\stor\\vss\\modules\\jetwriter\\ijetwriter.cpp @ 1704\]
 0a 00000086\`b357ccc0 00007ffc\`e8022193 VSSAPI\!CVssWriterImpl::OnPostSnapshotGuard+0x1d \
[d:\\rs1\\base\\stor\\vss\\modules\\vswriter\\vswrtimp.cpp @ 5228\]
 0b 00000086\`b357ccf0 00007ffc\`e80214f0 VSSAPI\!CVssWriterImpl::PostSnapshotInternal+0xc3b \
[d:\\rs1\\base\\stor\\vss\\modules\\vswriter\\vswrtimp.cpp @ 3552\]
```

BitLocker kann ein Laufwerk nicht verschlüsseln: bekannte TPM-Probleme

03.12.2019 • 4 minutes to read

In diesem Artikel werden häufige Probleme beschrieben, die sich auf das Trusted Platform Module (TPM) auswirken und verhindern, dass BitLocker ein Laufwerk verschlüsseln kann. Dieser Artikel enthält auch Anleitungen zur Behebung dieser Probleme.

> **NOTE**
>
> Wenn Sie festgestellt haben, dass das BitLocker-Problem nicht das TPM umfasst, lesen Sie BitLocker kann ein Laufwerk nicht verschlüsseln: bekannte Probleme.

Das TPM ist gesperrt, und Sie sehen "das TPM verteidigt sich gegen Wörterbuchangriffe und befindet sich in einem Timeoutzeitraum"

Wenn Sie die BitLocker-Laufwerkverschlüsselung aktivieren, wird Sie nicht gestartet. Stattdessen wird eine Meldung angezeigt, die ähnelt "das TPM verteidigt sich gegen Wörterbuchangriffe und befindet sich in einem Timeoutzeitraum."

Ursache

Das TPM ist gesperrt.

Auflösung

Führen Sie die folgenden Schritte aus, um dieses Problem zu beheben:

1. Öffnen Sie ein erweitertes PowerShell-Fenster, und führen Sie das folgende Skript aus:

```
$Tpm = Get-WmiObject -class Win32_Tpm -namespace "root\CIMv2\Security\MicrosoftTpm" $ConfirmationStatus
= $Tpm.GetPhysicalPresenceConfirmationStatus(22).ConfirmationStatus if($ConfirmationStatus -ne 4)
{$Tpm.SetPhysicalPresenceRequest(22)}
```

2. Starten Sie den Computer neu. Wenn Sie beim Neustart aufgefordert werden, drücken Sie F12, um sich zu einigen.

3. Versuchen Sie erneut, die BitLocker-Laufwerkverschlüsselung zu starten.

Sie können das TPM nicht vorbereiten, und Sie sehen "das TPM verteidigt sich gegen Wörterbuchangriffe und befindet sich in einem Timeoutzeitraum"

Sie können die BitLocker-Laufwerkverschlüsselung auf einem Gerät nicht aktivieren. Sie verwenden die TPM-Verwaltungskonsole (TPM. msc), um das TPM auf einem Gerät vorzubereiten. Der Vorgang schlägt fehl, und es wird eine Meldung angezeigt, die ähnelt "das TPM verteidigt sich gegen Wörterbuchangriffe und befindet sich in einem Timeoutzeitraum."

Ursache

Das TPM ist gesperrt.

Auflösung

Um dieses Problem zu beheben, deaktivieren Sie das TPM, und aktivieren Sie es erneut. Gehen Sie hierzu folgendermaßen vor:

1. Starten Sie das Gerät neu, und ändern Sie die BIOS-Konfiguration, um das TPM zu deaktivieren.
2. Starten Sie das Gerät erneut, und kehren Sie zur TPM-Verwaltungskonsole zurück. Sie sollten eine Meldung erhalten, die der folgenden ähnelt:

   > Kompatibles Trusted Platform Module (TPM) kann auf diesem Computer nicht gefunden werden. Vergewissern Sie sich, dass dieser Computer 1,2-TPM hat und im BIOS aktiviert ist.

3. Starten Sie das Gerät neu, und ändern Sie die BIOS-Konfiguration, um das TPM zu aktivieren.
4. Starten Sie das Gerät neu, und kehren Sie zur TPM-Verwaltungskonsole zurück.

Wenn Sie das TPM weiterhin nicht vorbereiten können, löschen Sie die vorhandenen TPM-Schlüssel. Befolgen Sie dazu die Anweisungen unter Problembehandlung beim TPM: Löschen Sie alle Schlüssel aus dem TPM.

> **WARNING**
>
> Das Löschen des TPMs kann zu Datenverlusten führen.

Zugriff verweigert: Fehler beim Sichern der TPM-Besitzer Autorisierungsinformationen für Active Directory-Domänendienste. ErrorCode: 0x80070005

Sie verfügen über eine Umgebung, in der die Funktion **BitLocker nicht aktivieren, bis Wiederherstellungsinformationen in der AD DS** -Richtlinie gespeichert sind. Sie versuchen, die BitLocker-Laufwerkverschlüsselung auf einem Computer zu aktivieren, auf dem Windows 7 ausgeführt wird, aber der Vorgang schlägt fehl. Sie erhalten eine Nachricht, die "Zugriff verweigert" oder "unzureichende Rechte" ähnelt.

Ursache

Das TPM hatte nicht genügend Berechtigungen für den TPM-Gerätecontainer in Active Directory-Domänendienste (AD DS). Daher konnten die BitLocker-Wiederherstellungsinformationen nicht in AD DS gesichert werden, und die BitLocker-Laufwerkverschlüsselung konnte nicht ausgeführt werden.

Dieses Problem ist anscheinend auf Computer mit Windows-Versionen, die älter als Windows 10 sind, zu begrenzen.

Auflösung

Verwenden Sie eine der folgenden Methoden, um zu überprüfen, ob Sie dieses Problem richtig erkannt haben:

- Deaktivieren Sie die Richtlinie, oder entfernen Sie den Computer aus der Domäne. Versuchen Sie dann erneut, die BitLocker-Laufwerkverschlüsselung zu aktivieren. Der Vorgang sollte jetzt erfolgreich sein.
- Verwenden Sie LDAP-und Netzwerk Ablaufverfolgungstools, um den LDAP-Austausch zwischen dem Client und dem AD DS-Domänencontroller zu untersuchen, um die Ursache für den Fehler "Zugriff verweigert" oder "unzureichende Rechte" zu ermitteln. In diesem Fall sollte der Fehler angezeigt werden, wenn der Client versucht, auf sein Objekt im Container "CN = TPM Devices, DC = \ <*Domain*>, DC = com" zuzugreifen.

1. Wenn Sie die TPM-Informationen für den betroffenen Computer überprüfen möchten, öffnen Sie ein erweitertes Windows PowerShell-Fenster, und führen Sie den folgenden Befehl aus:

```
Get-ADComputer -Filter {Name -like "ComputerName"} -Property * | Format-Table name,msTPM-TPMInformationForComputer
```

In diesem Befehl ist *Computer* Name der Name des betroffenen Computers.

2. Um das Problem zu beheben, verwenden Sie ein Tool wie DSACLS. exe, um sicherzustellen, dass die Zugriffssteuerungsliste von msTPM-TPMInformationForComputer sowohl Lese-als auch Schreibberechtigungen für NTAUTHORITY/Self gewährt.

Das TPM kann nicht vorbereitet werden, Fehler 0x80072030: "Es gibt kein solches Objekt auf dem Server"

Ihre Domänencontroller wurden von Windows Server 2008 R2to Windows Server 2012 R2 aktualisiert. Ein Gruppenrichtlinienobjekt (GPO) erzwingt die **Option "BitLocker nicht aktivieren, bis Wiederherstellungsinformationen in der AD DS** -Richtlinie gespeichert werden.

Sie können die BitLocker-Laufwerkverschlüsselung auf einem Gerät nicht aktivieren. Sie verwenden die TPM-Verwaltungskonsole (TPM. msc), um das TPM auf einem Gerät vorzubereiten. Der Vorgang schlägt fehl, und es wird eine Meldung angezeigt, die der folgenden ähnelt:

> 0x80072030 kein solches Objekt auf dem Server vorhanden ist, wenn eine Richtlinie zum Sichern von TPM-Informationen in Active Directory aktiviert ist

Sie haben bestätigt, dass die Attribute **ms-TPM-OwnerInformation** und **msTPM-TpmInformationForComputer** vorhanden sind.

Ursache

Die Funktionsebene Domäne und Gesamtstruktur der Umgebung ist möglicherweise weiterhin auf Windows 2008 R2 eingestellt. Darüber hinaus sind die Berechtigungen in AD DS möglicherweise nicht ordnungsgemäß eingestellt.

Auflösung

Führen Sie die folgenden Schritte aus, um dieses Problem zu beheben:

1. Aktualisieren Sie die Funktionsebene der Domäne und der Gesamtstruktur auf Windows Server 2012 R2.
2. Laden Sie Add-TPMSelfWriteACE. vbsherunter.
3. Ändern Sie im Skript den Wert von **strPathToDomain** in Ihren Domänennamen.
4. Öffnen Sie ein erweitertes PowerShell-Fenster, und führen Sie den folgenden Befehl aus:

```
cscript <Path>Add-TPMSelfWriteACE.vbs
```

In diesem Befehl \ <*path*> der Pfad zur Skriptdatei.

Weitere Informationen finden Sie in den folgenden Artikeln:

- Sichern der TPM-Wiederherstellungsinformationen in AD DS
- Vorbereiten Ihrer Organisation auf BitLocker: Planung und Richtlinien

BitLocker und TPM: andere bekannte Probleme

03.12.2019 • 4 minutes to read

In diesem Artikel werden häufige Probleme beschrieben, die sich direkt auf das Trusted Platform Module (TPM) beziehen, und es werden Anleitungen zur Behebung dieser Probleme bereitgestellt.

Azure AD: Windows Hello for Business und einmaliges Anmelden funktionieren nicht

Sie haben einen Azure Active Directory (Azure AD)-Clientcomputer, der sich nicht richtig authentifizieren kann. Sie können eines oder mehrere der folgenden Symptome auftreten:

- Windows Hello for Business funktioniert nicht.
- Der bedingte Zugriff schlägt fehl.
- Einmaliges Anmelden (Single Sign-on, SSO) funktioniert nicht.

Darüber hinaus protokolliert der Computer einen Eintrag für die Ereignis-ID 1026, die wie folgt aussieht:

```
Protokoll Name: System
Quelle: Microsoft-Windows-TPM-WMI
Datum: \
Ereignis-ID: 1026
Aufgabenkategorie: keine
Ebene: Informationen
Schlüsselwörter:
Benutzer: System
Computer: \ <Computername \ #a1
Beschreibung:
Die TPM-Hardware (Trusted Platform Module) auf diesem Computer kann nicht zur automatischen
Verwendung bereitgestellt werden.Wenn Sie das TPM interaktiv einrichten möchten, verwenden Sie die TPM-
Verwaltungskonsole (Start-\ >TPM. msc), und verwenden Sie die Aktion, um das TPM bereitzustellen.
Fehler: das TPM verteidigt sich gegen Wörterbuchangriffe und befindet sich in einem Timeoutzeitraum.
Weitere Informationen: 0x840000
```

Ursache

Dieses Ereignis zeigt an, dass das TPM nicht bereit ist oder über eine bestimmte Einstellung verfügt, die den Zugriff auf die TPM-Schlüssel verhindert.

Darüber hinaus zeigt das Verhalten an, dass der Clientcomputer kein Primäres Aktualisierungs Token (FHM)abrufen kann.

Auflösung

Um den Status des PRT zu überprüfen, verwenden Sie den Befehl dsregcmd/Status , um Informationen zu sammeln. Überprüfen Sie in der Toolausgabe, ob der **Benutzerstatus** oder der **SSO-Zustand** das **AzureAdPrt** -Attribut enthält. Wenn der Wert dieses Attributs " **Nein**" lautet, wurde das FHM nicht ausgestellt. Dies kann darauf hindeuten, dass der Computer sein Zertifikat nicht für die Authentifizierung präsentieren konnte.

Um dieses Problem zu beheben, führen Sie die folgenden Schritte aus, um das TPM zu beheben:

1. Öffnen Sie die TPM-Verwaltungskonsole (TPM. msc). Wählen Sie dazu **Start**aus, und geben Sie im **Suchfeld**

TPM. msc ein.

2. Wenn ein Hinweis angezeigt wird, ob Sie das TPM entsperren oder die Sperrung zurücksetzen möchten, befolgen Sie diese Anweisungen.
3. Wenn diese Meldung nicht angezeigt wird, überprüfen Sie die BIOS-Einstellungen des Computers auf alle Einstellungen, die Sie zum Zurücksetzen oder Deaktivieren der Sperrung verwenden können.
4. Wenden Sie sich an den Hardwarehersteller, um festzustellen, ob ein bekannter Fix für das Problem vorliegt.
5. Wenn Sie das Problem immer noch nicht beheben können, deaktivieren Sie das TPM, und initialisieren Sie es erneut. Befolgen Sie dazu die Anweisungen unter Problembehandlung beim TPM: Löschen Sie alle Schlüssel aus dem TPM. > [!WARNING] > Das Löschen des TPMs kann zu Datenverlusten führen.

TPM 1,2-Fehler: beim Laden der Verwaltungskonsole ist ein Fehler aufgetreten. Das Gerät, das vom kryptografischen Anbieter benötigt wird, ist nicht einsatzbereit

Sie verfügen über einen Computer mit Windows 10, Version 1703, der TPM, Version 1,2, verwendet. Wenn Sie versuchen, die TPM-Verwaltungskonsole zu öffnen, wird eine Meldung angezeigt, die der folgenden ähnelt:

> Fehler beim Laden der Verwaltungskonsole. Das Gerät, das vom kryptografischen Anbieter benötigt wird, kann nicht verwendet werden.
> HRESULT 0x800900300x80090030-nte \ _DEVICE \ _NOT \ _READY
> Das Gerät, das von diesem kryptografischen Anbieter benötigt wird, kann nicht verwendet werden.
> TPM-spec-Version: TPM v 1.2

Auf einem anderen Gerät, auf dem dieselbe Version von Windows ausgeführt wird, können Sie die TPM-Verwaltungskonsole öffnen.

Ursache (vermutet)

Diese Symptome deuten darauf hin, dass das TPM Hardware-oder Firmware-Probleme aufweist.

Auflösung

Um dieses Problem zu beheben, wechseln Sie den TPM-Betriebsmodus von Version 1,2 auf Version 2,0.

Wenn das Problem dadurch nicht behoben wird, sollten Sie die Hauptplatine des Geräts ersetzen. Nachdem Sie die Hauptplatine ersetzt haben, wechseln Sie den TPM-Betriebsmodus von Version 1,2 auf Version 2,0.

Geräte werden aufgrund eines TPM-Problems nicht an Hybrid Azure AD teilnehmen

Sie verfügen über ein Gerät, das Sie zu einer Hybrid Azure AD hinzufügen möchten. Der Join-Vorgang scheint jedoch fehlgeschlagen zu sein.

Verwenden Sie den Befehl dsregcmd/Status, um zu überprüfen, ob die Verknüpfung erfolgreich war. In der Toolausgabe zeigen die folgenden Attribute an, dass die Verknüpfung erfolgreich war:

- **AzureAdJoined: Ja**
- **Domänenname: \ <*-Prem-Domänenname*>**

Wenn der Wert von **AzureADJoined nicht**ist, ist die Verknüpfung fehlgeschlagen.

Ursachen und Auflösungen

Dieses Problem kann auftreten, wenn das Windows-Betriebssystem nicht der Besitzer des TPM ist. Die spezifische Lösung für dieses Problem hängt davon ab, welche Fehler oder Ereignisse auftreten, wie in der folgenden Tabelle dargestellt:

NACHRICHT	GRUND	AUFLÖSUNG
NTE \ _BAD \ _KEYSET (0x80090016/-2146893802)	Der TPM-Vorgang ist fehlgeschlagen oder war ungültig.	Dieses Problem wurde wahrscheinlich durch ein fehlerhaftes Sysprep-Bild verursacht. Stellen Sie sicher, dass Sie das Sysprep-Abbild mithilfe eines Computers erstellen, der nicht mit Azure AD oder Hybrid Azure AD verbunden oder registriert ist.
TPM \ _E \ _PCP \ _INTERNAL \ _ERROR (0x80290407/-2144795641)	Allgemeiner TPM-Fehler.	Wenn das Gerät diesen Fehler zurückgibt, deaktivieren Sie sein TPM. Windows 10, Version 1809 und höhere Versionen erkennen TPM-Fehler automatisch und beenden die Hybrid Azure AD-Verknüpfung, ohne das TPM zu verwenden.
TPM \ _E \ _NOTFIPS (0x80280036/-2144862154)	Der FIPS-Modus des TPM wird derzeit nicht unterstützt.	Wenn das Gerät diesen Fehler aufweist, deaktivieren Sie sein TPM. Windows 10, Version 1809 und höhere Versionen erkennen TPM-Fehler automatisch und beenden die Hybrid Azure AD-Verknüpfung, ohne das TPM zu verwenden.
NTE \ _AUTHENTICATION \ _IGNORED (0x80090031/-2146893775)	Das TPM ist gesperrt.	Dieser Fehler ist vorübergehend. Warten Sie auf die Abklingzeit, und wiederholen Sie dann den Join-Vorgang.

Weitere Informationen zu TPM-Problemen finden Sie in den folgenden Artikeln:

- TPM-Grundlagen: Anti-hämmern
- Problembehandlung bei Hybrid Azure Active Directory-verbundenen Geräten
- Behandeln von Problemen mit dem TPM

Decodieren der gemessenen Start Protokolle zum nachvollziehen von PCR-Änderungen

03.12.2019 • 2 minutes to read

Platform Configuration Registers (PCRs) sind Speicherorte im Trusted Platform Module (TPM). BitLocker und die zugehörigen Technologien sind von bestimmten PCR-Konfigurationen abhängig. Darüber hinaus kann eine bestimmte Änderung in PCRs dazu führen, dass ein Gerät oder Computer in den BitLocker-Wiederherstellungsmodus wechselt.

Durch Nachverfolgen von Änderungen in der PCRs und erkennen, wann Sie sich geändert haben, können Sie Einblicke in Probleme gewinnen, die auftreten, oder erfahren, warum ein Gerät oder Computer in den BitLocker-Wiederherstellungsmodus gewechselt ist. Die gemessenen Start Protokolle zeichnen PCR-Änderungen und andere Informationen auf. Diese Protokolle befinden sich im Ordner C:\Windows\Logs\MeasuredBoot\.

In diesem Artikel werden die Tools beschrieben, die Sie zum Decodieren dieser Protokolle verwenden können: TBSLogGenerator und PCPTool.

Weitere Informationen zu gemessenen Start-und PCRs finden Sie in den folgenden Artikeln:

- TPM-Grundlagen: gemessener Start mit Unterstützung für die Bescheinigung
- Grundlegendes zu PCR-Bänken auf TPM2.0-Geräten

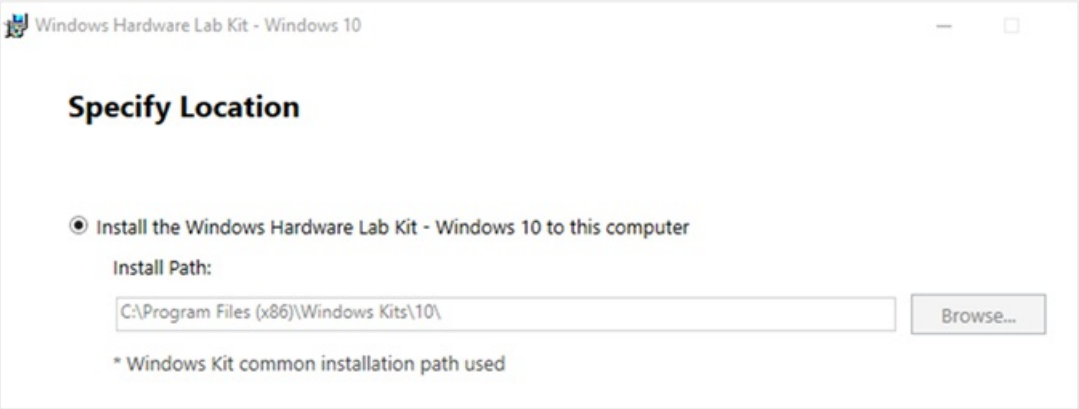
Verwenden von TBSLogGenerator zum Decodieren von gemessenen Start Protokollen

Verwenden Sie TBSLogGenerator, um gemessene Start Protokolle zu decodieren, die Sie in Windows 10 und früheren Versionen gesammelt haben. Sie können dieses Tool auf den folgenden Systemen installieren:

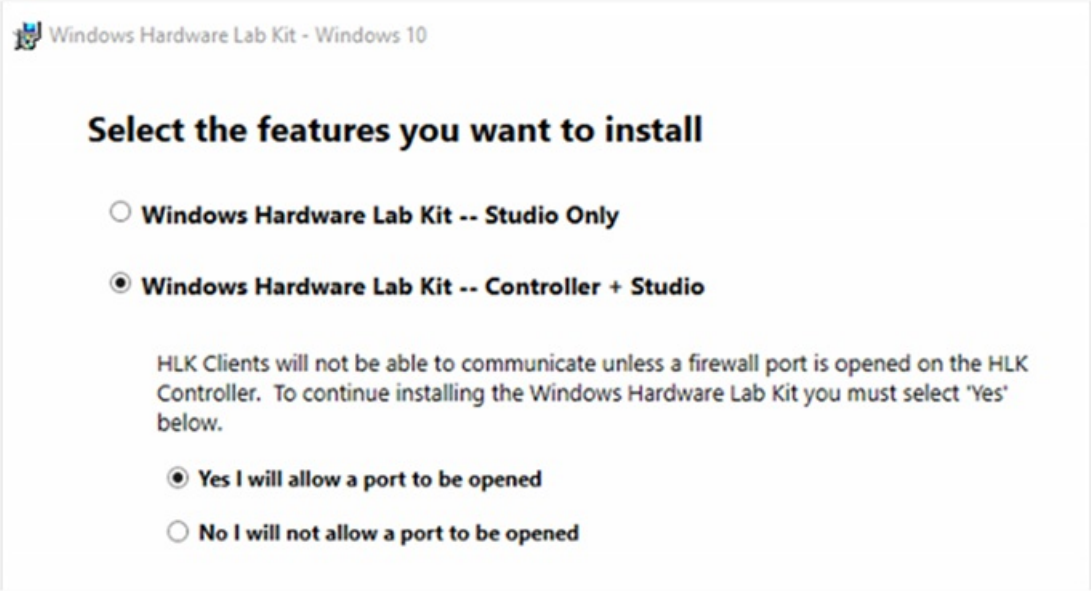
- Auf einem Computer, auf dem Windows Server 2016 ausgeführt wird und für den ein TPM aktiviert ist
- Einen virtuellen Computer der Generation 2 (mit Hyper-V), auf dem Windows Server 2016 ausgeführt wird (Sie können das virtuelle TPM verwenden)

Führen Sie die folgenden Schritte aus, um das Tool zu installieren:

1. Laden Sie das Windows Hardware Lab Kit von einem der folgenden Speicherorte herunter:
   - Windows Hardware Lab Kit
   - Direkter Download-Link für Windows Server 2016: Windows HLK, Version 1607
2. Übernehmen Sie den Standardinstallationspfad.



3. Wählen Sie unter **Wählen Sie die zu installierenden Features aus die**Option **Windows—Hardware Lab Kit Controller + Studio**aus.

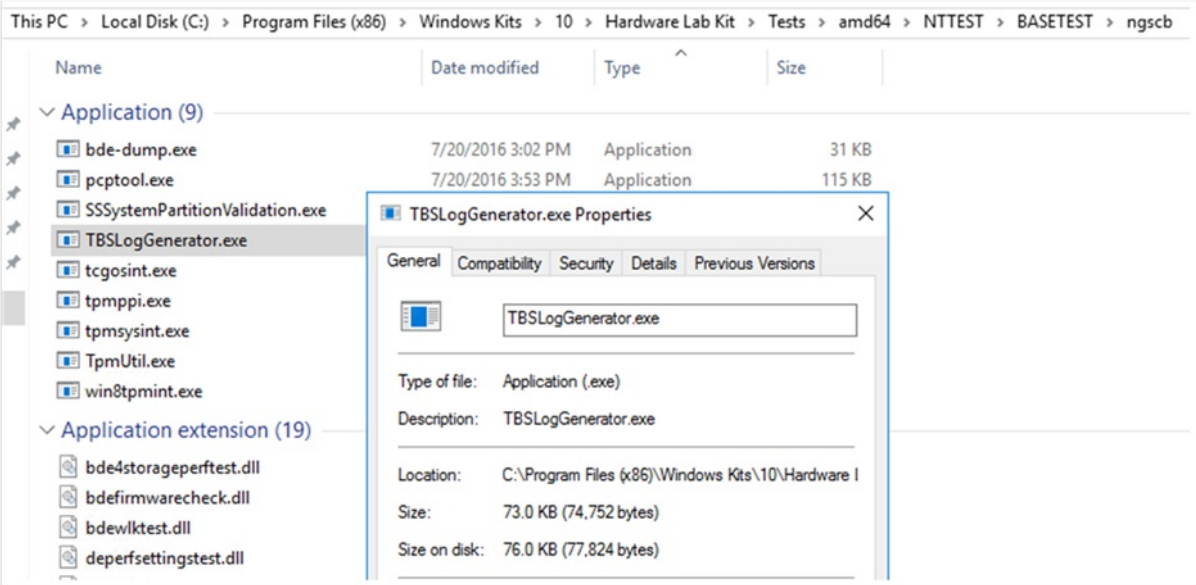


4. Beenden Sie die Installation.

Führen Sie die folgenden Schritte aus, um TBSLogGenerator zu verwenden:

1. Nachdem die Installation abgeschlossen ist, öffnen Sie ein Eingabeaufforderungsfenster mit erhöhten Rechten, und navigieren Sie zum folgenden Ordner:
   C:\Programme-Dateien (x86) \Windows Kits\10\Hardware Lab Kit\Tests\amd64\NTTEST\BASETEST\ngscb

   Dieser Ordner enthält die Datei "TBSLogGenerator. exe".



2. Führen Sie den folgenden Befehl aus:

```
TBSLogGenerator.exe -LF <LogFolderName>\<LogFileName>.log > <DestinationFolderName>\
<DecodedFileName>.txt
```

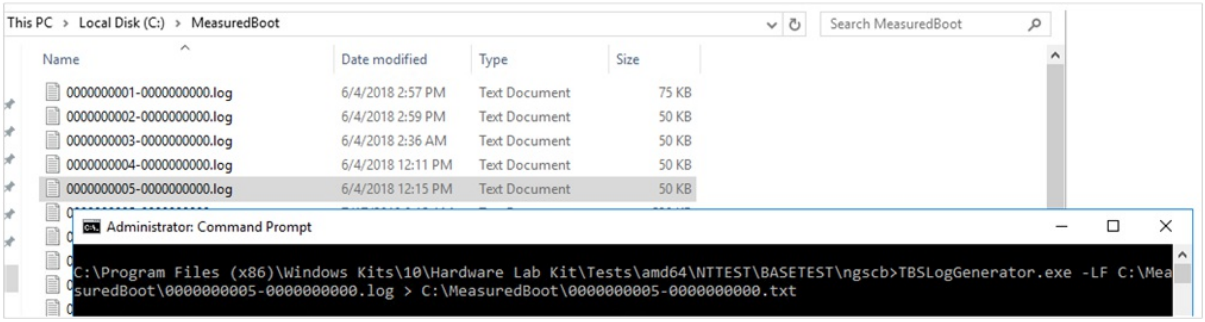
   wobei die Variablen die folgenden Werte darstellen:

   - *<LogFolderName>* = der Name des Ordners, der die zu decodierende Datei enthält.
   - *<LogFileName>* = der Name der zu decodierenden Datei

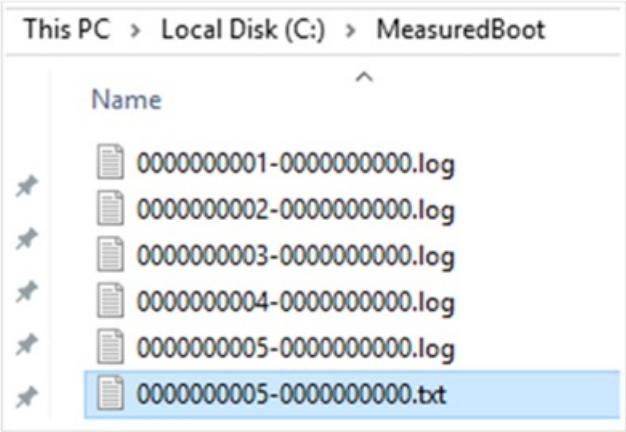
- <*DestinationFolderName*> = der Name des Ordners für die decodierte Textdatei
- <*DecodedFileName*> = der Name der decodierten Textdatei

Die folgende Abbildung zeigt beispielsweise gemessene Start Protokolle, die von einem Windows 10-Computer gesammelt und in den C:\MeasuredBoot\-Ordner eingefügt wurden. Die Abbildung zeigt auch ein Eingabeaufforderungsfenster und den Befehl zum Decodieren der **0000000005 -0000000000. log** -Datei:

```
TBSLogGenerator.exe -LF C:\MeasuredBoot\0000000005-0000000000.log > C:\MeasuredBoot\0000000005-
0000000000.txt
```



Der Befehl erzeugt eine Textdatei, die den angegebenen Namen verwendet. Im Fall des Beispiels ist die Datei **0000000005 -0000000000. txt**. Die Datei befindet sich im gleichen Ordner wie die ursprüngliche Log-Datei.



Der Inhalt dieser Textdatei ähnelt wie folgt.

```
0000000005-0000000000.txt - Notepad
File  Edit  Format  View  Help
TBS = Tbsi_Get_TCG_Log()
Length = 51094
=====================================================================
EventLog contains 51094 bytes.
00000000 | 00 00 00 00 03 00 00 00-00 00 00 00 00 00 00 00 |
00000010 | 00 00 00 00 00 00 00 00-00 00 00 00 25 00 00 00 |             %
00000020 | 53 70 65 63 20 49 44 20-45 76 65 6e 74 30 33 00 | Spec ID Event03
00000030 | 00 00 00 00 00 02 00 02-02 00 00 00 04 00 14 00 |
00000040 | 0b 00 20 00 00 00 00 00-00 08 00 00 00 02 00 00 |
00000050 | 00 04 00 38 98 b2 50 66-78 5e c6 ea 07 a4 c0 57 |    8˜²Pfx^Æê ¤ÀW
00000060 | 2f 31 84 22 28 eb b8 0b-00 68 f6 88 a1 9e fe 7a | /1„"(ë¸  hö^¡žþz
00000070 | ff 84 9f 5e b1 43 d7 31-80 bd 4e b3 ef f8 fe 79 | ÿ„Ÿ^±C×1€½N³ïøþy
00000080 | b1 69 c4 c7 3d 59 73 2b-0c 14 00 00 00 4e 00 31 | ±iÄÇ=Ys+     N 1
00000090 | 00 51 00 45 00 54 00 36-00 39 00 57 00 20 00 00 |  Q E T 6 9 W
000000a0 | 00 00 00 00 00 08 00 00-80 02 00 00 00 04 00 5b |         €      [
000000b0 | 18 ea 02 fe af ed 24 57-a8 0e 7f af 80 b1 bc 23 |  ê þ¯í$W¨ ¯€±¼#
000000c0 | c1 19 b9 0b 00 5e 37 7e-fa f2 2f 9a 47 93 1e 8e | Á ¹  ^7~úò/šG“ Ž
000000d0 | fd 7e 84 31 98 09 71 4e-6d 93 86 db d2 4c 7b 2c | ý~„1˜ qNm“†ÛÒL{,
000000e0 | da a6 cf f7 0e 10 00 00-00 00 00 fe ff 00 00 00 | Ú¦Ï÷       þÿ
000000f0 | 00 00 00 02 00 00 00 00-00 00 00 00 00 08 00 00 |
00000100 | 80 02 00 00 00 04 00 2f-15 95 c7 0b 52 08 f4 43 | €      / •Ç R ôC
```

Um die PCR-Informationen zu finden, wechseln Sie zum Ende der Datei.

```
0000000005-0000000000.txt - Notepad
File  Edit  Format  View  Help
000000e0 | f7 ac 1c 56 35 fd 5a 81-32 cd 75 81 2d f2 71 7a | ÷¬ V5ýZ2Íu-òqz
000000f0 | 3e fa 4c 1a dc 91 84 10-99 dd 29 04 83 c0 a8 9c | >úL Ü‘„ ™Ý) ƒÀ¨œ
END AGGREGATION
=====================================================================
| PCR[00] |  100ffab3d44a795eb3415d9432ce9e478905853cb8a7c017ad31809b4ac22245  | INVALID! |
|   TPM   | [c1a83c2d518990c532797f9fc544587827173ff72ab56a182e700c60448ffc64] |          |
| PCR[01] |  dd8b8ec0d7e6544dc79061c8ff89d1c4b2959a2b889abaea57cceb7e4e4b8c43  | INVALID! |
|   TPM   | [7f3842880eb9a9d050d4a71facda7897e868acea29ef707eb60216ae13bc5360] |          |
| PCR[02] |  50058edb288daee0f72e4fd6b6d3de351b78893e701ae98973cbe96b98e10e43  | INVALID! |
|   TPM   | [3d458cfe55cc03ea1f443f1562beec8df51c75e14a9fcf9a7234a13f198e7969] |          |
| PCR[03] |  3d458cfe55cc03ea1f443f1562beec8df51c75e14a9fcf9a7234a13f198e7969  |  MATCH!  |
| PCR[04] |  86ad8aaaecb8e2fe1d1a4c63a7d757989375045e4763f5a042e03dfef464587d  | INVALID! |
|   TPM   | [18d808fa43a0a3ed530e174e6d4e3a228a90bac4ee665fc38de99bd37a355d61] |          |
| PCR[05] |  49ceb793c870db3dab47968291ef77f9ad80ad7cf952761154e2e3a1899c5811  | INVALID! |
|   TPM   | [675daac0ff10dc82aa862329c53a6906492c88057a0aa5d228b687e33971e8d4] |          |
| PCR[06] |  3d458cfe55cc03ea1f443f1562beec8df51c75e14a9fcf9a7234a13f198e7969  |  MATCH!  |
| PCR[07] |  730777cfa2b4c2cf67a54ce7c80d7d15cebd0a443d1bc320e43fe338812ea67b  | INVALID! |
|   TPM   | [6dee7716b8b2bcd8d36ac7a3e37eeed3f08c30a4af1890928ba48836ad640d19] |          |
| PCR[08] |  0000000000000000000000000000000000000000000000000000000000000000  |  MATCH!  |
| PCR[09] |  0000000000000000000000000000000000000000000000000000000000000000  |  MATCH!  |
| PCR[10] |  0000000000000000000000000000000000000000000000000000000000000000  |  MATCH!  |
| PCR[11] |  0fe6e8f2110d5d53935c9e7d6f6bf722598b550595aabdc6e4fd2ecdf310f980  |  MATCH!  |
```

Verwenden von PCPTool zum Decodieren von gemessenen Start Protokollen

PCPTool ist Teil des TPM-Platt Form Krypto-Anbieter-Toolkits. Das Tool dekodiert eine gemessene Boot-Protokolldatei und wandelt sie in eine XML-Datei um.

Wenn Sie PCPTool herunterladen und installieren möchten, wechseln Sie zur Seite Toolkit, wählen Sie

herunterladenaus, und folgen Sie den Anweisungen.

Führen Sie zum Decodieren eines Protokolls den folgenden Befehl aus:

```
PCPTool.exe decodelog <LogFolderPath>\<LogFileName>.log > <DestinationFolderName>\<DecodedFileName>.xml
```

wobei die Variablen die folgenden Werte darstellen:

- <*LogFolderPath*> = der Pfad zu dem Ordner, der die zu decodierende Datei enthält.
- <*LogFileName*> = der Name der zu decodierenden Datei
- <*DestinationFolderName*> = der Name des Ordners für die decodierte Textdatei
- <*DecodedFileName*> = der Name der decodierten Textdatei

Der Inhalt der XML-Datei ähnelt wie folgt.

```
> .\PCPTool.exe decodelog C:\Windows\Logs\MeasuredBoot\0000000001-0000000000.log > TPM_log.xml
```

```
129     </EV_Event_Tag>
130     <EV_Event_Tag PCR="13" EventDigest="3db51a2ab6859f67510849226e545d7a193b66eb" Size="760">
131       <Trustboundary Size="752">
132         <SipaEvent Type="0x00040002" Size="46">
133           00ad31d5660ed001200000000b00f4247831deed0fc371f8e8a6b0746ae7b508c3c924e5b1c485c14631afa33879
134           <!-- ..1.f...........x1....q....tj...........F1..8y -->
135         </SipaEvent>
136         <LoadedModule_Aggregation Size="354">
137           <FilePath Size="86">\EFI\Microsoft\Boot\en-GB\bootmgfw.efi.MUI</FilePath>
138           <ImageSize Size="8">69632<!-- 0x0000000000011000 --></ImageSize>
139           <HashAlgorithmId Size="4">SHA-256</HashAlgorithmId>
140           <AuthenticodeHash Size="32">
141             a1cd73aee5d6f2c87e57573f0e50b8ab7f512dcf7c544df8ae231d492d5835b8
142             <!-- ..s......WW..P...Q...TM....I.X5. -->
143           </AuthenticodeHash>
144           <ImageValidated Size="1">TRUE</ImageValidated>
145           <AuthorityIssuer Size="76">Microsoft Windows Production PCA 2011</AuthorityIssuer>
146           <AuthorityPublisher Size="36">Microsoft Windows</AuthorityPublisher>
```

Verschlüsselte Festplatte

12.09.2019 • 6 minutes to read

Betrifft

- Windows 10
- Windows Server 2019
- Windows Server 2016

Verschlüsselte Festplatten verwenden die schnelle Verschlüsselung, die von der BitLocker-Laufwerkverschlüsselung bereitgestellt wird, um die Datensicherheit und-Verwaltung zu verbessern.

Durch eine Übertragung der Kryptografievorgänge auf die Hardware wird die Leistung von BitLocker mit verschlüsselten Festplatten verbessert, und CPU-Last und Energieverbrauch werden gesenkt. Da Daten auf verschlüsselten Festplatten schnell verschlüsselt werden, können Geräte die BitLocker-Bereitstellung mit minimalen Auswirkungen auf die Produktivität erweitern.

Verschlüsselte Festplatten sind eine neue Klasse von Festplatten, die sich auf Hardwareebene selbst verschlüsseln und die vollständige Festplatten Hardwareverschlüsselung ermöglichen. Sie können Windows auf verschlüsselte Festplatten ohne zusätzliche Änderungen installieren, beginnend mit Windows 8 und Windows Server 2012.

Verschlüsselte Festplatten bieten:

- **Bessere Leistung**: die im Laufwerkscontroller integrierte Verschlüsselungshardware ermöglicht es dem Laufwerk, mit der vollen Datenrate ohne Leistungseinbußen zu arbeiten.
- **Starke Sicherheit**auf der Basis von Hardware: die Verschlüsselung ist immer "aktiviert", und die Schlüssel für die Verschlüsselung belassen niemals die Festplatte. Die Benutzerauthentifizierung wird unabhängig vom Betriebssystem vom Laufwerk selbst durchgeführt, bevor es entsperrt wird.
- **Einfache Verwendung**: die Verschlüsselung ist für den Benutzer transparent und muss vom Benutzer nicht aktiviert werden. Verschlüsselte Festplatten lassen sich über den integrierten Kryptoschlüssel leicht löschen, daher ist keine Neuverschlüsselung von Festplattendaten erforderlich.
- **Geringere Betriebskosten**: Es ist keine neue Infrastruktur erforderlich, um Verschlüsselungsschlüssel zu verwalten, da BitLocker Ihre vorhandene Infrastruktur zum Speichern von Wiederherstellungsinformationen nutzt. Ihr Gerät arbeitet effizienter, da Prozessorzyklen nicht für den Verschlüsselungsprozess verwendet werden müssen.

Verschlüsselte Festplatten werden im Betriebssystem nativ unterstützt, und zwar über die folgenden Mechanismen:

- **Identifikation**: das Betriebssystem kann erkennen, dass es sich bei dem Laufwerk um einen verschlüsselten Festplatten-Gerätetyp handelt.
- **Aktivierung**: das Betriebssystem-Datenträger Verwaltungsdienstprogramm kann Volumes/Bands je nach Bedarf aktivieren, erstellen und zuordnen.
- **Konfiguration**: das Betriebssystem kann Volumes je nach Bedarf in Bereichen/Bändern erstellen und zuordnen.
- **API**: API-Unterstützung für Anwendungen, um verschlüsselte Festplatten unabhängig von der BitLocker-Laufwerkverschlüsselung (BDE) zu verwalten
- **BitLocker-Unterstützung**: die Integration in die BitLocker-Systemsteuerung bietet eine nahtlose BitLocker-Endbenutzererfahrung.

> **WARNING**
> Selbst verschlüsselte Festplatten und verschlüsselte Festplatten für Windows sind nicht derselbe Gerätetyp. Verschlüsselte Festplatten für Windows erfordern Compliance für bestimmte TCG-Protokolle sowie IEEE 1667-Compliance; Selbst verschlüsselte Festplatten verfügen nicht über diese Anforderungen. Es ist wichtig, zu bestätigen, dass der Gerätetyp eine verschlüsselte Festplatte für Windows ist, wenn die Bereitstellung geplant wird.

Wenn Sie ein Hersteller von Speichergeräten sind und weitere Informationen zum Implementieren von verschlüsselten Festplatten benötigen, lesen Sie den Leitfaden für verschlüsselte Festplattenlaufwerke.

Systemanforderungen

Um verschlüsselte Festplatten zu verwenden, gelten die folgenden Systemvoraussetzungen:

Für eine verschlüsselte Festplatte, die als **Datenlaufwerk**verwendet wird:

- Das Laufwerk muss einen nicht initialisierten Zustand aufweisen.
- Das Laufwerk muss sich im Status "Sicherheit inaktiv" befinden.

Für eine verschlüsselte Festplatte, die als **Startlaufwerk**verwendet wird:

- Das Laufwerk muss einen nicht initialisierten Zustand aufweisen.
- Das Laufwerk muss sich im Status "Sicherheit inaktiv" befinden.
- Auf dem Computer muss UEFI 2.3.1 basieren und die EFI_STORAGE_SECURITY_COMMAND_PROTOCOL definiert sein. (Mit diesem Protokoll können Programme, die in der EFI-Startdienste-Umgebung ausgeführt werden, Sicherheitsprotokoll Befehle an das Laufwerk senden).
- Auf dem Computer muss das Kompatibilitäts Support Modul (CSM) in UEFI deaktiviert sein.
- Der Computer muss immer nativ aus UEFI Booten.

> **WARNING**
> Alle verschlüsselten Festplatten müssen an nicht-RAID-Controller angeschlossen sein, damit Sie ordnungsgemäß funktionieren.

Technische Übersicht

Die schnelle Verschlüsselung in BitLocker richtet sich direkt an die Sicherheitsanforderungen von Unternehmen und bietet eine erheblich verbesserte Leistung. In früheren Versionen von Windows als Windows Server 2012 erforderte BitLocker einen zweistufigen Prozess zum Durchführen von Lese-und Schreibanforderungen. In Windows Server 2012, Windows 8 oder höher, werden verschlüsselte Festplatten die kryptografischen Vorgänge auf den Laufwerkcontroller umgeladen, um eine wesentlich höhere Effizienz zu erreichen. Wenn das Betriebssystem eine verschlüsselte Festplatte erkennt, wird der Sicherheitsmodus aktiviert. Mit dieser Aktivierung kann der Laufwerkcontroller für jedes Volume, das der Hostcomputer erstellt, einen Medien Schlüssel generieren. Dieser Medien Schlüssel, der niemals außerhalb des Datenträgers verfügbar gemacht wird, wird verwendet, um jedes Byte von Daten, die vom Datenträger gesendet oder empfangen werden, schnell zu verschlüsseln oder zu entschlüsseln.

Konfigurieren von verschlüsselten Festplatten als Start Laufwerke

Die Konfiguration verschlüsselte Festplatten als Start Laufwerke erfolgt mithilfe der gleichen Methoden wie Standardfestplatten Laufwerke. Zu diesen Methoden gehören:

- **Bereitstellen von Medien**: die Konfiguration von verschlüsselten Festplatten erfolgt automatisch über den

Installationsvorgang.

- **Bereitstellen aus dem Netzwerk**: Diese Bereitstellungsmethode umfasst das Booten einer Windows PE-Umgebung und die Verwendung von Imaging-Tools, um ein Windows-Abbild von einer Netzwerkfreigabe anzuwenden. Mit dieser Methode muss die optionale Komponente Enhanced Storage im Windows PE-Abbild enthalten sein. Sie können diese Komponente mit dem Server-Manager, Windows PowerShell oder dem DISM-Befehlszeilentool aktivieren. Wenn diese Komponente nicht vorhanden ist, funktioniert die Konfiguration verschlüsselte Festplatten nicht.
- **Bereitstellen vom Server**: Diese Bereitstellungsmethode umfasst den PXE-Start eines Clients, auf dem verschlüsselte Festplatten vorhanden sind. Die Konfiguration verschlüsselte Festplatten erfolgt in dieser Umgebung automatisch, wenn die erweiterte Speicherkomponente dem PXE-Startabbild hinzugefügt wird. Während der Bereitstellung steuert die Einstellung TCGSecurityActivationDisabled in Unattend. XML das Verschlüsselungs Verhalten von verschlüsselten Festplatten.
- **Datenträgerduplizierung**: Diese Bereitstellungsmethode umfasst die Verwendung einer zuvor konfigurierten Geräte-und Datenträger Duplizierungs Tools, um ein Windows-Abbild auf eine verschlüsselte Festplatte anzuwenden. Datenträger müssen mit mindestens Windows 8 oder Windows Server 2012 partitioniert sein, damit diese Konfiguration funktioniert. Bilder, die mithilfe von Datenträgerduplikaten erstellt wurden, funktionieren nicht.

Konfigurieren der hardwarebasierten Verschlüsselung mit Gruppenrichtlinien

Es gibt drei Verwandte Gruppenrichtlinieneinstellungen, mit denen Sie verwalten können, wie BitLocker hardwarebasierte envryption verwendet und welche Verschlüsselungsalgorithmen verwendet werden. Wenn diese Einstellungen auf Systemen, die mit verschlüsselten Laufwerken ausgestattet sind, nicht konfiguriert oder deaktiviert sind, verwendet BitLocker softwarebasierte Verschlüsselung:

- Konfigurieren der Verwendung von hardwarebasierter Verschlüsselung für fest Netzlaufwerke
- Konfigurieren der Verwendung von hardwarebasierter Verschlüsselung für Wechseldaten Laufwerke
- Konfigurieren der Verwendung von hardwarebasierter Verschlüsselung für Betriebssystemlaufwerke

Verschlüsselte Festplatten Architektur

Verschlüsselte Festplatten verwenden zwei Verschlüsselungsschlüssel auf dem Gerät, um das Sperren und Entsperren von Daten auf dem Laufwerk zu steuern. Hierbei handelt es sich um den Datenverschlüsselungsschlüssel (DEK) und den Authentifizierungsschlüssel (AK).

Der Datenverschlüsselungsschlüssel ist der Schlüssel, der zum Verschlüsseln aller Daten auf dem Laufwerk verwendet wird. Das Laufwerk generiert das DEK und verlässt das Gerät nie. Sie wird in einem verschlüsselten Format an einer beliebigen Stelle auf dem Laufwerk gespeichert. Wenn das DEK geändert oder gelöscht wird, sind Daten, die mit dem DEK verschlüsselt sind, unwiederbringlich.

Der Authentifizierungsschlüssel ist der Schlüssel, mit dem Daten auf dem Laufwerk freigegeben werden. Ein Hash des Schlüssels wird auf Drive gespeichert und erfordert eine Bestätigung zum Entschlüsseln des Dek.

Wenn sich ein Computer mit einer verschlüsselten Festplatte in einem ausgeschalteten Zustand befindet, wird das Laufwerk automatisch gesperrt. Wenn ein Computer eingeschaltet ist, verbleibt das Gerät in einem gesperrten Zustand und wird erst entriegelt, nachdem der Authentifizierungsschlüssel den Datenverschlüsselungsschlüssel entschlüsselt hat. Nachdem der Authentifizierungsschlüssel den Datenverschlüsselungsschlüssel entschlüsselt hat, können Lese-und Schreibvorgänge auf dem Gerät erfolgen.

Beim Schreiben von Daten auf das Laufwerk übergibt Sie ein Verschlüsselungsmodul, bevor der Schreibvorgang abgeschlossen ist. Ebenso erfordert das Lesen von Daten aus dem Laufwerk, dass das Verschlüsselungsmodul die Daten entschlüsselt, bevor diese Daten an den Benutzer zurückgegeben werden. Für den Fall, dass der DEK geändert oder gelöscht werden muss, müssen die Daten auf dem Laufwerk nicht erneut verschlüsselt werden. Es

muss ein neuer Authentifizierungsschlüssel erstellt und der DEK erneut verschlüsselt werden. Nach Abschluss des Vorgangs kann die DEK nun mit dem neuen AK entriegelt werden, und Lese-und Schreibvorgänge für das Volume können fortgesetzt werden.

Erneutes Konfigurieren von verschlüsselten Festplatten

Viele verschlüsselte Festplattenlaufwerke sind für die Verwendung vorkonfiguriert. Wenn die Neukonfiguration des Laufwerks erforderlich ist, gehen Sie folgendermaßen vor, nachdem Sie alle verfügbaren Volumes entfernt und das Laufwerk auf einen nicht initialisierten Zustand zurückgesetzt haben:

1. Öffnen der Datenträgerverwaltung (diskmgmt. msc)
2. Initialisieren des Datenträgers und auswählen des geeigneten Partitions Formats (MBR oder GPT)
3. Erstellen Sie ein oder mehrere Volumes auf dem Datenträger.
4. Verwenden Sie den BitLocker-Setup-Assistenten, um BitLocker auf dem Volume zu aktivieren.

Kernel-DMA-Schutz für Thunderbolt™ 3

04.12.2019 • 6 minutes to read

Gilt für:

- Windows 10

In Windows 10, Version 1803, hat Microsoft eine neue Funktion mit dem Namen Kernel DMA Protection eingeführt, um PCs vor Drive-through-DMA-Attacken (DMA) mit PCI-HotPlug-Geräten zu schützen, die mit Thunderbolt-™ 3-Ports verbunden sind. Drive-by-DMA-Angriffe können zur Offenlegung vertraulicher Informationen führen, die sich auf einem PC befinden, oder sogar zur Injektion von Schadsoftware, die Angreifern die Umgehung des sperrbildschirms oder die Remotesteuerung von PCs ermöglicht.

Dieses Feature schützt nicht vor DMA-Attacken über 1394/Firewire, PCMCIA, CardBus, ExpressCard usw.

Für den Thunderbolt-DMA-Schutz bei älteren Windows-Versionen und anderen Plattformen, die keinen Kernel-DMA-Schutz unterstützen, lesen Sie bitte die Intel Thunderbolt™ 3-Sicherheitsdokumentation.

Hintergrund

PCI-Geräte sind DMA-fähig, sodass Sie in der Lage sind, den Systemspeicher zu lesen und zu schreiben, ohne den Systemprozessor in diese Vorgänge einbinden zu müssen. Die DMA-Funktion macht PCI-Geräte zu den leistungsstärksten Geräten, die heute verfügbar sind. Diese Geräte sind historisch nur innerhalb des PC-Chassis vorhanden, entweder als Karte verbunden oder auf der Hauptplatine verlötet. Der Zugriff auf diese Geräte erforderte, dass der Benutzer die Stromversorgung des Systems ausschalten und das Chassis auseinander bauen musste. Heute ist dies bei Thunderbolt™ nicht mehr der Fall.

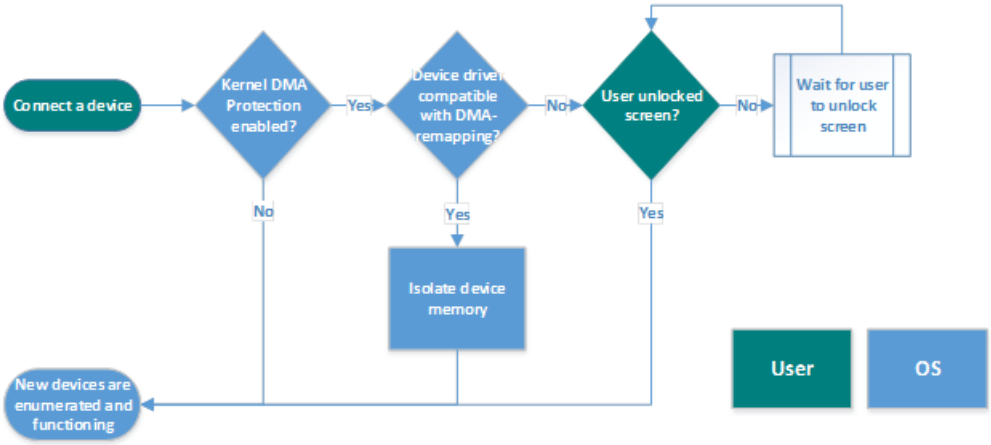
Die Thunderbolt-™ Technologie bietet modernen PCs eine Erweiterbarkeit, die zuvor für PCs nicht zur Verfügung stand. Es ermöglicht Benutzern, neue Klassen von externen Peripheriegeräten, wie Grafikkarten oder anderen PCI-Geräten, an Ihre PCs mit einem Hot-Plug-Erlebnis zu koppeln, das mit USB identisch ist. Wenn PCI-HotPlug-Anschlüsse extern und leicht zugänglich sind, sind PCs anfällig für DMA-Attacken.

Drive-by-DMA-Angriffe sind Angriffe, die auftreten, während der Besitzer des Systems nicht anwesend ist und normalerweise weniger als 10 Minuten benötigt, mit einfachen bis mittelschweren angreifenden Tools (erschwingliche, standardmäßige Hardware und Software), die keine Demontage des PCs erfordern. Ein einfaches Beispiel wäre ein PC-Besitzer, der den PC verlässt, um eine kurze Kaffeepause zu machen, und innerhalb des Breaks und des Angreifers ein USB-ähnliches Gerät anschließen und mit allen Geheimnissen auf dem Computer verschwindet oder eine Malware injiziert, die es Ihnen ermöglicht, die volle Kontrolle über den PC REM zu haben. otely.

So schützt Windows vor DMA Drive-by-Angriffen

Windows nutzt die System-Input/Output-Speicherverwaltungseinheit (IOMMU), um externe Peripheriegeräte vom starten und Durchführen von DMA zu blockieren, es sei denn, die Treiber für diese Peripheriegeräte unterstützen die speicherisolierung (wie DMA-Neuzuordnung). Peripheriegeräte mit kompatiblen Treibern werden automatisch aufgelistet, gestartet und können DMA für die zugeordneten Speicherbereiche ausführen. Standardmäßig werden Peripheriegeräte mit nicht kompatiblen Treibern blockiert, bevor ein autorisierter Benutzer sich am System anmeldet oder den Bildschirm entriegelt.

Benutzerfreundlichkeit



Ein Peripheriegerät, das mit der DMA-Neuzuordnung nicht kompatibel ist, wird vom starten blockiert, wenn das Peripheriegerät angeschlossen war, bevor sich ein autorisierter Benutzer anmeldet, oder während der Bildschirm gesperrt ist. Nachdem das System entriegelt wurde, wird der periphere Treiber vom Betriebssystem gestartet, und das Peripheriegerät funktioniert weiterhin normal, bis das System neu gestartet wird oder das Peripheriegerät nicht angeschlossen ist. Das Peripheriegerät funktioniert weiterhin normal, wenn der Benutzer den Bildschirm sperrt oder sich vom System abmeldet.

System Kompatibilität

Der Kernel-DMA-Schutz erfordert neue UEFI-Firmware-Unterstützung. Diese Unterstützung wird nur auf neu eingeführten, auf Intel basierenden Systemen erwartet, die mit Windows 10, Version 1803 (nicht alle Systeme) ausgeliefert werden. Die Virtualisierungs-basierte Sicherheit (VBS) ist nicht erforderlich.

Wenn Sie feststellen möchten, ob ein System den Kernel DMA-Schutz unterstützt, überprüfen Sie die Systeminformationen-Desktop-App (Msinfo32). Systeme, die vor Windows 10 Version 1803 freigegeben werden, unterstützen keinen Kernel-DMA-Schutz, können aber andere DMA-Angriffs milderungen nutzen, wie in BitLocker-gegen Maßnahmenbeschrieben.

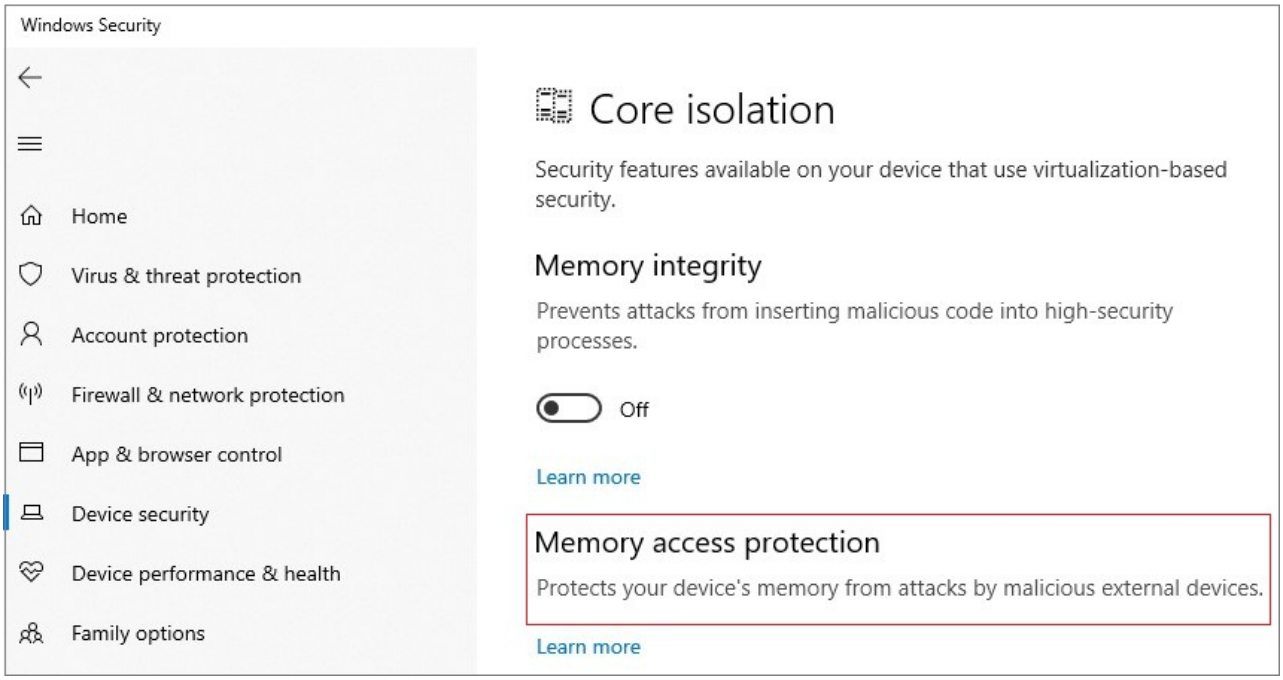
> **NOTE**
>
> Der Kernel-DMA-Schutz ist mit anderen BitLocker-DMA-Angriffen Gegenmaßnahmen nicht kompatibel. Es wird empfohlen, die BitLocker-DMA-Angriffe Gegenmaßnahmen zu deaktivieren, wenn das System den Kernel-DMA-Schutz unterstützt. Der Kernel-DMA-Schutz bietet eine höhere Sicherheitsleiste für das System als die BitLocker-DMA-Angriffe Gegenmaßnahmen und unter Beibehaltung der Benutzerfreundlichkeit externer Peripheriegeräte.

Überprüfen, ob der Kernel-DMA-Schutz aktiviert ist

Auf Systemen mit Windows 10, Version 1803, die den Kernel-DMA-Schutz unterstützen, ist dieses Sicherheitsfeature automatisch vom Betriebssystem aktiviert, ohne dass eine Benutzer-oder IT-Administratorkonfiguration erforderlich ist.

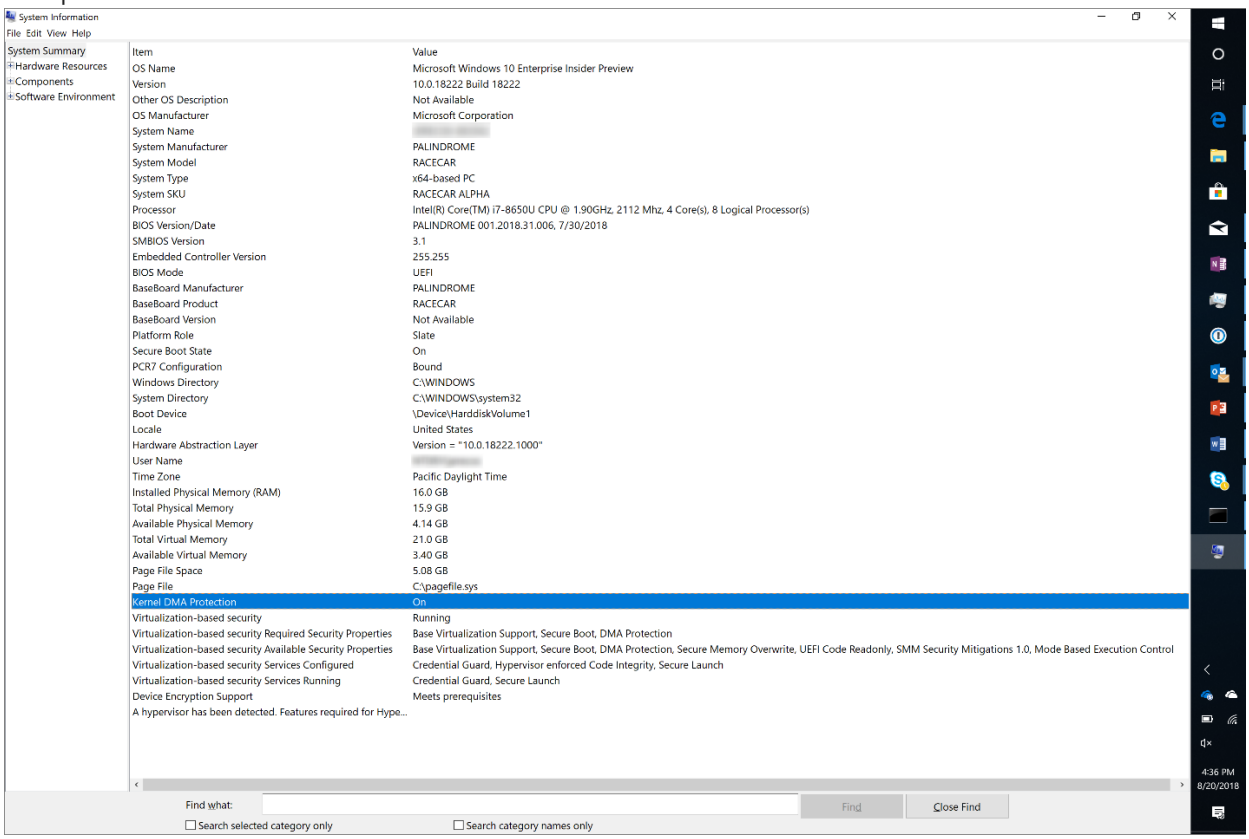
Verwenden des Sicherheitscenters

Ab Windows 10, Version 1809, können Sie mithilfe des Sicherheitscenters überprüfen, ob der Kernel-DMA-Schutz aktiviert ist. Klicken Sie auf **Start** > **Einstellungen** > **Aktualisieren #a0 Sicherheit** > **Windows Security** > **Open Windows** > Security**Device Security** > **Core Isolierung Details** > **Speicherzugriffs Schutz**.



Verwenden von System Informationen

1. Starten Sie msinfo32. exe an einer Eingabeaufforderung oder in der Windows-Suchleiste.
2. Überprüfen Sie den Wert des **Kernel-DMA-Schutzes**.



3. Wenn der aktuelle Zustand des **Kernel-DMA-Schutzes** deaktiviert ist und die **Virtualisierungstechnologie in der Firmware** nicht lautet:
   - Neustart in BIOS-Einstellungen
   - Aktivieren Sie die Intel Virtualization Technology.
   - Aktivieren Sie die Intel Virtualization Technology für I/O (VT-d). In Windows 10, Version 1803, wird nur Intel VT-d unterstützt. Andere Plattformen können DMA-Angriffs Begrenzungen verwenden, die unter BitLocker-gegen Maßnahmenbeschrieben werden.
   - Starten Sie das System in Windows 10 neu.
4. Wenn der Status des **Kernel-DMA-Schutzes** deaktiviert bleibt, wird dieses Feature vom System nicht

unterstützt.

Bei Systemen, die den Kernel-DMA-Schutz nicht unterstützen, lesen Sie die BitLocker-gegen Maßnahmen oder Thunderbolt™ 3 und Sicherheit auf dem Betriebssystem Microsoft Windows® 10 für andere Mittel des DMA-Schutzes.

Häufig gestellte Fragen

Unterstützen in-Market-Systeme den Kernel-DMA-Schutz für Thunderbolt™ 3?

In-Market-Systeme, die mit Windows 10, Version 1709 oder früher veröffentlicht wurden, unterstützen den Kernel-DMA-Schutz für Thunderbolt™ 3 nach dem Upgrade auf Windows 10, Version 1803, nicht, da für dieses Feature die Firmware-Änderungen von BIOS/Plattform und Garantien erforderlich sind, die nicht auf zuvor freigegebene Geräte portiert werden können. Informationen zu diesen Systemen finden Sie unter BitLocker-gegen Maßnahmen oder Thunderbolt™ 3 und Sicherheit auf dem Betriebssystem Microsoft Windows® 10 für andere DMA-Schutzmethoden.

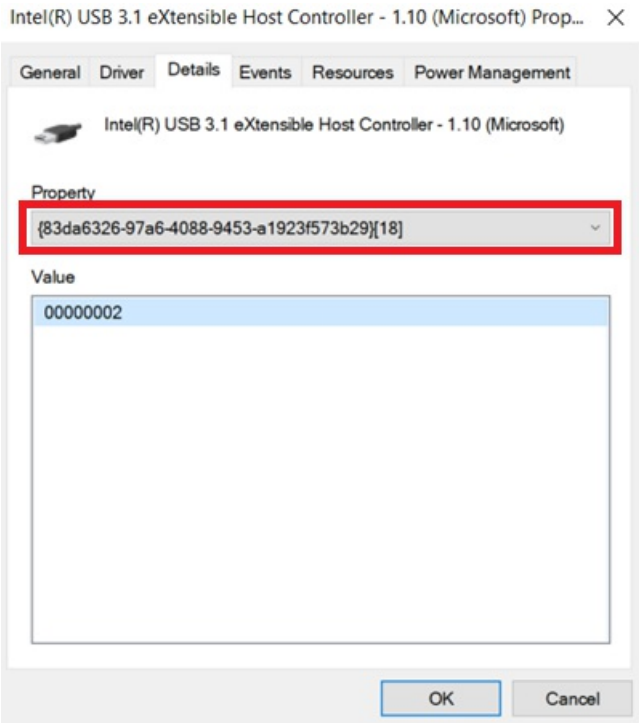
Verhindert der Kernel-DMA-Schutz Drive-by-DMA-Angriffe beim Booten?

Nein, der Kernel-DMA-Schutz schützt nur gegen Drive-by-DMA-Angriffe, nachdem das Betriebssystem geladen wurde. Das System-Firmware/-BIOS ist für den Schutz vor Angriffen über die Thunderbolt-™ 3-Ports während des Starts verantwortlich.

Wie kann ich überprüfen, ob ein bestimmter Treiber die DMA-Neuzuordnung unterstützt?

Die DMA-Neuzuordnung wird für bestimmte Gerätetreiber unterstützt und wird von allen Geräten und Treibern auf einer Plattform nicht universell unterstützt. Um zu überprüfen, ob ein bestimmter Treiber für die DMA-Neuzuordnung vorgesehen ist, überprüfen Sie die Werte, die der Eigenschaft DMA-neuzuordnungs Richtlinie entsprechen, auf der Registerkarte Details eines Geräts im Geräte-Manager *. Der Wert 0 oder 1 bedeutet, dass der Gerätetreiber keine DMA-Neuzuordnung unterstützt. Der Wert 2 bedeutet, dass der Gerätetreiber die DMA-Neuzuordnung unterstützt. Wenn die Eigenschaft nicht verfügbar ist, wird die Richtlinie nicht vom Gerätetreiber gesetzt (d. h., der Gerätetreiber unterstützt keine DMA-Neuzuordnung). Bitte überprüfen Sie die Treiberinstanz auf das Gerät, das Sie testen. Einige Treiber können je nach Standort des Geräts (intern vs. extern) unterschiedliche Werte aufweisen.

- Bei Windows 10-Versionen 1803 und 1809 verwendet das Eigenschaftenfeld im Geräte-Manager eine GUID, wie in der folgenden Abbildung hervorgehoben.



Was muss ich tun, wenn die Treiber für meine Thunderbolt-™ 3-Peripheriegeräte keine DMA-Neuzuordnung unterstützen?

Wenn die Peripheriegeräte über Klassentreiber verfügen, die von Windows 10 bereitgestellt werden, verwenden Sie diese Treiber auf Ihren Systemen. Wenn für Ihre Peripheriegeräte keine Kurs Treiber von Windows bereitgestellt werden, wenden Sie sich bitte an den Hersteller des peripheren Herstellers/Treibers, um den Treiber zu aktualisieren, um diese Funktion zu unterstützen. Details zu den Treiber Kompatibilitätsanforderungen finden Sie im Microsoft Partner Center.

Unterstützen Microsoft-Treiber die DMA-Neuzuordnung?

In Windows 10 1803 und darüber hinaus unterstützen die Microsoft-Posteingangs Treiber für USB XHCI (3. x)-Controller, Speicher-AHCI/SATA-Controller und Speicher-NVMe-Controller die DMA-Neuzuordnung.

Müssen Treiber für nicht-PCI-Geräte mit DMA-Remapping kompatibel sein?

Nein. Geräte für nicht-PCI-Peripheriegeräte wie USB-Geräte führen keinen DMA durch, daher ist es nicht erforderlich, dass der Treiber mit DMA-Remapping kompatibel ist.

Wie kann ein Unternehmen die Richtlinie für externe Geräte Aufzählungen aktivieren?

Die Richtlinie für externe Geräte Enumeration steuert, ob externe Peripheriegeräte aufgelistet werden, die mit der DMA-Neuzuordnung nicht kompatibel sind. Peripheriegeräte, die mit der DMA-Neuzuordnung kompatibel sind, werden immer aufgelistet. Peripheriegeräte, die nicht blockiert, zugelassen oder zugelassen werden können, wenn sich der Benutzer anmeldet (Standard).

Die Richtlinie kann mit folgenden Funktionen aktiviert werden:

- Gruppenrichtlinien: Richtlinien für administrative Templates\System\Kernel-DMA-Protection\Enumeration für externe Geräte, die mit dem Kernel-DMA-Schutz nicht kompatibel sind
- Mobile Device Management (MDM): DmaGuard-Richtlinien

Verwandte Themen

- BitLocker-Gegenmaßnahmen
- DmaGuard MDM-Richtlinien

Schutz von Unternehmensdaten mit Windows Information Protection (WIP)

06.03.2020 • 13 minutes to read

Gilt für:

- Windows10, Version 1607 und höher
- Windows10 Mobile, Version 1607 und höher

> Unter Vergleichen von Windows10-Editionen erfahren Sie, welche Features und Funktionen von den einzelnen Windows-Editionen unterstützt werden.

Mit der Zunahme privater Mitarbeitergeräte in Unternehmen steigt auch das Risiko versehentlicher Datenverluste durch Apps und Dienste, die nicht der Kontrolle des Unternehmens unterliegen, z.B. E-Mail, soziale Medien und die öffentliche Cloud. Ein solcher Datenverlust liegt vor, wenn ein Mitarbeiter beispielsweise die neuesten technischen Zeichnungen an sein persönliches E-Mail-Konto sendet, Produktinformationen kopiert und in einen Tweet einfügt oder einen aktuellen Vertriebsbericht in seinem öffentlichen Cloud-Speicher speichert.

Windows Information Protection (WIP), früher bekannt als Unternehmensdatenschutz (Enterprise Data Protection, EDP), trägt zum Schutz vor diesen potenziellen Datenlecks bei, ohne die Mitarbeiter zu beeinträchtigen. WIP schützt zudem Unternehmens-Apps und -daten auf unternehmenseigenen Geräten und auf persönlichen Geräten, die Mitarbeiter mit zur Arbeit bringen, vor versehentlichem Datenverlust. Dazu müssen weder die Unternehmensumgebung noch andere Apps geändert werden. Zuletzt lässt sich eine weitere Technologie zum Schutz von Daten – Azure Rights Management – auch mit WIP kombinieren, um den Schutz auf Daten auszudehnen, die das Gerät verlassen, z.B., wenn E-Mail-Anhänge von einer unternehmensfähigen Version eines Mailclients für die Rechteverwaltung gesendet werden.

> **IMPORTANT**
>
> Während WIP unbeabsichtigte Datenverluste von ehrlichen Mitarbeitern verhindern kann, ist es nicht beabsichtigt, böswillige Insider daran zu hindern, Unternehmensdaten zu entfernen. Weitere Informationen zu den Vorteilen, die WIP bietet, finden Sie unter Warum verwenden Sie WIP? weiter unten in diesem Thema.

Video: Schützen von Unternehmensdaten vor versehentlichem kopieren an die falsche Stelle

Voraussetzungen

Sie benötigen die folgende Software, um WIP in Ihrem Unternehmen auszuführen:

BETRIEBSSYSTEM	VERWALTUNGSLÖSUNG

BETRIEBSSYSTEM	VERWALTUNGSLÖSUNG
Windows10, Version 1607 oder höher	Microsoft Intune – ODER – Microsoft Endpoint Configuration Manager – ODER – Ihre aktuelle unternehmensweite Lösung für die mobile Geräteverwaltung (Mobile Device Management, MDM) eines Drittanbieters Informationen zu MDM-Lösungen von Drittanbietern finden Sie in der Begleitdokumentation Ihres Produkts. Wenn Ihre MDM-Lösung eines Drittanbieters keine UI-Unterstützung für die Richtlinien bietet, informieren Sie sich in der EnterpriseDataProtection CSP-Dokumentation.

Was wird unter einer unternehmensweiten Datenkontrolle verstanden?

Eine effektive Zusammenarbeit bedeutet, dass Sie Daten mit anderen Personen in Ihrem Unternehmen teilen müssen. Die Bandbreite hier ist groß – von einer Freigabe, bei der jeder Zugriff auf alles hat, ohne dass Sicherheitsfunktionen vorhanden sind, bis zu einer Freigabe, bei der niemand etwas teilen kann und alles hochgradig geschützt ist. Die meisten Unternehmen liegen irgendwo zwischen den beiden Extremen. Der Erfolg wird hier durch den gelungenen Ausgleich zwischen der Bereitstellung des notwendigen Zugriffs und dem Risiko einer nicht korrekten Offenlegung von Daten definiert.

Als Administrator können Sie die Frage, wer Zugriff auf die Daten erhält, durch eine Zugriffssteuerung beantworten, beispielsweise mithilfe von Anmeldeinformationen der Mitarbeiter. Eine Zugriffsberechtigung garantiert jedoch nicht, dass die Daten an den durch das Unternehmen geschützten Speicherorten bleiben. Das bedeutet, dass eine Zugriffssteuerung zwar ein guter Anfang ist, jedoch nicht ausreicht.

Am Ende haben alle diese Sicherheitsmaßnahmen eines gemeinsam: Mitarbeiter werden nur ein bestimmtes Maß an Aufwand tolerieren, bevor sie nach Möglichkeiten suchen, die Sicherheitseinschränkungen zu umgehen. Wenn Sie Mitarbeitern beispielsweise nicht gestatten, Daten über ein geschütztes System zu teilen, werden sie eine externe App nutzen, die sehr wahrscheinlich nicht über ausreichende Sicherheitsfunktionen verfügt.

Verwenden von Systemen zur Verhinderung von Datenverlusten

Um diese Sicherheits Knappheit zu beheben, entwickelten Unternehmen Datenverlust Verhinderung (auch bekannt als DLP-Systeme). Systeme zur Verhinderung von Datenverlusten erfordern:

- **Einen Satz von Regeln, wie das System die Daten identifizieren und kategorisieren kann, die geschützt werden müssen.** Beispielsweise kann ein Regelsatz eine Regel enthalten, die Kreditkartennummern identifiziert, und eine weitere Regel, die Sozialversicherungsnummern identifiziert.
- **Eine Möglichkeit, wie Unternehmensdaten überprüft werden können, besteht darin, festzustellen, ob sie einer der von Ihnen definierten Regeln entspricht.** Zurzeit stellen Microsoft Exchange Server und Exchange Online diesen Dienst für E-Mails während der Übertragung bereit. Microsoft SharePoint und SharePoint Online stellen diesen Dienst für Inhalte bereit, die in Dokumentbibliotheken gespeichert sind.
- **Eine Möglichkeit, anzugeben, was passieren soll, wenn Daten einer Regel entsprechen. Dies schließt die Angabe ein, ob Mitarbeiter die Durchsetzung umgehen dürfen.** Beispielsweise ermöglicht Ihnen das von Microsoft entwickelte System zur Verhinderung von Datenverlusten in Microsoft SharePoint und SharePoint Online, Ihre Mitglieder zu warnen, dass die geteilten Daten sensible Daten enthalten. Die Mitglieder können die Daten jedoch teilen (mit einem optionalen Eintrag in ein Überwachungsprotokoll).

Leider haben Systeme zur Verhinderung von Datenverlusten ihre eigenen Probleme. Je detaillierter beispielsweise ein Regelsatz ist, desto mehr falsch-positive Warnungen werden erstellt. Das führt dazu, dass die Mitarbeiter glauben, dass die Regeln ihre Arbeit verlangsamen und umgangen werden müssen, um produktiv zu bleiben. Das kann wiederum dazu führen, dass Daten fälschlicherweise gesperrt oder freigegeben werden. Ein anderes großes Problem besteht darin, dass Systeme zur Verhinderung von Datenverlusten umfassend implementiert werden müssen, um effektiv zu sein. Wenn Ihr Unternehmen beispielsweise ein System zur Verhinderung von Datenverlusten für E-Mails verwendet, jedoch nicht für Dateiverzeichnisse oder Dokumentspeicher, werden Sie möglicherweise feststellen, dass Ihre Daten über die ungeschützten Kanäle offengelegt werden. Das größte Problem bei der Verhinderung von Datenverlusten besteht aber vielleicht darin, dass es eine Erschütterungs Erfahrung bietet, die den natürlichen Workflow der Mitarbeiter unterbricht, indem einige Vorgänge gestoppt werden (beispielsweise das Senden einer Nachricht mit einer Anlage, die vom System als vertraulich etikettiert wird) beim zulassen anderer, oft nach subtilen Regeln, die der Mitarbeiter nicht sieht und nicht verstehen kann.

Verwenden von Information Rights Management-Systemen

Um die möglichen Probleme im Zusammenhang mit Systemen zur Verhinderung von Datenverlusten zu beheben, wurden Information Rights Systeme entwickelt, auch als IRM-Systeme bekannt. Information Rights Management-Systeme integrierten den Schutz direkt in Dokumente. Wenn Mitarbeiter Dokumente erstellen, können sie festlegen, welche Art von Schutz angewendet werden soll. Beispielsweise kann ein Mitarbeiter festlegen, dass ein Dokument nicht weitergeleitet, gedruckt oder mit Personen außerhalb des Unternehmens geteilt werden darf usw.

Nachdem die Art des Schutzes festgelegt wurde, wird das Dokument von der erstellenden App verschlüsselt, sodass nur autorisierte Personen sie öffnen können, und das nur in kompatiblen Apps. Nachdem ein Mitarbeiter das Dokument geöffnet hat, ist die App für die Durchsetzung der festgelegten Art von Schutz verantwortlich. Da der Schutz das Dokument stets begleitet, können nicht autorisierte Personen das Dokument weder lesen noch ändern, wenn es von einer autorisierten Person an eine nicht autorisierte Person gesendet wird. Damit dies jedoch effektiv funktioniert, erfordern Information Rights Management-Systeme die Bereitstellung eines Servers und einer Clientumgebung. Und da nur kompatible Clients mit geschützten Dokumenten arbeiten können, wird die Arbeit der Mitarbeiter möglicherweise unerwartet unterbrochen, wenn sie versuchen, eine nicht kompatible App zu verwenden.

Und was passiert, wenn ein Mitarbeiter das Unternehmen verlässt oder die Registrierung eines Geräts aufhebt?

Und schließlich besteht die Gefahr, dass Daten aus Ihrem Unternehmen offengelegt werden, wenn ein Mitarbeiter das Unternehmen verlässt oder die Registrierung eines Geräts aufhebt. Zuvor hätten Sie einfach sämtliche Unternehmensdaten und alle persönlichen Daten auf dem Gerät gelöscht.

Vorteile von WIP

WIP bietet Folgendes:

- Eindeutige Trennung zwischen persönlichen Daten und Unternehmensdaten, ohne dass Mitarbeiter zwischen Umgebungen oder Apps wechseln müssen
- Zusätzlicher Schutz von Daten für vorhandene Branchen-Apps, ohne dass die Apps aktualisiert werden müssen
- Zurücksetzen von Unternehmensdaten auf für MDM registrierten Geräten, ohne dass persönliche Daten davon betroffen sind
- Verwenden von Überwachungsberichten zum Nachverfolgen von Problemen und Einleiten von Gegenmaßnahmen
- Integration in Ihr vorhandenes Verwaltungssystem (Microsoft InTune, Microsoft Endpoint Configuration Manager oder Ihr aktuelles Mobile Device Management (MDM)-System) zum Konfigurieren, bereitstellen und Verwalten von WIP für Ihr Unternehmen.

Gründe für die Verwendung von WIP

WIP ist der Mobile Application Management (MAM)-Mechanismus unter Windows 10. WIP bietet Ihnen eine neue Möglichkeit zum Verwalten der Datenrichtlinien Erzwingung für apps und Dokumente auf Windows 10-Desktopbetriebssystemen sowie die Möglichkeit, den Zugriff auf Unternehmensdaten von Unternehmens-und Personal Geräten (nach der Registrierung in einem Unternehmen) zu entfernen. Verwaltungslösung wie InTune).

- **Sehen Sie die Durchsetzung von Datenrichtlinien mit anderen Augen.** Als Administrator eines Unternehmens müssen Sie für die Einhaltung Ihrer Datenrichtlinien und Datenzugriffsbeschränkungen sorgen. WIP schützt Unternehmen sowohl auf unternehmenseigenen als auch auf Mitarbeitern befindlichen Geräten, auch wenn der Mitarbeiter das Gerät nicht verwendet. Wenn Mitarbeiter Inhalte auf einem unternehmensgeschützten Gerät erstellen, können Sie sie als Arbeitsdokument speichern. Falls ja, werden die Dokumentinhalte zu lokal verwalteten Unternehmensdaten.
- **Verwalten Sie Ihre Unternehmensdokumente, Apps und Verschlüsselungsmodi.**
  - **Kopieren oder Herunterladen von Unternehmensdaten.** Wenn ein Mitarbeiter oder eine App Inhalte von einem Ort wie SharePoint, einer Netzwerkfreigabe oder einem Webspeicherort des Unternehmens auf ein WIP-geschütztes Gerät herunterlädt, werden die Daten auf dem Gerät durch WIP verschlüsselt.
  - **Verwenden geschützter apps.** Verwaltete Apps (apps, die Sie in der Liste der **geschützten apps** in ihrer WIP-Richtlinie enthalten haben) können auf Ihre Unternehmensdaten zugreifen und unterschiedlich interagieren, wenn Sie mit nicht zugelassenen, nicht-Enterprise-Aware-oder Personal-only-Apps verwendet werden. Wenn die WIP-Verwaltung z. B. auf **Blockieren**festgelegt ist, können Ihre Mitarbeiter Daten aus einer geschützten App kopieren und in eine andere geschützte App einfügen, nicht aber in eine persönliche App. Angenommen, ein Mitarbeiter der Personalverwaltung möchte eine Stellenbeschreibung aus einer geschützten App auf die interne Website mit Stellenausschreibungen kopieren, also an einen geschützten Speicherort des Unternehmens. Der Mitarbeiter macht aber einen Fehler und versucht, die Daten stattdessen in eine persönliche App einzufügen. Das Einfügen verursacht einen Fehler, und es wird eine Benachrichtigung mit dem Hinweis angezeigt, dass die App die Daten aufgrund einer Richtlinieneinschränkung nicht einfügen kann. Der Mitarbeiter fügt die Daten dann auf der Website mit den Stellenanzeigen ein, was problemlos funktioniert.
  - **Verwaltete Apps und Einschränkungen.** Mit WIP können Sie steuern, welche Apps auf Unternehmensdaten zugreifen und diese verwenden dürfen. Nachdem Sie Ihrer Liste geschützter Apps eine App hinzugefügt haben, wird diese als vertrauenswürdig für Unternehmensdaten eingestuft. Für alle Apps, die nicht in dieser Liste enthalten sind, wird der Zugriff auf Unternehmensdaten abhängig vom WIP-Verwaltungsmodus blockiert.

    Sie müssen keine Branchen-apps ändern, die niemals persönliche Daten berühren, um Sie als geschützte apps aufzulisten. Fügen Sie Sie einfach in die Liste der geschützten apps ein.
  - **Festlegen der Ebene für den Datenzugriff.** Mit WIP können Sie die Datenfreigabeaktionen Ihrer Mitarbeiter blockieren und überwachen oder Außerkraftsetzungen zulassen. Das Ausblenden von Außerkraftsetzungen hält die Aktion sofort an. Wird eine Außerkraftsetzung zugelassen, werden Mitarbeiter zwar gewarnt, dass ein Risiko besteht, können die Daten jedoch weiterhin teilen. Die Aktion wird aufgezeichnet und überwacht. Silent protokolliert einfach die Aktion, ohne etwas zu beenden, das der Mitarbeiter während der Verwendung dieser Einstellung überschrieben haben kann. Sammeln von Informationen, die Ihnen helfen können, Muster einer unangemessenen Freigabe anzuzeigen, damit Sie erzieherische Maßnahmen ergreifen oder apps finden können, die Ihrer Liste der geschützten apps hinzugefügt werden sollen. Weitere Informationen zum Erfassen Ihrer Überwachungsprotokolldateien finden Sie unter Erfassen von Windows Information Protection-Überwachungsprotokolldateien (WIP).

- **Verschlüsselung ruhender Daten.** WIP trägt zum Schutz von Unternehmensdaten in lokalen Dateien und auf Wechselmedien bei.

  Anwendungen wie Microsoft Word wirken mit WIP zusammen, um den Schutz Ihrer Daten auf lokale Dateien und Wechselmedien auszuweiten. Diese Apps werden als unternehmensfähig bezeichnet. Beispiel: Wenn ein Mitarbeiter WIP-verschlüsselte Inhalte aus Word öffnet, den Inhalt bearbeitet und dann versucht, die bearbeitete Version unter einem anderen Namen zu speichern, wendet Word automatisch WIP auf das neue Dokument an.

- **Verhindern der versehentlichen Offenlegung von Daten an öffentlichen Orten.** WIP schützt Ihre Unternehmensdaten davor, dass sie an öffentlichen Orten, z. B. im Public Cloud-Speicher, versehentlich geteilt werden. Falls Dropbox™ beispielsweise nicht in der Liste der geschützten Apps enthalten ist, können Mitarbeiter verschlüsselte Dateien nicht mit ihrem persönlichen Cloudspeicher synchronisieren. Wenn der Mitarbeiter den Inhalt stattdessen in einer App aus der Liste der geschützten Apps, wie Microsoft OneDrive for Business, speichert, können die verschlüsselten Dateien problemlos mit der Unternehmenscloud synchronisiert werden, während die Verschlüsselung lokal erhalten bleibt.

- **Verhindern der versehentlichen Offenlegung von Daten auf Wechselmedien.** WIP verhindert den Verlust von Unternehmensdaten, wenn Sie auf Wechselmedium kopiert oder übertragen werden. Angenommen, ein Mitarbeiter kopiert Unternehmensdaten auf ein USB (Universal Serial Bus)-Laufwerk, auf dem auch personenbezogene Daten enthalten sind. In diesem Fall bleiben die Unternehmensdaten verschlüsselt, die personenbezogenen Daten aber nicht.

- **Entfernen des Zugriffs auf Unternehmensdaten von unternehmensgeschützten Geräten.** Mithilfe von WIP können Administratoren Unternehmensdaten auf einzelnen oder mehreren, in MDM registrierten Geräten entfernen, ohne dass personenbezogene Daten davon betroffen sind. Dies ist ein Vorteil, wenn ein Mitarbeiter Ihr Unternehmen verlässt oder ein Gerät gestohlen wird. Nachdem Sie sich entschieden haben, den Datenzugriff zu widerrufen, können Sie die Geräteregistrierung mit Microsoft Intune aufheben. Sobald das Gerät dann eine Verbindung mit dem Netzwerk herstellt, wird der Verschlüsselungsschlüssel des Benutzers für das Gerät widerrufen, und die Unternehmensdaten werden unlesbar.

  > **NOTE**
  > Für die Verwaltung von Surface-Geräten empfiehlt es sich, die aktuelle Verzweigung des Microsoft Endpoint Configuration Manager zu verwenden.
  > Mit Microsoft Endpoint Configuration Manager können Sie auch Enterprise-Daten widerrufen. Dazu wird das Gerät jedoch auf die Werkseinstellungen zurückgesetzt.

Funktionsweise von WIP

WIP hilft Ihnen bei der Bewältigung der täglichen Herausforderungen im Unternehmen. Beispiele:

- Der Verlust von Unternehmensdaten kann selbst auf Mitarbeitergeräten verhindert werden, die nicht gesperrt werden können.
- Die Mitarbeiterzufriedenheit wird nicht durch restriktive Datenverwaltungsrichtlinien auf unternehmenseigenen Geräten beeinträchtigt.
- Geschäftsdaten bleiben Unternehmenseigentum und sind leichter zu kontrollieren.
- Der Netzwerk- und Datenzugriff sowie die Datenfreigabe für nicht unternehmenskompatible Apps können besser gesteuert werden.

Unternehmensszenarien

Mit WIP werden zurzeit die folgenden Unternehmensszenarien abgedeckt:

- Sie können Unternehmensdaten auf Geräten von Mitarbeitern und auf unternehmenseigenen Geräten verschlüsseln.
- Sie können Unternehmensdaten per Remotezugriff auf verwalteten Computern zurücksetzen, ohne dass dies Auswirkungen auf die persönlichen Daten hat. Dies gilt auch für Computer, die Mitarbeitern gehören.
- Sie können bestimmte apps schützen, die auf Unternehmensdaten zugreifen können, die für Mitarbeiter deutlich erkennbar sind. Außerdem haben Sie die Möglichkeit, den Zugriff auf Unternehmensdaten für ungeschützte Apps zu blockieren.
- Während die Richtlinien des Unternehmens aktiv sind, müssen Ihre Mitarbeiter die Arbeit nicht anderweitig unterbrechen, wenn sie zwischen persönlichen Apps und Apps des Unternehmens wechseln. Es ist nicht erforderlich, die Umgebung zu wechseln oder sich mehrfach anzumelden.

WIP-Schutzmodi

Unternehmensdaten werden automatisch verschlüsselt, nachdem sie aus einer Unternehmensquelle auf ein Gerät geladen wurden oder ein Mitarbeiter die Daten als Unternehmensdaten kennzeichnet. Wenn die Unternehmensdaten auf einen Datenträger geschrieben werden, verwendet WIP das von Windows bereitgestellte verschlüsselnde Dateisystem (Encrypting File System, EFS), um ihn zu schützen und mit der Identität Ihres Unternehmens zu verknüpfen.

Ihre WIP-Richtlinie enthält eine Liste der vertrauenswürdigen apps, die für den Zugriff auf und die Verarbeitung von Unternehmensdaten geschützt sind. Diese Liste von Apps wird über die AppLocker-Funktionen implementiert. Diese steuern, welche Apps ausgeführt werden dürfen, und teilen dem Windows-Betriebssystem mit, dass die Apps Unternehmensdaten bearbeiten dürfen. Apps, die in dieser Liste enthalten sind, müssen nicht geändert werden, um auf Unternehmensdaten zugreifen zu können, da ihr Vorhandensein auf der Liste Windows ermöglicht, zu entscheiden, ob ihnen Zugriff gewährt werden kann. Eine Neuerung in Windows10 stellt App-Entwicklern einen neuen Satz von Anwendungsprogrammierschnittstellen (APIs) zum Erstellen *kompatibler* Apps bereit, die sowohl unternehmenseigene als auch persönliche Daten verwenden und bearbeiten können. Ein großer Vorteil beim Arbeiten mit kompatiblen Apps besteht darin, dass Apps, die für das Unternehmen und privat verwendet werden können, wie z.B. Microsoft Word, mit weniger Bedenken hinsichtlich der versehentlichen Verschlüsselung persönlicher Daten verwendet werden können, da die APIs der App ermöglichen, festzustellen, ob es sich um Unternehmens- oder persönliche Daten handelt.

> **NOTE**
> Weitere Informationen zum Erfassen Ihrer Überwachungsprotokolldateien finden Sie unter Erfassen von Windows Information Protection-Überwachungsprotokolldateien (WIP).

Sie können für das WIP-System 1 von 4 verfügbaren Schutz- und Verwaltungsmodi festlegen:

MODUS	BESCHREIBUNG
Blockieren	WIP sucht nach unerwünschten Datenfreigaben und hindert Mitarbeiter daran, den Schritt auszuführen. Beispielsweise können Unternehmensdaten für Apps freigegeben werden, die keinem Unternehmensschutz unterliegen, und Unternehmensdaten können zwischen Apps oder außerhalb des Unternehmensnetzwerks freigegeben werden.
Außerkraftsetzungen zulassen	WIP ermittelt ungeeignete Datenfreigaben und warnt Mitarbeiter davor, eine potenziell unsichere Aktion auszuführen. Bei diesem Verwaltungsmodus können Mitarbeiter die Richtlinie jedoch außer Kraft setzen und die Daten freigeben, wobei die Aktion jedoch in ihrem Überwachungsprotokoll protokolliert wird.

MODUS	BESCHREIBUNG
Unbeaufsichtigt	Im Modus „Außerkraftsetzungen zulassen“ wird WIP im Hintergrund ausgeführt und protokolliert unerwünschte Datenfreigaben, ohne Aktionen zu blockieren, für die normalerweise die Interaktion eines Mitarbeiters erforderlich wäre. Unerlaubte Aktionen, z.B. wenn Apps unzulässigerweise versuchen, auf eine Netzwerkressource oder auf WIP-geschützte Daten zuzugreifen, werden weiterhin verhindert.
Deaktiviert	WIP ist deaktiviert, und Ihre Daten werden weder geschützt noch überwacht. Nachdem WIP deaktiviert wurde, wird versucht, alle durch WIP gekennzeichneten Dateien auf den lokal angeschlossenen Laufwerken zu entschlüsseln. Beachten Sie, dass frühere Entschlüsselungs- und Richtlinieninformationen nicht automatisch erneut angewendet werden, wenn Sie den WIP-Schutz wieder aktivieren.

Deaktivieren von WIP

Sie können Windows Information Protection und die Einschränkungen vollständig deaktivieren. Dadurch werden alle von WIP verwalteten Geräte entschlüsselt, und Sie kehren zum Zustand vor WIP zurück, ohne dass Daten verloren gehen. Diese Vorgehensweise wird jedoch nicht empfohlen. Wenn Sie sich für die Deaktivierung entscheiden, können Sie WIP jederzeit wieder aktivieren. Ihre Entschlüsselungs- und Richtlinieninformationen werden von WIP jedoch nicht automatisch neu angewendet.

Nächste Schritte

Nachdem Sie sich für die Verwendung von WIP in Ihrem Unternehmen entschieden haben, ist folgender Schritt erforderlich:

- Erstellen einer Windows Information Protection (WIP)-Richtlinie

NOTE

Tragen Sie dazu bei, dieses Thema zu verbessern, indem Sie uns Bearbeitungen, Ergänzungen und Feedback bereitstellen. Informationen dazu, wie Sie zu diesem Thema beitragen können, finden Sie unter Bearbeiten der Windows IT Professional-Dokumentation.

Erstellen einer Windows Information Protection-Richtlinie (WIP) mithilfe von Microsoft Intune

11.02.2020 • 2 minutes to read

Gilt für:

- Windows10, Version 1607 und höher
- Windows10 Mobile, Version 1607 und höher

Mit Microsoft Intune können Sie Ihre WIP-Richtlinie erstellen und bereitstellen, inklusive der Auswahl Ihrer geschützten Apps, Ihrer WIP-Schutzebene und Hinweisen, wie Sie Unternehmensdaten im Netzwerk finden können.

Inhalt dieses Abschnitts

THEMA	BESCHREIBUNG
Erstellen einer Windows Information Protection (WIP)-Richtlinie mithilfe des Azure-Portals für Microsoft InTune	Details zur Verwendung des Azure-Portals für Microsoft InTune zum Erstellen und Bereitstellen Ihrer WIP-Richtlinie mit MDM (Mobile Device Management), einschließlich der Auswahl ihrer geschützten apps, ihrer WIP-Schutzebene und zum Auffinden von Unternehmensdaten im Netzwerk.
Erstellen und Überprüfen eines DRA-Zertifikats (Data Recovery Agent, Datenwiederherstellungsagent) des verschlüsselnden Dateisystems (Encrypting File System, EFS)	Schritte zum Erstellen, Überprüfen und zur schnellen Wiederherstellung mithilfe eines DRA-Zertifikats (Data Recovery Agent, Datenwiederherstellungs-Agent) des verschlüsselnden Dateisystems (Encrypting File System, EFS).
Ermitteln des Unternehmenskontexts einer App, die in Windows Information Protection ausgeführt wird	Verwenden Sie den Task-Manager, um zu bestimmen, ob eine App als geschäftliche oder private App gilt oder ob sie von Windows Information Protection (WIP) ausgeschlossen ist.

Erstellen einer Windows Information Protection (WIP)-Richtlinie mithilfe des Azure-Portals für Microsoft InTune

24.12.2019 • 22 minutes to read

Gilt für:

- Windows10, Version 1607 und höher
- Windows10 Mobile, Version 1607 und höher (mit Ausnahme von Microsoft Azure Rights Management, das nur auf dem Desktop verfügbar ist)

Microsoft InTune bietet eine einfache Möglichkeit zum Erstellen und Bereitstelleneiner Windows Information Protection (WIP)-Richtlinie. Sie können auswählen, welche apps geschützt werden sollen, welche Schutzebene Sie haben und wie Sie Unternehmensdaten im Netzwerk finden. Die Geräte können vollständig von der mobilen Geräteverwaltung (Mobile Device Management, MDM) verwaltet oder von der mobilen Anwendungsverwaltung (Mobile Application Management, MAM) verwaltet werden, wobei InTune nur die apps auf dem persönlichen Gerät eines Benutzers verwaltet.

Unterschiede zwischen MDM und MAM für WIP

Sie können eine APP-Schutzrichtlinie in InTune entweder mit der Geräteregistrierung für MDM oder ohne Geräteregistrierung für MAM erstellen. Der Prozess zum Erstellen einer der Richtlinien ist ähnlich, aber es gibt wichtige Unterschiede:

- MAM verfügt über zusätzliche **Zugriffs** Einstellungen für Windows Hello for Business.
- MAM kann Unternehmensdaten selektiv vom persönlichen Gerät eines Benutzers abwischen.
- Für MAM ist eine Azure Active Directory (Azure AD) Premium-Lizenzerforderlich.
- Eine Azure AD Premium-Lizenz ist auch für die automatische Wiederherstellung von WIP erforderlich, in der ein Gerät erneut registrieren und den Zugriff auf geschützte Daten wiedererlangen kann. Die automatische Wiederherstellung von WIP hängt von der Azure AD-Registrierung ab, um die Verschlüsselungsschlüssel zu sichern, für die eine automatische Registrierung des Geräts mit MDM erforderlich ist.
- MAM unterstützt nur einen Benutzer pro Gerät.
- MAM kann nur erleuchtete appsverwalten.
- Nur MDM kann BitLocker-CSP -Richtlinien verwenden.
- Wenn derselbe Benutzer und dasselbe Gerät für MDM und MAM vorgesehen sind, wird die MDM-Richtlinie auf Geräte angewendet, die mit Azure AD verbunden sind. Für persönliche Geräte, die dem Arbeitsplatz beigetreten sind (also mithilfe von **Einstellungen** > **e-Mail-#a0 Konten** > **ein Geschäfts-oder Schulkonto hinzufügen**), wird die nur-MAM-Richtlinie bevorzugt, aber es ist möglich, die Geräteverwaltung auf MDM in **Einstellungen**zu aktualisieren. Windows Home Edition unterstützt nur WIP nur für MAM; durch das Upgrade auf die MDM-Richtlinie für Home Edition wird der WIP-geschützte Datenzugriff widerrufen.

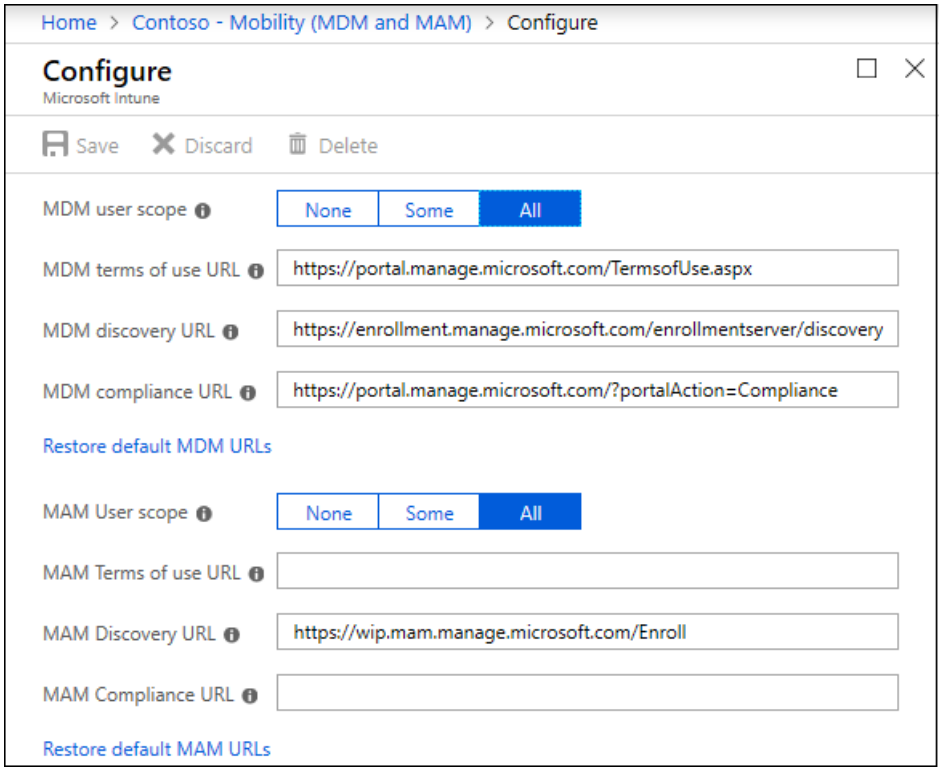
Voraussetzungen

Bevor Sie eine WIP-Richtlinie mithilfe von InTune erstellen können, müssen Sie einen MDM-oder MAM-Anbieter in Azure Active Directory (Azure AD) konfigurieren. Für MAM ist eine Azure Active Directory (Azure AD) Premium-Lizenzerforderlich. Eine Azure AD Premium-Lizenz ist auch für die automatische Wiederherstellung von WIP erforderlich, in der ein Gerät erneut registrieren und den Zugriff auf geschützte Daten wiedererlangen

kann. Die automatische Wiederherstellung von WIP basiert auf Azure AD-Registrierung, um die Verschlüsselungsschlüssel zu sichern, für die eine automatische Registrierung des Geräts mit MDM erforderlich ist.

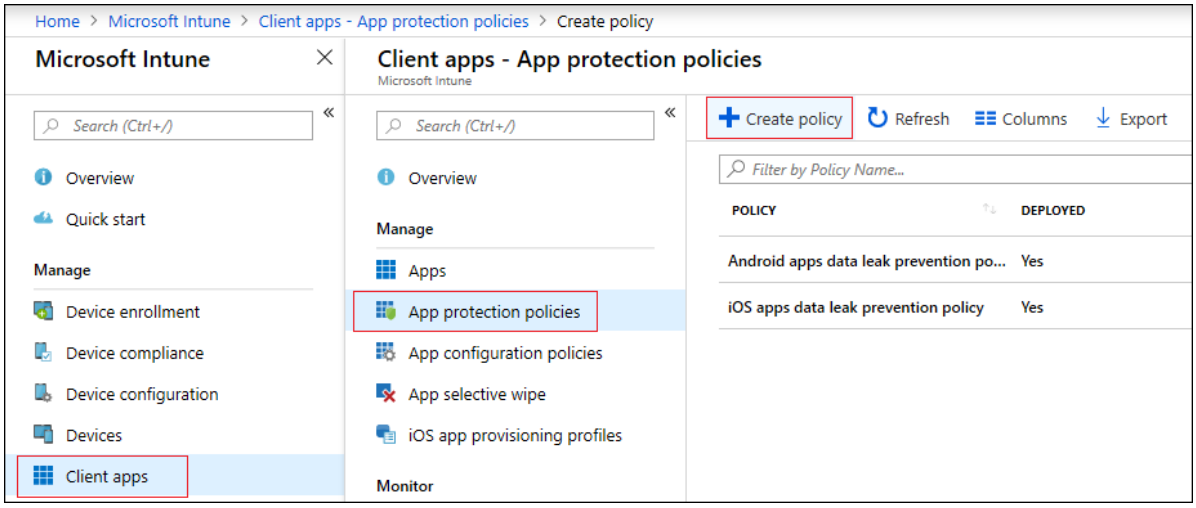
Konfigurieren des MDM-oder MAM-Anbieters

1. Anmelden beim Azure-Portal.
2. Klicken Sie auf **Azure Active Directory** > **Mobility (MDM und MAM)** > **Microsoft InTune**.
3. Klicken Sie auf **Standard-URLs wiederherstellen** , oder geben Sie den Benutzerbereich Einstellungen für MDM oder MAM ein, und klicken Sie auf **Speichern**:



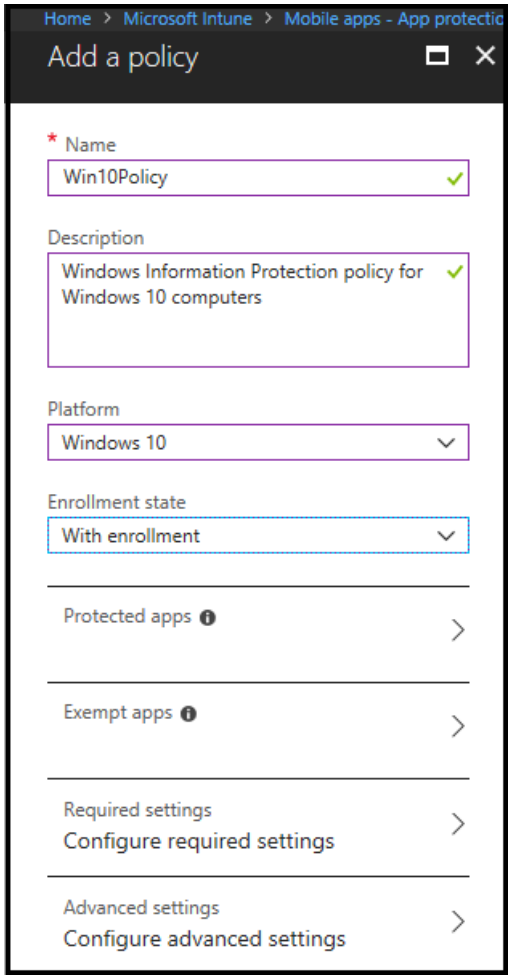
Erstellen einer WIP-Richtlinie

1. Anmelden beim Azure-Portal.
2. Öffnen Sie Microsoft InTune, und klicken Sie auf **Client apps** > -**App-Schutzrichtlinien Richt** > **Linie erstellen**.

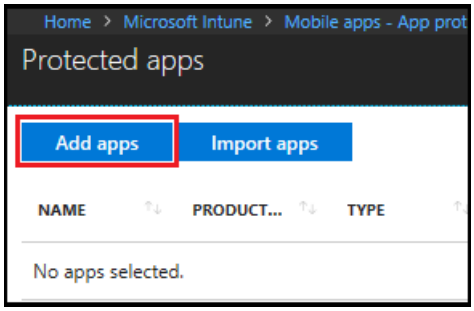


3. Klicken Sie im Bildschirm **App policy** auf **Add a policy**, und füllen Sie die folgenden Felder aus:

- **Name.** Geben Sie einen Namen (erforderlich) für Ihre neue Richtlinie ein.
- **Beschreibung.** Geben Sie eine optionale Beschreibung ein.
- **Plattform.** Wählen Sie **Windows 10**aus.
- **Anmeldungsstatus.** Wählen Sie **ohne Registrierung** für MAM oder **mit der Registrierung** für MDM aus.



4. Klicken Sie auf **geschützte apps** , und klicken Sie dann auf **apps hinzufügen**.



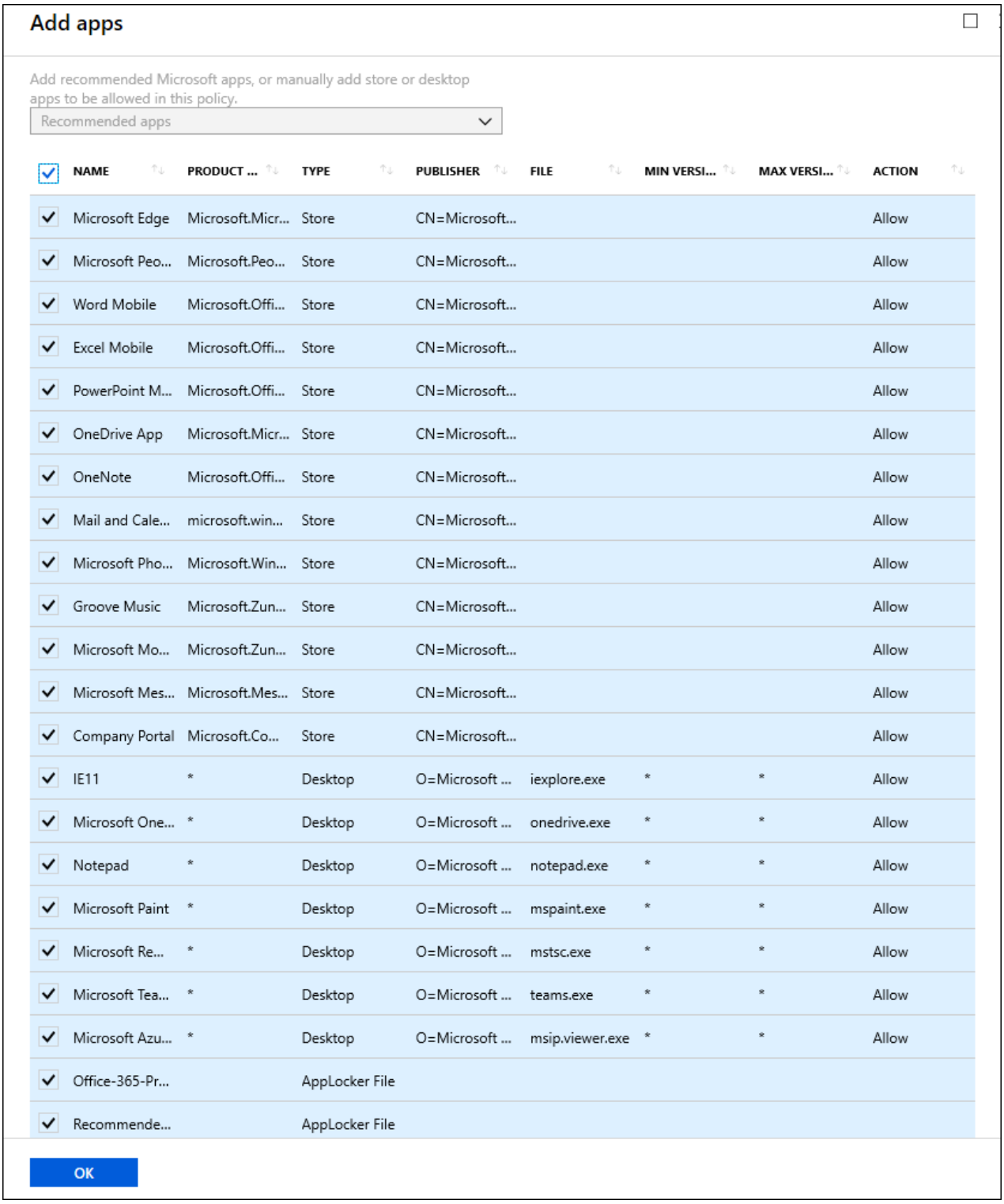
Sie können diese Arten von apps hinzufügen:

- Empfohlene apps
- Store-Apps
- Desktop-Apps

> **NOTE**
> Eine Anwendung gibt möglicherweise Zugriff verweigerte Fehler zurück, nachdem Sie aus der Liste der geschützten apps entfernt wurde. Anstatt Sie aus der Liste zu entfernen, deinstallieren Sie die Anwendung, und installieren Sie Sie erneut, oder befreien Sie Sie von der WIP-Richtlinie.

Hinzufügen von empfohlenen apps

Wählen Sie **Empfohlene apps** und dann jede APP aus, auf die Sie auf Ihre Unternehmensdaten zugreifen möchten, oder wählen Sie alle aus, und klicken Sie auf **OK**.

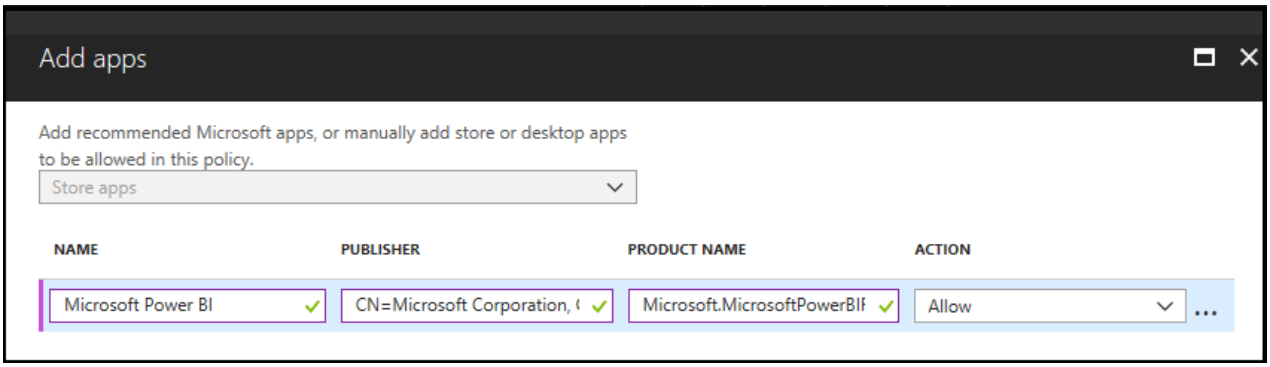


NAME	PRODUCT ...	TYPE	PUBLISHER	FILE	MIN VERSI...	MAX VERSI...	ACTION
Microsoft Edge	Microsoft.Micr...	Store	CN=Microsoft...				Allow
Microsoft Peo...	Microsoft.Peo...	Store	CN=Microsoft...				Allow
Word Mobile	Microsoft.Offi...	Store	CN=Microsoft...				Allow
Excel Mobile	Microsoft.Offi...	Store	CN=Microsoft...				Allow
PowerPoint M...	Microsoft.Offi...	Store	CN=Microsoft...				Allow
OneDrive App	Microsoft.Micr...	Store	CN=Microsoft...				Allow
OneNote	Microsoft.Offi...	Store	CN=Microsoft...				Allow
Mail and Cale...	microsoft.win...	Store	CN=Microsoft...				Allow
Microsoft Pho...	Microsoft.Win...	Store	CN=Microsoft...				Allow
Groove Music	Microsoft.Zun...	Store	CN=Microsoft...				Allow
Microsoft Mo...	Microsoft.Zun...	Store	CN=Microsoft...				Allow
Microsoft Mes...	Microsoft.Mes...	Store	CN=Microsoft...				Allow
Company Portal	Microsoft.Co...	Store	CN=Microsoft...				Allow
IE11	*	Desktop	O=Microsoft ...	iexplore.exe	*	*	Allow
Microsoft One...	*	Desktop	O=Microsoft ...	onedrive.exe	*	*	Allow
Notepad	*	Desktop	O=Microsoft ...	notepad.exe	*	*	Allow
Microsoft Paint	*	Desktop	O=Microsoft ...	mspaint.exe	*	*	Allow
Microsoft Re...	*	Desktop	O=Microsoft ...	mstsc.exe	*	*	Allow
Microsoft Tea...	*	Desktop	O=Microsoft ...	teams.exe	*	*	Allow
Microsoft Azu...	*	Desktop	O=Microsoft ...	msip.viewer.exe	*	*	Allow
Office-365-Pr...		AppLocker File					
Recommende...		AppLocker File					

Hinzufügen von Store-Apps

Wählen Sie **Store-Apps**aus, geben Sie den App-Produktnamen und Publisher ein, und klicken Sie auf **OK**. Wenn Sie beispielsweise die Mobile Power BI-App aus dem Store hinzufügen möchten, geben Sie Folgendes ein:

- **Name**: Microsoft Power BI
- **Publisher**: `CN=Microsoft Corporation, O=Microsoft Corporation, L=Redmond, S=Washington, C=US`
- **Produkt Name**: `Microsoft.MicrosoftPowerBIForWindows`



Wenn Sie mehrere Store-Apps hinzufügen möchten, klicken Sie auf das Auslassungszeichen **...**.

Wenn Sie den Publisher oder den Produktnamen des Store-App nicht kennen, können Sie ihn finden, indem Sie die folgenden Schritte ausführen.

1. Wechseln Sie zur Website Microsoft Store für Unternehmen, und suchen Sie Ihre App. Beispiel: *Mobile Power BI-App*.

2. Kopieren Sie den ID-Wert aus der App-URL. Die URL der mobilen Power BI-APP-ID lautet https://www.microsoft.com/store/p/microsoft-power-bi/9nblgggzlxn1beispielsweise, und Sie möchten den ID- `9nblgggzlxn1` Wert kopieren.

3. Führen Sie in einem Browser die Web-API im Microsoft Store für Unternehmen-Portal aus, um eine JavaScript Object Notation (JSON)-Datei zurückzugeben, die die Werte für den Herausgeber- und Produktnamen enthält. Beispiel: Run https://bspmts.mp.microsoft.com/v1/public/catalog/Retail/Products/9nblgggzlxn1/applockerdata, where `9nblgggzlxn1` wird durch ihren ID-Wert ersetzt.

   Die API wird ausgeführt und öffnet einen Text-Editor mit allen App-Details.

   ```
   {
       "packageIdentityName": "Microsoft.MicrosoftPowerBIForWindows",
       "publisherCertificateName": "CN=Microsoft Corporation, O=Microsoft Corporation, L=Redmond,
   S=Washington, C=US"
   }
   ```

4. Kopieren Sie den Wert `publisherCertificateName` in das Feld **Publisher** und den Wert `packageIdentityName` in das Feld **Name** in Intune.

   > **IMPORTANT**
   >
   > Die JSON-Datei kann auch einen Wert `windowsPhoneLegacyId` für die Felder **Publisher Name** und **Product Name** zurückgeben. Dies bedeutet, dass Sie über eine App verfügen, die ein XAP-Paket verwendet, und dass Sie den **Produktnamen** als `windowsPhoneLegacyId` und den **Herausgebernamen** als `CN=` gefolgt von `windowsPhoneLegacyId` festlegen müssen.
   >
   > Beispiel:
   >
   > ```
   > {
   > "windowsPhoneLegacyId": "ca05b3ab-f157-450c-8c49-a1f127f5e71d",
   > }
   > ```

Wenn Sie Windows 10 Mobile-Apps hinzufügen müssen, die nicht über den Store für Unternehmen verteilt sind,

müssen Sie das **Windows Device Portal** -Feature verwenden.

> **Hinweis**
> Ihr PC und Telefon müssen im selben drahtlosen Netzwerk sein.

1. Wechseln Sie auf dem Windows Phone zu **Einstellungen**, wählen Sie **Update und Sicherheit**, und wählen Sie dann **Für Entwickler**.
2. Aktivieren Sie im Bildschirm **Für Entwickler** den **Entwicklermodus**, aktivieren Sie **Gerätesuche**, und aktivieren Sie dann **Geräteportal**.
3. Kopieren Sie die URL im Bereich **Geräteportal** in den Browser Ihres Geräts, und akzeptieren Sie dann das SSL-Zertifikat.
4. Drücken Sie im Bereich **Geräteerkennung** auf **Koppeln**, und geben Sie dann die PIN der Website aus dem vorherigen Schritt ein.
5. Auf der **Apps**-Registerkarte der Website sehen Sie die Details für die ausgeführten Apps, einschließlich der Herausgeber- und Produktnamen.
6. Starten Sie die App, für die Sie die Werte der Herausgeber- und Produktnamen suchen.
7. Kopieren Sie den Wert `publisherCertificateName`, und fügen Sie ihn in das Feld **Herausgebername** und den Wert `packageIdentityName` in das Feld **Produktname** von Intune ein.

> **IMPORTANT**
> Die JSON-Datei kann auch einen Wert `windowsPhoneLegacyId` für die Felder **Herausgebername** und **Produktname** zurückgeben. Dies bedeutet, dass Sie über eine App verfügen, die ein XAP-Paket verwendet, und dass Sie den **Produktnamen** als `windowsPhoneLegacyId` und den **Herausgebernamen** als `CN=` gefolgt von `windowsPhoneLegacyId` festlegen müssen.
>
> Beispiel:
> ```
> {
> "windowsPhoneLegacyId": "ca05b3ab-f157-450c-8c49-a1f127f5e71d",
> }
> ```

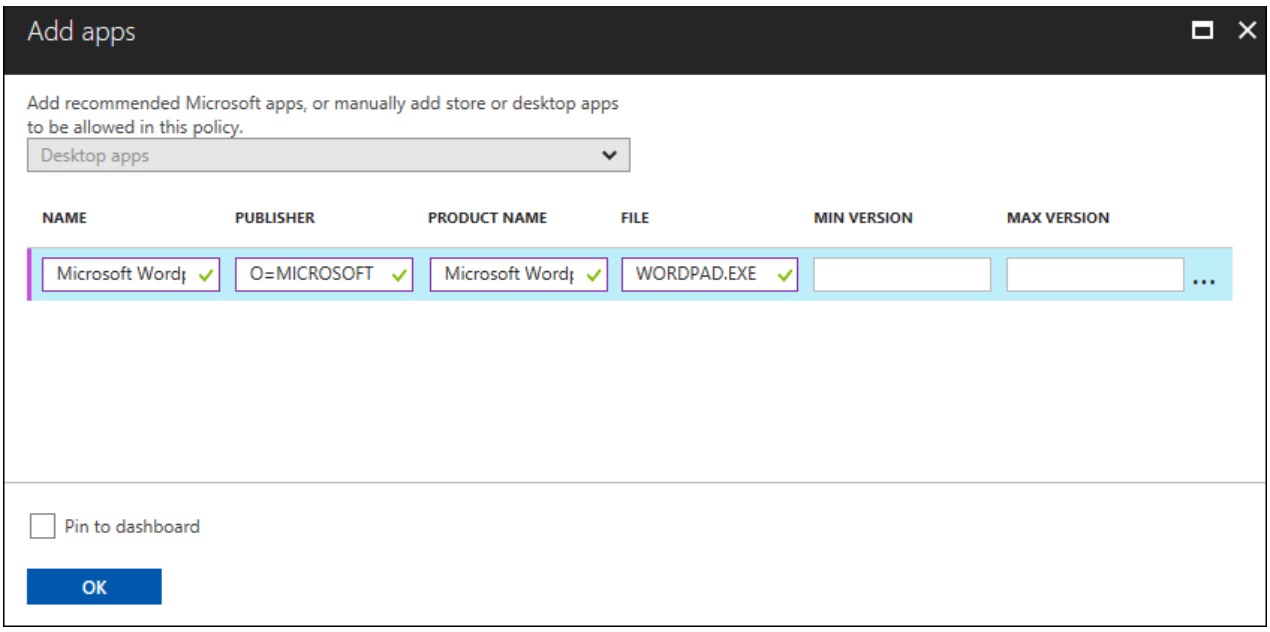
Hinzufügen von Desktop-Apps

Wenn Sie **Desktop-Apps**hinzufügen möchten, füllen Sie die folgenden Felder aus, basierend auf den Ergebnissen, die zurückgegeben werden sollen.

FELD	VERWALTET
Alle als „*“ markierte Felder	Alle von einem Herausgeber signierten Dateien. (Nicht empfohlen und funktioniert möglicherweise nicht)
Nur Herausgeber	Wenn Sie nur dieses Feld ausfüllen, erhalten Sie alle vom benannten Herausgeber signierten Dateien. Dies kann nützlich sein, wenn Ihr Unternehmen der Herausgeber und Signaturgeber interner Branchen-Apps ist.
Nur Herausgeber und Name	Wenn Sie nur diese Felder ausfüllen, erhalten Sie alle Dateien für das angegebene Produkt, die vom benannten Herausgeber signiert sind.

Nur Herausgeber, Name und Datei	Wenn Sie nur diese Felder ausfüllen, erhalten Sie alle Versionen der benannten Datei oder des Pakets für das angegebene Produkt, die vom benannten Herausgeber signiert sind.
Nur Herausgeber, Name, Datei und Min-Version	Wenn Sie nur diese Felder ausfüllen, erhalten Sie die angegebene Version oder neuere Versionen der benannten Datei oder des Pakets für das angegebene Produkt, die vom benannten Herausgeber signiert. Diese Option wird für optimierte Apps empfohlen, die zuvor nicht optimiert wurden.
Nur Herausgeber, Name, Datei und Max-Version	Wenn Sie nur diese Felder ausfüllen, erhalten Sie die angegebene Version oder ältere Versionen der benannten Datei oder des Pakets für das angegebene Produkt, die vom benannten Herausgeber signiert.
Alle Felder ausgefüllt	Wenn Sie alle Felder ausfüllen, erhalten Sie die angegebene Version der benannten Datei oder des Pakets für das angegebene Produkt, die vom benannten Herausgeber signiert ist.

Wenn Sie eine weitere Desktop-App hinzufügen möchten, klicken Sie auf die drei Punkte **...**. Nachdem Sie die Informationen in die Felder eingegeben haben, klicken Sie auf **OK**.



Wenn Sie nicht sicher sind, was Sie für den Herausgeber angeben sollen, können Sie den folgenden PowerShell-Befehl ausführen:

```
Get-AppLockerFileInformation -Path "<path_of_the_exe>"
```

Dabei gibt `"<path_of_the_exe>"` den Speicherort der App auf dem Gerät an. Beispiel:

```
Get-AppLockerFileInformation -Path "C:\Program Files\Windows NT\Accessories\wordpad.exe"
```

In diesem Beispiel erhalten Sie die folgenden Informationen:

```
Path                    Publisher
----                    ---------
%PROGRAMFILES%\WINDOWS NT\ACCESSORIES\WORDPAD.EXE O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US
```

Hierbei `O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US` handelt es sich um den `WORDPAD.EXE` Namen des **Herausgebers** und den **Datei** Namen.

Importieren einer Liste von apps

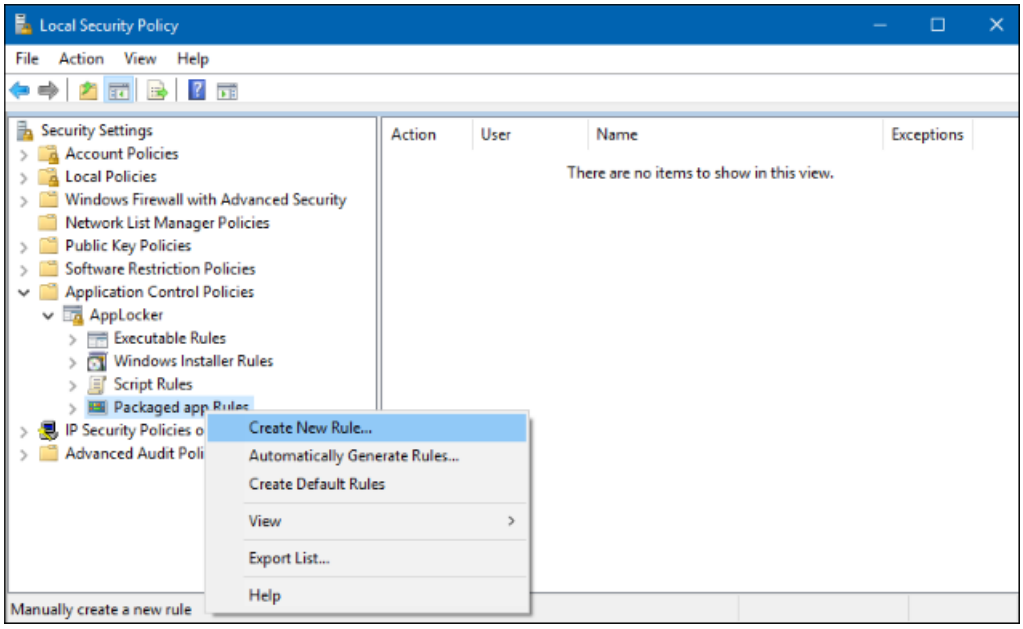
Dieser Abschnitt behandelt zwei Beispiele für die Verwendung einer AppLocker-XML-Datei in der Liste der **geschützten apps** . Sie können diese Option verwenden, wenn Sie gleichzeitig mehrere Apps hinzufügen möchten.

- Erstellen einer verpackten App-Regel für Store-Apps
- Erstellen einer ausführbaren Regel für nicht signierte apps

Weitere Informationen zu AppLocker finden Sie im Thema AppLocker.

Erstellen einer verpackten App-Regel für Store-Apps

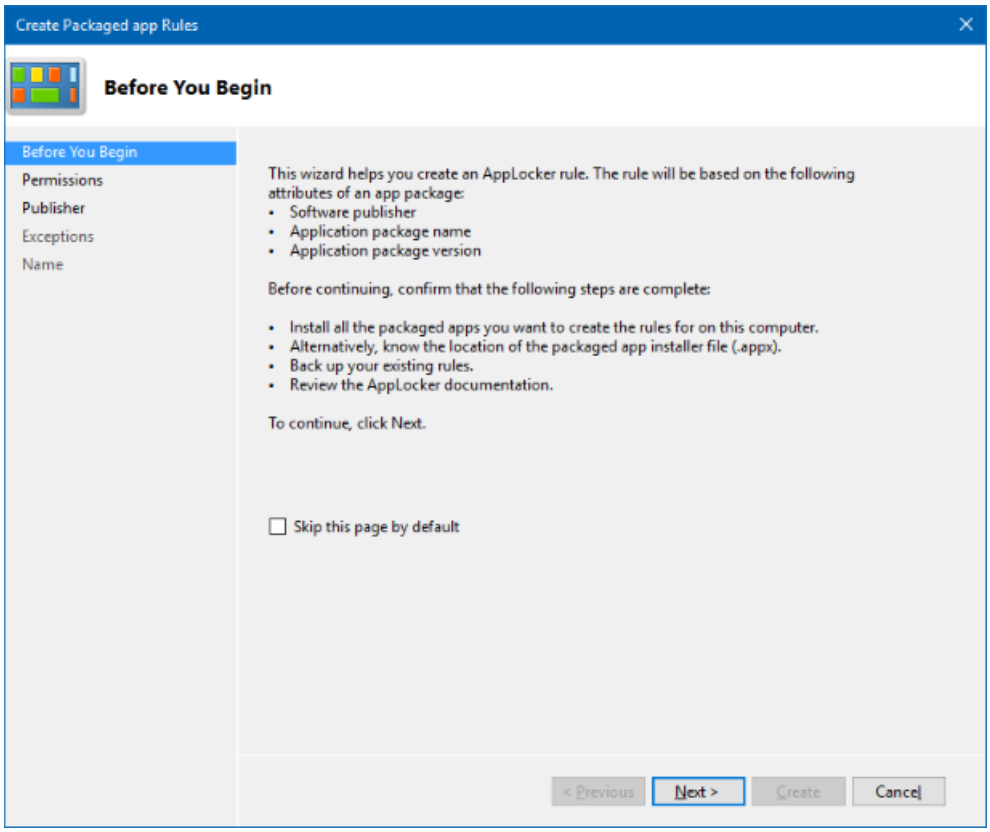
1. Öffnen Sie das Snap-In „Lokale Sicherheitsrichtlinie“ (SecPol.msc).
2. Erweitern Sie im linken Blatt **Application Control Policies** den Eintrag **AppLocker**, und klicken Sie auf **Packaged App Rules**.



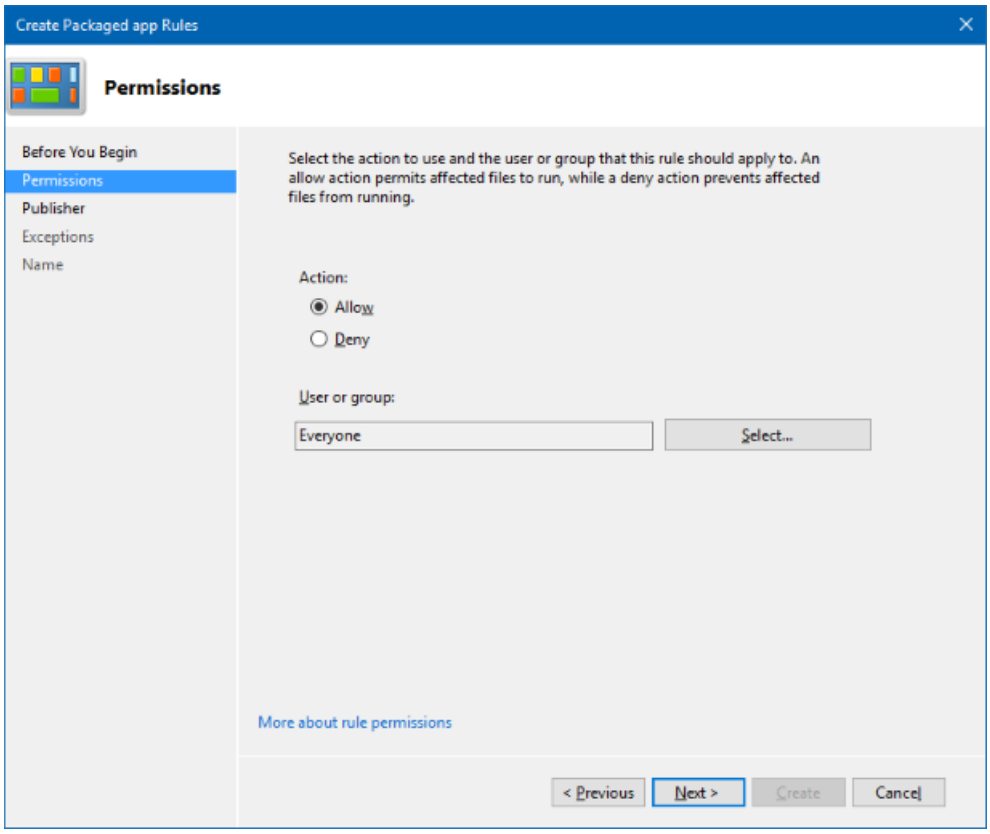
3. Klicken Sie mit der rechten Maustaste in das Blatt auf der rechten Seite, und klicken Sie dann auf **Create New Rule**.

   Der Assistent **Create Packaged app Rules** wird angezeigt.

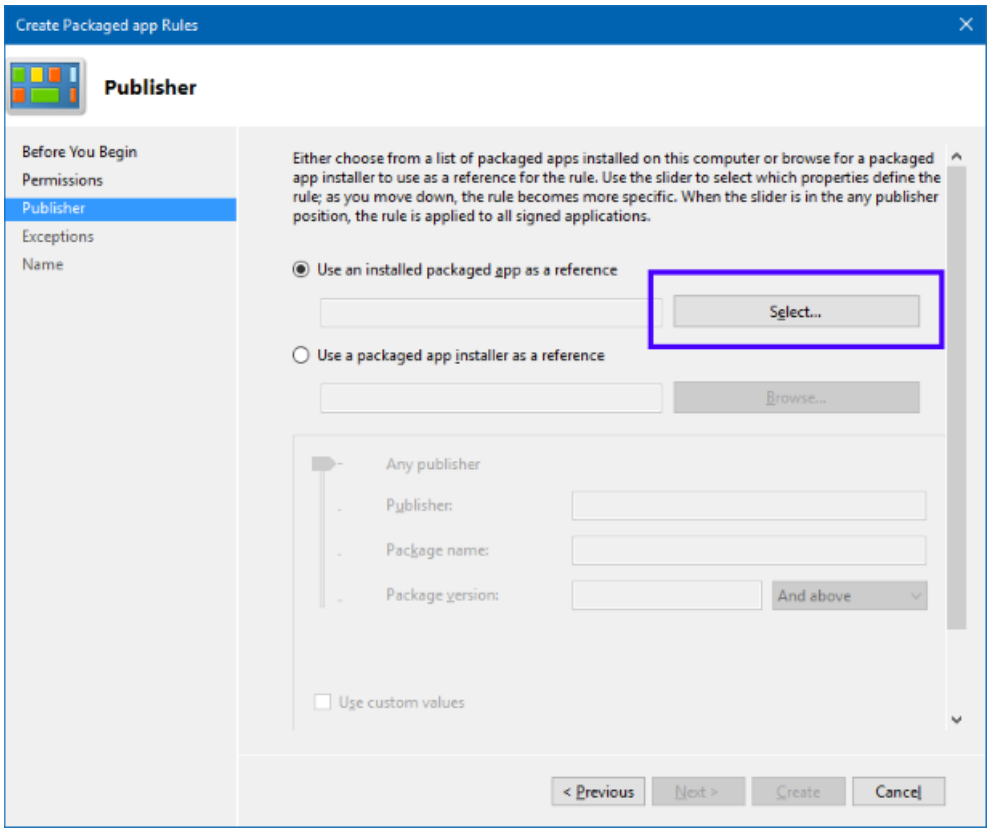
4. Klicken Sie auf der Seite **Vorbereitung** auf **Weiter**.



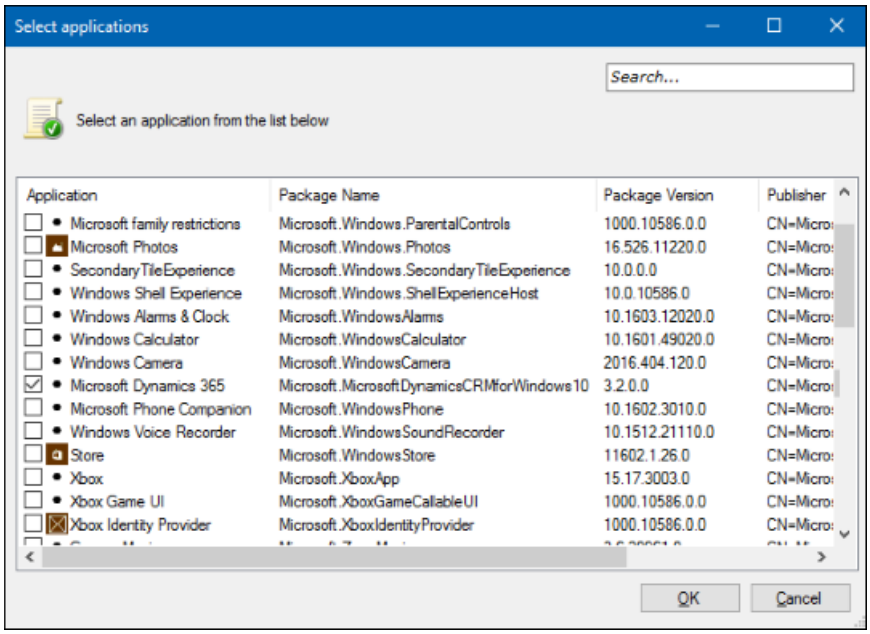
5. Stellen Sie auf der Seite **Berechtigungen** sicher, dass **Aktion** auf **Zulassen** und **Benutzer oder Gruppe** auf **Jeder** festgelegt ist, und klicken Sie dann auf **Weiter**.



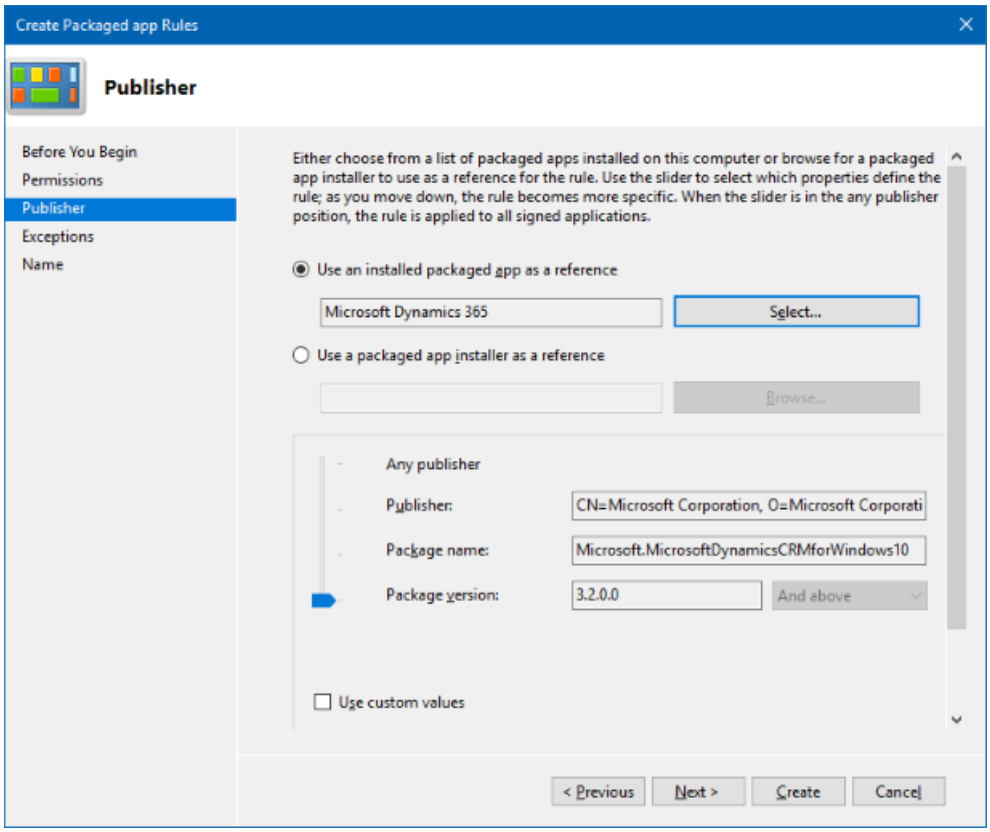
6. Klicken Sie auf der Seite **Herausgeber** im Bereich **Ein installiertes App-Paket als Referenz verwenden** auf **Auswählen**.



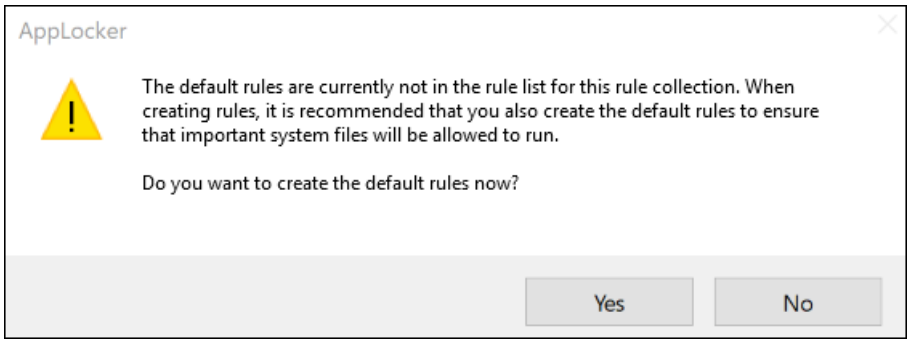
7. Wählen Sie im Feld **Select applications** die App aus, die Sie als Referenz für die Regel verwenden möchten, und klicken Sie dann auf **OK**. In diesem Beispiel verwenden wir Microsoft Dynamics 365.



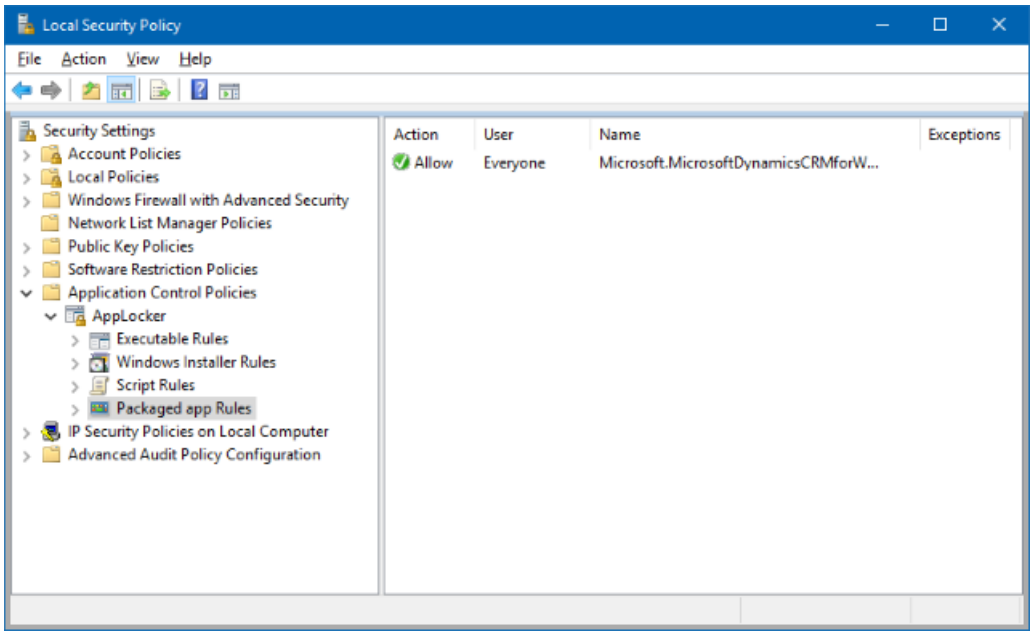
8. Klicken Sie auf der aktualisierten Seite **Publisher** auf **Create**.



9. Klicken Sie auf **No** im Dialogfeld, wenn Sie gefragt werden, ob Sie die Standardregeln erstellen möchten. Erstellen Sie keine Standardregeln für Ihre WIP-Richtlinie.



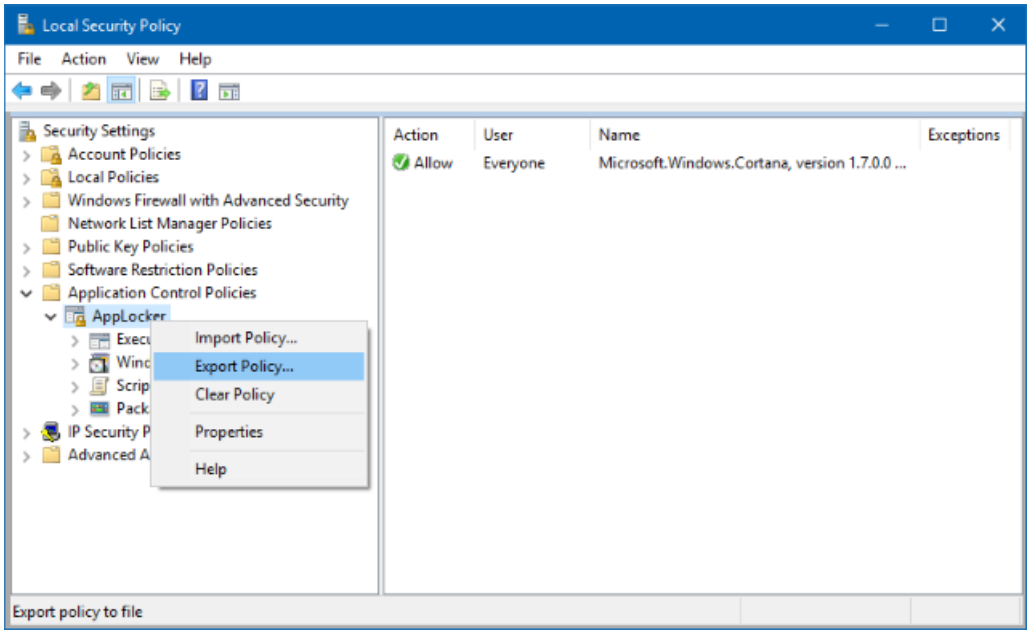
10. Überprüfen Sie das Snap-In „Lokale Sicherheitsrichtlinie", um sicherzustellen, dass die Regel richtig ist.



11. Klicken Sie mit der rechten Maustaste im linken Blatt auf **AppLocker**, und klicken Sie dann auf **Export**

policy.

Das Feld **Richtlinie exportieren** wird geöffnet, in dem Sie die neue Richtlinie im XML-Format exportieren und speichern können.



12. Navigieren Sie im Feld **Richtlinie exportieren** zum Speicherort, an dem die Richtlinie gespeichert werden soll, legen Sie einen Namen für die Richtlinie fest, und klicken Sie auf **Speichern**.

    Die Richtlinie wird gespeichert, und die Meldung wird angezeigt, dass eine Regel aus der Richtlinie exportiert wurde.

    XML-Beispieldatei
    Dies ist die XML-Datei, die AppLocker für Microsoft Dynamics 365 erstellt.

```
    <?xml version="1.0"?>
    <AppLockerPolicy Version="1">
        <RuleCollection EnforcementMode="NotConfigured" Type="Appx">
            <FilePublisherRule Action="Allow" UserOrGroupSid="S-1-1-0" Description=""
Name="Microsoft.MicrosoftDynamicsCRMforWindows10, version 3.2.0.0 and above, from Microsoft
Corporation" Id="3da34ed9-aec6-4239-88ba-0afdce252ab4">
                <Conditions>
                    <FilePublisherCondition BinaryName="*"
ProductName="Microsoft.MicrosoftDynamicsCRMforWindows10" PublisherName="CN=Microsoft Corporation,
O=Microsoft Corporation, L=Redmond, S=Washington, C=US">
                        <BinaryVersionRange HighSection="*" LowSection="3.2.0.0"/>
                    </FilePublisherCondition>
                </Conditions>
            </FilePublisherRule>
        </RuleCollection>
        <RuleCollection EnforcementMode="NotConfigured" Type="Dll"/>
        <RuleCollection EnforcementMode="NotConfigured" Type="Exe"/>
        <RuleCollection EnforcementMode="NotConfigured" Type="Msi"/>
        <RuleCollection EnforcementMode="NotConfigured" Type="Script"/>
    </AppLockerPolicy>
```

13. Nachdem Sie die XML-Datei erstellt haben, müssen Sie sie mithilfe von Microsoft Intune importieren.

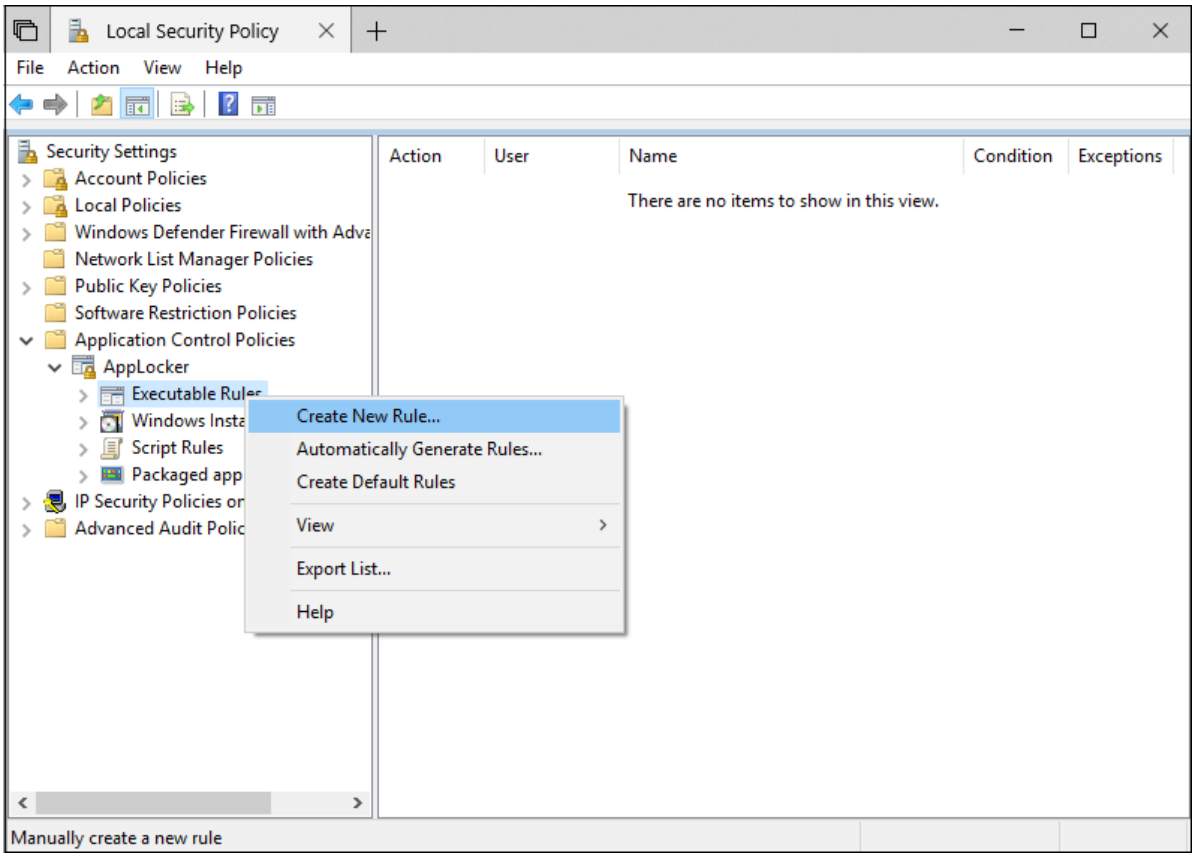
Erstellen einer ausführbaren Regel für nicht signierte apps

Die ausführbare Regel hilft beim Erstellen einer AppLocker-Regel zum Signieren von nicht signierten apps. Sie ermöglicht das Hinzufügen des Dateipfads oder des App-Verlegers, der in der digitalen Signatur der Datei enthalten ist, damit die WIP-Richtlinie angewendet werden kann.

1. Öffnen Sie das Snap-In „Lokale Sicherheitsrichtlinie“ (secpol.msc).

2. Klicken Sie im linken Bereich auf**AppLocker** > -**ausführbare Regeln**für **Anwendungssteuerungsrichtlinien** > .

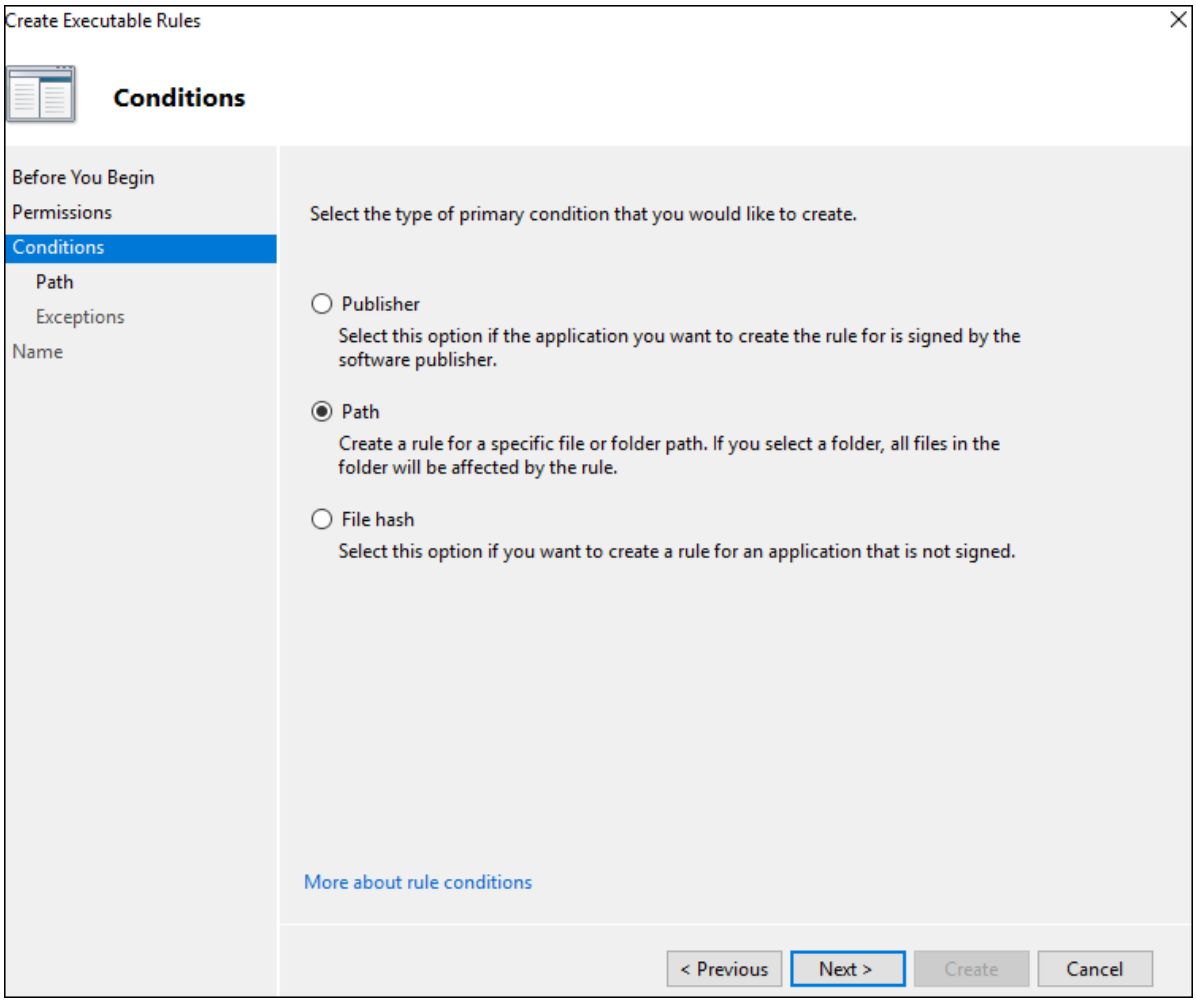
3. Klicken Sie mit der rechten Maustaste auf **ausführbare Regeln** > **neue Regel erstellen**.



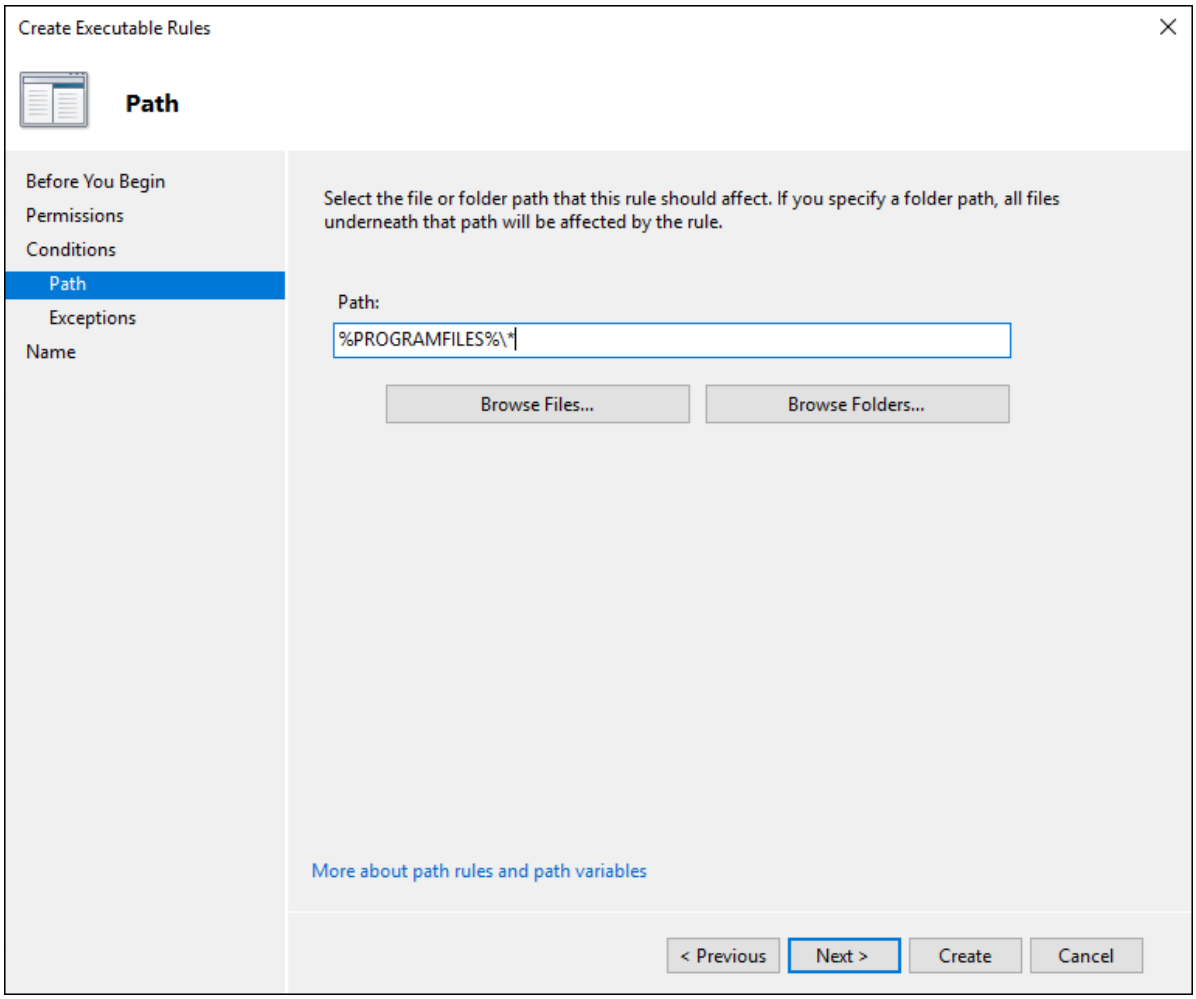
4. Klicken Sie auf der Seite **Vorbereitung** auf **Weiter**.

5. Stellen Sie auf der Seite **Berechtigungen** sicher, dass **Aktion** auf **Zulassen** und **Benutzer oder Gruppe** auf **Jeder** festgelegt ist, und klicken Sie dann auf **Weiter**.

6. Klicken Sie auf der Seite **Bedingungen** auf **Pfad** , und klicken Sie dann auf **weiter**.



7. Klicken Sie auf **Ordner durchsuchen** , und wählen Sie den Pfad für die nicht signierten Apps aus. Für dieses Beispiel verwenden wir "C:\Program Files".

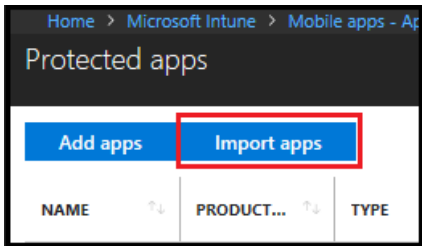


8. Fügen Sie auf der Seite **Ausnahmen** alle Ausnahmen hinzu, und klicken Sie dann auf **weiter**.
9. Geben Sie auf der Seite **Name** einen Namen und eine Beschreibung für die Regel ein, und klicken Sie dann auf **Erstellen**.
10. Klicken Sie im linken Bereich mit der rechten Maustaste auf **AppLocker** > -**Export Richtlinie**.
11. Navigieren Sie im Feld **Richtlinie exportieren** zum Speicherort, an dem die Richtlinie gespeichert werden soll, legen Sie einen Namen für die Richtlinie fest, und klicken Sie auf **Speichern**.

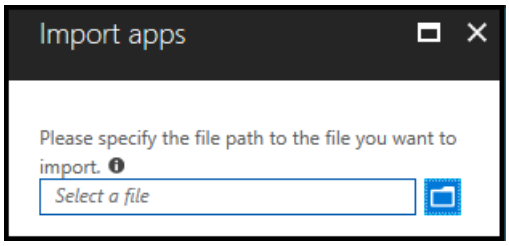
    Die Richtlinie wird gespeichert, und die Meldung wird angezeigt, dass eine Regel aus der Richtlinie exportiert wurde.
12. Nachdem Sie die XML-Datei erstellt haben, müssen Sie sie mithilfe von Microsoft Intune importieren.

So importieren Sie eine Liste geschützter apps mit Microsoft InTune

1. Klicken Sie in **geschützten apps**auf **apps importieren**.



Importieren Sie dann Ihre Datei.



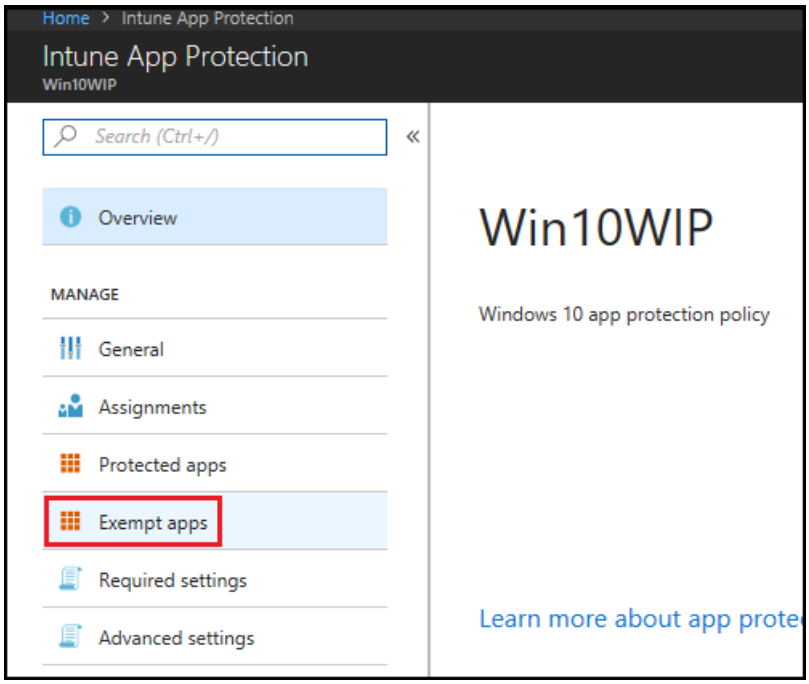
2. Navigieren Sie zu Ihrer exportierten AppLocker-Richtliniendatei, und klicken Sie auf **Open**.

   Die Datei Importe und die apps werden Ihrer Liste der **geschützten apps** hinzugefügt.

Ausschließen von Apps aus einer WIP-Richtlinie

Wenn Ihre APP mit WIP nicht kompatibel ist, aber dennoch mit Unternehmensdaten verwendet werden muss, können Sie die APP von den WIP-Einschränkungen ausschließen. Dies bedeutet, dass Ihre Apps keine automatische Verschlüsselung oder Tags enthalten und nicht die Netzwerkbeschränkungen berücksichtigen. Dies bedeutet auch, dass bei den ausgenommenen Apps Datenverluste auftreten können.

1. Klicken Sie in **Client-apps-App-Schutzrichtlinien**auf ausgenommene **apps**.



2. Klicken Sie unter **Ausgeschlossene Apps**auf **apps hinzufügen**.

   Beachten Sie, dass beim Ausnehmen von Apps diese die WIP-Einschränkungen umgehen und auf Unternehmensdaten zugreifen dürfen.

3. Füllen Sie die restlichen Informationen für die App aus, basierend auf dem Typ der hinzugefügten App:

   - Hinzufügen von empfohlenen apps
   - Hinzufügen von Store-Apps
   - Hinzufügen von Desktop-Apps
   - Importieren von apps

4. Klicken Sie auf **OK**.

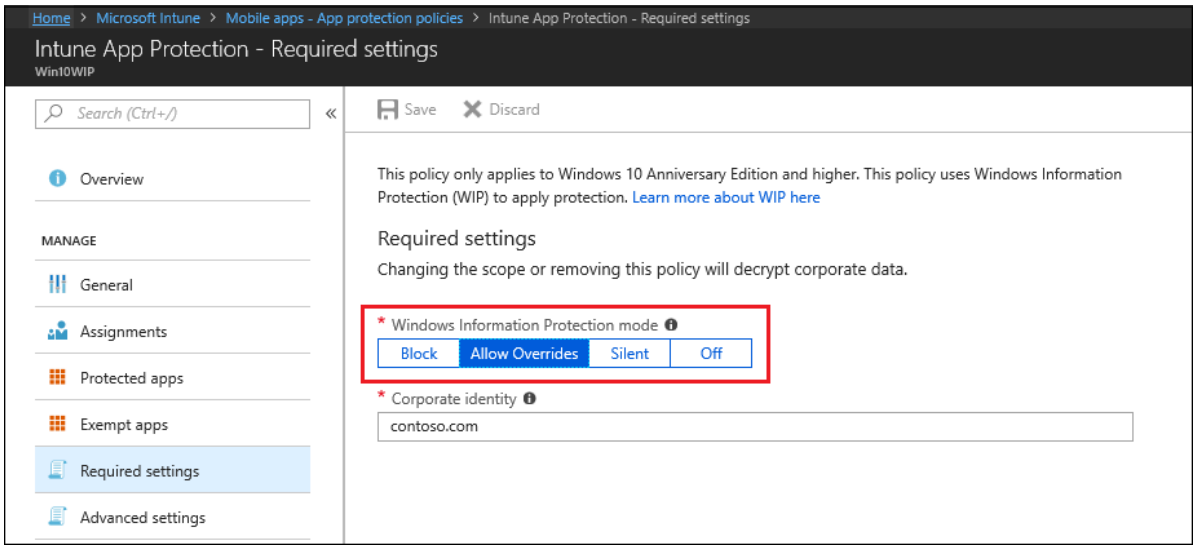
Verwalten des WIP-Schutzmodus für Ihre Unternehmensdaten

Nachdem Sie die Apps hinzugefügt haben, die mit WIP geschützt werden sollen, müssen Sie einen Verwaltungs-

und Schutzmodus anwenden.

Es wird empfohlen, dass Sie mit **Unbeaufsichtigt** oder **Außerkraftsetzungen zulassen** beginnen und für eine kleine Gruppe überprüfen, dass die richtigen Apps in der Liste der geschützten Apps enthalten sind. Nachdem Sie fertig sind, können Sie zu ihrer endgültigen Erzwingungsrichtlinie wechseln, **blockieren**.

1. Klicken Sie in der **App-Schutzrichtlinien** -Blade auf den Namen Ihrer Richtlinie, und klicken Sie dann auf **erforderliche Einstellungen**.



MODUS	BESCHREIBUNG
Blockieren	WIP sucht nach unerwünschten Datenfreigaben und hindert Mitarbeiter daran, den Schritt auszuführen. Beispielsweise können Informationen zwischen Apps geteilt werden, die keinem Unternehmensschutz unterliegen, und Unternehmensdaten für andere Personen und Geräte außerhalb Ihres Unternehmens freigegeben werden.
Allow Overrides	WIP ermittelt ungeeignete Datenfreigaben und warnt Mitarbeiter davor, eine potenziell unsichere Aktion auszuführen. Bei diesem Verwaltungsmodus können Mitarbeiter die Richtlinie jedoch außer Kraft setzen und die Daten freigeben, wobei die Aktion jedoch in ihrem Überwachungsprotokoll protokolliert wird. Weitere Informationen zum Erfassen Ihrer Überwachungsprotokolldateien finden Sie unter Erfassen von Windows Information Protection-Überwachungsprotokolldateien (WIP).
Unbeaufsichtigt	Im Modus zur Außerkraftsetzung wird WIP im Hintergrund ausgeführt und protokolliert unerwünschte Datenfreigaben, ohne Aktionen zu blockieren, für die normalerweise die Interaktion eines Mitarbeiters erforderlich wäre. Unerlaubte Aktionen, z.B. wenn Apps unzulässigerweise versuchen, auf eine Netzwerkressource oder auf WIP-geschützte Daten zuzugreifen, werden weiterhin verhindert.

MODUS	BESCHREIBUNG
Off (nicht empfohlen)	WIP ist deaktiviert, und Ihre Daten werden weder geschützt noch überwacht. Nachdem WIP deaktiviert wurde, wird versucht, alle durch WIP gekennzeichneten Dateien auf den lokal angeschlossenen Laufwerken zu entschlüsseln. Beachten Sie, dass frühere Entschlüsselungs- und Richtlinieninformationen nicht automatisch erneut angewendet werden, wenn Sie den WIP-Schutz wieder aktivieren.

2. Klicken Sie auf **Save**.

Definieren der intern verwalteten Unternehmensidentität

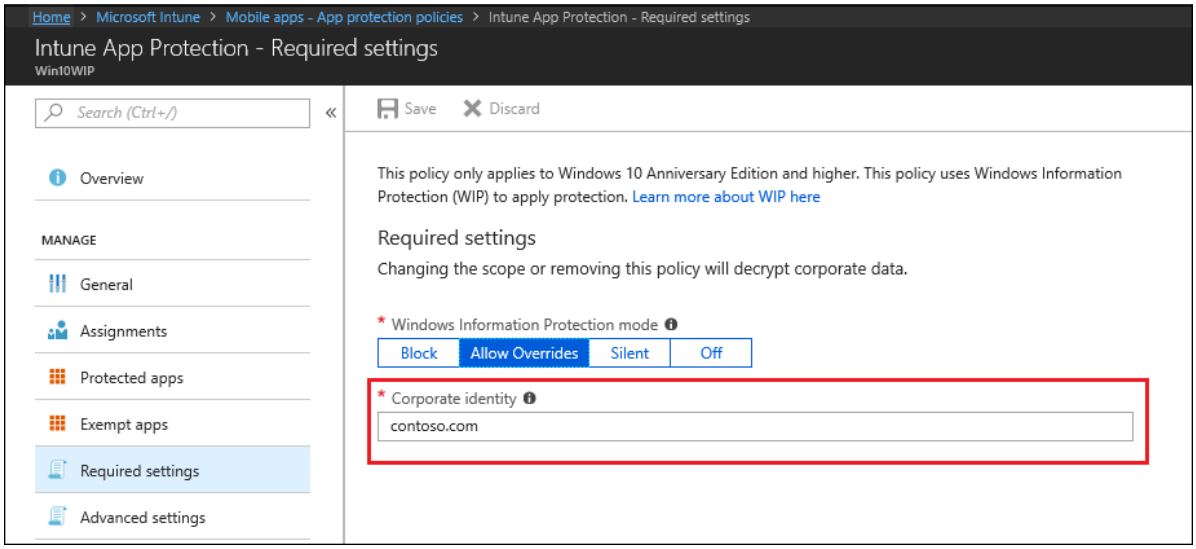
Die Unternehmensidentität, in der Regel Ihre primäre Internetdomäne (z.B. contoso.com), kann zum Identifizieren und Kennzeichnen von Unternehmensdaten von Apps verwendet werden, die Sie als WIP-geschützt gekennzeichnet haben. Beispielsweise werden E-Mails mit contoso.com als Unternehmensdaten gekennzeichnet und durch die Windows Information Protection-Richtlinien eingeschränkt.

Ab Windows10, Version 1703, bestimmt Intune Ihre Unternehmensidentität automatisch und fügt sie dem Feld **Unternehmensidentität** hinzu.

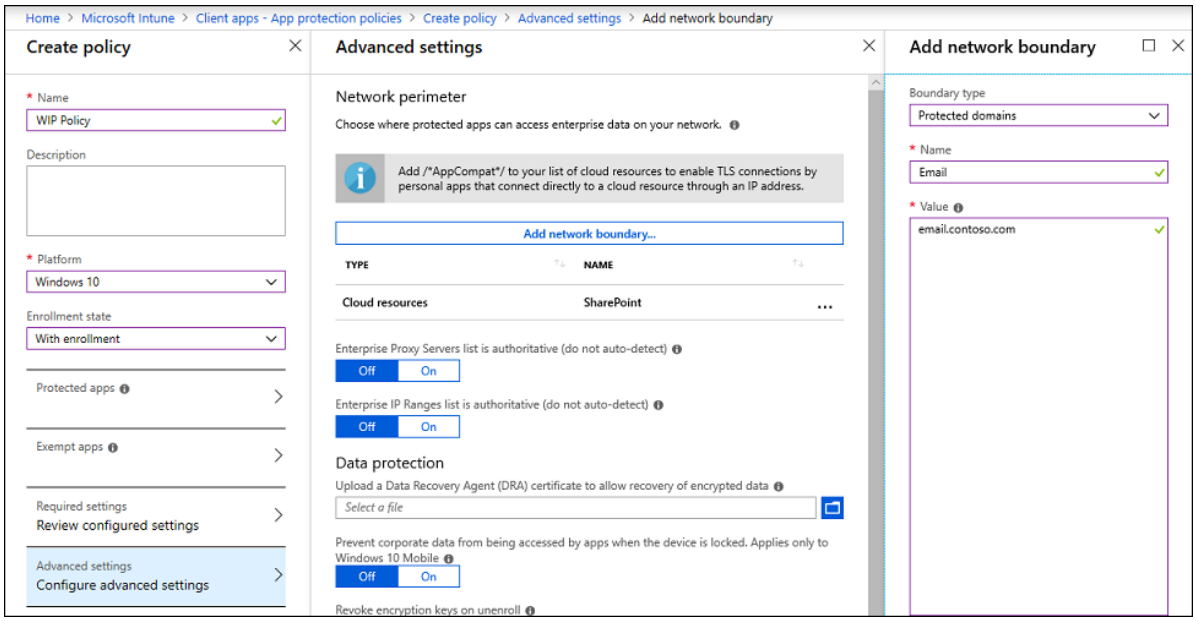
So ändern Sie Ihre Unternehmensidentität

1. Klicken Sie in der **App-Richtlinien** Klinge auf den Namen Ihrer Richtlinie, und klicken Sie dann auf **erforderliche Einstellungen**.

2. Wenn die automatisch definierte Identität falsch ist, können Sie die Informationen im Feld **Unternehmensidentität** ändern.



3. Zum Hinzufügen von Domänen, wie Ihren e-Mail-Domänennamen, klicken Sie auf **Erweiterte Einstellungen** > konfigurieren**Hinzufügen Netzwerkgrenze** , und wählen Sie **geschützte Domänen**aus.

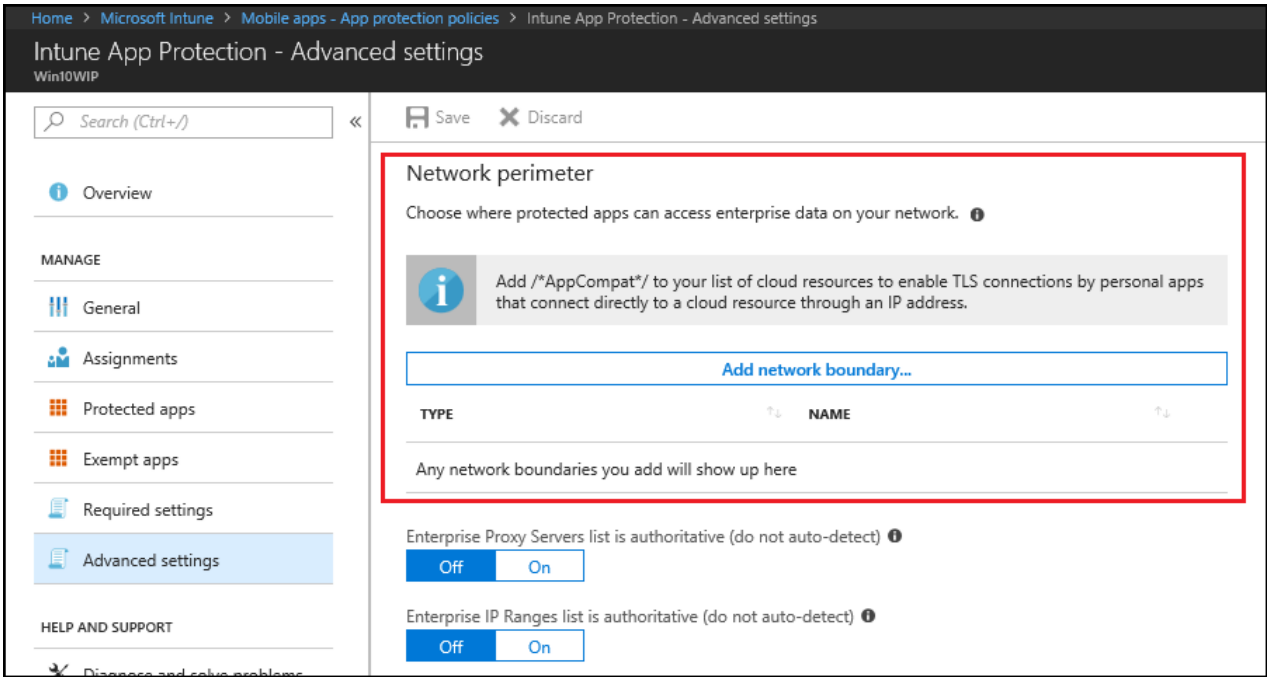


Auswählen der Speicherorte, an denen Apps Zugriff auf Unternehmensdaten haben

Nachdem Sie Ihren Apps einen Schutzmodus hinzugefügt haben, müssen Sie entscheiden, wo diese Apps in Ihrem Netzwerk auf Unternehmensdaten zugreifen können. Jede WIP-Richtlinie sollte Ihre Unternehmensnetzwerk Standorte umfassen.

Es gibt keine in WIP enthaltenen Standardspeicherorte, Sie müssen alle Ihre Netzwerkadressen hinzufügen. Dieser Bereich bezieht sich auf alle Netzwerkendpunkt-Geräte, die eine IP-Adresse im Bereich Ihres Unternehmens abrufen und auch an eine der Unternehmensdomänen gebunden sind, darunter SMB-Freigaben. Speicherorte im lokalen Dateisystem sollten nur die Verschlüsselung verwalten (z.B. auf dem lokalen NTFS, FAT, ExFAT).

Wenn Sie die Netzwerkgrenzen definieren möchten, klicken Sie auf **App-Richtlinie** #a0 den Namen Ihrer Richtlinie #a1 **Erweiterte Einstellungen** > **Netzwerkgrenze hinzufügen**.



Wählen Sie den Typ der Netzwerkgrenze im Feld **Boundary type** aus. Geben Sie einen Namen für ihre Grenze in das Feld **Name** ein, fügen Sie Ihre Werte dem **Wertfeld** entsprechend den in den folgenden Unterabschnitten behandelten Optionen hinzu, und klicken Sie dann auf **OK**.

Cloud-Ressourcen

Geben Sie die Cloudressourcen an, die als unternehmenseigen behandelt und durch WIP geschützt werden sollen. Für jede Cloudressource können Sie optional auch einen Proxyserver aus der Liste der internen Proxyserver angeben, um den Datenverkehr für diese Cloudressource weiterzuleiten. Beachten Sie, dass sämtliche über interne Proxyserver weitergeleiteten Daten als Unternehmensdaten gelten.

Trennen Sie mehrere Ressourcen mit dem Trennzeichen "|". Wenn Sie keine Proxyserver verwenden, müssen Sie auch das Trennzeichen „,“ unmittelbar vor „|“ angeben. Beispiel:

```
URL <,proxy>|URL <,proxy>
```

Persönliche Anwendungen können auf eine Cloud-Ressource zugreifen, die ein Leerzeichen oder ein ungültiges Zeichen enthält, beispielsweise einen nachgestellten Punkt in der URL.

Wenn Sie eine Unterdomäne für eine Cloud-Ressource hinzufügen möchten, verwenden Sie einen Punkt (.) anstelle eines Sternchens (*). Wenn Sie beispielsweise alle Unterdomänen innerhalb von Office.com hinzufügen möchten, verwenden Sie ". Office.com" (ohne die Anführungszeichen).

In einigen Fällen, z.B. wenn eine App über eine IP-Adresse direkt eine Verbindung mit einer Cloudressource herstellt, kann Windows nicht feststellen, ob die App versucht, eine Verbindung mit einer Ressource in der Unternehmenscloud oder mit einer persönlichen Website herzustellen. In diesem Fall wird die Verbindung von Windows standardmäßig blockiert. Um zu verhindern, dass Windows diese Verbindungen automatisch blockiert, fügen Sie der Einstellung die Zeichenfolge `/*AppCompat*/` hinzu. Beispiel:

```
URL <,proxy>|URL <,proxy>/*AppCompat*/
```

Wenn Sie diese Zeichenfolge verwenden, empfehlen wir, dass Sie auch Azure Active Directory-bedingter Zugriffaktivieren, indem Sie die Option **Domäne verbunden oder als kompatibel kennzeichnen** verwenden, die verhindert, dass apps auf Enterprise-Cloud-Ressourcen zugreifen, die durch bedingten Zugriff geschützt sind.

Wert Format mit Proxy:

```
contoso.sharepoint.com,contoso.internalproxy1.com|contoso.visualstudio.com,contoso.internalproxy2.com
```

Wert Format ohne Proxy:

```
contoso.sharepoint.com|contoso.visualstudio.com
```

Geschützte Domänen

Geben Sie die Domänen an, die für Identitäten in Ihrer Umgebung verwendet werden. Der gesamte Datenverkehr zu den vollqualifizierten Domänen, die in dieser Liste enthalten sind, wird geschützt. Trennen Sie mehrere Domänen mit dem Trennzeichen ",".

```
exchange.contoso.com,contoso.com,region.contoso.com
```

Netzwerkdomänen

Geben Sie die in Ihrer Umgebung verwendeten DNS-Suffixe an. Der gesamte Datenverkehr zu den vollqualifizierten Domänen, die in dieser Liste enthalten sind, wird geschützt. Trennen Sie mehrere Ressourcen mit dem Trennzeichen ",".

```
corp.contoso.com,region.contoso.com
```

Proxyserver

Geben Sie die Proxyserver an, die Ihre Geräte durchlaufen, um die Cloudressourcen zu erreichen. Die Verwendung dieses Servertyps gibt an, dass die Cloudressourcen, mit denen Sie eine Verbindung herstellen, Unternehmensressourcen sind.

Diese Liste sollte keine Server aus Ihrer Liste der internen Proxyserver enthalten. Interne Proxyserver dürfen nur für den WIP-geschützten (Unternehmens-)Datenverkehr verwendet werden. Trennen Sie mehrere Ressourcen mit dem Trennzeichen ";".

```
proxy.contoso.com:80;proxy2.contoso.com:443
```

Interne Proxyserver

Geben Sie die internen Proxyserver an, die Ihre Geräte durchlaufen, um die Cloudressourcen zu erreichen. Die Verwendung dieses Servertyps gibt an, dass die Cloudressourcen, mit denen Sie sich verbinden, Unternehmensressourcen sind.

Diese Liste sollte keine Server aus Ihrer Liste der Proxyserver enthalten. Proxyserver dürfen nur für den nicht mit WIP-geschützten (nicht-Unternehmens-)Datenverkehr verwendet werden. Trennen Sie mehrere Ressourcen mit dem Trennzeichen ";".

```
contoso.internalproxy1.com;contoso.internalproxy2.com
```

IPv4-Bereiche

Ab Windows10, Version 1703, ist dieses Feld optional.

Geben Sie die Adressen für einen gültigen IPv4-Wertebereich in Ihrem Intranet an. Diese in Verbindung mit Ihren Netzwerkdomänennamen verwendeten Adressen definieren die Grenzen Ihres Unternehmensnetzwerks. Die CIDR-Notation (klassenübergreifend) wird nicht unterstützt.

Trennen Sie mehrere Bereiche mit dem Trennzeichen ",".

IPv4-Adresse wird gestartet: 3.4.0.1 **Endung der IPv4-Adresse:** 3.4.255.254 **benutzerdefinierter URI:** 3.4.0.1-3.4.255.254,
10.0.0.1-10.255.255.254

IPv6-Bereiche

Ab Windows10, Version 1703, ist dieses Feld optional.

Geben Sie die Adressen für einen gültigen IPv6-Wertebereich in Ihrem Intranet an. Diese Adressen, die in Verbindung mit ihren Netzwerkdomänennamen verwendet werden, definieren die Netzwerkgrenzen Ihres Unternehmens. Die CIDR-Notation (klassenübergreifend) wird nicht unterstützt.

Trennen Sie mehrere Bereiche mit dem Trennzeichen ",".

Starten der IPv6-Adresse: 2a01:110:: **Ending IPv6-Adresse:** 2a01:110:7fff: FFFF: FFFF: FFFF: FFFF: FFFF **benutzerdefinierter URI:** 2a01:110:7fff: FFFF: FFFF: FFFF: FFFF: FFFF;
fd00::-fdff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

Neutrale Ressourcen

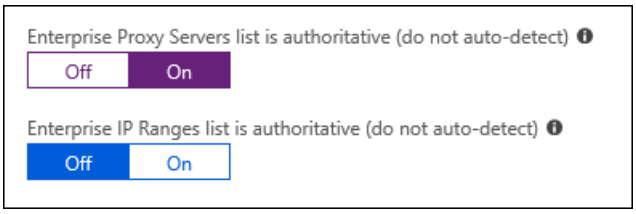
Geben Sie die Endpunkte für die Authentifizierungsumleitung in Ihrem Unternehmen an. Diese Adressen gelten als unternehmenseigen oder persönlich, basierend auf dem Kontext der Verbindung vor der Umleitung. Trennen

Sie mehrere Ressourcen mit dem Trennzeichen ",".

```
sts.contoso.com,sts.contoso2.com
```

Entscheiden Sie, ob Windows nach zusätzlichen Netzwerkeinstellungen suchen soll:

- **Liste der Unternehmensproxyserver ist autoritativ (keine automatische Erkennung).** Aktivieren Sie diese Option, wenn Sie möchten, dass Windows die in der Definition der Netzwerkgrenze angegebenen Proxy Server als vollständige Liste der in Ihrem Netzwerk verfügbaren Proxy Server behandelt. Wenn Sie diese Option deaktivieren, sucht Windows in Ihrem unmittelbaren Netzwerk nach weiteren Proxyservern.
- **Liste der Unternehmens-IP-Bereiche ist autoritativ (keine automatische Erkennung).** Aktivieren Sie diese Option, wenn Windows die IP-Bereiche behandeln soll, die Sie in der Definition der Netzwerkgrenze angegeben haben, als vollständige Liste der IP-Bereiche, die in Ihrem Netzwerk zur Verfügung stehen. Wenn Sie diese Option deaktivieren, sucht Windows nach zusätzlichen IP-Bereichen auf allen von der Domäne verbundenen Geräten, die mit Ihrem Netzwerk verbunden sind.



Hochladen des Datenwiederherstellungs-Agent-Zertifikats

Nachdem Sie die WIP Richtlinie erstellt und für Ihre Mitarbeiter bereitgestellt haben, beginnt Windows mit dem Verschlüsseln der Unternehmensdaten auf dem lokalen Gerätelaufwerk der Mitarbeiter. Wenn aus irgendeinem Grund lokale Verschlüsselungsschlüssel der Mitarbeiter verloren gehen oder widerrufen werden, können die verschlüsselten Daten unter Umständen nicht wiederhergestellt werden. Um dies zu vermeiden, ermöglicht das Data Recovery Agent (DRA)-Zertifikat Windows die Verwendung eines angegebenen öffentlichen Schlüssels zum Verschlüsseln der lokalen Daten, während Sie den privaten Schlüssel verwalten, der die Daten entschlüsseln kann.

> **IMPORTANT**
> Die Verwendung eines DRA-Zertifikats ist nicht obligatorisch. Wir empfehlen dies jedoch dringend. Weitere Informationen zum Suchen und Exportieren des Datenwiederherstellungszertifikats finden Sie im Thema Datenwiederherstellung und verschlüsselndes Dateisystem (EFS). Weitere Informationen zum Erstellen und Überprüfen des EFS DRA-Zertifikats finden Sie im Thema Erstellen und Überprüfen eines DRA-Zertifikats (Data Recovery Agent, Datenwiederherstellungs-Agent) des verschlüsselnden Dateisystems (Encrypting File System, EFS).

So laden Sie Ihr DRA-Zertifikat hoch

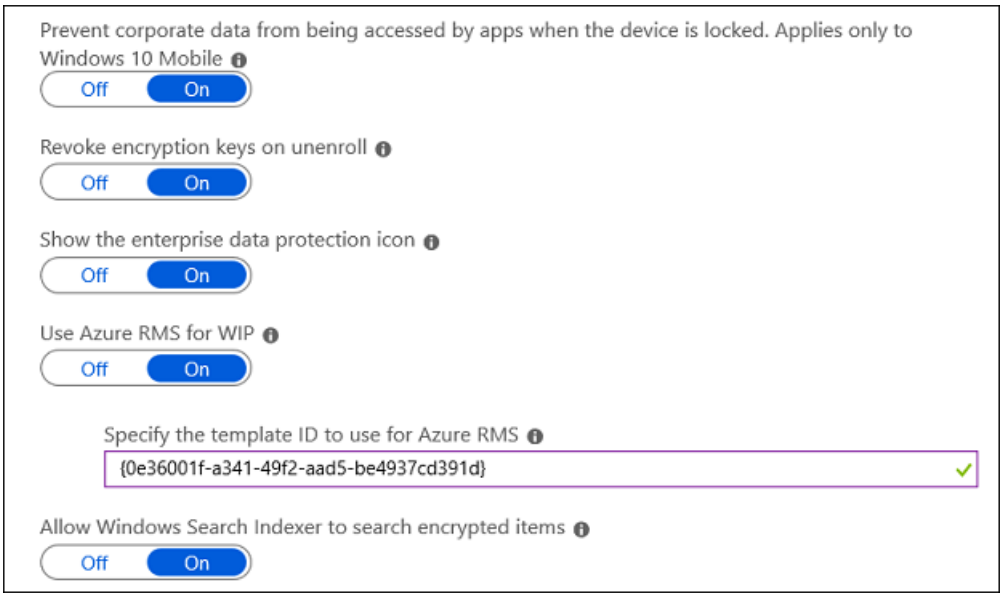
1. Klicken Sie im Blatt **App policy** auf den Namen Ihrer Richtlinie, und dann im neu angezeigten Menü auf **Advanced settings**.

   Das Dialogfeld **Advanced settings** wird angezeigt.

2. Klicken Sie im Feld **Laden Sie ein Datenwiederherstellungs-Agent-Zertifikat hoch, um die Wiederherstellung verschlüsselter Daten zuzulassen** auf **Durchsuchen**, um ein Datenwiederherstellungszertifikat für die Richtlinie hinzuzufügen.

Auswählen der optionalen WIP-bezogenen Einstellungen

Nachdem Sie entschieden haben, wo Ihre geschützten apps auf Unternehmensdaten in Ihrem Netzwerk zugreifen können, können Sie optionale Einstellungen auswählen.



Verhindern Sie, dass Apps auf Unternehmensdaten zugreifen können, wenn das Gerät gesperrt ist. Gilt nur für Windows 10 Mobile. Legt fest, ob Unternehmensdaten mit einem Schlüssel verschlüsselt werden, der durch den PIN-Code eines Mitarbeiters auf einem gesperrten Gerät geschützt ist. Apps können keine Unternehmensdaten lesen, wenn das Gerät gesperrt ist. Die Optionen sind:

- **Ein.** Aktiviert die Funktion und bietet den zusätzlichen Schutz.
- **Aus, oder nicht konfiguriert.** Aktiviert diese Funktion nicht.

Beim Aufheben der Registrierung Verschlüsselungsschlüssel widerrufen. Legt fest, ob die lokalen Verschlüsselungsschlüssel eines Benutzers von einem Gerät widerrufen werden, wenn die Registrierung des Geräts in Windows Information Protection aufgehoben wird. Wenn die Verschlüsselungsschlüssel widerrufen werden, kann ein Benutzer nicht mehr auf verschlüsselte Unternehmensdaten zugreifen. Die Optionen sind:

- **Aus, oder nicht konfiguriert (empfohlen).** Die lokalen Verschlüsselungsschlüssel werden während der Aufhebung der Registrierung von einem Gerät widerrufen.
- **Deaktiviert.** Das Widerrufen lokaler Verschlüsselungsschlüssel von einem Gerät während der Aufhebung der Registrierung wird beendet. Beispiel: Sie migrieren zwischen Lösungen für die mobile Geräteverwaltung (MDM).

Zeigen Sie das Datenschutzsymbol des Unternehmens an. Legt fest, ob die WIP-Symbolüberlagerung (Windows Information Protection) für Unternehmensdateien in der Ansicht „Speichern unter" und im Datei-Explorer angezeigt wird. Die Optionen sind:

- **Ein.** Lässt zu, dass die WIP-Symbolüberlagerung (Windows Information Protection) für Unternehmensdateien in der Ansicht „Speichern unter" und im Datei-Explorer angezeigt wird. Darüber hinaus wird für unaufgeklärte, aber geschützte Apps die Symbolüberlagerung auch auf der APP-Kachel und mit verwaltetem Text im APP-Namen im **Startmenü** angezeigt.
- **Aus, oder nicht konfiguriert (empfohlen).** Verhindert, dass die Windows-Informationsschutz-Symbolüberlagerung auf Unternehmensdateien oder unaufgeklärten, aber geschützten apps angezeigt wird. Die Standardoption ist „Nicht konfiguriert".

Verwenden Sie Azure RMS für WIP. Bestimmt, ob WIP die Microsoft Azure-Rechteverwaltung verwendet, um EFS-Verschlüsselung auf Dateien anzuwenden, die von Windows 10 auf USB oder andere Wechseldatenträger

kopiert werden, damit Sie von den Mitarbeitern sicher freigegeben werden können. Mit anderen Worten: WIP verwendet die Azure Rights Management-"Maschinerie", um die EFS-Verschlüsselung auf Dateien anzuwenden, wenn Sie auf Wechseldatenträger kopiert werden. Sie müssen bereits Azure Rights Management eingerichtet haben. Der EFS-Dateiverschlüsselungsschlüssel ist durch die Lizenz der RMS-Vorlage geschützt. Nur Benutzer, die über die Berechtigung für diese Vorlage verfügen, können Sie über das Wechsellaufwerk lesen. WIP kann auch in Azure RMS mithilfe der **AllowAzureRMSForEDP** -und **RMSTemplateIDForEDP** -MDM-Einstellungen im EnterpriseDataProtection-CSPintegriert werden.

- **Ein.** Schützt Dateien, die auf ein Wechsellaufwerk kopiert werden. Sie können eine GUID für die Vorlagen-GUID eingeben, um anzugeben, wer auf die Azure Rights Management-geschützten Dateien zugreifen kann, und wie lange. Die RMS-Vorlage wird nur auf die Dateien auf Wechselmedien angewendet, und Sie wird nur für die Zugriffssteuerung verwendet – es wird nicht wirklich Azure Information Protection auf die Dateien angewendet. Um die RMS- {} Vorlagen-ID sind geschweifte Klammern erforderlich, die aber nach dem Speichern der Richtlinie entfernt werden.

  Wenn Sie keine RMS- Vorlageangeben, handelt es sich um eine reguläre EFS-Datei, die eine standardmäßige RMS-Vorlage verwendet, auf die alle Benutzer zugreifen können.

- **Aus, oder nicht konfiguriert.** Stoppt WIP, um Azure Rights Management-Dateien zu verschlüsseln, die auf ein Wechsellaufwerk kopiert werden.

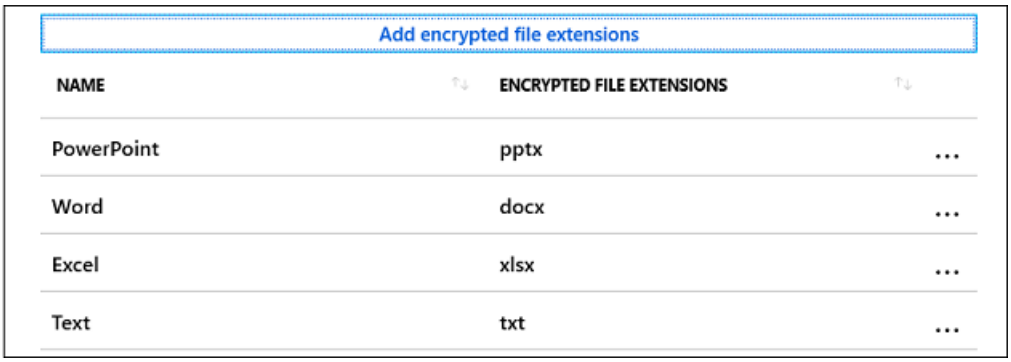
> **NOTE**
> Unabhängig von dieser Einstellung werden alle Dateien in OneDrive for Business verschlüsselt, einschließlich verschobener bekannter Ordner.

Windows Search-Indexer können verschlüsselte Dateien durchsuchen. Bestimmt, ob der Windows Search-Indexer Elemente indizieren kann, die verschlüsselt sind, beispielsweise WIP-geschützte Dateien.

- **Ein.** Startet den Windows Search-Indexer, um verschlüsselte Dateien zu indizieren.
- **Aus, oder nicht konfiguriert.** Verhindert, dass der Windows Search-Indexer verschlüsselte Dateien indiziert.

Verschlüsselte Dateierweiterungen

Sie können einschränken, welche Dateien durch WIP geschützt werden, wenn Sie von einer SMB-Freigabe innerhalb ihrer Unternehmensnetzwerk Speicherorte heruntergeladen werden. Wenn diese Einstellung konfiguriert ist, werden nur Dateien mit den Erweiterungen in der Liste verschlüsselt. Wenn diese Einstellung nicht angegeben wird, wird das vorhandene Verhalten der automatischen Verschlüsselung angewendet.



Verwandte Themen

- Sammeln von Windows Information Protection (WIP)-Überwachungsprotokollen

- Allgemeiner Leitfaden und bewährte Methoden für Windows Information Protection (WIP)
- Was ist Azure Rights Management?
- Erstellen und Bereitstellen von Windows Information Protection (WIP)-App-Schutz-Richtlinien mit Intune und MAM
- Intune MAM ohne Registrierung
- Azure RMS-Dokumentationsupdate für Mai 2016

> **NOTE**
> Tragen Sie dazu bei, dieses Thema zu verbessern, indem Sie uns Bearbeitungen, Ergänzungen und Feedback schicken. Informationen dazu, wie Sie zu diesem Thema beitragen können, finden Sie unter Bearbeiten der Windows IT Professional-Dokumentation.

Bereitstellen der Windows Information Protection-Richtlinie (WIP) mithilfe des Azure-Portals für Microsoft Intune

12.09.2019 • 2 minutes to read

Betrifft:

- Windows10, Version 1607 und höher
- Windows10 Mobile, Version 1607 und höher (mit Ausnahme von Microsoft Azure Rights Management, das nur auf dem Desktop verfügbar ist)

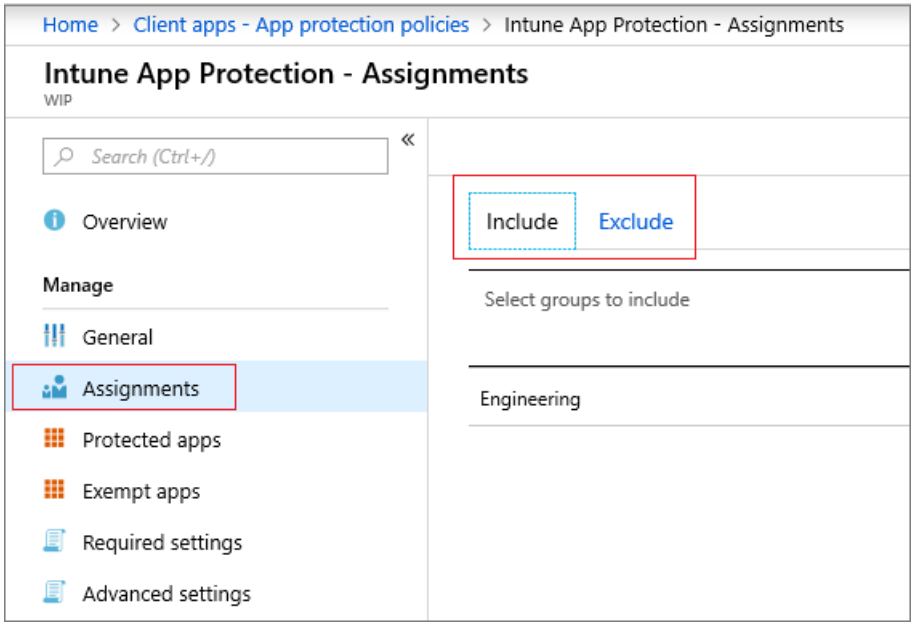
Nachdem Sie die Windows Information Protection (WIP)-Richtlinie erstellt haben, müssen Sie sie auf den in Ihrer Organisation registrierten Geräten bereitstellen. Die Registrierung kann für Unternehmensgeräte oder persönliche Geräte erfolgen. Dadurch können die Geräte Ihre verwalteten Apps verwenden und die Synchronisierung mit Ihren verwalteten Inhalten und Informationen vornehmen.

So stellen Sie Ihre WIP-Richtlinie bereit

1. Klicken Sie im Bereich **App-Schutzrichtlinien** auf Ihre neu erstellte Richtlinie, klicken Sie auf **Aufgaben**, und wählen Sie dann Gruppen aus, die Sie in die Richtlinie einbeziehen oder ausschließen möchten.

2. Wählen Sie die Gruppe aus, für die Sie Ihre Richtlinie anwenden möchten, und klicken Sie auf **Auswählen**, um die Richtlinie bereitzustellen.

   Die Richtlinie wird auf den Geräten der ausgewählten Benutzer bereitgestellt.



NOTE

Tragen Sie dazu bei, dieses Thema zu verbessern, indem Sie uns Bearbeitungen, Ergänzungen und Feedback schicken. Informationen dazu, wie Sie zu diesem Thema beitragen können, finden Sie unter Bearbeiten der Windows IT Professional-Dokumentation.

Verwandte Themen

- Allgemeiner Leitfaden und bewährte Methoden für Windows Information Protection (WIP)

Zuordnen und Bereitstellen einer VPN-Richtlinie für Windows Information Protection (WIP) mithilfe des Azure-Portals für Microsoft Intune

24.12.2019 • 2 minutes to read

Betrifft:

- Windows10, Version 1607 und höher
- Windows10 Mobile, Version 1607 und höher (mit Ausnahme von Microsoft Azure Rights Management, das nur auf dem Desktop verfügbar ist)

Nachdem Sie die Windows Information Protection (WIP)-Richtlinie erstellt und bereitgestellt haben, können Sie mithilfe von Microsoft Intune die Virtual Private Network (VPN)-Richtlinie zuordnen und bereitstellen und mit der WIP-Richtlinie verknüpfen.

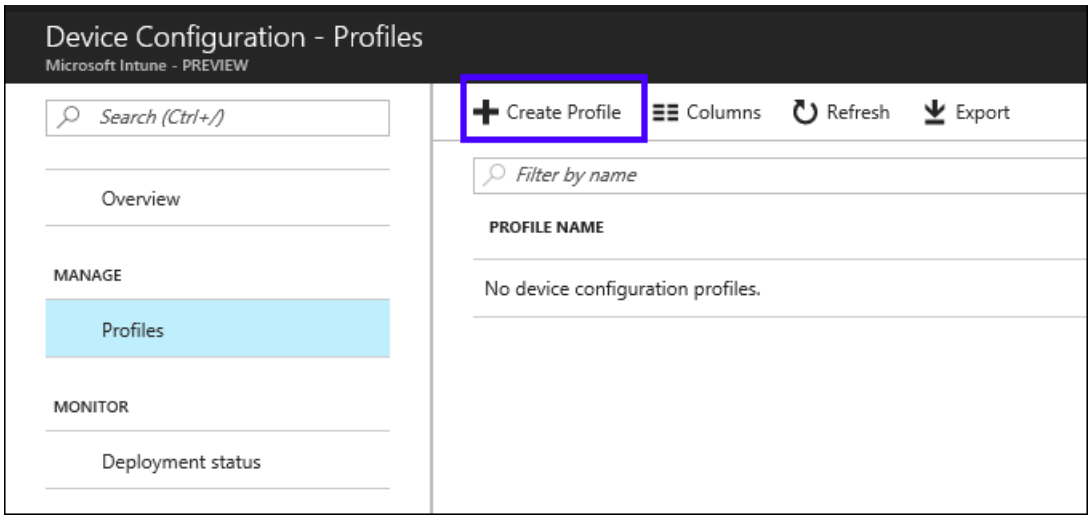
Zuordnen der WIP-Richtlinie zur VPN-Richtlinie mithilfe von Microsoft Intune

Führen Sie diese Schritteaus, um Ihre WIP-Richtlinie zur vorhandenen VPN-Richtlinie Ihrer Organisation zuzuordnen.

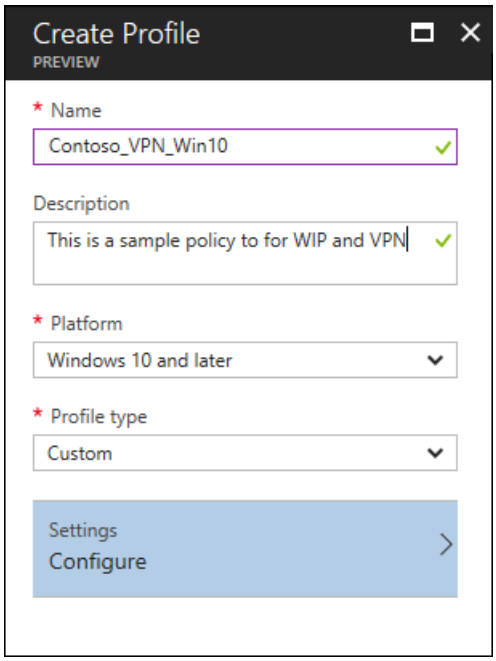
So verknüpfen Sie Ihre Richtlinien

1. Erstellen Sie Ihr VPN-Profil. Informationen hierzu finden Sie unter Konfigurieren von VPN-Einstellungen in Microsoft Intune und Erstellen von benutzerdefinierten VPN-Profilen in Microsoft Intune.

2. Öffnen die Microsoft Intune-Konsole für die mobile Anwendungsverwaltung, und klicken Sie auf **Gerätekonfiguration** und dann auf **Profil erstellen**.



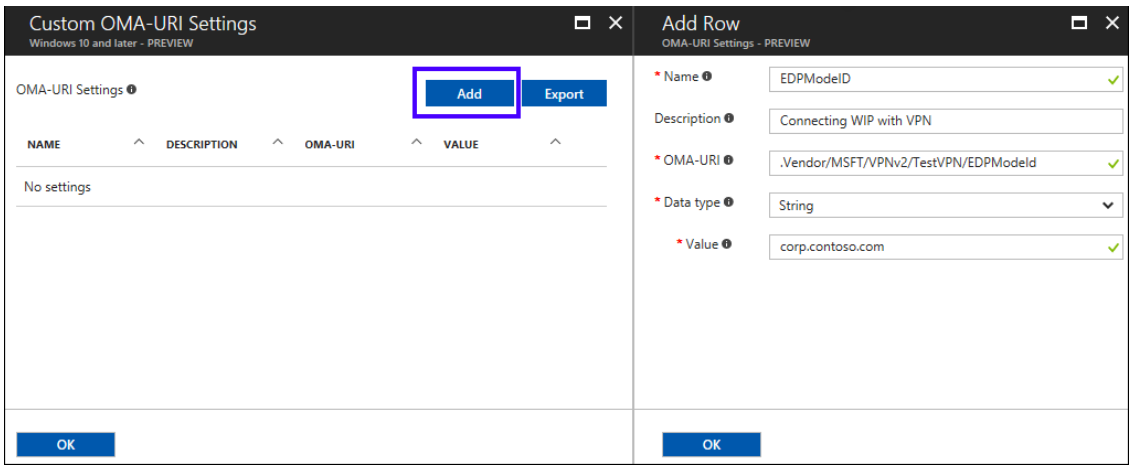
3. Geben Sie im Blatt **Profil erstellen** einen Namen für Ihr Profil, z.B. *Contoso_VPN_Win10*, in das Feld **Name** ein, geben Sie eine optionale Beschreibung für Ihre Richtlinie in das Feld **Beschreibung** ein, wählen Sie **Windows10 und höher** im Dropdownfeld **Plattform** aus, wählen Sie **Benutzerdefiniert** im Dropdownfeld **Profiltyp** aus, und klicken Sie auf **Konfigurieren**.



4. Klicken Sie im Blatt **Benutzerdefinierte OMA-URI-Einstellungen** auf **Hinzufügen**.

5. Geben Sie im Blatt **Zeile hinzufügen** Folgendes ein:

   - **Name.** Geben Sie einen Namen für die Einstellung ein, z.B. *EDPModeID*.
   - **Beschreibung.** Geben Sie eine optionale Beschreibung für Ihre Einstellung ein.
   - **OMA-URI.** Geben Sie *./Vendor/MSFT/VPNv2/<VPNProfileName>/EDPModeId* in das Feld ein.
   - **Datentyp.** Wählen Sie die Option **Zeichenfolge** in der Dropdownliste aus.
   - **Wert.** Geben Sie Ihre vollqualifizierte Domäne ein, die die OMA-URI-Einstellung verwenden soll. Zum Beispiel: *corp.contoso.com*.



6. Klicken Sie auf **OK**, um Ihre Einstellungsinformationen im Blatt **Zeile hinzufügen** zu speichern, und klicken Sie auf **OK** im Blatt **Benutzerdefinierte OMA-URI-Einstellungen**, um die Einstellung zusammen mit Ihrer Richtlinie zu speichern.

7. Klicken Sie auf **Erstellen**, um die Richtlinie, einschließlich der OMA_URI-Informationen, zu erstellen.

Bereitstellen der VPN-Richtlinie mithilfe von Microsoft Intune

Nachdem Sie die VPN-Richtlinie erstellt haben, müssen Sie sie für dieselbe Gruppe wie die Windows Information Protection-Richtlinie (WIP) bereitstellen.

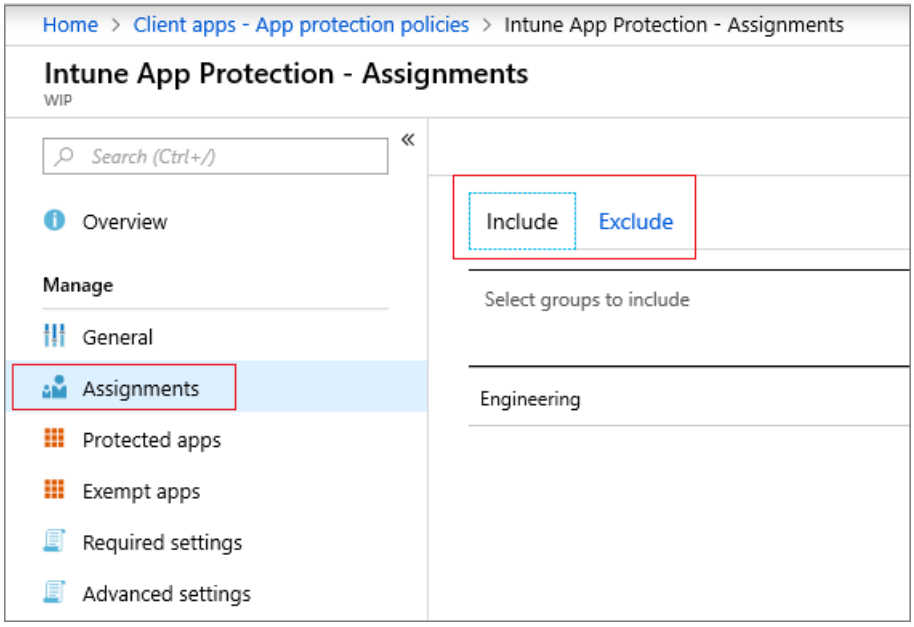
So stellen Sie Ihre benutzerdefinierte VPN-Richtlinie bereit

1. Klicken Sie im Blatt **App-Richtlinie** auf die neu erstellte Richtlinie, klicken Sie im neu angezeigten Menü auf **Benutzergruppen**, und klicken Sie dann auf **Benutzergruppe hinzufügen**.

   Eine Liste der Benutzergruppen, bestehend aus allen Sicherheitsgruppen in Ihrem Azure Active Directory, wird im Blatt **Benutzergruppe hinzufügen** angezeigt.

2. Wählen Sie die Gruppe aus, für die Sie Ihre Richtlinie anwenden möchten, und klicken Sie auf **Auswählen**, um die Richtlinie bereitzustellen.

   Die Richtlinie wird auf den Geräten der ausgewählten Benutzer bereitgestellt.



NOTE

Tragen Sie dazu bei, dieses Thema zu verbessern, indem Sie uns Bearbeitungen, Ergänzungen und Feedback schicken. Informationen dazu, wie Sie zu diesem Thema beitragen können, finden Sie unter Bearbeiten der Windows IT Professional-Dokumentation.

Erstellen und Überprüfen eines Datenwiederherstellungs-Agent-Zertifikats des verschlüsselnden Dateisystems (Encrypting File System, EFS)

11.02.2020 • 6 minutes to read

Gilt für:

- Windows10, Version 1607 und höher
- Windows10 Mobile, Version 1607 und höher

Wenn Sie nicht bereits über ein EFS DRA-Zertifikat verfügen, müssen Sie ein Zertifikat erstellen und aus dem System extrahieren, bevor Sie Windows Information Protection (WIP) (früher als Unternehmensdatenschutz (EDP) bezeichnet) in Ihrer Organisation verwenden können. Für die Zwecke dieses Abschnitts verwenden wir den Dateinamen EFSDRA. Dieser Name kann jedoch durch einen für Sie sinnvollen Namen ersetzt werden.

Der in diesem Thema enthaltene Wiederherstellungsprozess funktioniert nur für Desktopgeräte. WIP löscht die Daten auf Windows10 Mobile-Geräten.

> **IMPORTANT**
>
> Wenn Sie bereits über ein EFS DRA-Zertifikat für Ihre Organisation verfügen, können Sie das Erstellen eines neuen Zertifikats überspringen. Verwenden Sie einfach Ihr aktuelles EFS DRA-Zertifikat in der Richtlinie. Weitere Informationen dazu, wann Sie eine PKI und die allgemeine Strategie zum Bereitstellen von DRA-Zertifikaten verwenden, finden Sie im Artikel Sicherheit auf dem Prüfstand Bereitstellen von EFS: Teil 1 bei TechNet. Allgemeine Informationen zum EFS-Schutz finden Sie unter Schützen von Daten mit EFS zum Verschlüsseln von Festplatten.
>
> Wenn Ihr DRA-Zertifikat abgelaufen ist, können Sie damit keine Dateien verschlüsseln. Um dieses Problem zu beheben, müssen Sie ein neues Zertifikat mithilfe der Schritte in diesem Thema erstellen und dann durch Richtlinien bereitstellen.

Manuelles Erstellen eines EFS-DRA-Zertifikats

1. Öffnen Sie auf einem Computer ohne installiertes EFS DRA-Zertifikat eine Eingabeaufforderung mit erhöhten Rechten, und navigieren Sie zu dem Speicherort, an dem das Zertifikat gespeichert werden soll.

2. Führen Sie folgenden Befehl aus:

   ```
   cipher /r:EFSRA
   ```

   Dabei ist *EFSRA* der Name der CER- und PFX-Datei, die Sie erstellen möchten.

3. Geben Sie bei Aufforderung ein Kennwort zum Schutz der neuen Personal Information Exchange-Datei (.pfx) ein, und bestätigen Sie dieses.

   Die Dateien EFSDRA.cer und EFSDRA.pfx werden an dem Speicherort erstellt, den Sie in Schritt1 angegeben haben.

> **IMPORTANT**
> Da die privaten Schlüssel in den DRA PFX-Dateien zum Entschlüsseln aller WIP-Dateien verwendet werden können, müssen sie entsprechend geschützt werden. Es wird dringend empfohlen, diese Dateien offline zu speichern und dabei Kopien auf einer Smartcard mit starkem Schutz zur normalen Nutzung und Masterkopien an einem sicheren physischen Speicherort beizubehalten.

4. Fügen Sie Ihr EFS-DRA-Zertifikat mit einem Bereitstellungstool wie Microsoft InTune oder Microsoft Endpoint Configuration Managerzu ihrer WIP-Richtlinie hinzu.

> **NOTE**
> Dieses Zertifikat kann in InTune für Richtlinien sowohl *mit* der Geräteregistrierung (MDM) als auch *ohne* Geräteregistrierung (MAM) verwendet werden.

Überprüfen, ob Ihr Datenwiederherstellungszertifikat auf einem WIP-Clientcomputer ordnungsgemäß eingerichtet ist

1. Suchen oder erstellen Sie eine mit Windows Information Protection verschlüsselte Datei. Sie können z.B. eine App in der Liste der zulässigen Apps öffnen und dann eine Datei erstellen und speichern, damit sie mit WIP verschlüsselt wird.

2. Öffnen Sie eine App in der Liste der geschützten Apps, und erstellen und speichern Sie dann eine Datei, damit sie mit WIP verschlüsselt wird.

3. Öffnen Sie eine Eingabeaufforderung mit erhöhten Rechten, navigieren Sie zu dem Speicherort, an dem Sie die gerade erstellte Datei gespeichert haben, und führen Sie folgenden Befehl aus:

   ```
   cipher /c filename
   ```

   Dabei ist *filename* der Name der Datei, die Sie in Schritt1 erstellt haben.

4. Stellen Sie sicher, dass das Datenwiederherstellungszertifikat in der Liste **Wiederherstellungszertifikate** aufgeführt ist.

Wiederherstellen Ihrer Daten mithilfe des EFS-DRA-Zertifikats in einer Testumgebung

1. Kopieren Sie die WIP-verschlüsselte Datei an einen Speicherort, für den Sie Administratorzugriff haben.

2. Installieren Sie die Datei EFSDRA.pfx unter Verwendung des Kennworts.

3. Öffnen Sie eine Eingabeaufforderung mit erhöhten Rechten, navigieren Sie zu der verschlüsselten Datei, und führen Sie folgenden Befehl aus:

   ```
   cipher /d encryptedfile.extension
   ```

   Dabei ist *encryptedfile.extension* der Name der verschlüsselten Datei. Beispiel: corporatedata.docx.

Wiederherstellung von WIP-Protected nach der Registrierung

Unter Umständen widerrufen Sie Daten von einem nicht registrierten Gerät, nur um sie später alle wiederherstellen zu wollen. Dies kann passieren, wenn ein fehlendes Gerät zurückgegeben wird oder wenn sich ein nicht registrierter Mitarbeiter erneut registriert. Wenn sich der Mitarbeiter erneut mit dem ursprünglichen Benutzerprofil anmeldet und der gesperrte Schlüsselspeicher weiterhin auf dem Gerät gespeichert ist, können alle

gesperrten Daten gleichzeitig wiederhergestellt werden.

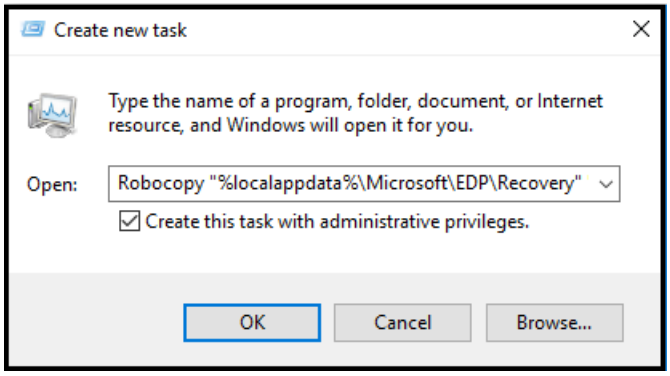
> **IMPORTANT**
> Um die Kontrolle über die Unternehmensdaten zu behalten und in Zukunft erneut widerrufen zu können, müssen Sie nur den folgenden Vorgang durchführen, nachdem der Mitarbeiter das Gerät erneut registriert hat.

1. Melden Sie sich beim Mitarbeiter des nicht registrierten Geräts an, öffnen Sie eine Eingabeaufforderung mit erhöhten Rechten, und geben Sie Folgendes ein:

   ```
   Robocopy "%localappdata%\Microsoft\EDP\Recovery" "new_location" * /EFSRAW
   ```

   Wobei sich "*new_location*" in einem anderen Verzeichnis befindet. Dies kann auf dem Gerät des Mitarbeiters oder in einem freigegebenen Ordner auf einem Computer erfolgen, auf dem Windows 8 oder Windows Server 2012 oder höher ausgeführt wird und auf die Sie zugreifen können, während Sie als Daten Wiederherstellungs-Agent angemeldet sind.

   Öffnen Sie den Task-Manager, um Robocopy im S-Modus zu starten. Klicken Sie auf**neue Aufgabe Datei** > ausführen, geben Sie den Befehl ein, und klicken Sie auf **diese Aufgabe mit Administratorrechten erstellen**.

   Wenn der Mitarbeiter eine Neuinstallation durchgeführt hat und kein Benutzerprofil vorhanden ist, müssen Sie die Schlüssel aus dem Ordner "System Volume" auf jedem Laufwerk wiederherstellen. Typ:

   ```
   Robocopy "drive_letter:\System Volume Information\EDP\Recovery" "new_location" * /EFSRAW
   ```

2. Melden Sie sich an einem anderen Gerät mit Administratoranmeldeinformationen mit Zugriff auf das DRA-Zertifikat Ihrer Organisation an, und führen Sie die Entschlüsselung und Wiederherstellung der Datei durch, indem Sie Folgendes eingeben:

   ```
   cipher.exe /D "new_location"
   ```

3. Lassen Sie Ihren Mitarbeiter sich am nicht registrierten Gerät anmelden, und geben Sie Folgendes ein:

   ```
   Robocopy "new_location" "%localappdata%\Microsoft\EDP\Recovery\Input"
   ```

4. Bitten Sie den Mitarbeiter, das Gerät zu sperren und zu entsperren.

   Der Windows-Dienst für Anmeldeinformationen stellt die zuvor gesperrten Schlüssel des Mitarbeiters aus dem `Recovery\Input`-Speicherort automatisch wieder her.

Automatische Wiederherstellung von Verschlüsselungsschlüsseln

WIP enthält ab Windows10, Version 1709, eine Datenwiederherstellungsfunktion, die Ihren Mitarbeitern eine automatische Wiederherstellung des Zugriff auf die Arbeitsdateien ermöglichen, wenn der Verschlüsselungsschlüssel verloren geht und auf die Dateien nicht mehr zugegriffen werden kann. Dies erfolgt in der Regel dann, wenn ein Mitarbeiter ein Re-Imaging der Betriebssystempartition durchführt, die WIP-

Schlüsselinformationen entfernt oder ein Gerät als verloren meldet und versehentlich das falsche Gerät für die Deregistrierung verwendet.

Um sicherzustellen, dass Mitarbeiter immer auf Dateien zugreifen können, erstellt WIP einen automatischen Wiederherstellungsschlüssel, der in der Identität des Azure Active Directory (Azure AD) gesichert ist.

Die Erfahrung der Mitarbeiter hängt von der Anmeldung auf dem Azure AD-Geschäftskonto ab. Der Mitarbeiter kann:

- Fügen Sie ein Geschäftskontos über das Menü **Windows-Einstellungen > Konten > Geschäfts- oder Schulkonto öffnen > Verbinden** hinzu.

  – ODER –

- Öffnen Sie **Windows-Einstellungen > Konten > Geschäfts- oder Schulkonto öffnen > Verbinden**, und wählen Sie den Link **Dieses Gerät in Azure Active Directory einbinden** unter **alternative Aktionen**.

  > **NOTE**
  > Um einer Azure AD-Domäne von der Seite "Einstellungen" beizutreten, muss der Mitarbeiter auf dem Gerät Administratorrechte haben.

Nach der Anmeldung wird die erforderliche WIP-Schlüssel-Informationen automatisch heruntergeladen und Mitarbeiter können auf die Dateien erneut zugreifen.

Testen Sie, was der Mitarbeiter während des WIP-Schlüssel-Wiederherstellungsprozesses sieht

1. Versuchen Sie, eine Arbeitsdatei auf einem nicht registrierten Gerät zu öffnen.

   Das Feld **Verbinden mit Ihrem Arbeitsplatz, um auf Arbeitsdateien zuzugreifen** wird angezeigt.

2. Klicken Sie auf **Verbinden**.

   Die Seite **Auf Arbeits- oder Schulkonto zugreifen** wird angezeigt.

3. Melden Sie sich bei Azure AD als Mitarbeiter an und stellen Sie sicher, dass Sie die Dateien jetzt öffnen können

Verwandte Themen

- Sicherheit auf dem Prüfstand – Bereitstellen von EFS: Teil 1
- Schützen von Daten durch Verschlüsseln von Festplatten mit EFS
- Erstellen einer Windows Information Protection (WIP)-Richtlinie mithilfe von Microsoft Intune
- Erstellen einer Windows Information Protection (WIP)-Richtlinie mit Microsoft Endpoint Configuration Manager
- Erstellen eines domänenbasierten Wiederherstellungs-Agents

> **NOTE**
> Tragen Sie dazu bei, dieses Thema zu verbessern, indem Sie uns Bearbeitungen, Ergänzungen und Feedback schicken. Weitere Informationen zur Teilnahme an diesem Thema finden Sie unter Zu diesem Artikel beitragen.

Ermitteln des Unternehmenskontexts einer App, die in Windows Information Protection ausgeführt wird

12.09.2019 • 2 minutes to read

Betrifft:

- Windows10, Version 1607 und höher
- Windows10 Mobile, Version 1607 und höher

> Unter Vergleichen von Windows10-Editionen erfahren Sie, welche Features und Funktionen von den einzelnen Windows-Editionen unterstützt werden.

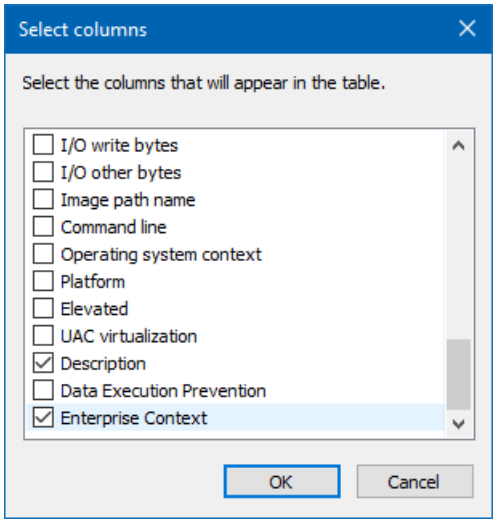
Verwenden Sie Task-Manager, um den Kontext Ihrer Apps während der Ausführung in Windows Information Protection (WIP) zu überprüfen und sicherzustellen, dass die Richtlinien Ihres Unternehmens angewendet und ordnungsgemäß ausgeführt werden.

Anzeigen der Unternehmenskontextspalte im Task-Manager

Sie müssen die Unternehmenskontextspalte der Registerkarte **Details** im Task-Manager hinzufügen.

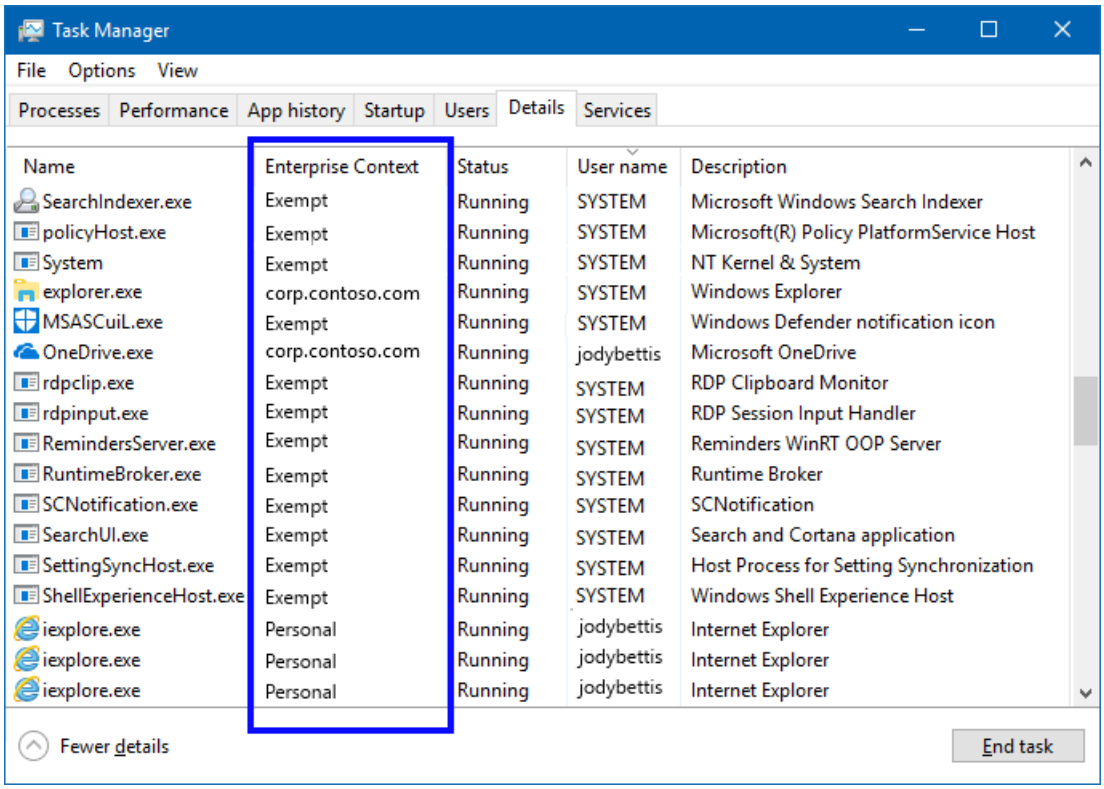
1. Stellen Sie sicher, dass Sie eine aktive WIP-Richtlinie bereitgestellt und in Ihrer Organisation aktiviert haben.
2. Öffnen Sie den Task-Manager (taskmgr.exe), klicken Sie auf die Registerkarte **Details**, klicken Sie mit der rechten Maustaste in den Bereich der Spaltenüberschrift, und klicken Sie auf **Spalten auswählen**.

   Das Feld **Spalten auswählen** wird angezeigt.

3. Führen Sie einen Bildlauf nach unten aus, und aktivieren Sie die Option für den **Unternehmenskontext**, und klicken Sie dann auf **OK**, um das Dialogfeld zu schließen.

   Die Spalte **Unternehmenskontext** sollte nun im Task-Manager verfügbar sein.



Überprüfen des Unternehmenskontexts

Die Spalte **Unternehmenskontext** zeigt, wie die einzelnen Apps Ihre Unternehmensdaten nutzen können:

- **Domäne.** Zeigt die Arbeitsdomänen des Mitarbeiters (z.B. corp.contoso.com). Diese App gilt als geschäftliche und kann ungehindert auf Arbeitsdaten und -ressourcen zugreifen und diese öffnen.
- **Persönlich.** Zeigt den Text *Persönlich*. Diese App wird als nicht geschäftlich eingestuft und kann nicht auf Arbeitsdaten oder -ressourcen zugreifen.
- **Ausnahme.** Zeigt den Text *Ausnahme*. WIP-Richtlinien gelten nicht für diese Apps (z.B. Systemkomponenten).

> **Wichtig**
> Optimierte Apps können zwischen „Geschäftlich" und „Persönlich" wechseln, abhängig von den Daten, auf die zugegriffen wird. Microsoft Word 2016 wird z.B. als **Persönlich** angezeigt, wenn ein Mitarbeiter einen persönlichen Brief öffnet. Das Programm wird zu **Geschäftlich**, wenn derselbe Mitarbeiter die Finanzdaten des Unternehmens öffnet.

Erstellen einer Windows Information Protection (WIP)-Richtlinie mit Microsoft Endpoint Configuration Manager

11.02.2020 • 2 minutes to read

Betrifft

- Windows10, Version 1607 und höher
- Windows10 Mobile, Version 1607 und höher

Microsoft Endpoint Configuration Manager unterstützt Sie beim Erstellen und Bereitstellen Ihrer WIP-Richtlinie (Enterprise Data Protection), einschließlich der Auswahl ihrer geschützten apps, ihrer WIP-Schutzebene und der Suche nach Unternehmensdaten im Netzwerk.

Inhalt dieses Abschnitts

THEMA	BESCHREIBUNG
Erstellen und Bereitstelleneiner Windows Information Protection (WIP)-Richtlinie mit Microsoft Endpoint Configuration Manager	Microsoft Endpoint Configuration Manager unterstützt Sie beim Erstellen und Bereitstellen Ihrer WIP-Richtlinie, einschließlich der Auswahl ihrer geschützten apps, ihrer WIP-Schutzebene und der Suche nach Unternehmensdaten im Netzwerk.
Erstellen und Überprüfen eines DRA-Zertifikats (Data Recovery Agent, Datenwiederherstellungsagent) des verschlüsselnden Dateisystems (Encrypting File System, EFS)	Schritte zum Erstellen, Überprüfen und zur schnellen Wiederherstellung mithilfe eines DRA-Zertifikats (Data Recovery Agent, Datenwiederherstellungs-Agent) des verschlüsselnden Dateisystems (Encrypting File System, EFS).
Ermitteln des Unternehmenskontexts einer App, die in Windows Information Protection ausgeführt wird	Verwenden Sie den Task-Manager, um zu bestimmen, ob eine App als geschäftliche oder private App gilt oder ob sie von Windows Information Protection (WIP) ausgeschlossen ist.

Erstellen und Bereitstelleneiner Windows Information Protection (WIP)-Richtlinie mit Microsoft Endpoint Configuration Manager

11.02.2020 • 20 minutes to read

Betrifft:

- Windows10, Version1607 und höher
- Windows10 Mobile, Version1607, und höher
- Microsoft Endpoint Configuration Manager

Microsoft Endpoint Configuration Manager unterstützt Sie beim Erstellen und Bereitstellen Ihrer Windows Information Protection (WIP)-Richtlinie, einschließlich der Auswahl ihrer geschützten apps, Ihres WIP-Schutzmodus und der Suche nach Unternehmensdaten im Netzwerk.

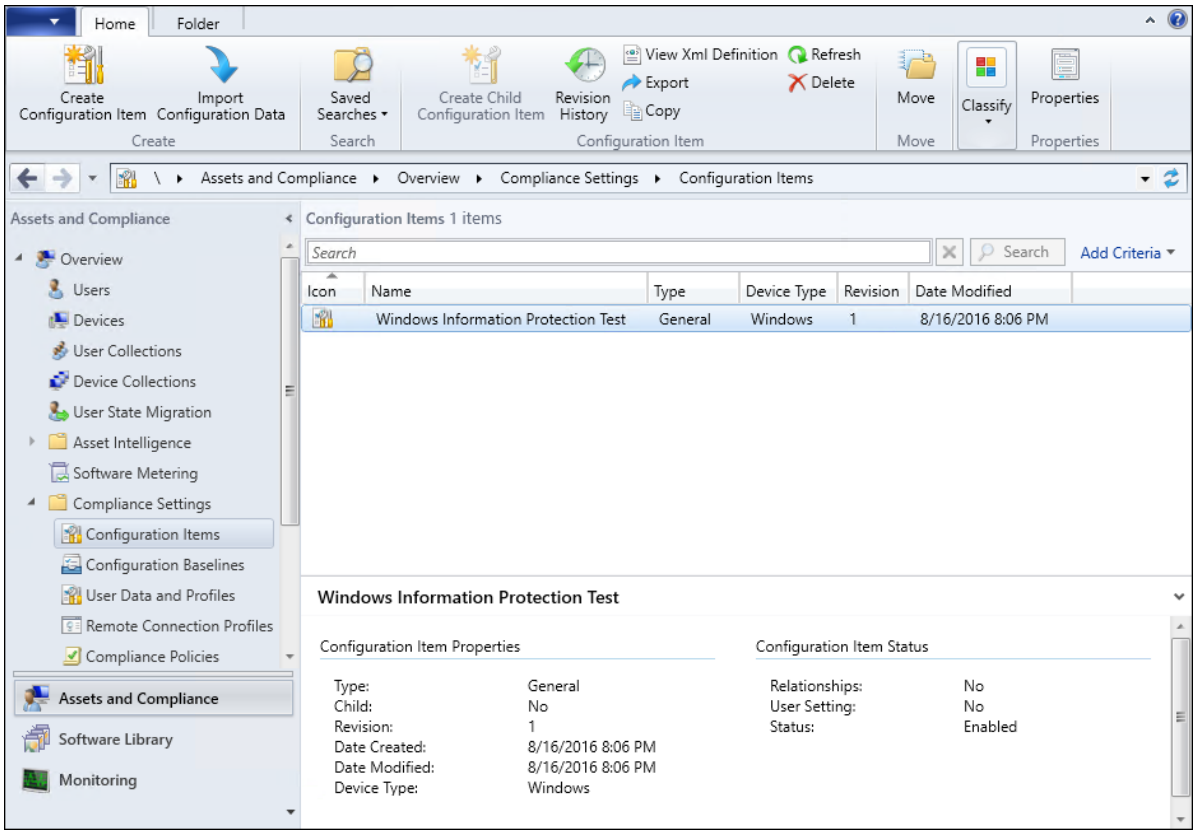
Hinzufügen einer WIP-Richtlinie

Nachdem Sie Configuration Manager für Ihre Organisation installiert und eingerichtet haben, müssen Sie ein Konfigurationselement für WIP erstellen, das ihrerseits zur WIP-Richtlinie wird.

> **TIP**
> Überprüfen Sie die Einschränkungen bei der Verwendung des Windows Information Protection (WIP)- Artikels, bevor Sie ein neues Konfigurationselement erstellen, um häufige Probleme zu vermeiden.

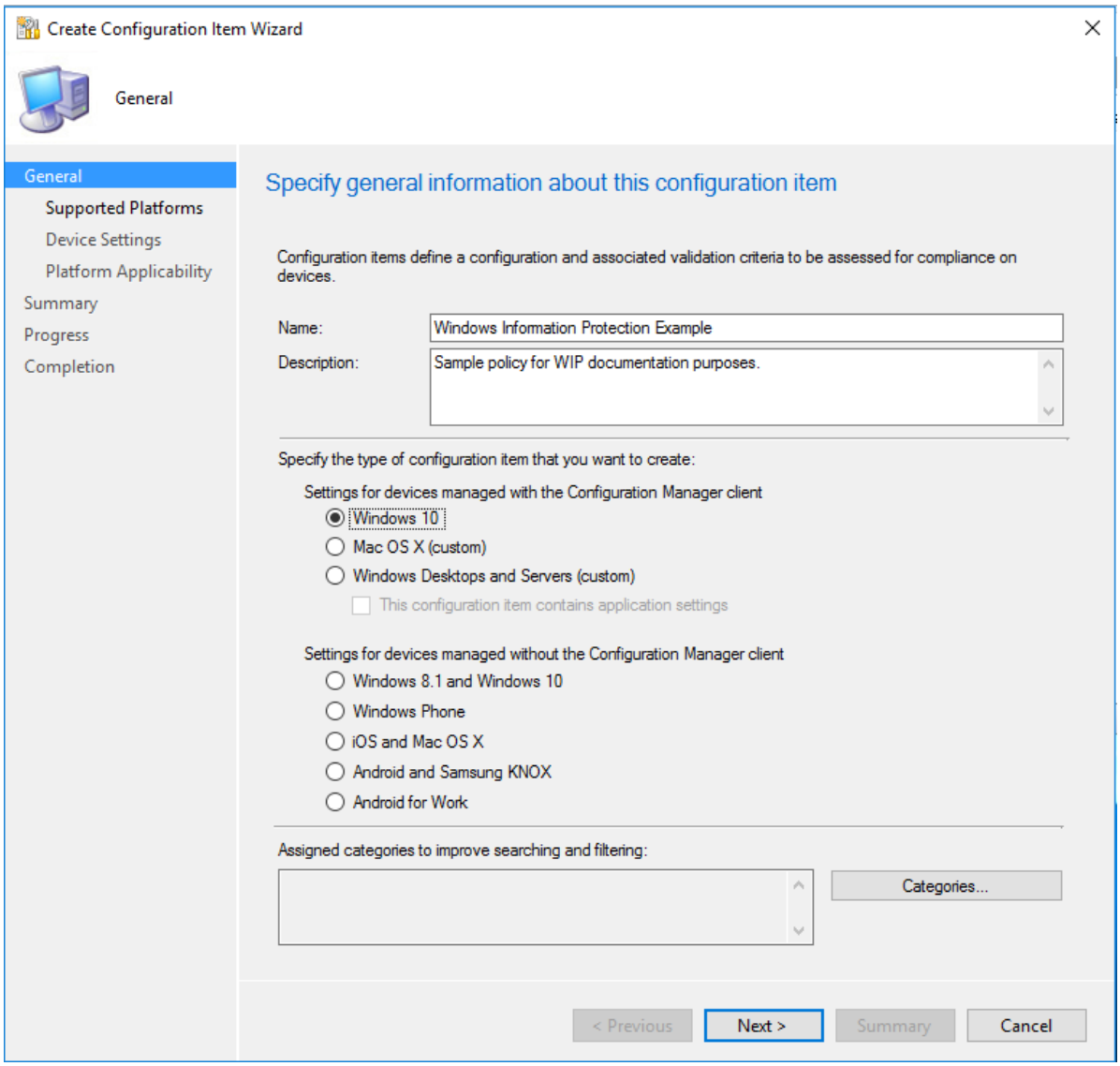
So erstellen Sie ein Konfigurationselement für WIP

1. Öffnen Sie die Configuration Manager-Konsole, klicken Sie auf den Knoten **Ressourcen und Kompatibilität** , erweitern Sie den Knoten **Übersicht** , erweitern Sie den Knoten **Konformitäts Einstellungen** , und erweitern Sie dann den Knoten **Konfigurationselemente** .



2. Klicken Sie auf die Schaltfläche **Konfigurationselement erstellen** .

   Der **Assistent zum Erstellen von Konfigurationselementen** wird gestartet.



3. Geben Sie auf dem Bildschirm **Allgemeine Informationen**einen Namen (erforderlich) und eine optionale Beschreibung für die Richtlinie in die Felder **Name** und **Beschreibung** ein.

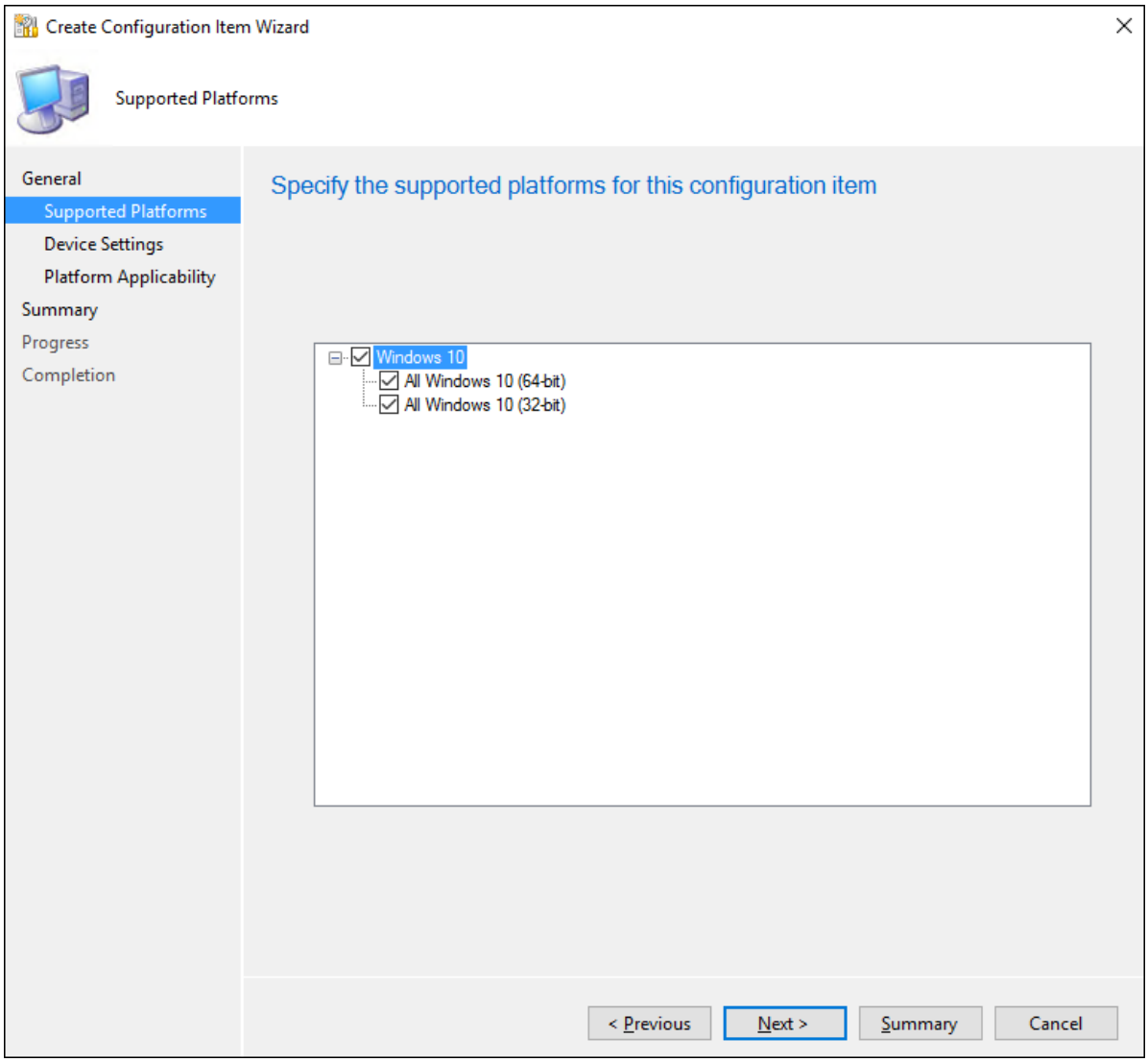
4. Wählen Sie im Bereich **Geben Sie den Typ des zu erstellenden Konfigurationselements an** die Option aus, die darstellt, ob Sie den Microsoft Endpoint Configuration Manager für die Geräteverwaltung verwenden, und klicken Sie dann auf **weiter**.

   - **Einstellungen für mit dem Konfigurations-Manager-Client verwaltete Geräte:** Windows10

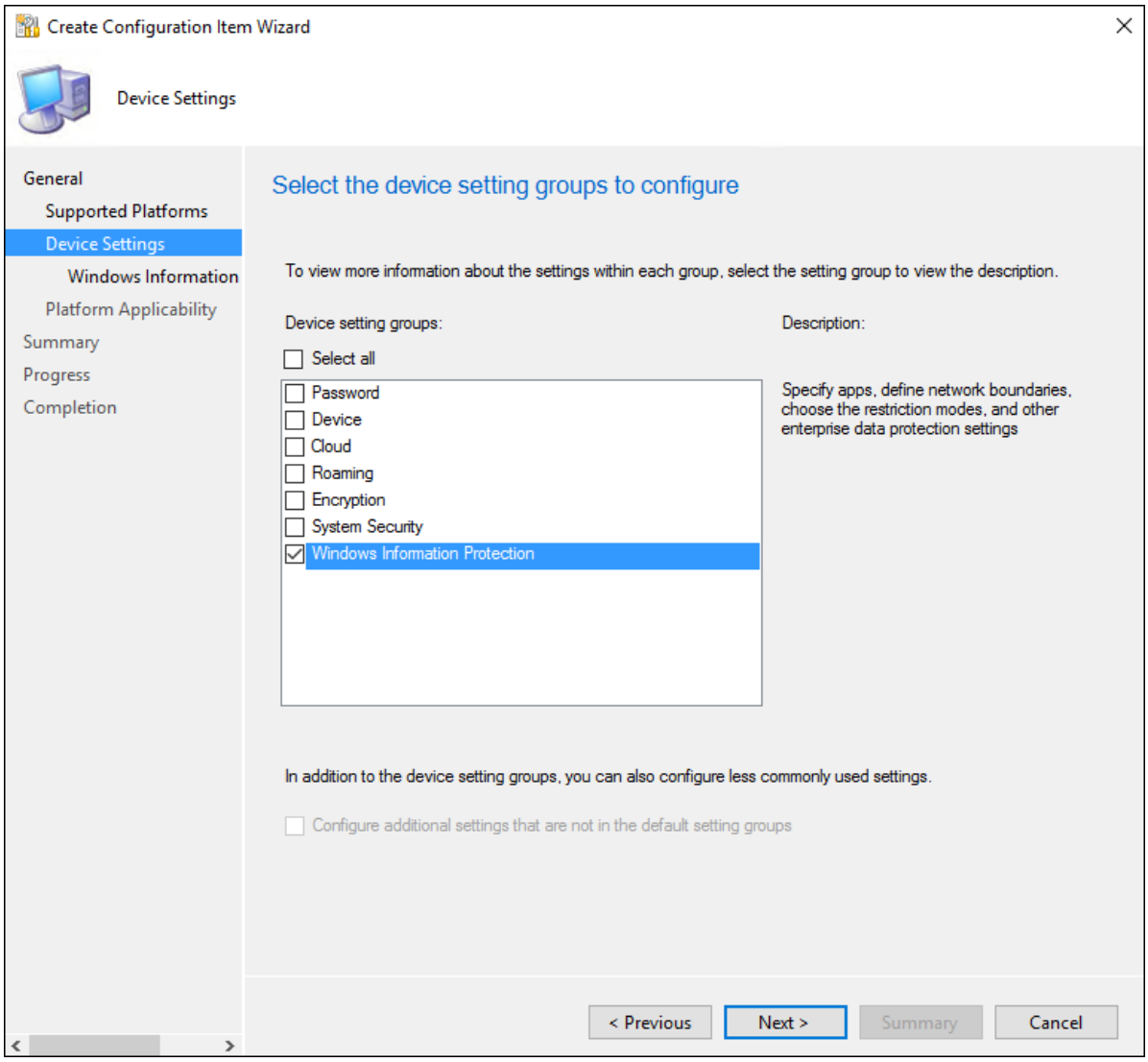
     -oder-

   - **Einstellungen für ohne den Konfigurations-Manager-Client verwaltete Geräte:** Windows8.1 und Windows10

5. Klicken Sie auf dem Bildschirm **Unterstützte Plattformen** auf das Feld **Windows 10**, und klicken Sie dann auf **Weiter**.



6. Klicken Sie auf dem Bildschirm **Geräteeinstellungen** auf **Windows Information Protection**, und klicken Sie dann auf **Weiter**.



Die Seite **Configure Windows Information Protection settings** wird angezeigt. Hier konfigurieren Sie die Richtlinie für Ihre Organisation.

Hinzufügen von App-Regeln zur Richtlinie

Während des Prozesses zur Richtlinienerstellung in Microsoft Endpoint Configuration Manager können Sie die apps auswählen, die Sie über WIP auf Ihre Unternehmensdaten zugreifen möchten. In dieser Liste enthaltene App können Daten im Namen des Unternehmens schützen und können Unternehmensdaten nicht an ungeschützte Apps kopieren oder verschieben.

Die Schritte zum Hinzufügen der App-Regeln basieren auf dem Typ der angewendeten Regelvorlage. Sie können eine Store-App (wird auch als Universelle Windows-Plattform (UWP)-App bezeichnet), eine signierte Windows-Desktop-App oder eine AppLocker-Richtliniendatei hinzufügen.

> **IMPORTANT**
>
> Optimierte Apps sollten verhindern, dass Unternehmensdaten an ungeschützte Netzwerkadressen gesendet werden, und vermeiden, dass persönliche Daten verschlüsselt werden. Andererseits berücksichtigen nicht mit WIP geschützte Apps unter Umständen nicht die Netzwerkgrenze und verschlüsseln alle Dateien, die sie erstellen oder ändern. Dies bedeutet, dass sie persönliche Daten verschlüsseln und Datenverluste während des Sperrvorgangs verursachen könnten.
>
> Achten Sie beim Abrufen einer Supportzusage vom Softwareanbieter darauf, dass dessen App mit WIP gesichert ist, bevor Sie sie der Liste **App-Regeln** hinzufügen. Wenn Sie diese Zusage nicht abrufen, ist es möglich, dass App-Kompatibilitätsprobleme auftreten, da eine App nach der Sperrung nicht auf eine erforderliche Datei zugreifen kann.

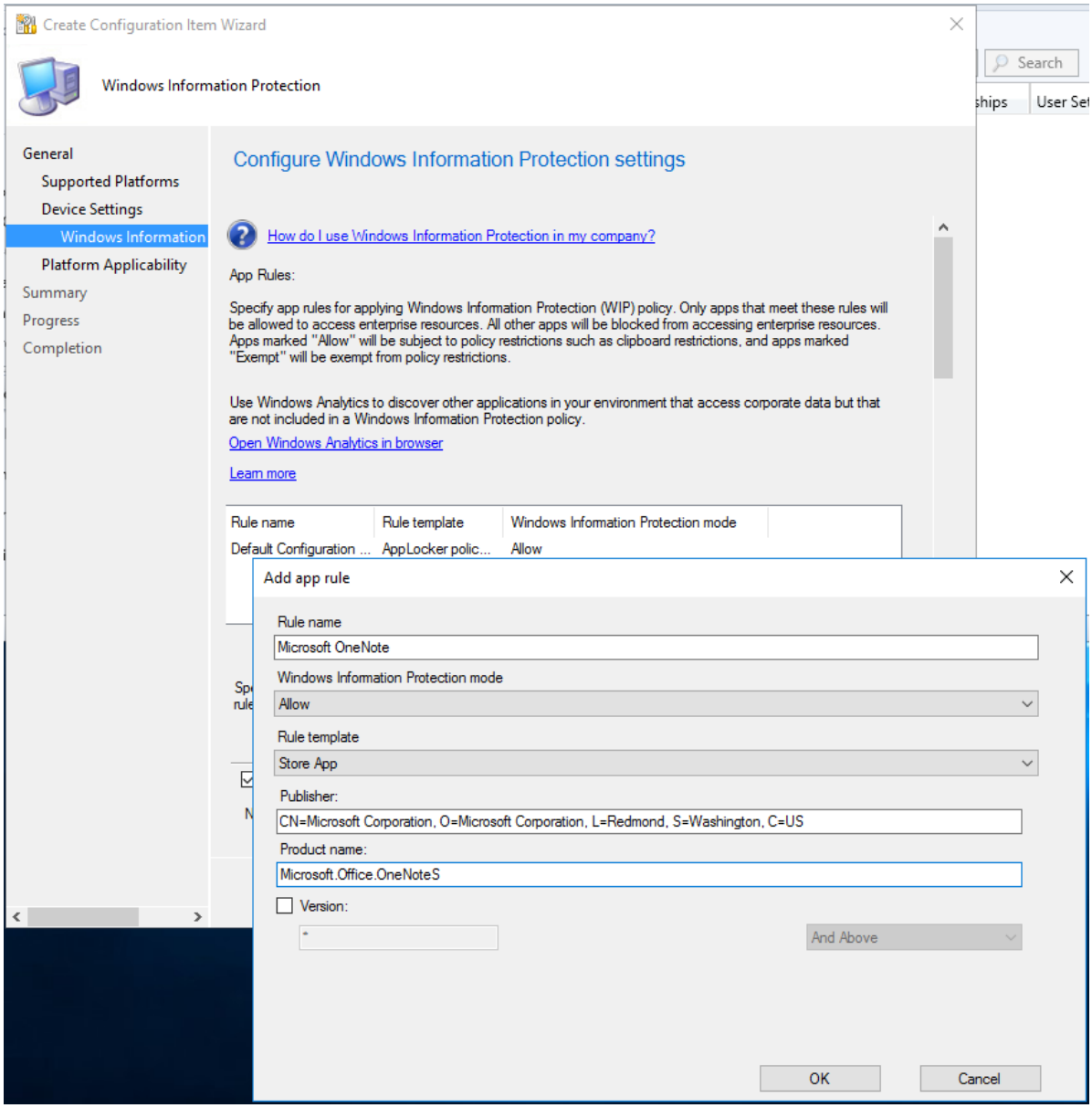
Hinzufügen einer Store-App-Regel zur Richtlinie

In diesem Beispiel fügen wir Microsoft OneNote, eine Store-App, der Liste **App-Regeln** hinzu.

So fügen Sie eine Store-App hinzu

1. Klicken Sie im Bereich **App-Regeln** auf **Hinzufügen**.

   Das Feld **App-Regel hinzufügen** wird angezeigt.



2. Fügen Sie einen Anzeigenamen für die App im Feld **Titel** ein. In diesem Beispiel ist der Name *Microsoft OneNote*.

3. Klicken Sie in der Dropdownliste **WIP-Modus (Windows Information Protection)** auf **Zulassen**.

   Lassen Sie das Aktivieren von WIP zu, um Unternehmensdaten dieser App durch die Durchsetzung von WIP-Einschränkungen zu schützen. Wenn Sie eine App ausnehmen möchten, können Sie die Schritte im Abschnitt Ausnehmen von Apps aus WIP-Einschränkungen ausführen.

4. Wählen Sie **Store-App** in der Dropdownliste **Regelvorlage** aus.

   Im Feld werden nun die Store-App-Regeloptionen angezeigt.

5. Geben Sie den Namen der App und den Namen des Herausgebers ein, und klicken Sie auf **OK**. In diesem Beispiel einer UWP-App ist `CN=Microsoft Corporation, O=Microsoft Corporation, L=Redmond, S=Washington, C=US` der **Herausgeber**, und

der **Produktname** ist `Microsoft.Office.OneNote`.

Wenn Sie den Namen des Herausgebers oder Produkts nicht kennen, können Sie ihn für Desktopgeräte und Windows10-Mobiltelefone durch folgende Schritte herausfinden.

So finden Sie den Herausgeber- und Produktnamen für Store-Apps heraus, ohne diese zu installieren

1. Wechseln Sie zur Website Microsoft Store für Unternehmen, und suchen Sie Ihre App. Beispiel: Microsoft OneNote.

   > **NOTE**
   > Wenn Ihre App bereits auf Desktopgeräten installiert ist, können Sie über das MMC-Snap-In „Lokale Sicherheitsrichtlinie" von AppLocker die Informationen zum Hinzufügen der App zur Liste der geschützten Apps sammeln. Informationen hierzu finden Sie in den Schritten im Abschnitt Hinzufügen einer AppLocker-Richtliniendatei.

2. Kopieren Sie den ID-Wert aus der App-URL. Beispielsweise ist https://www.microsoft.com/store/apps/onenote/9wzdncrfhvjldie ID-URL von Microsoft OneNote, und Sie möchten den ID-Wert `9wzdncrfhvjl` kopieren.

3. Führen Sie in einem Browser die Web-API im Microsoft Store für Unternehmen-Portal aus, um eine JavaScript Object Notation (JSON)-Datei zurückzugeben, die die Werte für den Herausgeber- und Produktnamen enthält. Beispiel: Run https://bspmts.mp.microsoft.com/v1/public/catalog/Retail/Products/9wzdncrfhvjl/applockerdata, where `9wzdncrfhvjl` wird durch ihren ID-Wert ersetzt.

   Die API führt einen Text-Editor aus und öffnet diesen mit allen App-Details.

   ```
   {
   "packageIdentityName": "Microsoft.Office.OneNote",
   "publisherCertificateName": "CN=Microsoft Corporation, O=Microsoft Corporation, L=Redmond,
S=Washington, C=US"
   }
   ```

4. Kopieren Sie den Wert `publisherCertificateName`, und fügen Sie ihn in das Feld **Herausgebername** ein. Kopieren Sie den Wert `packageIdentityName` in das Feld **Produktname** von Intune.

   > **IMPORTANT**
   > Die JSON-Datei kann auch einen Wert `windowsPhoneLegacyId` für die Felder **Herausgebername** und **Produktname** zurückgeben. Dies bedeutet, dass Sie über eine App verfügen, die ein XAP-Paket verwendet, und dass Sie den **Produktnamen** als `windowsPhoneLegacyId` und den **Herausgebernamen** als „CN=" gefolgt von `windowsPhoneLegacyId` festlegen müssen.
   >
   > Beispiel:
   >
   > ```
   > {
   > "windowsPhoneLegacyId": "ca05b3ab-f157-450c-8c49-a1f127f5e71d",
   > }
   > ```

So finden Sie den Herausgeber- und Produktnamen für auf Windows10-Mobiltelefonen installierte Apps

1. Wenn Sie mobile Apps hinzufügen müssen, die nicht über den Microsoft Store für Unternehmen verteilt werden, müssen Sie das Feature **Windows Device Portal** verwenden.

> **NOTE**
> Ihr PC und Telefon müssen im selben drahtlosen Netzwerk sein.

2. Wechseln Sie auf dem Windows Phone zu **Einstellungen**, wählen Sie **Update und Sicherheit**, und wählen Sie dann **Für Entwickler**.
3. Aktivieren Sie auf dem Bildschirm **Für Entwickler** den **Entwicklermodus**, aktivieren Sie **Gerätesuche**, und aktivieren Sie dann **Geräteportal**.
4. Kopieren Sie die URL im Bereich **Geräteportal** in den Browser Ihres Geräts, und akzeptieren Sie dann das SSL-Zertifikat.
5. Drücken Sie im Bereich **Geräteerkennung** auf **Koppeln**, und geben Sie dann die PIN der Website aus dem vorherigen Schritt ein.
6. Auf der **Apps**-Registerkarte der Website sehen Sie die Details für die ausgeführten Apps, einschließlich der Herausgeber- und Produktnamen.
7. Starten Sie die App, für die Sie die Werte der Herausgeber- und Produktnamen suchen.
8. Kopieren Sie den Wert `publisherCertificateName`, und fügen Sie ihn in das Feld **Herausgebername** und den Wert `packageIdentityName` in das Feld **Produktname** von Intune ein.

> **IMPORTANT**
> Die JSON-Datei kann auch einen Wert `windowsPhoneLegacyId` für die Felder **Herausgebername** und **Produktname** zurückgeben. Dies bedeutet, dass Sie über eine App verfügen, die ein XAP-Paket verwendet, und dass Sie den **Produktnamen** als `windowsPhoneLegacyId` und den **Herausgebernamen** als „CN=“ gefolgt von `windowsPhoneLegacyId` festlegen müssen. Beispiel:
>
> ```
> {
>  "windowsPhoneLegacyId": "ca05b3ab-f157-450c-8c49-a1f127f5e71d",
> }
> ```

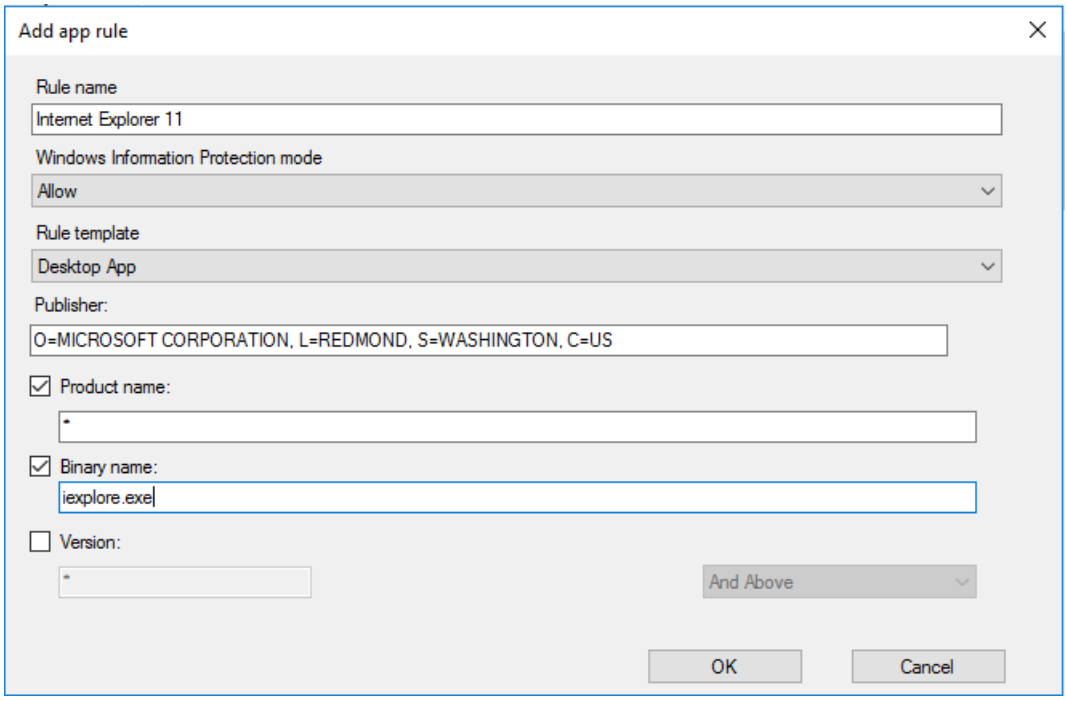
Hinzufügen einer Desktop-App-Regel zur Richtlinie

In diesem Beispiel fügen wir Internet Explorer, eine Desktop-App, der Liste **App-Regeln** hinzu.

So fügen Sie eine Desktop-App zur Richtlinie hinzu

1. Klicken Sie im Bereich **App-Regeln** auf **Hinzufügen**.

   Das Feld **App-Regel hinzufügen** wird angezeigt.



2. Fügen Sie einen Anzeigenamen für die App im Feld **Titel** ein. In diesem Beispiel ist der Name *Internet Explorer*.

3. Klicken Sie in der Dropdownliste **WIP-Modus (Windows Information Protection)** auf **Zulassen**.

   Lassen Sie das Aktivieren von WIP zu, um Unternehmensdaten dieser App durch die Durchsetzung von WIP-Einschränkungen zu schützen. Wenn Sie eine App ausnehmen möchten, können Sie die Schritte im Abschnitt Ausnehmen von Apps aus WIP-Einschränkungen ausführen.

4. Wählen Sie **Desktop-App** in der Dropdownliste **Regelvorlage** aus.

   Im Feld werden nun die Desktop-App-Regeloptionen angezeigt.

5. Wählen Sie die Optionen aus, die in der App-Regel enthalten sein sollen (siehe Tabelle), und klicken Sie auf **OK**.

OPTION	VERWALTET
Alle als „*“ belassene Felder	Alle von einem Herausgeber signierten Dateien. (Nicht empfohlen.)
Herausgeber ausgewählt	Alle vom benannten Herausgeber signierten Dateien. Dies kann nützlich sein, wenn Ihr Unternehmen der Herausgeber und Signaturgeber interner Branchen Apps ist.
Herausgeber und **Produktname** ausgewählt	Alle Dateien für das angegebene Produkt, die vom benannten Herausgeber signiert sind.
Herausgeber, **Produktname** und **Name der Binärdatei** ausgewählt	Alle Versionen der benannten Datei oder des Pakets für das angegebene Produkt, die vom benannten Herausgeber signiert sind.

Herausgeber, **Produktname**, **Name der Binärdatei** und **File Version, and above** ausgewählt	Angegebene Version oder neuere Versionen der benannten Datei oder des Pakets für das angegebene Produkt, die vom benannten Herausgeber signiert sind. Diese Option wird für optimierte Apps empfohlen, die zuvor nicht optimiert wurden.
Herausgeber, **Produktname**, **Name der Binärdatei** und **File Version, And below** ausgewählt	Angegebene Version oder ältere Versionen der benannten Datei oder des Pakets für das angegebene Produkt, die vom benannten Herausgeber signiert sind.
Herausgeber, **Produktname**, **Name der Binärdatei** und **File Version, Exactly** ausgewählt	Die angegebene Version der benannten Datei oder des Pakets für das angegebene Produkt, die vom benannten Herausgeber signiert ist.

Wenn Sie nicht sicher sind, was Sie für den Herausgeber angeben sollen, können Sie den folgenden PowerShell-Befehl ausführen:

```
Get-AppLockerFileInformation -Path "<path of the exe>"
```

Dabei gibt `"<path of the exe>"` den Speicherort der App auf dem Gerät an. Beispiel: `Get-AppLockerFileInformation -Path "C:\Program Files\Internet Explorer\iexplore.exe"`.

In diesem Beispiel erhalten Sie die folgenden Informationen:

```
Path                   Publisher
----                   ---------
%PROGRAMFILES%\INTERNET EXPLORER\IEXPLORE.EXE O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US\INTERNET
EXPLOR...
```

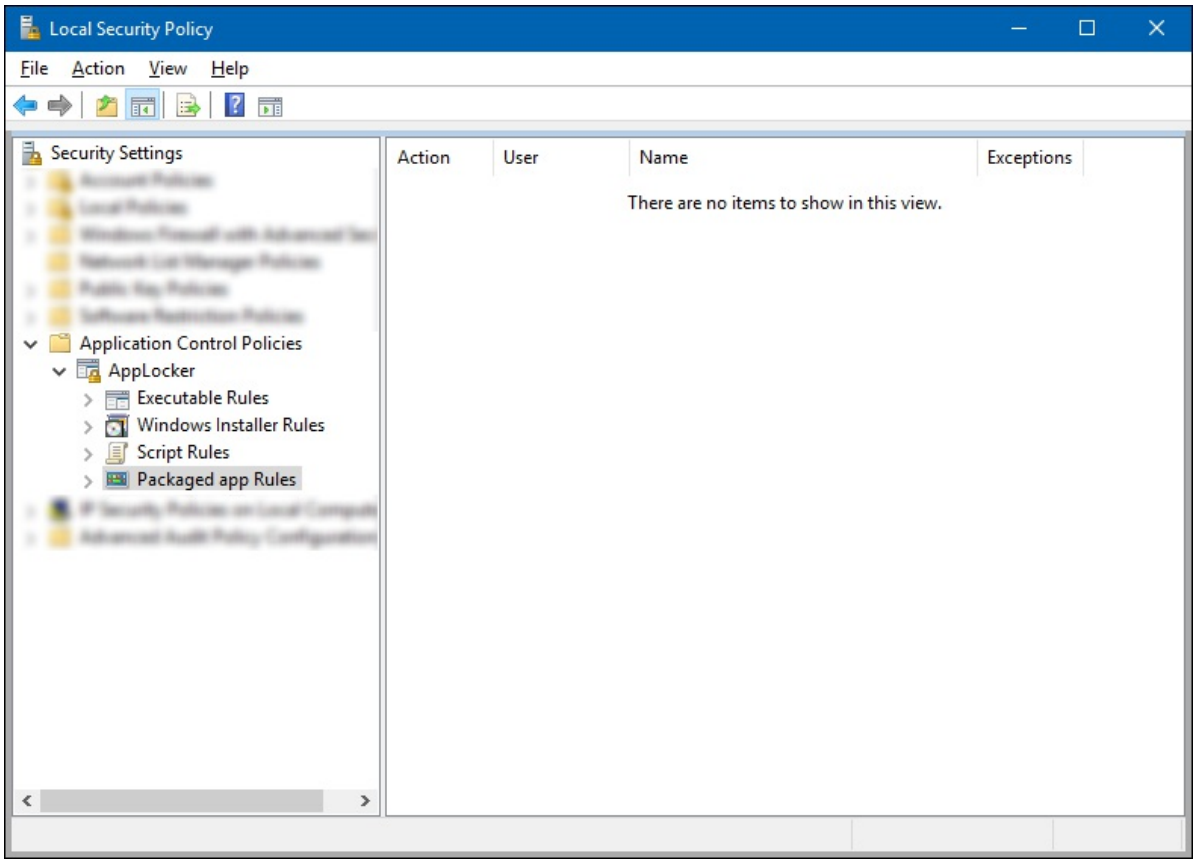
Dabei ist der Text `O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US` der Herausgebername, der im Feld **Herausgebername** eingegeben wird.

Hinzufügen einer AppLocker-Richtliniendatei

In diesem Beispiel fügen wir eine AppLocker-XML-Datei der Liste **App-Regeln** hinzu. Sie können diese Option verwenden, wenn Sie gleichzeitig mehrere Apps hinzufügen möchten. Weitere Informationen zu AppLocker finden Sie im Thema AppLocker.

So erstellen Sie eine App-Regel und XML-Datei mit dem AppLocker-Tool

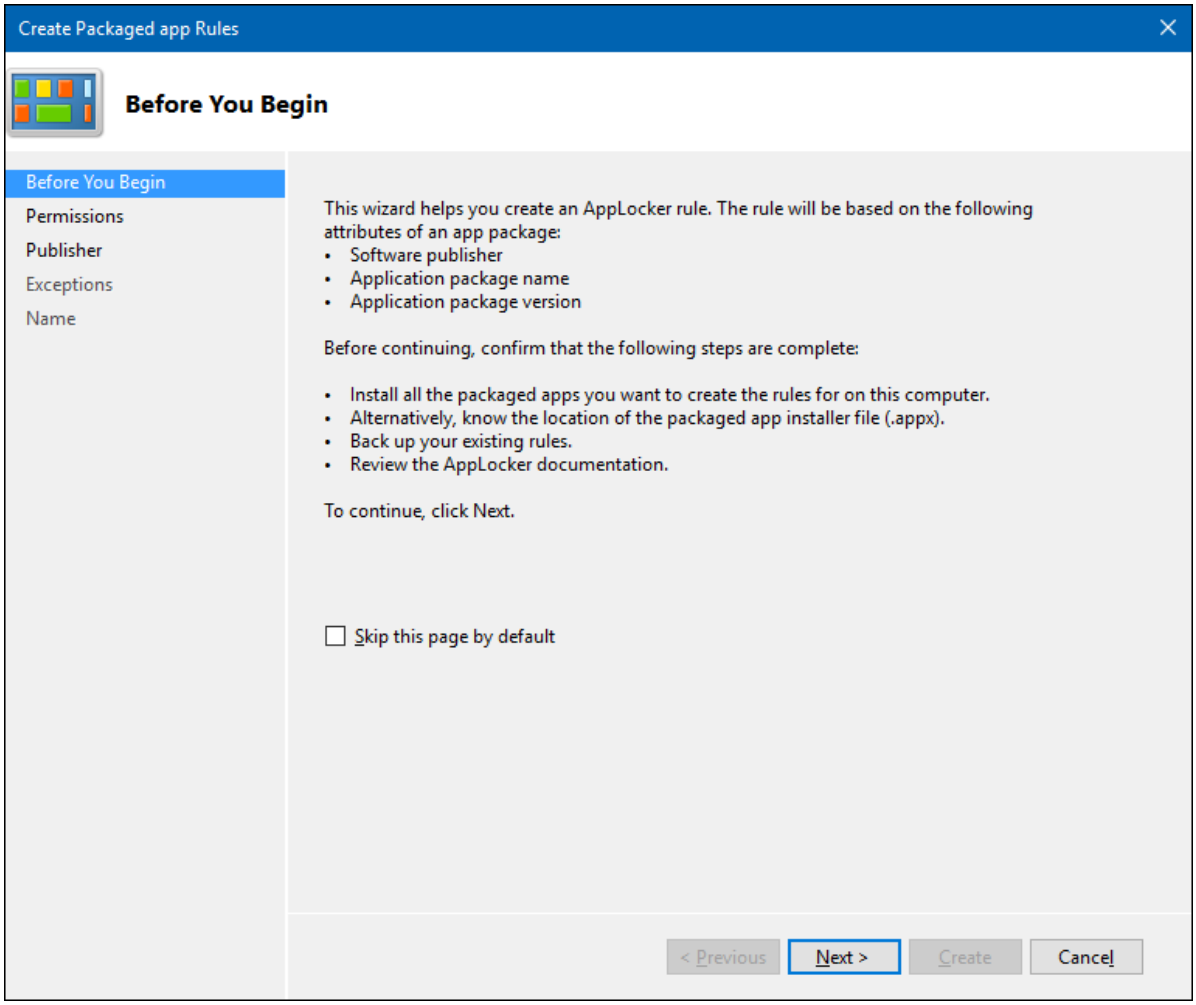
1. Öffnen Sie das Snap-In „Lokale Sicherheitsrichtlinie“ (secpol.msc).
2. Erweitern Sie im linken Bereich **Anwendungssteuerungsrichtlinien**, erweitern Sie **AppLocker**, und klicken Sie dann auf **App-Paketregeln**.



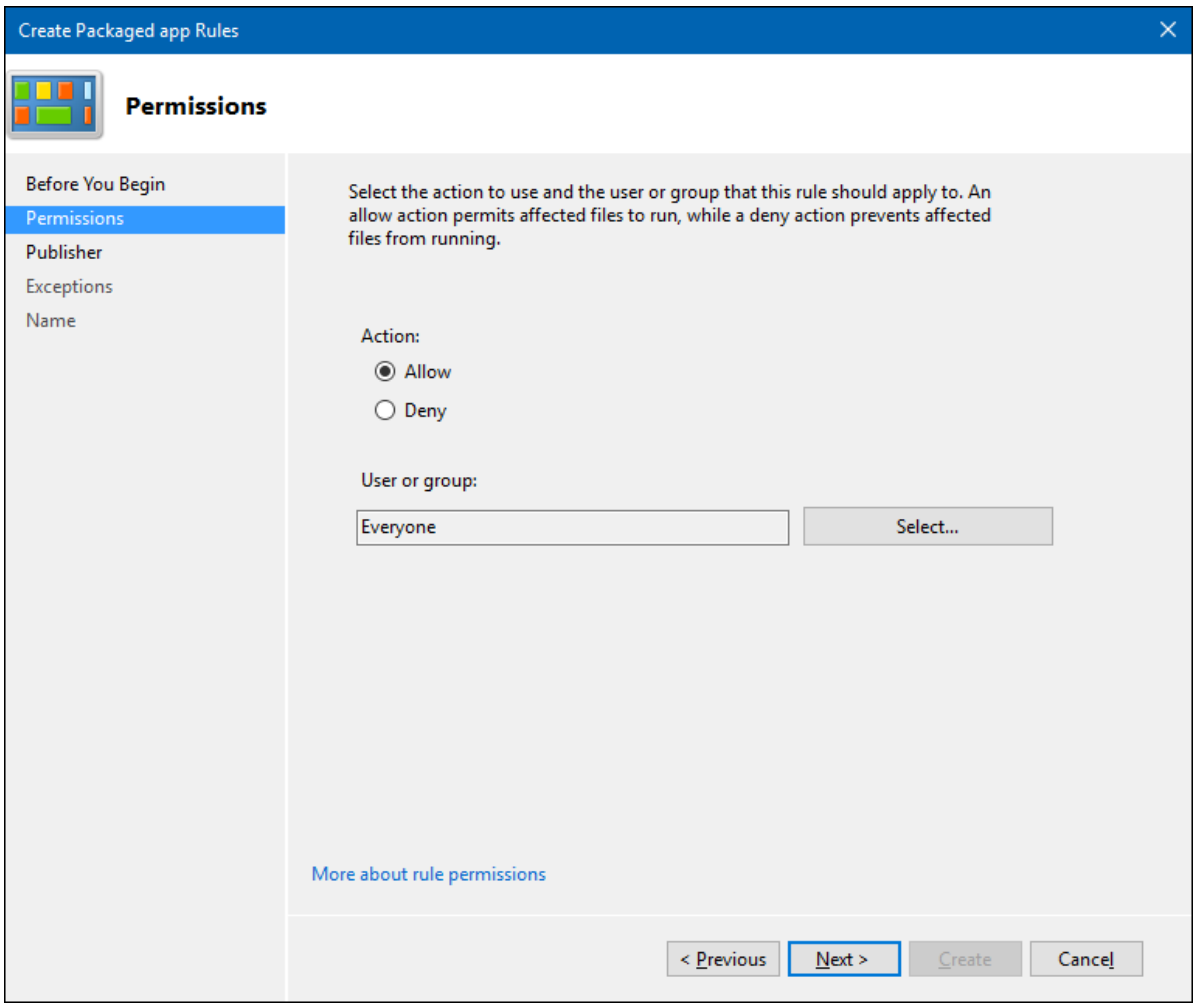
3. Klicken Sie mit der rechten Maustaste im rechten Bereich, und klicken Sie dann auf **Neue Regel erstellen**.

   Der Assistent **Create Packaged app Rules** wird angezeigt.

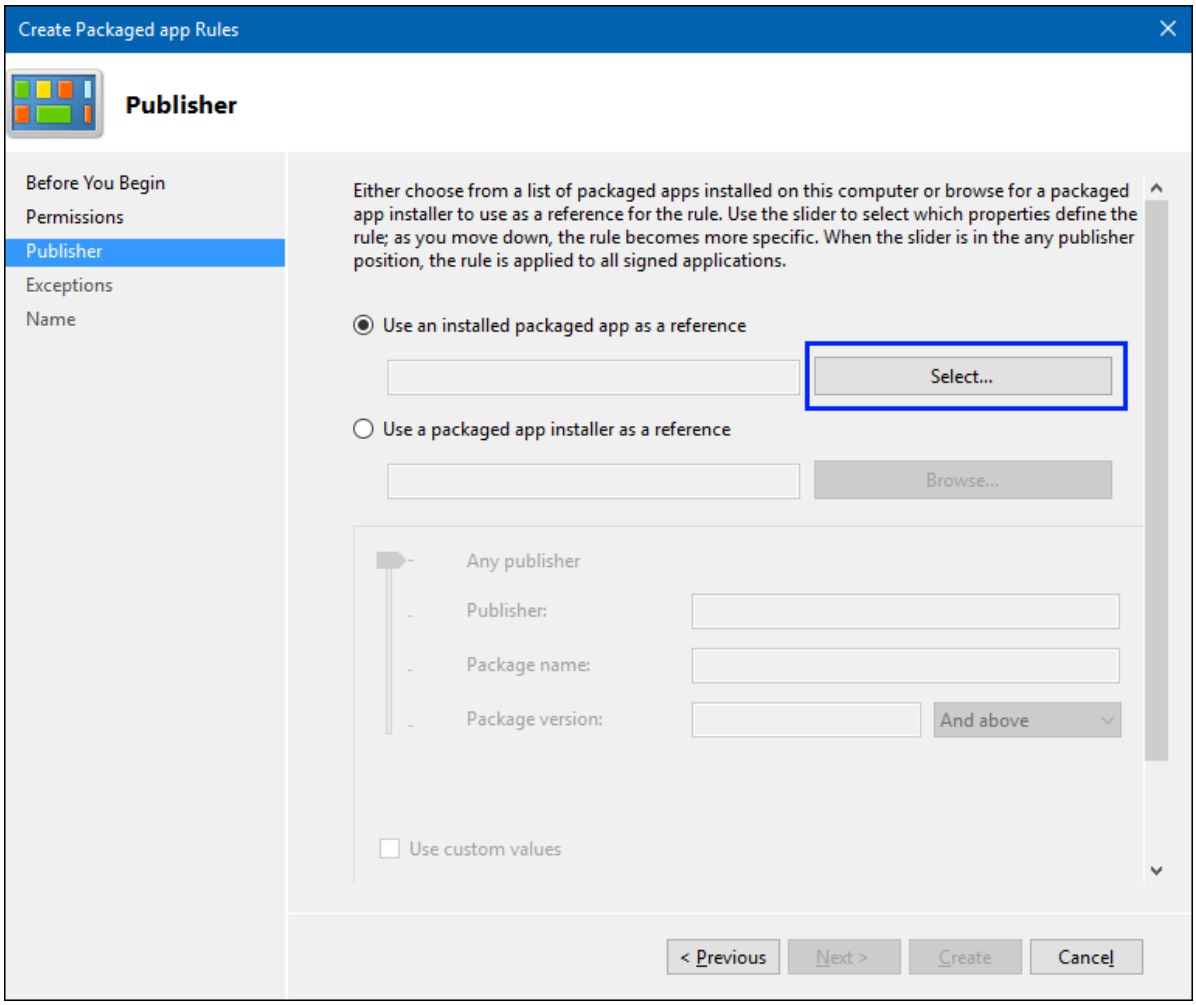
4. Klicken Sie auf der Seite **Vorbereitung** auf **Weiter**.



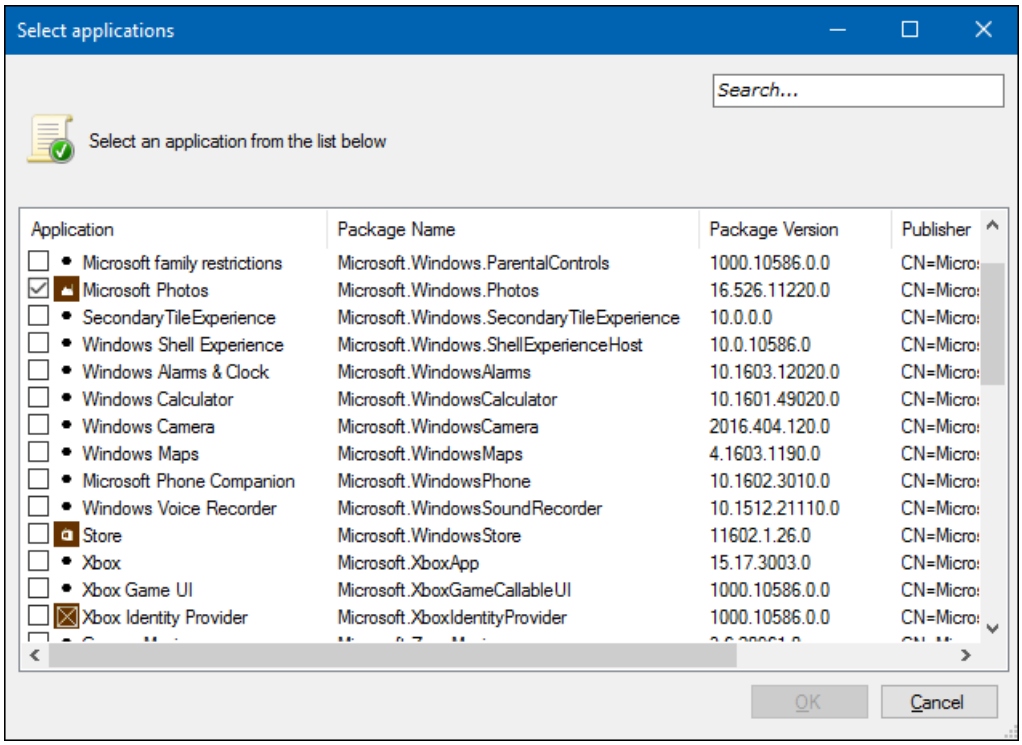
5. Stellen Sie auf der Seite **Berechtigungen** sicher, dass **Aktion** auf **Zulassen** und **Benutzer oder Gruppe** auf **Jeder** festgelegt ist, und klicken Sie dann auf **Weiter**.



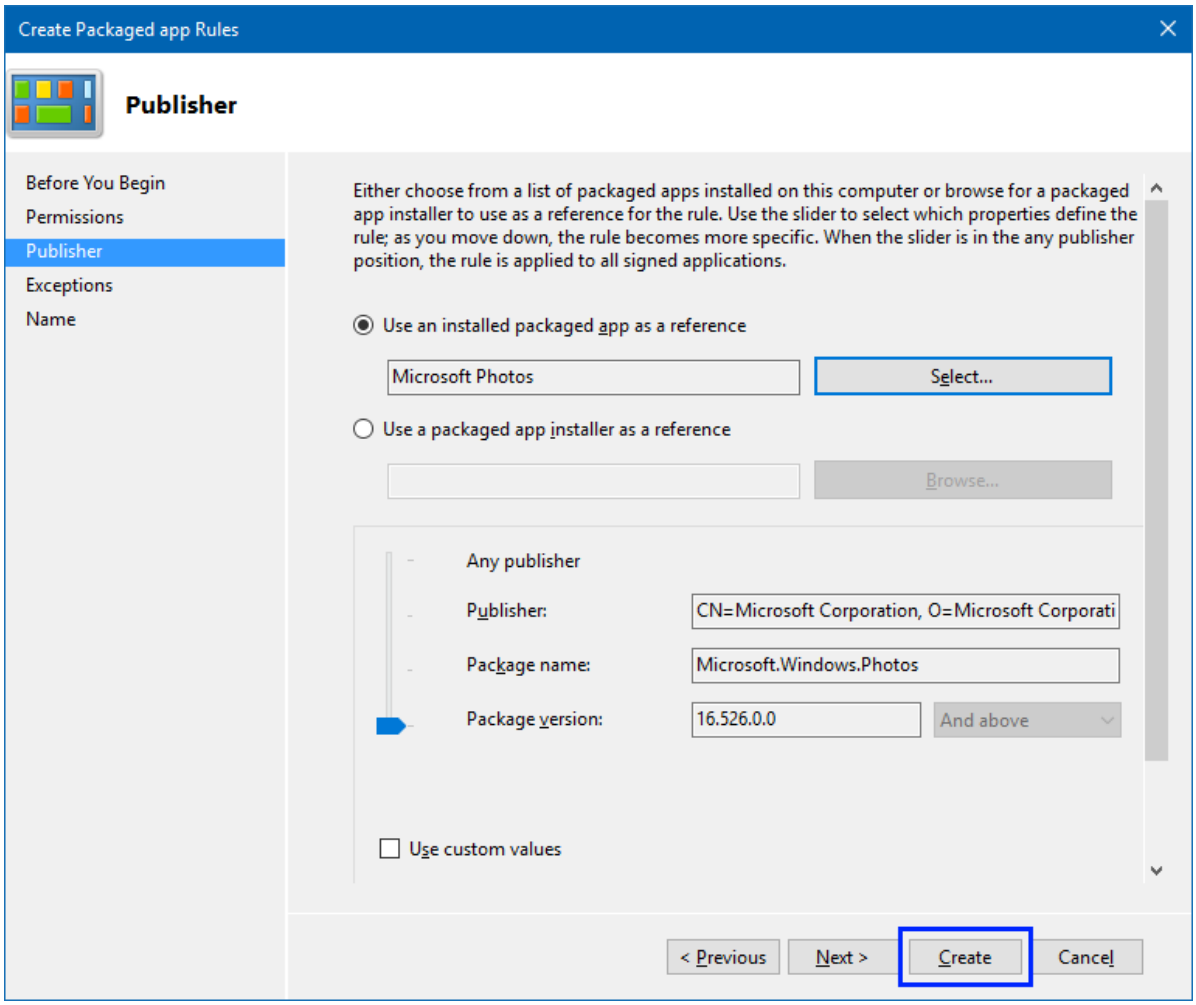
6. Klicken Sie auf der Seite **Herausgeber** im Bereich **Ein installiertes App-Paket als Referenz verwenden** auf **Auswählen**.



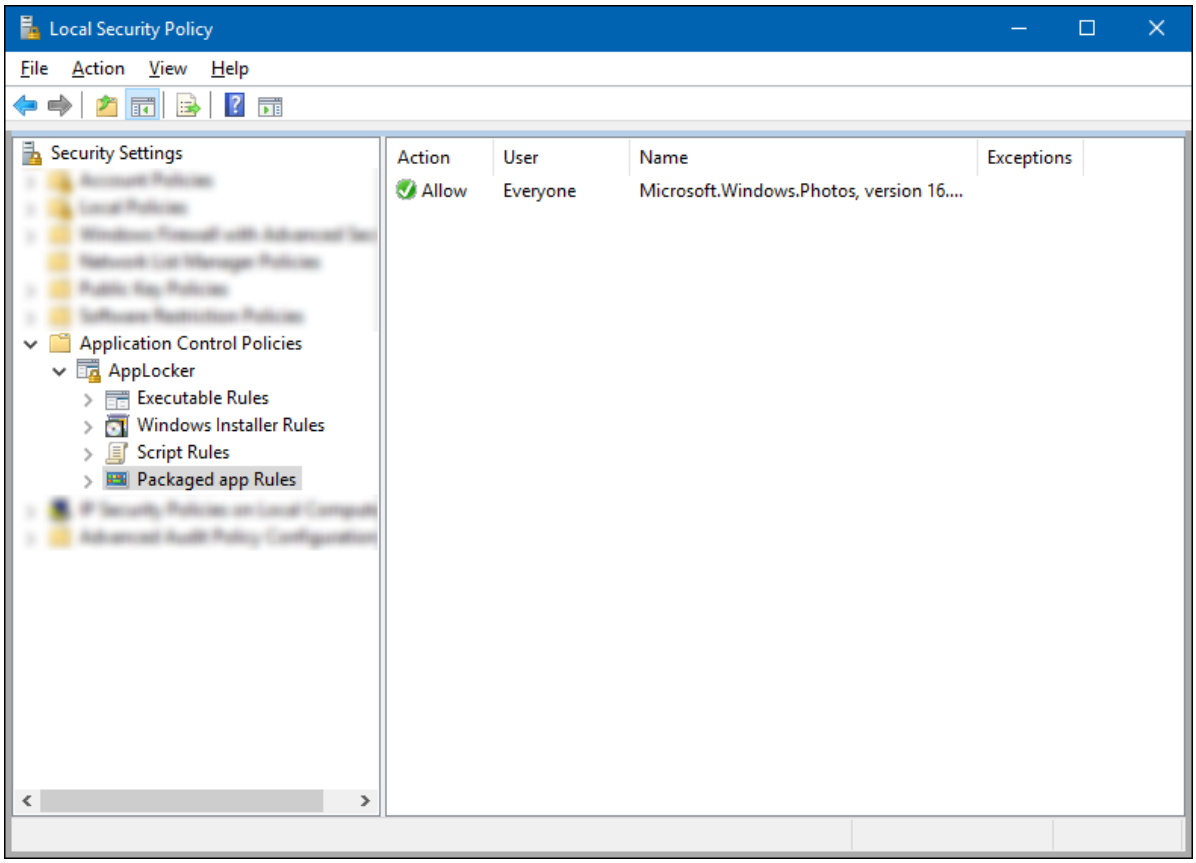
7. Wählen Sie im Feld **Anwendungen auswählen** die App aus, die Sie als Referenz für die Regel verwenden möchten, und klicken Sie dann auf **OK**. In diesem Beispiel verwenden wir Microsoft Fotos.



8. Klicken Sie auf der aktualisierten Seite **Herausgeber** auf **Erstellen**.

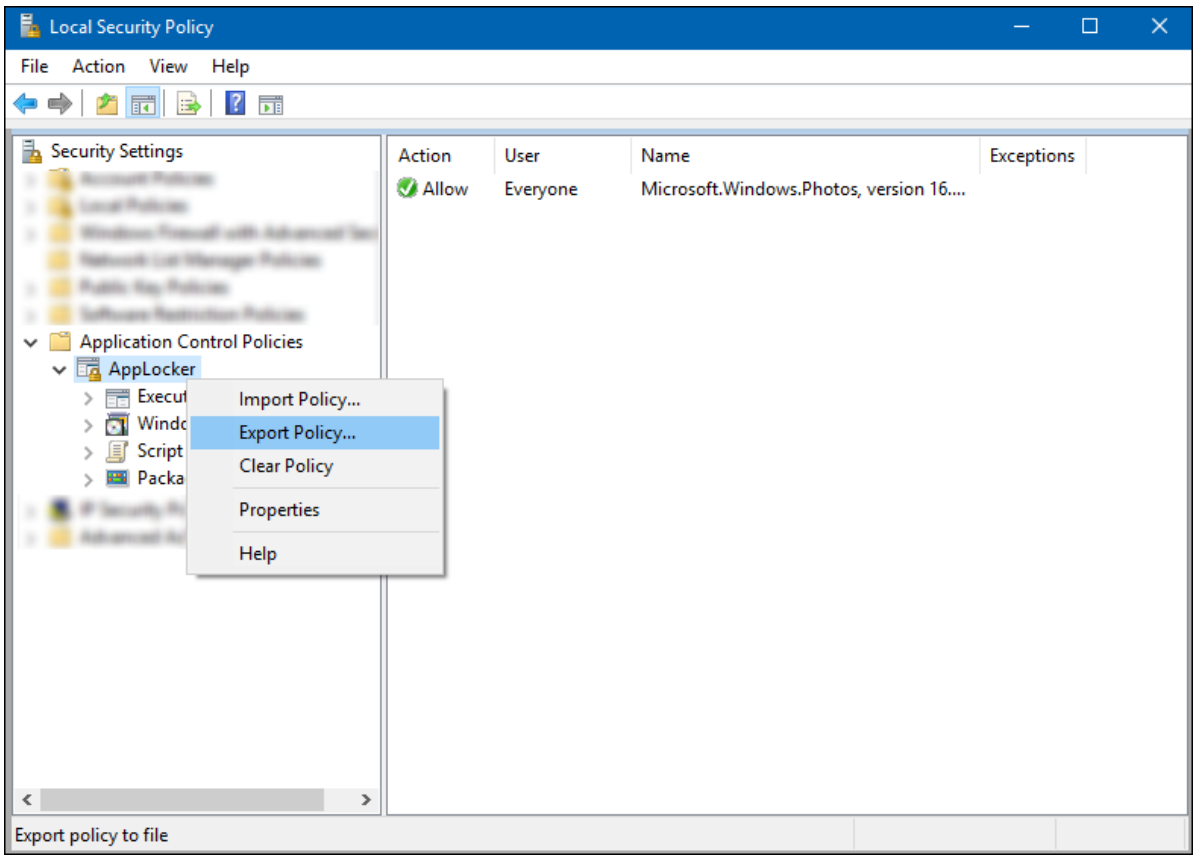


9. Überprüfen Sie das Snap-In „Lokale Sicherheitsrichtlinie", um sicherzustellen, dass die Regel richtig ist.



10. Klicken Sie mit der rechten Maustaste im linken Bereich auf **AppLocker**, und klicken Sie dann auf **Richtlinie exportieren**.

Das Feld **Richtlinie exportieren** wird geöffnet, in dem Sie die neue Richtlinie im XML-Format exportieren und speichern können.



11. Navigieren Sie im Feld **Richtlinie exportieren** zum Speicherort, an dem die Richtlinie gespeichert werden soll, legen Sie einen Namen für die Richtlinie fest, und klicken Sie auf **Speichern**.

    Die Richtlinie wird gespeichert, und die Meldung wird angezeigt, dass eine Regel aus der Richtlinie exportiert wurde.

    XML-Beispieldatei

    Dies ist der XML-Datei, die AppLocker für Microsoft Fotos erstellt.

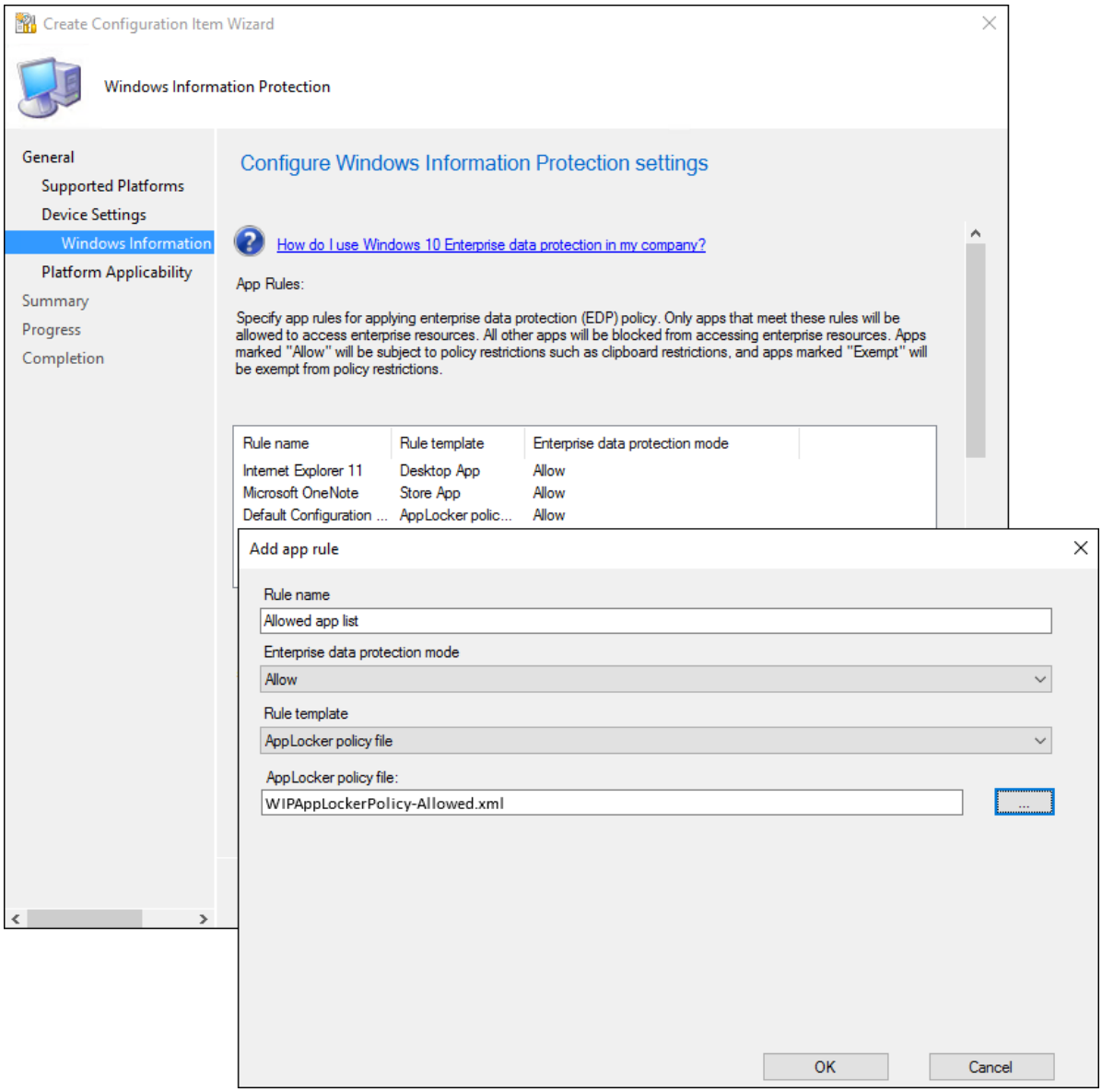
```
<AppLockerPolicy Version="1">
   <RuleCollection Type="Exe" EnforcementMode="NotConfigured" />
   <RuleCollection Type ="Msi" EnforcementMode="NotConfigured" />
   <RuleCollection Type ="Script" EnforcementMode="NotConfigured" />
   <RuleCollection Type ="Dll" EnforcementMode="NotConfigured" />
   <RuleCollection Type ="Appx" EnforcementMode="NotConfigured">
       <FilePublisherRule Id="5e0c752b-5921-4f72-8146-80ad5f582110" Name="Microsoft.Windows.Photos,
version 16.526.0.0 and above, from Microsoft Corporation" Description="" UserOrGroupSid="S-1-1-0"
Action="Allow">
           <Conditions>
               <FilePublisherCondition PublisherName="CN=Microsoft Corporation, O=Microsoft
Corporation, L=Redmond, S=Washington, C=US" ProductName="Microsoft.Windows.Photos" BinaryName="*">
                   <BinaryVersionRange LowSection="16.526.0.0" HighSection="*" />
               </FilePublisherCondition>
           </Conditions>
       </FilePublisherRule>
   </RuleCollection>
</AppLockerPolicy>
```

12. Nachdem Sie Ihre XML-Datei erstellt haben, müssen Sie Sie mithilfe von Microsoft Endpoint Configuration Manager importieren.

So importieren Sie die APP-Regel der AppLocker-Richtliniendatei mithilfe von Configuration Manager

1. Klicken Sie im Bereich **App-Regeln** auf **Hinzufügen**.

   Das Feld **App-Regel hinzufügen** wird angezeigt.



2. Fügen Sie einen Anzeigenamen für die App im Feld **Titel** ein. In diesem Beispiel ist der Name *Allowed app list*.

3. Klicken Sie in der Dropdownliste **WIP-Modus (Windows Information Protection)** auf **Zulassen**.

   Lassen Sie das Aktivieren von WIP zu, um Unternehmensdaten dieser App durch die Durchsetzung von WIP-Einschränkungen zu schützen. Wenn Sie eine App ausnehmen möchten, können Sie die Schritte im Abschnitt Ausnehmen von Apps aus WIP-Einschränkungen ausführen.

4. Wählen Sie die **AppLocker-Richtliniendatei** in der Dropdownliste **Regelvorlage** aus.

   Im Feld können Sie nun die AppLocker-XML-Richtliniendatei importieren.

5. Klicken Sie auf die Auslassungspunkte (...) zum Suchen nach der AppLocker-XML-Datei, klicken Sie auf **Öffnen**, und klicken Sie dann auf **OK**, um das Feld **App-Regel hinzufügen** zu schließen.

   Die Datei wird importiert, und die Apps werden der Liste **App-Regeln** hinzugefügt.

Ausnehmen von Apps aus WIP-Einschränkungen

Wenn Kompatibilitätsprobleme auftreten, weil Ihre App nicht kompatibel mit WIP ist, aber dennoch mit Unternehmensdaten verwendet werden muss, können Sie die App aus den WIP-Einschränkungen ausnehmen. Dies bedeutet, dass Ihre Apps keine automatische Verschlüsselung oder Tags enthalten und nicht die

Netzwerkbeschränkungen berücksichtigen. Dies bedeutet auch, dass bei den ausgenommenen Apps Datenverluste auftreten können.

So nehmen Sie eine Store-App, eine Desktop-App oder eine AppLocker-Richtliniendatei-App-Regel aus

1. Klicken Sie im Bereich **App-Regeln** auf **Hinzufügen**.

   Das Feld **App-Regel hinzufügen** wird angezeigt.

2. Fügen Sie einen Anzeigenamen für die App im Feld **Titel** ein. In diesem Beispiel ist der Name *Exempt apps list*.

3. Klicken Sie in der Dropdownliste **WIP-Modus (Windows Information Protection)** auf **Ausnahme**.

   Beachten Sie, dass beim Ausnehmen von Apps diese die WIP-Einschränkungen umgehen und auf Unternehmensdaten zugreifen dürfen. Informationen zum Zulassen von Apps finden Sie im Abschnitt Hinzufügen von App-Regeln zur Richtlinie dieses Themas.

4. Füllen Sie die übrigen Informationen der App-Regel aus, basierend auf dem Typ der Regel, die Sie hinzufügen:

   - **Store-App.** Befolgen Sie die Anweisungen zu **Herausgeber** und **Produktname** im Abschnitt Hinzufügen einer Store-App-Regel zur Richtlinie dieses Themas.
   - **Desktop-App.** Befolgen Sie die Anweisungen zu **Herausgeber**, **Produktname**, **Name der Binärdatei** und **Version** im Abschnitt Hinzufügen einer Store-App-Regel zur Richtlinie dieses Themas.
   - **AppLocker-Richtliniendatei.** Befolgen Sie die Anweisungen zu **Importieren** im Abschnitt Hinzufügen einer AppLocker-Richtliniendatei dieses Themas anhand einer Liste der ausgenommenen Apps.

5. Klicken Sie auf **OK**.

Verwalten der WIP-Schutzebene für Ihre Unternehmensdaten

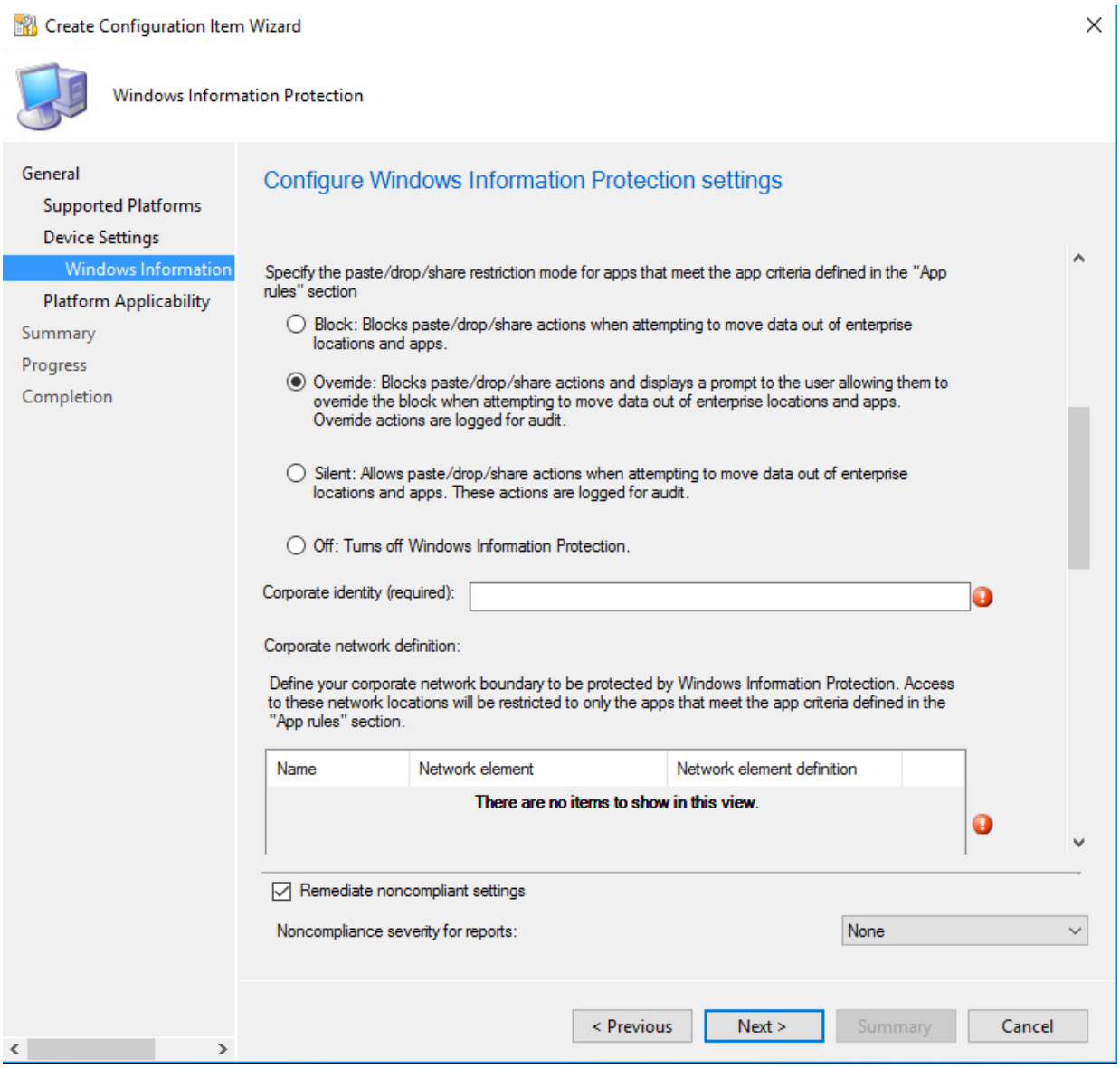
Nachdem Sie die Apps hinzugefügt haben, die mit WIP geschützt werden sollen, müssen Sie einen Verwaltungs- und Schutzmodus anwenden.

Es wird empfohlen, dass Sie mit **Unbeaufsichtigt** oder **Außer Kraft setzen** beginnen und für eine kleine Gruppe überprüfen, dass die richtigen Apps in der Liste der geschützten Apps enthalten sind. Danach können Sie zur endgültigen Erzwingungsrichtlinie wechseln, entweder **Außer Kraft setzen** oder **Blockieren**.

> **NOTE**
> Weitere Informationen zum Erfassen Ihrer Überwachungsprotokolldateien finden Sie unter Erfassen von Windows Information Protection-Überwachungsprotokolldateien (WIP).

MODUS	BESCHREIBUNG
Blockieren	WIP sucht nach unerwünschten Datenfreigaben und hindert Mitarbeiter daran, den Schritt auszuführen. Beispielsweise können Informationen zwischen Apps geteilt werden, die keinem Unternehmensschutz unterliegen, und Unternehmensdaten für andere Personen und Geräte außerhalb Ihres Unternehmens freigegeben werden.

MODUS	BESCHREIBUNG
Außer Kraft setzen	WIP ermittelt ungeeignete Datenfreigaben und warnt Mitarbeiter davor, eine potenziell unsichere Aktion auszuführen. Bei diesem Verwaltungsmodus können Mitarbeiter die Richtlinie jedoch außer Kraft setzen und die Daten freigeben, wobei die Aktion jedoch in ihrem Überwachungsprotokoll protokolliert wird.
Unbeaufsichtigt	WIP wird im Hintergrund ausgeführt, und die unerwünschte Datenfreigabe wird protokolliert, ohne dass eine Aktion blockiert wird, die im Modus zur Außerkraftsetzung die Interaktion eines Mitarbeiters erforderlich gemacht hätte. Unerlaubte Aktionen, z.B. dass Apps unzulässigerweise versuchen, auf eine Netzwerkressource oder WIP-geschützte Daten zuzugreifen, werden weiterhin blockiert.
Deaktiviert (nicht empfohlen)	WIP ist deaktiviert, und Ihre Daten werden weder geschützt noch überwacht. Nachdem WIP deaktiviert wurde, wird versucht, alle durch WIP gekennzeichneten Dateien auf den lokal angeschlossenen Laufwerken zu entschlüsseln. Beachten Sie, dass frühere Entschlüsselungs- und Richtlinieninformationen nicht automatisch erneut angewendet werden, wenn Sie den WIP-Schutz wieder aktivieren.



Definieren der vom Unternehmen verwalteten Identitätsdomänen

Die Unternehmensidentität, in der Regel Ihre primäre Internetdomäne (z.B. contoso.com), kann zum Identifizieren und Kennzeichnen von Unternehmensdaten von Apps verwendet werden, die Sie als WIP-geschützt gekennzeichnet haben. Beispielsweise werden E-Mails mit contoso.com als Unternehmensdaten gekennzeichnet und durch die Windows Information Protection-Richtlinien eingeschränkt.

Durch die Trennung mit dem Zeichen „|“ können Sie mehrere Domänen angeben, die sich im Besitz Ihres Unternehmens befinden. Beispiel: (contoso.com|newcontoso.com). Bei mehreren Domänen wird die erste als Ihre Unternehmensidentität und alle weiteren als im Besitz der ersten befindlich festgelegt. Es wird dringend empfohlen, dass Sie alle Ihre E-Mail-Adresse-Domänen in diese Liste aufnehmen.

So fügen Sie Ihre Unternehmensidentität hinzu

- Geben Sie den Namen Ihrer Unternehmensidentität im Feld **Unternehmensidentität** ein. Beispiel: `contoso.com` oder `contoso.com|newcontoso.com`

Auswählen der Speicherorte, an denen Apps Zugriff auf Unternehmensdaten haben

Nachdem Sie Ihren Apps einen Schutzmodus hinzugefügt haben, müssen Sie entscheiden, wo diese Apps in Ihrem Netzwerk auf Unternehmensdaten zugreifen können.

Es gibt keine in WIP enthaltenen Standardspeicherorte, Sie müssen alle Ihre Netzwerkadressen hinzufügen. Dieser Bereich bezieht sich auf alle Netzwerkendpunkt-Geräte, die eine IP-Adresse im Bereich Ihres Unternehmens abrufen und auch an eine der Unternehmensdomänen gebunden sind, darunter SMB-Freigaben. Speicherorte im lokalen Dateisystem sollten nur die Verschlüsselung verwalten (z.B. auf dem lokalen NTFS, FAT, ExFAT).

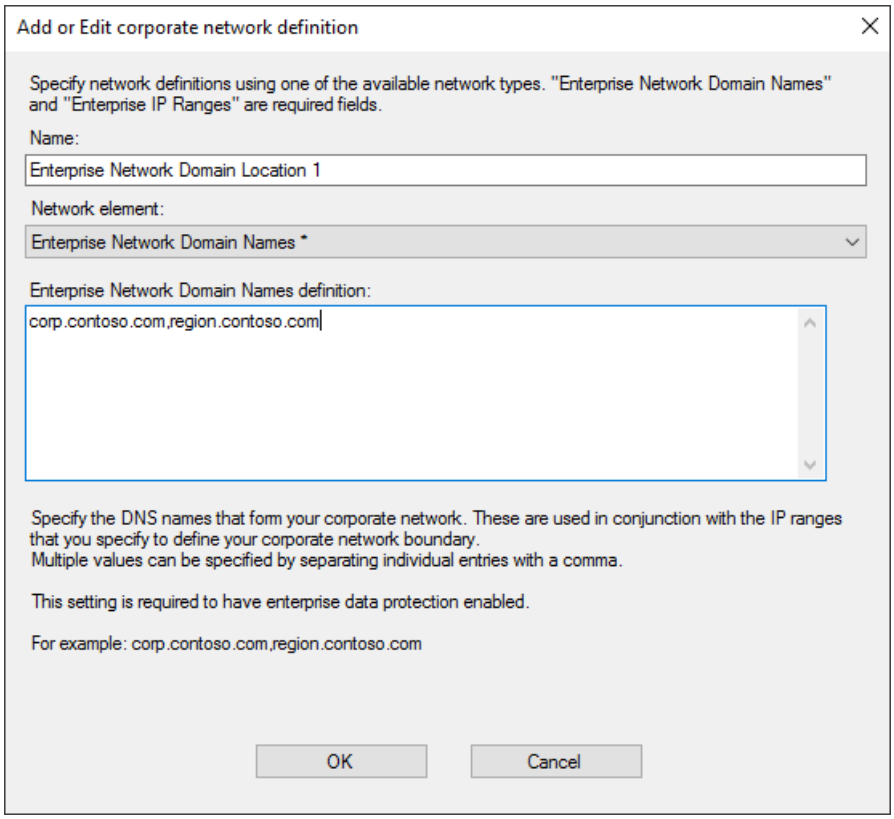
> **IMPORTANT**
>
> Jede WIP-Richtlinie sollten Richtlinien enthalten, die Ihre Unternehmensnetzwerkadressen definieren.
> Classless Inter-Domain Routing (CIDR)-Notation wird für WIP-Konfigurationen nicht unterstützt.

So legen Sie fest, wo Ihre geschützten Apps Unternehmensdaten im Netzwerk finden und senden können

1. Klicken Sie auf **Hinzufügen**, um zusätzliche Netzwerkadressen hinzuzufügen, auf die Ihre Apps zugreifen können.

   Das Feld **Unternehmensnetzwerkdefinition hinzufügen oder bearbeiten** wird angezeigt.

2. Geben Sie einen Namen für Ihr Unternehmensnetzwerkelement im Feld **Name** ein, und wählen Sie dann den Typ des Netzwerkelements im Dropdownfeld **Netzwerkelement** aus. Dies kann eine beliebige Option aus der folgenden Tabelle sein.



NETZWERKADRESSTYP	FORMAT	BESCHREIBUNG

Unternehmenscloudressourcen	**Mit Proxy:** contoso.sharepoint.com,contoso.internalproxy1.com|contoso.visualstudio.com,contoso.internalproxy2.com **Ohne Proxy:** contoso.sharepoint.com|contoso.visualstudio.com	Geben Sie die Cloudressourcen an, die als unternehmenseigen behandelt und durch WIP geschützt werden sollen. Für jede Cloudressource können Sie optional auch einen Proxyserver aus der Liste der internen Proxyserver angeben, um den Datenverkehr für diese Cloudressource weiterzuleiten. Beachten Sie, dass sämtliche über interne Proxyserver weitergeleiteten Daten als Unternehmensdaten gelten. Wenn Sie über mehrere Ressourcen verfügen, müssen Sie diese mithilfe des " | " Trennzeichens trennen. Wenn Sie keine Proxy Server verwenden, müssen Sie auch "das," Trennzeichen direkt vor dem " | "einfügen. Beispiel: `URL <,proxy>|URL <,proxy>`. **Wichtig** In einigen Fällen, z.B. wenn eine App über eine IP-Adresse direkt eine Verbindung mit einer Cloudressource herstellt, kann Windows nicht feststellen, ob die App versucht, eine Verbindung mit einer Ressource in der Unternehmenscloud oder mit einer persönlichen Website herzustellen. In diesem Fall wird die Verbindung von Windows standardmäßig blockiert. Um zu verhindern, dass Windows diese Verbindungen automatisch blockiert, fügen Sie der Einstellung die Zeichenfolge `/*AppCompat*/` hinzu. Beispiel: `URL <,proxy>|URL <,proxy>|/*AppCompat*/` .

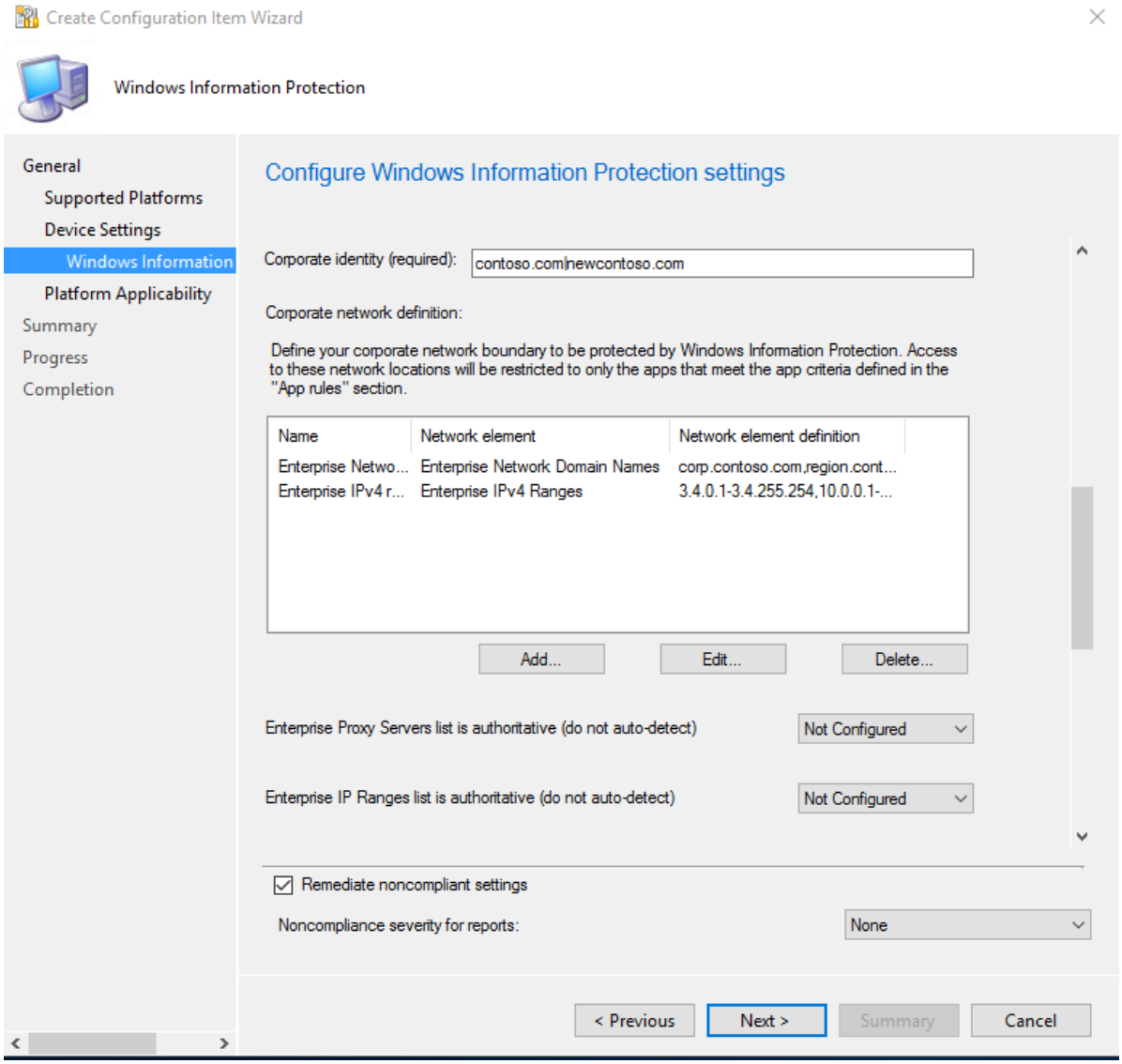
Netzwerkdomänennamen des Unternehmens (erforderlich)	corp.contoso.com,region.contoso.com	Geben Sie die in Ihrer Umgebung verwendeten DNS-Suffixe an. Der gesamte Datenverkehr zu den vollqualifizierten Domänen, die in dieser Liste enthalten sind, wird geschützt. Diese Einstellung funktioniert mit den Einstellungen für die IP-Bereiche, um festzustellen, ob ein Netzwerkendpunkt in privaten Netzwerken unternehmenseigen oder persönlich ist. Wenn Sie über mehrere Ressourcen verfügen, müssen Sie Sie mit dem "" Trennzeichen trennen.
Proxyserver	proxy.contoso.com:80;proxy2.contoso.com:443	Geben Sie die Proxyserver an, die Ihre Geräte durchlaufen, um die Cloudressourcen zu erreichen. Die Verwendung dieses Servertyps gibt an, dass die Cloudressourcen, mit denen Sie eine Verbindung herstellen, Unternehmensressourcen sind. Diese Liste sollte keine Server aus Ihrer Liste der internen Proxyserver enthalten. Interne Proxyserver dürfen nur für den WIP-geschützten (Unternehmens-)Datenverkehr verwendet werden. Wenn Sie über mehrere Ressourcen verfügen, müssen Sie diese mithilfe von "; " Trennzeichen.
Interne Proxyserver	contoso.internalproxy1.com;contoso.internalproxy2.com	Geben Sie die internen Proxyserver an, die Ihre Geräte durchlaufen, um die Cloudressourcen zu erreichen. Die Verwendung dieses Servertyps gibt an, dass die Cloudressourcen, mit denen Sie sich verbinden, Unternehmensressourcen sind. Diese Liste sollte keine Server aus Ihrer Liste der Proxyserver enthalten. Proxyserver dürfen nur für den nicht mit WIP-geschützten (nicht-Unternehmens-)Datenverkehr verwendet werden. Wenn Sie über mehrere Ressourcen verfügen, müssen Sie diese mithilfe von "; " Trennzeichen.

IPv4-Bereiche des Unternehmens (erforderlich)	**IPv4-Adresse wird** gestartet: 3.4.0.1 **IPv4-Adresse wird** beendet: 3.4.255.254 **Benutzerdefinierter** URI: 3.4.0.1-3.4.255.254, 10.0.0.1-10.255.255.254	Geben Sie die Adressen für einen gültigen IPv4-Wertebereich in Ihrem Intranet an. Diese in Verbindung mit Ihren Unternehmensnetzwerk-Domänennamen verwendeten Adressen definieren die Grenzen Ihres Unternehmensnetzwerks. Wenn Sie über mehrere Bereiche verfügen, müssen Sie Sie mit dem "" Trennzeichen trennen.
IPv6-Bereiche des Unternehmens	**IPv6-Startadresse** : 2a01:110:: **IPv6-Adresse wird** beendet: 2a01:110:7fff: FFFF: FFFF: FFFF: FFFF: FFFF **Benutzerdefinierter** URI: 2a01:110:7fff: FFFF: FFFF: FFFF: FFFF: FFFF; fd00::-fdff:ffff:ffff:ffff:ffff:ffff:ffff:ffff	Geben Sie die Adressen für einen gültigen IPv6-Wertebereich in Ihrem Intranet an. Diese in Verbindung mit Ihren Unternehmensnetzwerk-Domänennamen verwendeten Adressen definieren die Grenzen Ihres Unternehmensnetzwerks. Wenn Sie über mehrere Bereiche verfügen, müssen Sie Sie mit dem "" Trennzeichen trennen.
Neutrale Ressourcen	sts.contoso.com,sts.contoso2.com	Geben Sie die Endpunkte für die Authentifizierungsumleitung in Ihrem Unternehmen an. Diese Adressen gelten als unternehmenseigen oder persönlich, basierend auf dem Kontext der Verbindung vor der Umleitung. Wenn Sie über mehrere Ressourcen verfügen, müssen Sie Sie mit dem "" Trennzeichen trennen.

3. Fügen Sie so viele Adressen wie benötigt hinzu, und klicken Sie dann auf **OK**.

   Das Feld **Unternehmensnetzwerkdefinition hinzufügen oder bearbeiten** wird geschlossen.

4. Legen Sie fest, ob Windows nach zusätzlichen Netzwerkeinstellungen suchen soll und ob das WIP-Symbol für Ihre Unternehmensdateien im Datei-Explorer angezeigt werden soll.

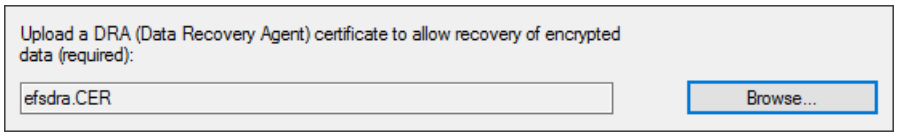


- **Liste der Unternehmensproxyserver ist autoritativ (keine automatische Erkennung).** Aktivieren Sie dieses Kontrollkästchen, wenn Windows die in den Definitionen der Netzwerkgrenzen angegebenen Proxyserver als die vollständige Liste der im Netzwerk verfügbaren Proxyserver einstufen soll. Wenn Sie dieses Kontrollkästchen deaktivieren, sucht Windows nach weiteren Proxyservern im jeweiligen Netzwerk. Die Standardoption ist „Nicht konfiguriert".

- **Liste der Unternehmens-IP-Bereiche ist autoritativ (keine automatische Erkennung).** Aktivieren Sie dieses Kontrollkästchen, wenn Windows die in den Definitionen der Netzwerkgrenzen angegebenen IP-Bereiche als die vollständige Liste der im Netzwerk verfügbaren IP-Bereiche einstufen soll. Wenn Sie dieses Kontrollkästchen deaktivieren, sucht Windows nach weiteren IP-Bereichen auf allen in eine Domäne eingebundenen Geräten, die mit dem Netzwerk verbunden sind. Die Standardoption ist „Nicht konfiguriert".

- **Zeigt die WIP-Symbolüberlagerung (Windows Information Protection) für Ihre zugelassenen, nicht WIP-kompatiblen Apps für Unternehmensdateien im Datei-Explorer an.** Aktivieren Sie dieses Kontrollkästchen, wenn die WIP-Symbolüberlagerung (Windows Information Protection) für Unternehmensdateien in der Ansicht „Speichern unter" und im Datei-Explorer angezeigt werden soll. Darüber hinaus wird die Symbolüberlagerung für nicht optimierte, aber zulässige Apps auch auf der App-Kachel und mit dem Text *Verwaltet* für den App-Namen im Menü **Start** angezeigt. Die Standardoption ist „Nicht konfiguriert".

5. Klicken Sie im erforderlichen Feld **Laden Sie ein Datenwiederherstellungs-Agent-Zertifikat hoch, um die Wiederherstellung verschlüsselter Daten zuzulassen** auf **Durchsuchen**, um ein Datenwiederherstellungszertifikat für die Richtlinie hinzuzufügen.

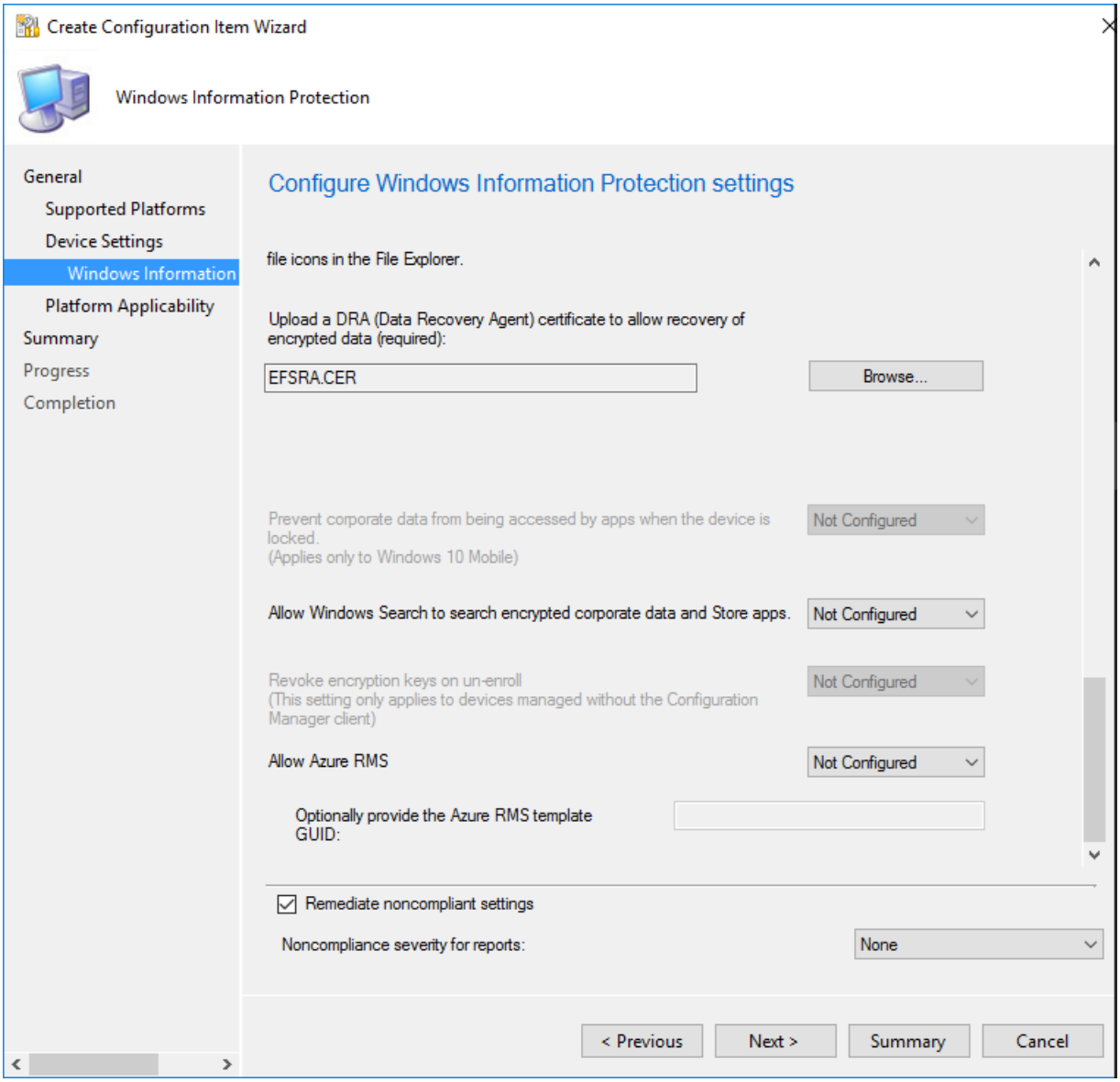


Nachdem Sie die WIP Richtlinie erstellt und für Ihre Mitarbeiter bereitgestellt haben, beginnt Windows mit dem Verschlüsseln der Unternehmensdaten auf dem lokalen Gerätelaufwerk der Mitarbeiter. Wenn aus irgendeinem Grund lokale Verschlüsselungsschlüssel der Mitarbeiter verloren gehen oder widerrufen werden, können die verschlüsselten Daten unter Umständen nicht wiederhergestellt werden. Um dies zu vermeiden, ermöglicht das DRA-Zertifikat Windows die Verwendung eines angegebenen öffentlichen Schlüssels zum Verschlüsseln der lokalen Daten, während Sie den privaten Schlüssel verwalten, der die Daten entschlüsseln kann.

Weitere Informationen zum Suchen und Exportieren des Datenwiederherstellungszertifikats finden Sie im Thema Datenwiederherstellung und verschlüsselndes Dateisystem (EFS). Weitere Informationen zum Erstellen und Überprüfen des DRA EFS-Zertifikat finden Sie unter Erstellen und Überprüfen eines Datenwiederherstellungs-Agent-Zertifikats des verschlüsselnden Dateisystems (Encrypting File System, EFS).

Auswählen der optionalen WIP-bezogenen Einstellungen

Nachdem Sie entschieden haben, wo Ihre geschützten Apps auf Unternehmensdaten im Netzwerk zugreifen können, werden Sie aufgefordert zu entscheiden, ob optionale WIP-Einstellungen hinzugefügt werden sollen.



So legen Sie die optionalen Einstellungen fest

1. Sie können einige oder alle optionalen Einstellungen festlegen:

   - **App-Zugriff auf Unternehmensdaten verhindern, wenn das Gerät gesperrt ist (gilt nur für Windows10 Mobile)**. Legt fest, ob Unternehmensdaten mit einem Schlüssel verschlüsselt werden, der durch den PIN-Code eines Mitarbeiters auf einem gesperrten Gerät geschützt ist. Apps können keine Unternehmensdaten lesen, wenn das Gerät gesperrt ist. Die Optionen sind:

     - **Ja (empfohlen).** Aktiviert die Funktion und bietet den zusätzlichen Schutz.

     - **Nein, oder nicht konfiguriert.** Aktiviert diese Funktion nicht.

   - **Die Suche nach verschlüsselten Daten und Store-Apps durch Windows Search zulassen.** Legt fest, ob Windows Search nach verschlüsselten Unternehmensdaten und Store-Apps suchen und diese indizieren kann. Die Optionen sind:

     - **Ja.** Ermöglicht Windows Search das Suchen und Indizieren verschlüsselter Unternehmensdaten und Store-Apps.

     - **Nein, oder nicht konfiguriert (empfohlen).** Verhindert, dass Windows Search verschlüsselte Unternehmensdaten und Store-Apps sucht und indiziert.

   - **Widerrufen Sie die lokalen Verschlüsselungsschlüssel während des Registrierungsvorgangs.** Legt fest, ob die lokalen Verschlüsselungsschlüssel eines Benutzers von einem Gerät widerrufen werden, wenn die Registrierung des Geräts in Windows Information Protection aufgehoben wird. Wenn die Verschlüsselungsschlüssel widerrufen werden, kann ein Benutzer nicht mehr auf verschlüsselte Unternehmensdaten zugreifen. Die Optionen sind:

     - **Ja, oder nicht konfiguriert (empfohlen).** Die lokalen Verschlüsselungsschlüssel werden während der Aufhebung der Registrierung von einem Gerät widerrufen.

     - **Nein.** Das Widerrufen lokaler Verschlüsselungsschlüssel von einem Gerät während der Aufhebung der Registrierung wird beendet. Beispiel: Sie migrieren zwischen Lösungen für die mobile Geräteverwaltung (MDM).

   - **Azure RMS zulassen** Ermöglicht die sichere Freigabe von Dateien mithilfe von Wechselmedien wie USB-Laufwerken. Weitere Informationen dazu, wie RMS mit WIP funktioniert, finden Sie unter Erstellen einer WIP-Richtlinie mit InTune. Um zu bestätigen, welche Vorlagen Ihr Mandant hat, führen Sie Get-AadrmTemplate aus dem AADRM-PowerShell-Modulaus. Wenn Sie keine Vorlage angeben, verwendet WIP einen Schlüssel aus einer RMS-Standardvorlage, auf die jeder Benutzer im Mandanten zugreifen kann.

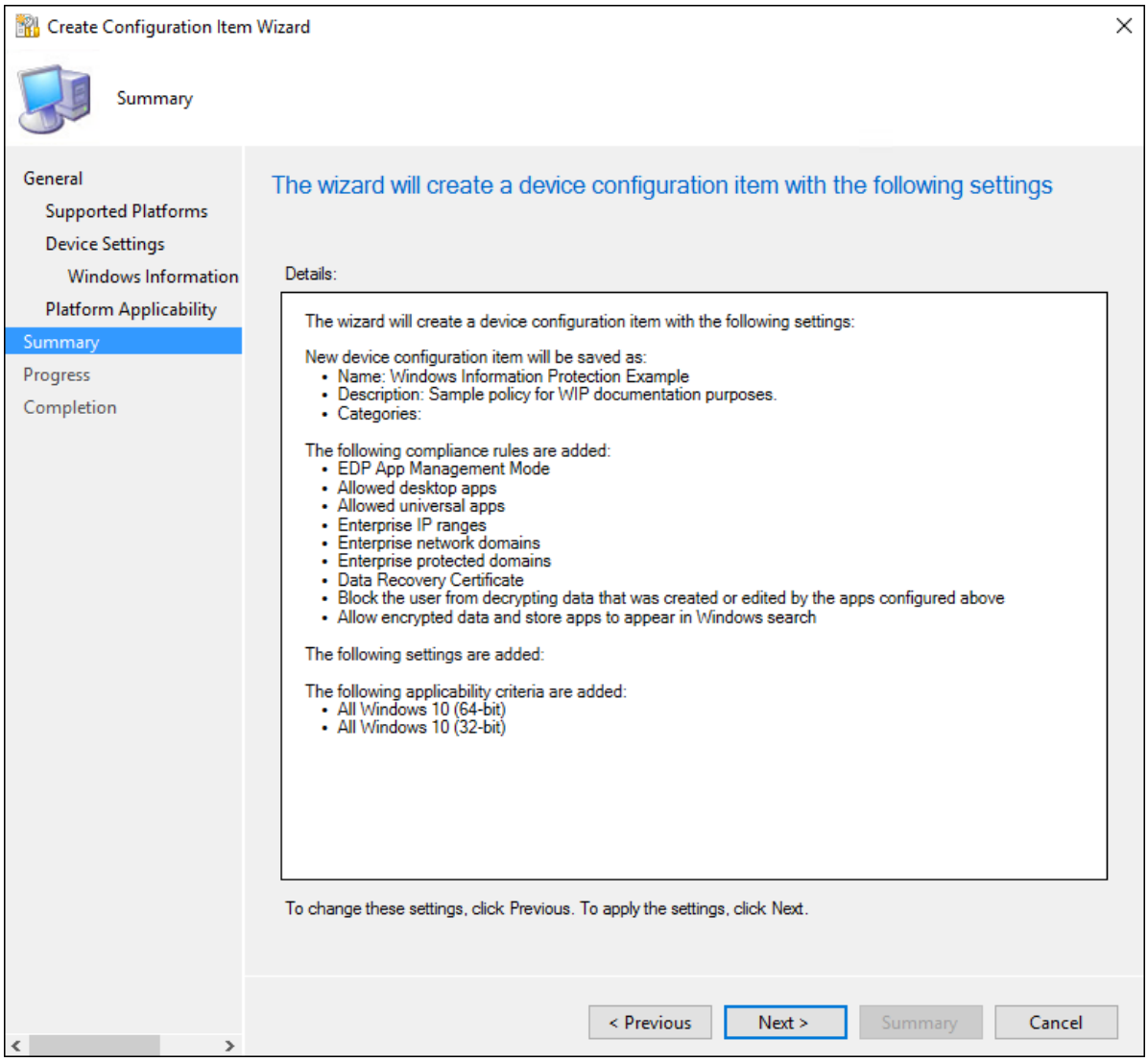
2. Nachdem Sie alle gewünschten Einstellungen ausgewählt haben, klicken Sie auf **Zusammenfassung**.

Überprüfen der Konfigurationsoptionen auf dem Bildschirm „Zusammenfassung“

Nachdem Sie die Konfiguration der Richtlinie abgeschlossen haben, können Sie Ihre Informationen auf dem Bildschirm **Zusammenfassung** überprüfen.

So zeigen Sie den Bildschirm „Zusammenfassung“ an

- Klicken Sie auf die Schaltfläche **Zusammenfassung**, um die Auswahl für die Richtlinie zu überprüfen. Klicken Sie dann auf **Weiter**, um die Richtlinie fertigzustellen und zu speichern.



Es wird eine Statusleiste mit dem Fortschritt der Richtlinie angezeigt. Klicken Sie nach Abschluss des Vorgangs auf **Schließen**, um zur Seite **Konfigurationselemente** zurückzukehren.

Bereitstellen der WIP-Richtlinie

Nachdem Sie die WIP-Richtlinie erstellt haben, müssen Sie sie auf den Geräten in Ihrer Organisation bereitstellen. Informationen zu den Bereitstellungsoptionen finden Sie unter folgenden Themen:

- Vorgänge und die Wartung für Kompatibilitätseinstellungen in Konfigurations-Manager
- Erstellen von Konfigurationsbaselines für Kompatibilitätseinstellungen in Konfigurations-Manager
- Bereitstellen von Konfigurationsbaselines in Konfigurations-Manager

Verwandte Themen

- Sammeln von Windows Information Protection (WIP)-Überwachungsprotokollen
- Allgemeiner Leitfaden und bewährte Methoden für Windows Information Protection (WIP)
- Einschränkungen bei der Verwendung von Windows Information Protection (WIP)

Erstellen und Überprüfen eines Datenwiederherstellungs-Agent-Zertifikats des verschlüsselnden Dateisystems (Encrypting File System, EFS)

11.02.2020 • 6 minutes to read

Gilt für:

- Windows10, Version 1607 und höher
- Windows10 Mobile, Version 1607 und höher

Wenn Sie nicht bereits über ein EFS DRA-Zertifikat verfügen, müssen Sie ein Zertifikat erstellen und aus dem System extrahieren, bevor Sie Windows Information Protection (WIP) (früher als Unternehmensdatenschutz (EDP) bezeichnet) in Ihrer Organisation verwenden können. Für die Zwecke dieses Abschnitts verwenden wir den Dateinamen EFSDRA. Dieser Name kann jedoch durch einen für Sie sinnvollen Namen ersetzt werden.

Der in diesem Thema enthaltene Wiederherstellungsprozess funktioniert nur für Desktopgeräte. WIP löscht die Daten auf Windows10 Mobile-Geräten.

> **IMPORTANT**
>
> Wenn Sie bereits über ein EFS DRA-Zertifikat für Ihre Organisation verfügen, können Sie das Erstellen eines neuen Zertifikats überspringen. Verwenden Sie einfach Ihr aktuelles EFS DRA-Zertifikat in der Richtlinie. Weitere Informationen dazu, wann Sie eine PKI und die allgemeine Strategie zum Bereitstellen von DRA-Zertifikaten verwenden, finden Sie im Artikel Sicherheit auf dem Prüfstand Bereitstellen von EFS: Teil 1 bei TechNet. Allgemeine Informationen zum EFS-Schutz finden Sie unter Schützen von Daten mit EFS zum Verschlüsseln von Festplatten.
>
> Wenn Ihr DRA-Zertifikat abgelaufen ist, können Sie damit keine Dateien verschlüsseln. Um dieses Problem zu beheben, müssen Sie ein neues Zertifikat mithilfe der Schritte in diesem Thema erstellen und dann durch Richtlinien bereitstellen.

Manuelles Erstellen eines EFS-DRA-Zertifikats

1. Öffnen Sie auf einem Computer ohne installiertes EFS DRA-Zertifikat eine Eingabeaufforderung mit erhöhten Rechten, und navigieren Sie zu dem Speicherort, an dem das Zertifikat gespeichert werden soll.

2. Führen Sie folgenden Befehl aus:

   ```
   cipher /r:EFSRA
   ```

   Dabei ist *EFSRA* der Name der CER- und PFX-Datei, die Sie erstellen möchten.

3. Geben Sie bei Aufforderung ein Kennwort zum Schutz der neuen Personal Information Exchange-Datei (.pfx) ein, und bestätigen Sie dieses.

   Die Dateien EFSDRA.cer und EFSDRA.pfx werden an dem Speicherort erstellt, den Sie in Schritt1 angegeben haben.

> **IMPORTANT**
> Da die privaten Schlüssel in den DRA PFX-Dateien zum Entschlüsseln aller WIP-Dateien verwendet werden können, müssen sie entsprechend geschützt werden. Es wird dringend empfohlen, diese Dateien offline zu speichern und dabei Kopien auf einer Smartcard mit starkem Schutz zur normalen Nutzung und Masterkopien an einem sicheren physischen Speicherort beizubehalten.

4. Fügen Sie Ihr EFS-DRA-Zertifikat mit einem Bereitstellungstool wie Microsoft InTune oder Microsoft Endpoint Configuration Managerzu ihrer WIP-Richtlinie hinzu.

> **NOTE**
> Dieses Zertifikat kann in InTune für Richtlinien sowohl *mit* der Geräteregistrierung (MDM) als auch *ohne* Geräteregistrierung (MAM) verwendet werden.

Überprüfen, ob Ihr Datenwiederherstellungszertifikat auf einem WIP-Clientcomputer ordnungsgemäß eingerichtet ist

1. Suchen oder erstellen Sie eine mit Windows Information Protection verschlüsselte Datei. Sie können z.B. eine App in der Liste der zulässigen Apps öffnen und dann eine Datei erstellen und speichern, damit sie mit WIP verschlüsselt wird.

2. Öffnen Sie eine App in der Liste der geschützten Apps, und erstellen und speichern Sie dann eine Datei, damit sie mit WIP verschlüsselt wird.

3. Öffnen Sie eine Eingabeaufforderung mit erhöhten Rechten, navigieren Sie zu dem Speicherort, an dem Sie die gerade erstellte Datei gespeichert haben, und führen Sie folgenden Befehl aus:

   ```
   cipher /c filename
   ```

   Dabei ist *filename* der Name der Datei, die Sie in Schritt1 erstellt haben.

4. Stellen Sie sicher, dass das Datenwiederherstellungszertifikat in der Liste **Wiederherstellungszertifikate** aufgeführt ist.

Wiederherstellen Ihrer Daten mithilfe des EFS-DRA-Zertifikats in einer Testumgebung

1. Kopieren Sie die WIP-verschlüsselte Datei an einen Speicherort, für den Sie Administratorzugriff haben.

2. Installieren Sie die Datei EFSDRA.pfx unter Verwendung des Kennworts.

3. Öffnen Sie eine Eingabeaufforderung mit erhöhten Rechten, navigieren Sie zu der verschlüsselten Datei, und führen Sie folgenden Befehl aus:

   ```
   cipher /d encryptedfile.extension
   ```

   Dabei ist *encryptedfile.extension* der Name der verschlüsselten Datei. Beispiel: corporatedata.docx.

Wiederherstellung von WIP-Protected nach der Registrierung

Unter Umständen widerrufen Sie Daten von einem nicht registrierten Gerät, nur um sie später alle wiederherstellen zu wollen. Dies kann passieren, wenn ein fehlendes Gerät zurückgegeben wird oder wenn sich ein nicht registrierter Mitarbeiter erneut registriert. Wenn sich der Mitarbeiter erneut mit dem ursprünglichen Benutzerprofil anmeldet und der gesperrte Schlüsselspeicher weiterhin auf dem Gerät gespeichert ist, können alle

gesperrten Daten gleichzeitig wiederhergestellt werden.

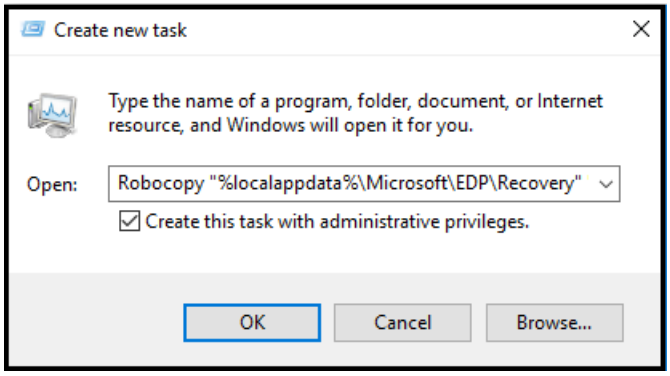
> **IMPORTANT**
> Um die Kontrolle über die Unternehmensdaten zu behalten und in Zukunft erneut widerrufen zu können, müssen Sie nur den folgenden Vorgang durchführen, nachdem der Mitarbeiter das Gerät erneut registriert hat.

1. Melden Sie sich beim Mitarbeiter des nicht registrierten Geräts an, öffnen Sie eine Eingabeaufforderung mit erhöhten Rechten, und geben Sie Folgendes ein:

   ```
   Robocopy "%localappdata%\Microsoft\EDP\Recovery" "new_location" * /EFSRAW
   ```

   Wobei sich "*new_location*" in einem anderen Verzeichnis befindet. Dies kann auf dem Gerät des Mitarbeiters oder in einem freigegebenen Ordner auf einem Computer erfolgen, auf dem Windows 8 oder Windows Server 2012 oder höher ausgeführt wird und auf die Sie zugreifen können, während Sie als Daten Wiederherstellungs-Agent angemeldet sind.

   Öffnen Sie den Task-Manager, um Robocopy im S-Modus zu starten. Klicken Sie auf**neue Aufgabe Datei** > ausführen, geben Sie den Befehl ein, und klicken Sie auf **diese Aufgabe mit Administratorrechten erstellen**.

   Wenn der Mitarbeiter eine Neuinstallation durchgeführt hat und kein Benutzerprofil vorhanden ist, müssen Sie die Schlüssel aus dem Ordner "System Volume" auf jedem Laufwerk wiederherstellen. Typ:

   ```
   Robocopy "drive_letter:\System Volume Information\EDP\Recovery" "new_location" * /EFSRAW
   ```

2. Melden Sie sich an einem anderen Gerät mit Administratoranmeldeinformationen mit Zugriff auf das DRA-Zertifikat Ihrer Organisation an, und führen Sie die Entschlüsselung und Wiederherstellung der Datei durch, indem Sie Folgendes eingeben:

   ```
   cipher.exe /D "new_location"
   ```

3. Lassen Sie Ihren Mitarbeiter sich am nicht registrierten Gerät anmelden, und geben Sie Folgendes ein:

   ```
   Robocopy "new_location" "%localappdata%\Microsoft\EDP\Recovery\Input"
   ```

4. Bitten Sie den Mitarbeiter, das Gerät zu sperren und zu entsperren.

   Der Windows-Dienst für Anmeldeinformationen stellt die zuvor gesperrten Schlüssel des Mitarbeiters aus dem `Recovery\Input`-Speicherort automatisch wieder her.

Automatische Wiederherstellung von Verschlüsselungsschlüsseln

WIP enthält ab Windows10, Version 1709, eine Datenwiederherstellungsfunktion, die Ihren Mitarbeitern eine automatische Wiederherstellung des Zugriff auf die Arbeitsdateien ermöglichen, wenn der Verschlüsselungsschlüssel verloren geht und auf die Dateien nicht mehr zugegriffen werden kann. Dies erfolgt in der Regel dann, wenn ein Mitarbeiter ein Re-Imaging der Betriebssystempartition durchführt, die WIP-

Schlüsselinformationen entfernt oder ein Gerät als verloren meldet und versehentlich das falsche Gerät für die Deregistrierung verwendet.

Um sicherzustellen, dass Mitarbeiter immer auf Dateien zugreifen können, erstellt WIP einen automatischen Wiederherstellungsschlüssel, der in der Identität des Azure Active Directory (Azure AD) gesichert ist.

Die Erfahrung der Mitarbeiter hängt von der Anmeldung auf dem Azure AD-Geschäftskonto ab. Der Mitarbeiter kann:

- Fügen Sie ein Geschäftskontos über das Menü **Windows-Einstellungen > Konten > Geschäfts- oder Schulkonto öffnen > Verbinden** hinzu.

  – ODER –

- Öffnen Sie **Windows-Einstellungen > Konten > Geschäfts- oder Schulkonto öffnen > Verbinden**, und wählen Sie den Link **Dieses Gerät in Azure Active Directory einbinden** unter **alternative Aktionen**.

  > **NOTE**
  > Um einer Azure AD-Domäne von der Seite "Einstellungen" beizutreten, muss der Mitarbeiter auf dem Gerät Administratorrechte haben.

Nach der Anmeldung wird die erforderliche WIP-Schlüssel-Informationen automatisch heruntergeladen und Mitarbeiter können auf die Dateien erneut zugreifen.

Testen Sie, was der Mitarbeiter während des WIP-Schlüssel-Wiederherstellungsprozesses sieht

1. Versuchen Sie, eine Arbeitsdatei auf einem nicht registrierten Gerät zu öffnen.

   Das Feld **Verbinden mit Ihrem Arbeitsplatz, um auf Arbeitsdateien zuzugreifen** wird angezeigt.

2. Klicken Sie auf **Verbinden**.

   Die Seite **Auf Arbeits- oder Schulkonto zugreifen** wird angezeigt.

3. Melden Sie sich bei Azure AD als Mitarbeiter an und stellen Sie sicher, dass Sie die Dateien jetzt öffnen können

Verwandte Themen

- Sicherheit auf dem Prüfstand – Bereitstellen von EFS: Teil 1
- Schützen von Daten durch Verschlüsseln von Festplatten mit EFS
- Erstellen einer Windows Information Protection (WIP)-Richtlinie mithilfe von Microsoft Intune
- Erstellen einer Windows Information Protection (WIP)-Richtlinie mit Microsoft Endpoint Configuration Manager
- Erstellen eines domänenbasierten Wiederherstellungs-Agents

> **NOTE**
> Tragen Sie dazu bei, dieses Thema zu verbessern, indem Sie uns Bearbeitungen, Ergänzungen und Feedback schicken. Weitere Informationen zur Teilnahme an diesem Thema finden Sie unter Zu diesem Artikel beitragen.

Ermitteln des Unternehmenskontexts einer App, die in Windows Information Protection ausgeführt wird

12.09.2019 • 2 minutes to read

Betrifft:

- Windows10, Version 1607 und höher
- Windows10 Mobile, Version 1607 und höher

> Unter Vergleichen von Windows10-Editionen erfahren Sie, welche Features und Funktionen von den einzelnen Windows-Editionen unterstützt werden.

Verwenden Sie Task-Manager, um den Kontext Ihrer Apps während der Ausführung in Windows Information Protection (WIP) zu überprüfen und sicherzustellen, dass die Richtlinien Ihres Unternehmens angewendet und ordnungsgemäß ausgeführt werden.

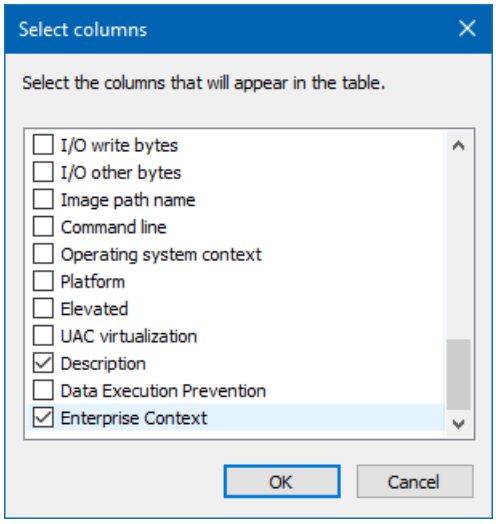
Anzeigen der Unternehmenskontextspalte im Task-Manager

Sie müssen die Unternehmenskontextspalte der Registerkarte **Details** im Task-Manager hinzufügen.

1. Stellen Sie sicher, dass Sie eine aktive WIP-Richtlinie bereitgestellt und in Ihrer Organisation aktiviert haben.

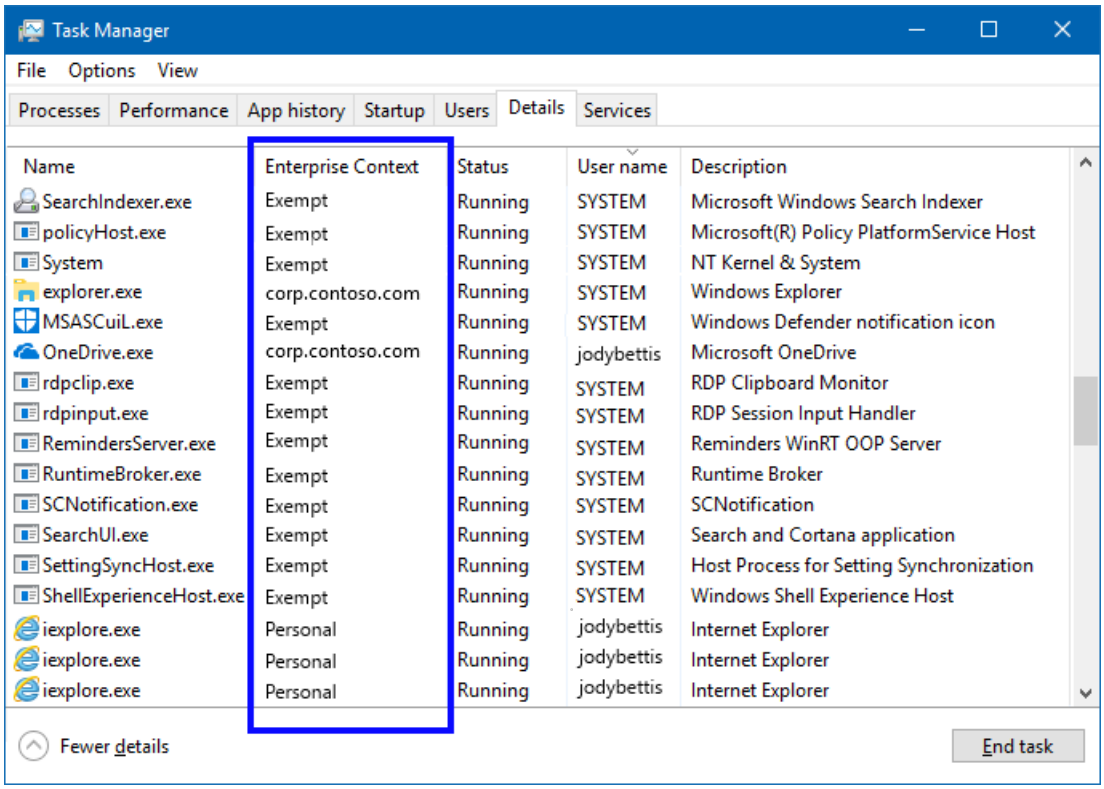
2. Öffnen Sie den Task-Manager (taskmgr.exe), klicken Sie auf die Registerkarte **Details**, klicken Sie mit der rechten Maustaste in den Bereich der Spaltenüberschrift, und klicken Sie auf **Spalten auswählen**.

   Das Feld **Spalten auswählen** wird angezeigt.



3. Führen Sie einen Bildlauf nach unten aus, und aktivieren Sie die Option für den **Unternehmenskontext**, und klicken Sie dann auf **OK**, um das Dialogfeld zu schließen.

   Die Spalte **Unternehmenskontext** sollte nun im Task-Manager verfügbar sein.



Überprüfen des Unternehmenskontexts

Die Spalte **Unternehmenskontext** zeigt, wie die einzelnen Apps Ihre Unternehmensdaten nutzen können:

- **Domäne.** Zeigt die Arbeitsdomänen des Mitarbeiters (z.B. corp.contoso.com). Diese App gilt als geschäftliche und kann ungehindert auf Arbeitsdaten und -ressourcen zugreifen und diese öffnen.
- **Persönlich.** Zeigt den Text *Persönlich*. Diese App wird als nicht geschäftlich eingestuft und kann nicht auf Arbeitsdaten oder -ressourcen zugreifen.
- **Ausnahme.** Zeigt den Text *Ausnahme*. WIP-Richtlinien gelten nicht für diese Apps (z.B. Systemkomponenten).

> **Wichtig**
> Optimierte Apps können zwischen „Geschäftlich" und „Persönlich" wechseln, abhängig von den Daten, auf die zugegriffen wird. Microsoft Word 2016 wird z.B. als **Persönlich** angezeigt, wenn ein Mitarbeiter einen persönlichen Brief öffnet. Das Programm wird zu **Geschäftlich**, wenn derselbe Mitarbeiter die Finanzdaten des Unternehmens öffnet.

Obligatorische Aufgaben und Einstellungen, die zum Aktivieren von Windows Information Protection (WIP) erforderlich sind

24.12.2019 • 2 minutes to read

Gilt für:

- Windows10, Version 1607 und höher
- Windows10 Mobile, Version 1607 und höher

Diese Liste enthält alle Aufgaben und Einstellungen, die für das Betriebssystem erforderlich sind, damit Windows Information Protection (vormals Enterprise Data Protection, EDP) in Ihrem Unternehmen aktiviert werden kann.

AUFGABE	BESCHREIBUNG
Fügen Sie der Liste der **geschützten apps** in ihrer WIP-Richtlinie mindestens eine APP hinzu.	Sie müssen mindestens eine App zur Liste der **geschützten apps** hinzugefügt haben. Weitere Informationen dazu, wo sich dieser Bereich befindet und wie apps hinzugefügt werden, finden Sie im Abschnitt **Hinzufügen von apps zu ihrer geschützten apps-Liste** in den Themen zur Richtlinienerstellung.
Wählen Sie Ihre WIP-Schutzebene aus.	Sie müssen die Schutzebene auswählen, die Sie auf Ihre WIP-geschützten Inhalte anwenden möchten, einschließlich **Zulassen von Überschreibungen**, **Silent**oder **Block**. Weitere Informationen dazu, wo Sie diesen Bereich finden und wie Sie die Schutzebene bestimmen, finden Sie in den Themen zum Erstellen von Richtlinien im Abschnitt **Verwalten des WIP-Schutzmodus für Ihre Unternehmensdaten**. Weitere Informationen zum Erfassen Ihrer Überwachungsprotokolldateien finden Sie unter Erfassen von Windows Information Protection (WIP)-Überwachungsprotokolldateien.
Geben Sie Ihre Unternehmensidentität an.	Dieses Feld wird von Microsoft Intune automatisch für Sie ausgefüllt. Korrigieren Sie diesen Wert manuell, falls Sie einen Fehler finden oder zusätzliche Domänen hinzufügen möchten. Weitere Informationen dazu, wo Sie diesen Bereich finden und wozu Sie ihn verwenden, finden Sie in den Themen zum Erstellen von Richtlinien im Abschnitt **Definieren der intern verwalteten Unternehmensidentität**.
Geben Sie Ihre Netzwerkdomänennamen an.	Ab Windows10, Version 1703, ist dieses Feld optional. Geben Sie die in Ihrer Umgebung verwendeten DNS-Suffixe an. Der gesamte Datenverkehr zu den vollqualifizierten Domänen, die in dieser Liste enthalten sind, wird geschützt. Weitere Informationen dazu, wo Sie diesen Bereich finden und wie Sie Suffixe hinzufügen, finden Sie in den Themen zum Erstellen von Richtlinien in der Tabelle im Abschnitt **Auswählen der Speicherorte, an denen Apps Zugriff auf Unternehmensdaten haben**.

AUFGABE	BESCHREIBUNG
Geben Sie die IPv4- oder IPv6-Bereiche Ihres Unternehmens an.	Ab Windows10, Version 1703, ist dieses Feld optional. Geben Sie die Adressen für einen gültigen IPv4- oder IPv6-Wertbereich in Ihrem Intranet an. Diese in Verbindung mit Ihren Netzwerkdomänennamen verwendeten Adressen definieren die Grenzen Ihres Unternehmensnetzwerks. Weitere Informationen dazu, wo Sie diesen Bereich finden und wozu Sie ihn verwenden, finden Sie in den Themen zum Erstellen von Richtlinien in der Tabelle im Abschnitt **Definieren der intern verwalteten Unternehmensidentität**.
Schließen Sie Ihr Datenwiederherstellungs-Agent-Zertifikat ein.	Ab Windows10, Version 1703, ist dieses Feld optional. Wir empfehlen jedoch dringend, ein Zertifikat hinzuzufügen. Dieses Zertifikat stellt sicher, dass alle WIP-verschlüsselten Daten selbst beim Verlust der Sicherheitsschlüssel entschlüsselt werden können. Weitere Informationen dazu, wo Sie diesen Bereich finden und welche Bedeutung er hat, finden Sie im Thema Erstellen und Überprüfen eines DRA-Zertifikats (Data Recovery Agent, Datenwiederherstellungs-Agent) des verschlüsselnden Dateisystems (Encrypting File System, EFS)).

NOTE

Tragen Sie dazu bei, dieses Thema zu verbessern, indem Sie uns Bearbeitungen, Ergänzungen und Feedback schicken. Informationen dazu, wie Sie zu diesem Thema beitragen können, finden Sie unter Bearbeiten der Windows IT Professional-Dokumentation.

Testszenarios für Windows Information Protection (WIP)

11.02.2020 • 9 minutes to read

Betrifft:

- Windows10, Version1607 und höher
- Windows10 Mobile, Version1607 und höher

Wir haben eine Liste mit Vorschlägen für Testszenarien zusammengestellt, die Sie verwenden können, um Windows Information Protection (WIP) in Ihrem Unternehmen zu testen.

Testszenarios

Sie können versuchen, alle Prozesse in diesen Szenarien zu testen. Sie sollten jedoch den Schwerpunkt auf die Szenarien legen, die in Ihrer Organisation auftreten können.

> **IMPORTANT**
>
> Wenn eines dieser Szenarien nicht funktioniert, notieren Sie sich zunächst, ob WIP gesperrt wurde. Wenn dies der Fall ist, müssen unaufgeklärte apps deinstalliert und neu installiert werden, da ihre Einstellungsdateien verschlüsselt bleiben.

SZENARIO	PROZESSE

Verschlüsseln und Entschlüsseln von Dateien mit dem Datei-Explorer	**Desktops:** 1. Öffnen Sie den Datei-Explorer, klicken Sie mit der rechten Maustaste auf ein Arbeitsdokument, und klicken Sie dann auf **Arbeit** im Menü **Dateibesitz**. Stellen Sie sicher, dass die Datei verschlüsselt ist, indem Sie mit der rechten Maustaste erneut auf die Datei klicken, auf der Registerkarte **Allgemein** auf **Erweitert** klicken und anschließend im Bereich **Komprimierungs- und Verschlüsselungsattribute** auf **Details** klicken. Die Datei sollte unter der Überschrift **Der Zugriff kann von der folgenden Unternehmensdomäne entfernt oder widerrufen werden:** <*Identität_Ihres_Unternehmens*> angezeigt werden. Ein Beispiel ist contoso.com. 2. Klicken Sie im Datei-Explorer mit der rechten Maustaste auf das gleiche Dokument und anschließend im Menü **Dateibesitz** auf **Privat**. Stellen Sie sicher, dass die Datei entschlüsselt ist, indem Sie mit der rechten Maustaste erneut auf die Datei klicken, auf der Registerkarte **Allgemein** auf **Erweitert** klicken und anschließend überprüfen, ob die Schaltfläche **Details** nicht verfügbar ist. **Mobile Geräte:** 1. Öffnen Sie die Datei-Explorer-App, navigieren Sie zum Speicherort einer Datei, klicken Sie auf die Auslassungspunkte (...), und klicken Sie dann auf **Auswählen**, um mindestens eine Datei als arbeitsbezogen zu markieren. 2. Klicken Sie erneut auf die Auslassungspunkte (...), klicken Sie im Dropdownmenü auf **Dateibesitz**, und klicken Sie dann auf **Arbeit**. Stellen Sie sicher, dass die Datei verschlüsselt ist, indem Sie das Symbol **Aktenkoffer** neben dem Dateinamen suchen. 3. Wählen Sie dieselbe Datei aus, klicken Sie im Dropdownmenü auf **Dateibesitz**, und klicken Sie anschließend auf **Privat**. Stellen Sie sicher, dass die Datei entschlüsselt ist und Sie'das Symbol "Akten **Koffer** " nicht mehr neben dem Dateinamen sehen.

Erstellen von Arbeitsdokumenten in für das Unternehmen zugelassenen Apps	**Desktops:** • Starten Sie eine nicht optimierte, jedoch zulässige App, z.B. eine Branchen-App, erstellen Sie ein neues Dokument, und speichern Sie Ihre Änderungen. Stellen Sie sicher, dass das Dokument für Ihre Unternehmensidentität verschlüsselt wird. Dies kann einige Minuten dauern. Sie müssen die Datei schließen und erneut öffnen. **Wichtig** Bestimmte Dateitypen, z.B. `.exe` und `.dll`, sowie bestimmte Dateipfade, z.B. `%windir%` und `%programfiles%`, sind von der automatischen Verschlüsselung ausgenommen. Weitere Informationen zu Ihrer Unternehmensidentität und zum Hinzufügen von apps zur Liste der zulässigen apps finden Sie unter Erstellen einer Windows Information Protection (WIP)- Richt Linie mithilfe von Microsoft InTune oder Erstellen einer Windows Information Protection (WIP)-Richtlinie mithilfe von Microsoft Endpoint Configuration Manager, basierend auf Ihrem Bereitstellungssystem. **Mobile Geräte:** 1. Starten Sie eine zulässige mobile App, z.B. Word Mobile, erstellen Sie ein neues Dokument, und speichern Sie dann Ihre Änderungen als **Arbeit** an einem lokalen, arbeitsbezogenen Speicherort. Stellen Sie sicher, dass das Dokument verschlüsselt ist, indem Sie das Symbol **Aktenkoffer** neben dem Dateinamen suchen. 2. Öffnen Sie dasselbe Dokument, und versuchen Sie, es an einem nicht arbeitsbezogenen Speicherort zu speichern. WIP sollte Sie daran hindern, die Datei an diesem Speicherort zu speichern. 3. Öffnen Sie dasselbe Dokument ein letztes Mal, ändern Sie den Inhalt, und speichern Sie es erneut mithilfe der Option **Privat**. Stellen Sie sicher, dass die Datei entschlüsselt ist und Sie'das Symbol "Akten **Koffer** " nicht mehr neben dem Dateinamen sehen.
Blockieren von Unternehmensdaten aus anderen als Unternehmens-Apps	1. Starten Sie eine APP, die't in der Liste der zulässigen apps angezeigt wird, und versuchen Sie dann, eine Arbeits verschlüsselte Datei zu öffnen. Die APP sollte't in der Lage sein, auf die Datei zuzugreifen. 2. Versuchen Sie, auf die verschlüsselte arbeitsbezogene doppelzuklicken oder zu tippen. Wenn es sich bei der standardmäßig verknüpften App um eine App handelt, die nicht in der Liste der zugelassenen Apps enthalten ist, sollte Ihnen die Fehlermeldung **Zugriff verweigert** angezeigt werden.

Kopieren und Einfügen aus Unternehmens-Apps in andere als Unternehmens-Apps	1. Kopieren Sie (STRG + C) Inhalte aus einer APP in der Liste der zulässigen apps, und versuchen Sie dann, den Inhalt in eine APP einzufügen, die in der Liste der zulässigen apps nicht'angezeigt wird. Ihnen sollte ein WIP-bezogenes Warnungsfeld angezeigt werden, in dem Sie aufgefordert werden, entweder auf **In „Privat“ ändern** oder **Keep at work** (Als arbeitsbezogen beibehalten) zu klicken. 2. Klicken Sie auf **Keep at work** (Als arbeitsbezogen beibehalten). Der Inhalt wird nicht in die nicht-Enterprise-App'eingefügt. 3. Wiederholen Sie Schritt1, klicken Sie dieses Mal jedoch auf **In „Privat“ ändern**, und versuchen Sie erneut, den Inhalt einzufügen. Der Inhalt wird in die App eingefügt, die nicht in der Liste der zulässigen Apps enthalten ist. 4. Versuchen Sie, Inhalte zwischen Apps in der Liste der zulässigen Apps zu kopieren und einzufügen. Das Kopieren und Einfügen zwischen den Apps sollte möglich sein, ohne dass Warnmeldungen angezeigt werden.
Ziehen und Ablegen aus Unternehmens-Apps in andere als Unternehmens-Apps	1. Ziehen Sie Inhalte aus einer APP in der Liste der zulässigen apps, und versuchen Sie dann, den Inhalt in einer APP zu löschen, die in der Liste der zulässigen apps nicht'angezeigt wird. Ihnen sollte ein WIP-bezogenes Warnungsfeld angezeigt werden, in dem Sie aufgefordert werden, entweder auf **Keep at work** (Als arbeitsbezogen beibehalten) oder auf **In „Privat“ ändern** zu klicken. 2. Klicken Sie auf **Keep at work** (Als arbeitsbezogen beibehalten). Der Inhalt isn't in der nicht-Enterprise-App abgelegt. 3. Wiederholen Sie Schritt1, klicken Sie dieses Mal jedoch auf **In „Privat“ ändern**, und versuchen Sie erneut, den Inhalt abzulegen. Der Inhalt wird in der App abgelegt, die nicht in der Liste der zulässigen Apps enthalten ist. 4. Versuchen Sie Inhalt zwischen Apps in der Liste der zulässigen Apps zu ziehen und abzulegen. Der Inhalt sollte zwischen den Apps verschoben werden können, ohne dass eine Warnmeldung angezeigt wird.

Teilen zwischen Unternehmens-Apps und anderen als Unternehmens-Apps	1. Öffnen Sie eine app in der Liste der zulässigen apps wie Microsoft Fotos, und versuchen Sie, Inhalte für eine APP freizugeben, die in der Liste der zulässigen apps wie Facebook nicht angezeigt'. Ihnen sollte ein WIP-bezogenes Warnungsfeld angezeigt werden, in dem Sie aufgefordert werden, entweder auf **Keep at work** (Als arbeitsbezogen beibehalten) oder auf **In „Privat“ ändern** zu klicken. 2. Klicken Sie auf **Keep at work** (Als arbeitsbezogen beibehalten). Der Inhalt ist't in Facebook geteilt. 3. Wiederholen Sie Schritt1, klicken Sie dieses Mal jedoch auf **In „Privat“ ändern**, und versuchen Sie erneut, den Inhalt zu teilen. Der Inhalt wird auf Facebook geteilt. 4. Versuchen Sie, Inhalt zwischen Apps in der Liste der zulässigen Apps zu teilen. Der Inhalt sollte zwischen den Apps geteilt werden können, ohne dass eine Warnmeldung angezeigt wird.
Überprüfen, ob Windows-Systemkomponenten WIP verwenden können	1. Starten Sie Windows Journal und Internet Explorer11, und erstellen, bearbeiten und speichern Sie Dateien in beiden Apps. Stellen Sie sicher, dass alle Dateien, mit denen Sie gearbeitet haben, für Ihre konfigurierte Unternehmensidentität verschlüsselt sind. In einigen Fällen müssen Sie die Datei schließen und einige Minuten warten, bis die Datei automatisch verschlüsselt wurde. 2. Öffnen Sie den Datei-Explorer, und stellen Sie sicher, dass die geänderten Dateien mit einem **Schlosssymbol** angezeigt werden. 3. Versuchen Sie, Inhalte durch Kopieren und Einfügen, durch Ziehen und Ablegen und durch Teilen zwischen diesen Apps und anderen Apps (sowohl solchen auf der Liste der zulässigen Apps als auch anderen) zu übertragen. **Hinweis** Die meisten Windows-signierten Komponenten wie der Datei-Explorer (bei Ausführung im Kontext des Benutzers) sollten auf Unternehmensdaten zugreifen können. Einige wichtige Ausnahmen sind bestimmte Apps, die zur Interaktion mit dem Benutzer konzipiert sind, beispielsweise Wordpad, Editor, und Microsoft Paint. Diese apps haben standardmäßig keinen Zugriff auf't, können aber der Liste der zugelassenen apps hinzugefügt werden.

Verwenden von WIP auf NTFS-, FAT- und exFAT-Systemen	1. Starten Sie eine App, die das FAT- oder ExFAT-Dateisystem verwendet (z.B. eine SD-Karte oder ein USB-Speicherstick) und in der Liste der zulässigen Apps angezeigt wird. 2. Erstellen, bearbeiten, schreiben, speichern, kopieren und verschieben Sie Dateien. Grundlegende Datei- und Ordnervorgänge wie Kopieren, Verschieben, Umbenennen, Löschen usw. sollten bei verschlüsselten Dateien ordnungsgemäß funktionieren.
Überprüfen, ob Ihre freigegebenen Dateien WIP verwenden können	1. Laden Sie eine Datei von einer geschützten Dateifreigabe herunter, und stellen Sie sicher, dass die Datei verschlüsselt ist, indem Sie das Symbol **Aktenkoffer** neben dem Dateinamen suchen. 2. Öffnen Sie dieselbe Datei, führen Sie eine Änderung durch, speichern Sie die Datei, und versuchen Sie anschließend, die Datei wieder zur Dateifreigabe hochzuladen. Auch dieser Vorgang sollte ohne Warnungen funktionieren. 3. Öffnen Sie eine APP, die't in der Liste der zulässigen apps angezeigt wird, und versuchen Sie, auf eine Datei auf der WIP-aktivierten Dateifreigabe zuzugreifen. Die APP sollte't in der Lage sein, auf die Dateifreigabe zuzugreifen.
Überprüfen, ob Ihre Cloudressourcen WIP verwenden können	1. Fügen Sie der Liste zulässiger Apps sowohl Internet Explorer11 als auch Microsoft Edge hinzu. 2. Öffnen Sie SharePoint (oder eine andere Cloud-Ressource,'die Teil ihrer Richtlinie ist), und greifen Sie mithilfe von IE11 und Microsoft Edge auf eine WIP-fähige Ressource zu. Beide Browser sollten die Grenze zwischen Unternehmen und Privat respektieren. 3. Entfernen Sie Internet Explorer11 aus der Liste der zulässigen Apps, und versuchen Sie anschließend, auf eine Intranetsite oder eine unternehmensbezogenen Cloudressource zuzugreifen. IE11 sollte't auf die Websites zugreifen können. **Hinweis** Jede Datei, die von der arbeitsbezogenen SharePoint-Site oder einer anderen WIP-fähigen Cloudressource heruntergeladen wird, wird automatisch als **arbeitsbezogen** gekennzeichnet.

Überprüfen, ob Ihr Virtual Private Network (VPN) automatisch ausgelöst werden kann	1. Richten Sie das VPN-Netzwerk für einen Start auf der Basis der Einstellung **WIPModeID** ein. Spezifische Informationen dazu, wie Sie dies tun können, finden Sie im Thema Erstellen und Bereitstellen einer VPN-Richtlinie für Windows Information Protection (WIP) mithilfe von Microsoft Intune. 2. Starten Sie eine App aus der Liste der zulässigen Apps. Das VPN-Netzwerk sollte automatisch gestartet werden. 3. Trennen Sie die Verbindung zu Ihrem Netzwerk, und starten Sie dann eine APP, die nicht't in der Liste der zulässigen Apps ist. Das VPN sollte't starten, und die APP sollte't in der Lage sein, auf Ihr Unternehmensnetzwerk zuzugreifen.
Aufheben der Registrierung von Clientgeräten in WIP	• Sie können die Registrierung eines Geräts in WIP aufheben, indem Sie unter **Einstellungen** nacheinander auf **Konten**, **Arbeit** und dann auf den Namen des Geräts klicken, für das Sie die Registrierung aufheben möchten. Klicken Sie dann auf **Entfernen**. Das Gerät sollte nun entfernt sein, und alle Unternehmensinhalte für das verwaltete Konto sollten gelöscht sein. **Wichtig** Auf Desktopgeräten werden die Daten nicht't entfernt und können wiederhergestellt werden, daher müssen Sie sicherstellen, dass der Inhalt **als wider** rufen gekennzeichnet ist und der Zugriff für den Mitarbeiter verweigert wird. Auf mobilen Geräten werden die Daten entfernt.
Stellen Sie sicher, dass App-Inhalte geschützt sind, wenn ein Windows10 Mobile-Telefon gesperrt ist.	• Überprüfen Sie, ob geschützte App-Daten't auf dem Sperrbildschirm eines Windows 10-Mobiltelefons angezeigt werden.
Beenden Sie die Synchronisierung von WIP-geschützten Dateien und Ordnern durch Google Drive.	• Fügen Sie in der unbeaufsichtigten Konfiguration Google Drive zu geschützten apps hinzu, und setzen Sie es auf verweigern. Auf diese Weise synchronisiert Google Drive keine WIP-geschützten Dateien und Ordner. • Informationen zu Google Drive Publisher = O = Google LLC, L = Mountain View, S = ca, C = US File = GOOGLEDRIVESYNC. EXE

NOTE

Tragen Sie dazu bei, dieses Thema zu verbessern, indem Sie uns Bearbeitungen, Ergänzungen und Feedback schicken. Informationen dazu, wie Sie zu diesem Thema beitragen können, finden Sie unter Bearbeiten der Windows IT Professional-Dokumentation.

Einschränkungen bei der Verwendung von Windows Information Protection (WIP)

15.02.2020 • 6 minutes to read

Betrifft:

- Windows10, Version1607 und höher
- Windows10 Mobile, Version1607 und höher

Diese Tabelle enthält Informationen zu den häufigsten Problemen, die während der Ausführung von WIP in Ihrer Organisation auftreten können.

EINSCHRÄNKUNG	PROBLEM	PROBLEMUMGEHUNG
Ihre Unternehmensdaten auf USB-Laufwerken sind möglicherweise an das Gerät gebunden, auf dem sie geschützt wurden, basierend auf Ihrer Azure RMS-Konfiguration.	**Wenn Sie Azure RMS verwenden:** Authentifizierte Benutzer auf Computern mit Windows10 Version 1703 können Unternehmensdaten auf USB-Laufwerken öffnen. **Wenn Sie Azure RMS nicht verwenden:** Daten am neuen Speicherort bleiben verschlüsselt, auf anderen Geräten bzw. von anderen Benutzern kann nicht mehr auf die Daten zugegriffen werden. Beispielsweise wird die Datei gewonnen't öffnen oder die Datei wird geöffnet, aber't enthalten lesbaren Text.	Geben Sie Dateien über Unternehmensdateiserver oder in der Unternehmenscloud für Mitarbeiter frei. Wenn Daten über USB freigegeben werden müssen, können Mitarbeiter geschützte Dateien entschlüsseln, die Daten werden aber überwacht. Sie sollten Ihre Mitarbeiter unbedingt aufklären, wie sie Situationen einschränken oder gänzlich vermeiden, in denen diese Entschlüsselung erforderlich ist.
Direct Access ist nicht mit WIP kompatibel.	Bei Direct Access können Probleme dadurch auftreten, wie WIP das App-Verhalten und Datenverschiebungen erzwingt. Dies liegt an der Weise, wie WIP bestimmt, welche Ressource eine Unternehmensnetzwerkressource ist und welche nicht.	Wir empfehlen die Verwendung eines VPNs für den Clientzugriff auf Ihre Intranetressourcen. **Hinweis** Ein VPN ist optional und nicht für WIP erforderlich.
NetworkIsolation: Die Einstellung dieser Gruppenrichtlinie hat Vorrang vor den Einstellungen in der MDM-Richtlinie.	Die Gruppenrichtlinien-Einstellung **NetworkIsolation** kann Netzwerkeinstellungen festlegen, die auch mithilfe von MDM konfiguriert werden können. WIP verlässt sich darauf, dass diese Richtlinien ordnungsgemäß konfiguriert sind.	Wenn Sie sowohl Gruppenrichtlinien und MDM für die Konfiguration Ihrer **NetworkIsolation**-Einstellungen verwenden, müssen Sie darauf achten, dass Gruppenrichtlinien und MDM dieselben Einstellungen für Ihre Organisation bereitstellen.

Cortana kann Datenverluste verursachen, wenn sie in der Liste zugelassener Apps enthalten ist.	Wenn Cortana in der Liste zugelassener Apps enthalten ist, können einige Dateien unerwartet verschlüsselt werden, nachdem ein Mitarbeiter eine Suche mit Cortana ausgeführt hat. Ihre Mitarbeiter können Cortana weiterhin für die Suche und zum Bereitstellen von Ergebnissen aus Unternehmensdokumenten und -verzeichnissen verwenden, allerdings können Ergebnisse an Microsoft gesendet werden.	Es wird davon abgeraten, Cortana der Liste zugelassener Apps hinzuzufügen. Wenn Sie jedoch Cortana verwenden möchten und'nicht davon ausgehen, ob die Ergebnisse potenziell zu Microsoft führen, können Sie Cortana zu einer ausgeschlossenen app machen.
WIP ist für die Verwendung durch einen Einzelbenutzer pro Gerät vorgesehen.	Wenn das Gerät von einem zweiten Benutzer verwendet wird, können App-Kompatibilitätsprobleme auftreten, sobald nicht optimierte Apps automatisch eine Verschlüsselung für alle Benutzer starten. Außerdem können nur Inhalte des ursprünglichen, registrierten Benutzers widerrufen werden, während die Registrierung aufgehoben wird.	Ein verwaltetes Gerät sollte jeweils nur von einem Benutzer verwendet werden.
Installationsprogramme, die von einer Dateifreigabe im Unternehmensnetzwerk kopiert wurden, funktionieren möglicherweise nicht ordnungsgemäß.	Eine App wird u. U. nicht ordnungsgemäß installiert, da eine erforderliche Konfigurations- oder Datendatei nicht gelesen werden kann. Dies kann z.B. eine für die Installation benötigte CAB-oder XML-Datei sein, die die durch die Kopieraktion geschützt wurde.	Sie können das Problem wie folgt beheben: • Starten Sie das Installationsprogramm direkt von der Dateifreigabe. –ODER– • Entschlüsseln Sie die vom Installationsprogramm benötigten, lokal kopierten Dateien. –ODER– • Kennzeichnen Sie die Dateifreigabe mit dem Installationsmedium als „Persönlich". Dazu müssen Sie die Unternehmens-IP-Bereiche auf **Autoritativ** festlegen und dann die IP-Adresse des Dateiservers ausschließen. Alternativ müssen Sie den Dateiserver in die Liste der Unternehmensproxyserver aufnehmen.
Das Ändern der primären Unternehmensidentität wird nicht unterstützt.	Es können verschiedene Instabilitäten auftreten, u. a. Netzwerk- und Dateizugriffsfehler und mögliche Fehler beim Gewähren von Zugriffsrechten.	Deaktivieren Sie WIP für alle Geräte, bevor Sie die primäre Unternehmensidentität (den ersten Eintrag in der Liste) ändern und einen Neustart und anschließend eine erneute Bereitstellung ausführen.

Umgeleitete Ordner mit clientseitiger Zwischenspeicherung sind nicht mit WIP kompatibel.	In Apps können beim Versuch, eine zwischengespeicherte Offlinedatei zu lesen, Zugriffsfehler auftreten.	Verwenden Sie eine andere Dateisynchronisierungsmethode, z.B. Arbeitsordner oder OneDrive for Business. **Hinweis** Weitere Informationen zur Verwendung von Arbeitsordnern und Offlinedateien finden Sie im Blogbeitrag Arbeitsordner- und Offlinedateiunterstützung für Windows Information Protection. Wenn Sie Probleme beim Öffnen von Dateien offline während der Verwendung von Offlinedateien und WIP'haben, lesen Sie den Support Artikel, können Sie Dateien offline öffnen', wenn Sie Offlinedateienund Windows-Informationsschutz verwenden.
Ein nicht verwaltetes Gerät kann Remote Desktop Protokoll (RDP) verwenden, um eine Verbindung mit einem WIP-verwalteten Gerät herzustellen.	Aus dem WIP-verwalteten Gerät kopierte Daten werden als "Arbeit" gekennzeichnet. Daten, die auf das WIP-verwaltete Gerät kopiert wurden, **sind**nicht als Arbeit markiert. Lokale **Arbeits** Daten, die auf das WIP-verwaltete Gerät **kopiert** wurden, bleiben Arbeitsdaten. **Arbeits** Daten, die zwischen zwei apps in derselben Sitzung kopiert werden, bleiben Daten.	Deaktivieren Sie RDP, um den Zugriff zu verhindern, da es keine Möglichkeit gibt, den Zugriff auf Geräte zu beschränken, die von WIP verwaltet werden. RDP ist standardmäßig deaktiviert.
Mit Microsoft Edge oder Internet Explorer können Sie eine Enterprise-Datei an einen persönlichen Speicherort't hochladen.	Es wird eine Meldung angezeigt, die besagt, dass der **Inhalt** als "Arbeit" markiert ist, und der Benutzer isn'**t**eine Option zum Überschreiben auf "persönlich" erhält.	Öffnen Sie den Datei-Explorer, und ändern Sie den Dateibesitz vor dem Hochladen in **Persönlich**.
ActiveX-Steuerelemente sollten mit Vorsicht verwendet werden.	Webseiten, die ActiveX-Steuerelemente verwenden, können potenziell mit anderen externen Prozessen kommunizieren, die nicht durch WIP geschützt sind.	Es wird empfohlen, Microsoft Edge zu verwenden. Dieser Browser ist sicherer und verhindert die Verwendung von ActiveX-Steuerelementen. Außerdem wird empfohlen, die Verwendung von Internet Explorer11 auf die Branchen-Apps zu beschränken, für die diese Vorgängertechnologie erforderlich ist. Weitere Informationen finden Sie unter Blockieren veralteter ActiveX-Steuerelemente.
Das elastische Datei System (ReFS) isn't derzeit mit WIP unterstützt.	Der Versuch, WIP-Dateien auf ReFS zu speichern oder zu übertragen wird fehlschlagen.	Formatieren Sie das Laufwerk für NTFS, oder verwenden Sie ein anderes Laufwerk.

WIP ist nicht aktiviert, wenn für einen der folgenden Ordner die Option **MakeFolderAvailableOfflineDisabled** auf **False** festgelegt ist: • AppDataRoaming • Desktop • StartMenu • Dokumente • Bilder • Musik • Videos • Favoriten • Kontakte • Downloads • Links • Suchvorgänge • SavedGames	WIP ist nicht für Mitarbeiter in Ihrer Organisation aktiviert. Fehlercode 0x807c0008 wird angezeigt, wenn WIP mithilfe von Microsoft Endpoint Configuration Manager bereitgestellt wird.	Legen Sie die Option **MakeFolderAvailableOfflineDisabled** für die genannten Ordner nicht auf **False** fest. Sie können diesen Parameter wie hier beschrieben konfigurieren. Wenn Sie umgeleitete Ordner verwenden, sollten Sie auf eine Lösung für die Dateisynchronisierung umsteigen, die WIP unterstützt, z.B. Arbeitsordner oder OneDrive for Business. Außerdem kann es passieren, dass Sie Ihre Dateien nicht mehr offline öffnen können, wenn Sie umgeleitete Ordner einrichten, nachdem WIP aktiviert wurde. Weitere Informationen zu diesen potenziellen Zugriffsfehlern finden Sie unter kann't Dateien offline öffnen, wenn Sie Offlinedateien und Windows-InformationsSchutz verwenden.
Nur erleuchtete Apps können ohne Geräteregistrierung verwaltet werden	Wenn ein Benutzer ein Gerät zur mobilen Anwendungsverwaltung (Mobile Application Management, MAM) ohne Geräteregistrierung anmeldet, werden nur aufgeklärte apps verwaltet. Dies ist beabsichtigt, um zu verhindern, dass persönliche Dateien von unenlighted-apps verschlüsselt unintenionally werden. Unenlighted-apps, die mit MAM auf Arbeit zugreifen müssen, müssen als Lob-apps neu kompiliert oder mithilfe von MDM mit Geräteregistrierung verwaltet werden.	Wenn alle apps verwaltet werden müssen, registrieren Sie das Gerät für MDM.
Im Design können Dateien im Windows-Verzeichnis (% windir% oder C:/Windows) nicht verschlüsselt werden, da Sie von jedem Benutzer aufgerufen werden müssen. Wenn eine Datei im Windows-Verzeichnis von einem Benutzer verschlüsselt einem wird, können andere Benutzer darauf't zugreifen.	Bei jedem Versuch, eine Datei im Windows-Verzeichnis zu verschlüsseln, wird der Fehler "Dateizugriff verweigert" zurückgegeben. Wenn Sie jedoch eine verschlüsselte Datei in das Windows-Verzeichnis kopieren oder ziehen und ablegen, bleibt die Verschlüsselung erhalten, um die Absicht des Besitzers zu berücksichtigen.	Wenn Sie eine verschlüsselte Datei im Windows-Verzeichnis speichern müssen, erstellen und verschlüsseln Sie die Datei in einem anderen Verzeichnis, und kopieren Sie Sie.

NOTE

Wenn Unternehmensdaten auf den Datenträger geschrieben werden, verwendet WIP das von Windows bereitgestellte verschlüsselnde Datei System (Encrypting File System, EFS), um es zu schützen und mit Ihrer Unternehmensidentität zu verknüpfen. Beachten Sie, dass der Vorschaubereich im Datei-Explorer für verschlüsselte Dateien nicht funktionieren kann.

NOTE

Chromium-basierte Versionen von Microsoft Edge (Versionen seit 79) unterstützen WIP noch nicht vollständig. Die Funktionalität kann teilweise aktiviert werden, indem Sie auf die lokale Seite **Edge://Flags/#Edge-DataProtection** wechseln und das **Windows-Informationsschutz** -Flag auf **Enabled**festlegen.

NOTE

Tragen Sie dazu bei, dieses Thema zu verbessern, indem Sie uns Bearbeitungen, Ergänzungen und Feedback schicken. Weitere Informationen zur Teilnahme an diesem Thema finden Sie unter Contributing to our content (in englischer Sprache).

Sammeln von Windows Information Protection (WIP)-Überwachungsprotokollen

31.12.2019 • 5 minutes to read

Betrifft:

- Windows10, Version 1607 und höher
- Windows10 Mobile, Version 1607 und höher

Windows Information Protection (WIP) erstellt Überwachungsereignisse für die folgenden Situationen:

- Wenn ein Mitarbeiter den Besitz einer Datei von **Arbeit** zu **Persönlich** ändert.
- Wenn Daten als **Arbeit** markiert sind und mit einer persönlichen App oder einer Webseite geteilt werden. Beispiele: Kopieren und Einfügen, Ziehen und Ablegen, Teilen von Kontakten, Upload auf eine persönliche Webseite, oder wenn ein Benutzer einer persönlichen App temporären Zugriff auf eine Arbeitsdatei erteilt.
- Wenn eine App benutzerdefinierte Überwachungsereignisse enthält.

Sammeln von WIP-Überwachungsprotokollen mit dem Reporting-Konfigurationsdienstanbieter (CSP)

Sie finden eine Anleitung zum Sammeln der WIP-Überwachungsprotokolle von den Geräten Ihrer Mitarbeiter in der Dokumentation des Reporting-Konfigurationsdienstanbieters (CSP). Dieses Thema enthält Informationen zu den eigentlichen Überwachungsereignissen.

> **NOTE**
>
> Das **Data**-Element in der Antwort enthält die angeforderten Überwachungsprotokolle in einem XML-codierten Format.

User-Element und Attribute

Diese Tabelle enthält alle verfügbaren Attribute für das **User**-Element.

ATTRIBUT	WERTTYP	BESCHREIBUNG
UserID	Zeichenfolge	Die Sicherheits-ID (SID) des entsprechenden Benutzers für diesen Überwachungsbericht.
EnterpriseID	Zeichenfolge	Die Enterprise-ID für diesen Überwachungsbericht.

Log-Element und Attribute

Diese Tabelle enthält alle verfügbaren Attribute/Elemente für das **Log**-Element. Die Antwort kann 0 (null) oder mehr **Log**-Elemente enthalten.

ATTRIBUT ODER ELEMENT	WERTTYP	BESCHREIBUNG
ProviderType	Zeichenfolge	Dieser Wert lautet immer **EDPAudit**.

ATTRIBUT ODER ELEMENT	WERTTYP	BESCHREIBUNG
LogType	Zeichenfolge	Enthält: • **DataCopied.** Arbeitsdaten wurden an einen persönlichen Speicherort kopiert oder freigegeben. • **ProtectionRemoved.** Der WIP-Schutz wurde von einer Arbeitsdatei entfernt. • **ApplicationGenerated.** Ein benutzerdefiniertes, von einer App bereitgestelltes Überwachungsprotokoll.
TimeStamp	Ganze Zahl	Verwendet die FILETIME-Struktur, um den Zeitpunkt darzustellen, zu dem das Ereignis aufgetreten ist.
Policy	Zeichenfolge	Gibt an, auf welche Art die Arbeitsdaten für den persönlichen Speicherort freigegeben wurden: • **CopyPaste.** Arbeitsdaten wurden in einen persönlichen Speicherort oder eine App eingefügt. • **ProtectionRemoved.** Der Schutz von Arbeitsdaten wurde aufgehoben. • **DragDrop.** Arbeitsdaten wurden per Ziehen und Ablegen in einen persönlichen Speicherort oder eine App eingefügt. • **Share.** Arbeitsdaten wurden für einen persönlichen Standort oder eine App freigegeben. • **NULL.** Alle nicht oben aufgeführten Methoden, mit denen Arbeitsdaten persönlich verwendet werden können. Beispiel: eine Arbeitsdatei wird mit einer persönlichen Anwendung (auch bekannt als temporärer Zugriff) geöffnet.
Justification	Zeichenfolge	Nicht implementiert. Dieser Wert ist immer leer oder NULL. **Hinweis:** Reserviert für die zukünftige Verwendung, um eine Begründung des Benutzers für den Wechsel von **Arbeit** zu **Persönlich** zu erfassen.

ATTRIBUT ODER ELEMENT	WERTTYP	BESCHREIBUNG
Object	Zeichenfolge	Eine Beschreibung der freigegebenen Arbeitsdaten. Wenn ein Mitarbeiter beispielsweise eine Datei mit einer persönlichen App öffnet, enthält dieses Feld den Dateipfad.
DataInfo	Zeichenfolge	Alle zusätzlichen Informationen zur Änderung der Arbeitsdatei: • **Ein Dateipfad.** Wenn ein Mitarbeiter eine Datei mit Microsoft Edge oder Internet Explorer auf einer persönlichen Website hochlädt, enthält dieses Feld den Pfad. • **Zwischenablage-Datentypen.** Wenn ein Mitarbeiter Arbeitsdaten in eine persönliche App einfügt, enthält dieses Feld die von der Arbeits-App bereitgestellte Liste der Zwischenablage-Datentypen. Weitere Informationen finden Sie im Abschnitt Beispiele in diesem Thema.
Action	Ganze Zahl	Enthält Informationen zum weiteren Ablauf, nachdem die Arbeitsdaten persönlich verwendet wurden, inklusive: • **1.** Datei entschlüsseln. • **2.** An Speicherort kopieren. • **3.** An Empfänger senden. • **4.** Sonstiges.
FilePath	Zeichenfolge	Der Pfad zu der im Überwachungsereignis angegebenen Datei. Beispielsweise der Speicherort einer Datei, die von einem Mitarbeiter entschlüsselt oder auf einer persönlichen Website hochgeladen wurde.
SourceApplicationName	Zeichenfolge	Die Quell-App oder Website. Für die Quell-App enthält dieses Feld die AppLocker-Identität. Für die Quell-Website enthält dieses Feld den Hostnamen.
SourceName	Zeichenfolge	Eine Zeichenfolge, die von der App bereitgestellt wird, die das Ereignis protokolliert. Diese Zeichenfolge beschreibt die Quelle der Arbeitsdaten.

ATTRIBUT ODER ELEMENT	WERTTYP	BESCHREIBUNG
DestinationEnterpriseID	Zeichenfolge	Der Enterprise-ID-Wert für die App oder Website, auf der die Daten freigegeben wurden. **NULL**, **Persönlich** oder **ein leerer Wert** bedeutet, dass keine Enterprise-ID vorhanden ist, da die Arbeitsdaten an einem persönlichen Speicherort freigegeben wurden. Mehrfache Registrierungen werden derzeit nicht unterstützt, daher wird immer einer dieser Werte angezeigt.
DestinationApplicationName	Zeichenfolge	Die Ziel-App oder Website. Für die Ziel-App enthält dieses Feld die AppLocker-Identität. Für die Ziel-Website enthält dieses Feld den Hostnamen.
DestinationName	Zeichenfolge	Eine Zeichenfolge, die von der App bereitgestellt wird, die das Ereignis protokolliert. Diese Zeichenfolge beschreibt das Ziel der Arbeitsdaten.
Application	Zeichenfolge	Die AppLocker-Identität der App, in der das Überwachungsereignis aufgetreten ist.

Beispiele

Hier sind einige Beispiele für die Antworten vom Reporting-CSP.

Der Besitz einer Datei wird von Arbeit zu Persönlich geändert.

```
<SyncML><SyncHdr/><SyncBody><Status><CmdID>1</CmdID><MsgRef>1</MsgRef><CmdRef>0</CmdRef><Cmd>SyncHdr</Cmd>
<Data>200</Data></Status><Status><CmdID>2</CmdID><MsgRef>1</MsgRef><CmdRef>2</CmdRef><Cmd>Replace</Cmd>
<Data>200</Data></Status><Status><CmdID>3</CmdID><MsgRef>1</MsgRef><CmdRef>4</CmdRef><Cmd>Get</Cmd>
<Data>200</Data></Status><Results><CmdID>4</CmdID><MsgRef>1</MsgRef><CmdRef>4</CmdRef><Item><Source>
<LocURI>./Vendor/MSFT/Reporting/EnterpriseDataProtection/RetrieveByTimeRange/Logs</LocURI></Source><Meta>
<Format xmlns="syncml:metinf">xml</Format></Meta><Data><?xml version="1.0" encoding="utf-8"?>
<Reporting Version="com.contoso/2.0/MDM/Reporting">
  <User UserID="S-1-12-1-1111111111-1111111111-1111111111-1111111111" EnterpriseID="corp.contoso.com">
    <Log ProviderType="EDPAudit" LogType="ProtectionRemoved" TimeStamp="131357166318347527">
      <Policy>Protection removed</Policy>
      <Justification>NULL</Justification>
      <FilePath>C:\Users\TestUser\Desktop\tmp\demo\Work document.docx</FilePath>
    </Log>
  </User>
</Reporting></Data></Item></Results><Final/></SyncBody></SyncML>
```

Eine Datei wird mit Edge auf eine persönliche Webseite hochgeladen

```
<SyncML><SyncHdr/><SyncBody><Status><CmdID>1</CmdID><MsgRef>1</MsgRef><CmdRef>0</CmdRef><Cmd>SyncHdr</Cmd>
<Data>200</Data></Status><Status><CmdID>2</CmdID><MsgRef>1</MsgRef><CmdRef>2</CmdRef><Cmd>Replace</Cmd>
<Data>200</Data></Status><Status><CmdID>3</CmdID><MsgRef>1</MsgRef><CmdRef>4</CmdRef><Cmd>Get</Cmd>
<Data>200</Data></Status><Results><CmdID>4</CmdID><MsgRef>1</MsgRef><CmdRef>4</CmdRef><Item><Source>
<LocURI>./Vendor/MSFT/Reporting/EnterpriseDataProtection/RetrieveByTimeRange/Logs</LocURI></Source><Meta>
<Format xmlns="syncml:metinf">xml</Format></Meta><Data><?xml version="1.0" encoding="utf-8"?>
<Reporting Version="com.contoso/2.0/MDM/Reporting">
  <User UserID="S-1-12-1-1111111111-1111111111-1111111111-1111111111" EnterpriseID="corp.contoso.com">
    <Log ProviderType="EDPAudit" LogType="DataCopied" TimeStamp="131357192409318534">
      <Policy>CopyPaste</Policy>
      <Justification>NULL</Justification>
      <SourceApplicationName>NULL</SourceApplicationName>
      <DestinationEnterpriseID>NULL</DestinationEnterpriseID>
      <DestinationApplicationName>mail.contoso.com</DestinationApplicationName>
      <DataInfo>C:\Users\TestUser\Desktop\tmp\demo\Work document.docx</DataInfo>
    </Log>
  </User>
</Reporting></Data></Item></Results><Final/></SyncBody></SyncML>
```


Arbeitsdaten werden in eine persönliche Webseite eingefügt


```
<SyncML><SyncHdr/><SyncBody><Status><CmdID>1</CmdID><MsgRef>1</MsgRef><CmdRef>0</CmdRef><Cmd>SyncHdr</Cmd>
<Data>200</Data></Status><Status><CmdID>2</CmdID><MsgRef>1</MsgRef><CmdRef>2</CmdRef><Cmd>Replace</Cmd>
<Data>200</Data></Status><Status><CmdID>3</CmdID><MsgRef>1</MsgRef><CmdRef>4</CmdRef><Cmd>Get</Cmd>
<Data>200</Data></Status><Results><CmdID>4</CmdID><MsgRef>1</MsgRef><CmdRef>4</CmdRef><Item><Source>
<LocURI>./Vendor/MSFT/Reporting/EnterpriseDataProtection/RetrieveByTimeRange/Logs</LocURI></Source><Meta>
<Format xmlns="syncml:metinf">xml</Format></Meta><Data><?xml version="1.0" encoding="utf-8"?>
<Reporting Version="com.contoso/2.0/MDM/Reporting">
  <User UserID="S-1-12-1-1111111111-1111111111-1111111111-1111111111" EnterpriseID="corp.contoso.com">
    <Log ProviderType="EDPAudit" LogType="DataCopied" TimeStamp="131357193734179782">
      <Policy>CopyPaste</Policy>
      <Justification>NULL</Justification>
      <SourceApplicationName>O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US\MICROSOFT OFFICE
2016\WINWORD.EXE\16.0.8027.1000</SourceApplicationName>
      <DestinationEnterpriseID>NULL</DestinationEnterpriseID>
      <DestinationApplicationName>mail.contoso.com</DestinationApplicationName>
      <DataInfo>EnterpriseDataProtectionId|Object Descriptor|Rich Text Format|HTML
Format|AnsiText|Text|EnhancedMetafile|Embed Source|Link Source|Link Source
Descriptor|ObjectLink|Hyperlink</DataInfo>
    </Log>
  </User>
</Reporting></Data></Item></Results><Final/></SyncBody></SyncML>
```


Eine Arbeitsdatei wird mit einer persönlichen Anwendung geöffnet

```
<SyncML><SyncHdr/><SyncBody><Status><CmdID>1</CmdID><MsgRef>1</MsgRef><CmdRef>0</CmdRef><Cmd>SyncHdr</Cmd>
<Data>200</Data></Status><Status><CmdID>2</CmdID><MsgRef>1</MsgRef><CmdRef>2</CmdRef><Cmd>Replace</Cmd>
<Data>200</Data></Status><Status><CmdID>3</CmdID><MsgRef>1</MsgRef><CmdRef>4</CmdRef><Cmd>Get</Cmd>
<Data>200</Data></Status><Results><CmdID>4</CmdID><MsgRef>1</MsgRef><CmdRef>4</CmdRef><Item><Source>
<LocURI>./Vendor/MSFT/Reporting/EnterpriseDataProtection/RetrieveByTimeRange/Logs</LocURI></Source><Meta>
<Format xmlns="syncml:metinf">xml</Format></Meta><Data><?xml version="1.0" encoding="utf-8"?>
<Reporting Version="com.contoso/2.0/MDM/Reporting">
  <User UserID="S-1-12-1-1111111111-1111111111-1111111111-1111111111" EnterpriseID="corp.contoso.com">
    <Log ProviderType="EDPAudit" LogType="ApplicationGenerated" TimeStamp="131357194991209469">
      <Policy>NULL</Policy>
      <Justification></Justification>
      <Object>C:\Users\TestUser\Desktop\tmp\demo\Work document.docx</Object>
      <Action>1</Action>
      <SourceName>O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US\MICROSOFT® WINDOWS® OPERATING
SYSTEM\WORDPAD.EXE\10.0.15063.2</SourceName>
      <DestinationEnterpriseID>Personal</DestinationEnterpriseID>
      <DestinationName>O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US\MICROSOFT® WINDOWS® OPERATING
SYSTEM\WORDPAD.EXE\10.0.15063.2</DestinationName>
      <Application>O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US\MICROSOFT® WINDOWS® OPERATING
SYSTEM\WORDPAD.EXE\10.0.15063.2</Application>
    </Log>
  </User>
</Reporting></Data></Item></Results><Final/></SyncBody></SyncML>
```

Arbeitsdaten werden in eine persönliche Anwendung eingefügt

```
<SyncML><SyncHdr/><SyncBody><Status><CmdID>1</CmdID><MsgRef>1</MsgRef><CmdRef>0</CmdRef><Cmd>SyncHdr</Cmd>
<Data>200</Data></Status><Status><CmdID>2</CmdID><MsgRef>1</MsgRef><CmdRef>2</CmdRef><Cmd>Replace</Cmd>
<Data>200</Data></Status><Status><CmdID>3</CmdID><MsgRef>1</MsgRef><CmdRef>4</CmdRef><Cmd>Get</Cmd>
<Data>200</Data></Status><Results><CmdID>4</CmdID><MsgRef>1</MsgRef><CmdRef>4</CmdRef><Item><Source>
<LocURI>./Vendor/MSFT/Reporting/EnterpriseDataProtection/RetrieveByTimeRange/Logs</LocURI></Source><Meta>
<Format xmlns="syncml:metinf">xml</Format></Meta><Data><?xml version="1.0" encoding="utf-8"?>
<Reporting Version="com.contoso/2.0/MDM/Reporting">
  <User UserID="S-1-12-1-1111111111-1111111111-1111111111-1111111111" EnterpriseID="corp.contoso.com">
    <Log ProviderType="EDPAudit" LogType="DataCopied" TimeStamp="131357196076537270">
      <Policy>CopyPaste</Policy>
      <Justification>NULL</Justification>
      <SourceApplicationName>O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US\MICROSOFT OFFICE
2016\WINWORD.EXE\16.0.8027.1000</SourceApplicationName>
      <DestinationEnterpriseID>NULL</DestinationEnterpriseID>
      <DestinationApplicationName></DestinationApplicationName>
      <DataInfo>EnterpriseDataProtectionId|Object Descriptor|Rich Text Format|HTML
Format|AnsiText|Text|EnhancedMetafile|Embed Source|Link Source|Link Source
Descriptor|ObjectLink|Hyperlink</DataInfo>
    </Log>
  </User>
</Reporting></Data></Item></Results><Final/></SyncBody></SyncML>
```

Sammeln von WIP-Überwachungsprotokollen mit der Windows-Ereignisweiterleitung (nur für Windows-Desktopgeräte, die mit einer Domäne verbunden sind)

Verwenden Sie die Windows-Ereignisweiterleitung, um Ihre WIP-Überwachungsereignisse zu sammeln und zu aggregieren. Sie können die Überwachungsereignisse in der Ereignisanzeige öffnen.

> **NOTE**
>
> Unter Windows10 Mobile müssen Sie stattdessen den Reporting CSP-Prozess verwenden.

So öffnen Sie die WIP-Ereignisse in der Ereignisanzeige

1. Öffnen Sie die Ereignisanzeige.
2. Klicken Sie in der Konsolenstruktur unter **Anwendungs- und Dienstprotokolle\Microsoft\Windows** auf **Unternehmensdatenschutz-Überwachung-Standard** und auf **Unternehmensdatenschutz-Überwachung-TCB**.

Erfassen von WIP-Überwachungsprotokollen mithilfe des Azure Monitors

Sie können Überwachungsprotokolle mithilfe des Azure Monitors sammeln. Informationen finden Sie unter Windows-Ereignisprotokoll-Datenquellen in Azure Monitor.

So zeigen Sie die WIP-Ereignisse in Azure Monitor an

1. Verwenden Sie einen vorhandenen oder erstellen Sie einen neuen Arbeitsbereich für die Protokollanalyse.
2. Wählen Sie unter**Erweiterte Einstellungen**für **Protokollanalyse** > die Option **Daten**aus. Fügen Sie in Windows-Ereignisprotokollen Protokolle hinzu, die empfangen werden sollen:

   ```
   Microsoft-Windows-EDP-Application-Learning/Admin
   Microsoft-Windows-EDP-Audit-TCB/Admin
   ```

   > **NOTE**
   > Wenn Sie Windows-Ereignisprotokolle verwenden, finden Sie die Ereignisprotokollnamen unter Eigenschaften des Ereignisses im Ordner "Ereignisse" (Application and Services Logs\Microsoft\Windows, klicken Sie auf EDP-Audit-Regular und EDP-Audit-TCB).

3. Microsoft- Überwachungs-Agentherunterladen.
4. Um die MSI-Installation für InTune zu erhalten, wie im Azure Monitor-Artikel angegeben, extrahieren Sie: MMASetup-. exe/c/t: Installieren des Microsoft-Überwachungs-Agents auf WIP-Geräten mithilfe der Arbeitsbereichs-ID und des Primärschlüssels. Weitere Informationen zur Arbeitsbereichs-ID und zum Primärschlüssel finden Sie unter**Erweiterte Einstellungen**für **Protokollanalyse** > .
5. Zum Bereitstellen von MSI über InTune fügen Sie in den Installationsparametern Folgendes hinzu:/q/norestart NOAPM = 1 ADD_OPINSIGHTS_WORKSPACE = 1 OPINSIGHTS_WORKSPACE_AZURE_CLOUD_TYPE = 0 OPINSIGHTS_WORKSPACE_ID = <WORKSPACE_ID> OPINSIGHTS_WORKSPACE_KEY =<WORKSPACE_KEY> AcceptEndUserLicenseAgreement = 1

> **NOTE**
> Ersetzen Sie <WORKSPACE_ID> & <WORKSPACE_KEY von Schritt 5 empfangenen>. Setzen Sie in den Installationsparametern <WORKSPACE_ID> & <WORKSPACE_KEY> in Anführungszeichen ("" oder "").

1. Nach der Bereitstellung des Agents werden die Daten innerhalb von ungefähr 10 Minuten empfangen.
2. Wenn Sie nach Protokollen suchen möchten, wechseln Sie zu **Protokollanalyse-Arbeitsbereichs** > **Protokollen**, und geben Sie **Ereignis** in Suche ein.

Beispiel

```
Event | where EventLog == "Microsoft-Windows-EDP-Audit-TCB/Admin"
```

Zusätzliche Ressourcen

- Bereitstellen der APP über InTune
- Erstellen eines Protokoll Arbeitsbereichs
- Verwenden von Microsoft-Überwachungs-Agents für Windows

Allgemeiner Leitfaden und bewährte Methoden für Windows Information Protection (WIP)

31.12.2019 • 2 minutes to read

Gilt für:

- Windows10, Version 1607 und höher
- Windows10 Mobile, Version 1607 und höher

Dieser Abschnitt enthält Informationen zu den optimierten Microsoft-Apps. Sie erfahren beispielsweise, wie Sie diese Apps zur Liste zugelassener Apps in Microsoft Intune hinzufügen. Darüber hinaus enthält er einige Testszenarien, deren Ausführung unter Verwendung von Windows Information Protection (WIP) empfohlen wird.

Inhalt dieses Abschnitts

THEMA	BESCHREIBUNG
Optimierte Apps für die Verwendung mit Windows Information Protection (WIP)	Hier erfahren Sie mehr über den Unterschied zwischen optimierten und nicht optimierten Apps. Sehen Sie sich anschließend die Liste mit den von Microsoft bereitgestellten optimierten Apps sowie den Text an, den Sie zum Hinzufügen der Apps zur Liste der zulässigen Apps benötigen.
Verhalten nicht optimierter und optimierter Apps bei Verwendung von Windows Information Protection (WIP)	Hier erfahren Sie, worin sich optimierte und nicht optimierte Apps hinsichtlich ihres Verhaltens unterscheiden.
Empfohlene Netzwerkeinstellungen für Enterprise Cloud Resources und Neutral Resources zur Verwendung mit Windows Information Protection (WIP)	Empfohlene Ergänzungen für die Enterprise Cloud Resources- und Neutral Resources-Netzwerkeinstellungen zur Verwendung mit Windows Information Protection (WIP)
Verwenden von Outlook im Web mit Windows Information Protection (WIP)	Optionen für die Verwendung von Outlook im Web mit Windows Information Protection (WIP)

NOTE

Tragen Sie dazu bei, dieses Thema zu verbessern, indem Sie uns Bearbeitungen, Ergänzungen und Feedback schicken. Informationen dazu, wie Sie zu diesem Thema beitragen können, finden Sie unter Bearbeiten der Windows IT Professional-Dokumentation.

Liste der optimierten Microsoft-Apps für die Verwendung mit Windows Information Protection (WIP)

15.02.2020 • 3 minutes to read

Betrifft:

- Windows10, Version 1607 und höher
- Windows10 Mobile, Version 1607 und höher

Hier erfahren Sie mehr über den Unterschied zwischen optimierten und nicht optimierten Apps. Sehen Sie sich anschließend die Liste mit den von Microsoft bereitgestellten optimierten Apps sowie den Text an, den Sie zum Hinzufügen der Apps zur Liste der zulässigen Apps benötigen.

Optimierte Apps im Vergleich zu nicht optimierten Apps

Apps können optimiert oder nicht optimiert sein:

- **Optimierte Apps** können zwischen Unternehmensdaten und privaten Daten unterscheiden und auf Grundlage Ihrer Richtlinien korrekt bestimmen, welche zu schützen sind.
- **Nicht optimierte Apps** behandeln alle Daten als Unternehmensdaten und verschlüsseln alles. Für eine nicht optimierte App gilt in der Regel Folgendes:
  - Auf dem Windows-Desktop wird sie immer als App im Unternehmensmodus angezeigt.
  - Mit der Windows-Funktion **Speichern unter** können Dateien ausschließlich als Unternehmensdaten gespeichert werden.
- **Nur WIP-Arbeit-apps** sind nicht erleuchtete Branchen-apps, die getestet wurden und für die Verwendung in einem Unternehmen mit WIP-und Mobile-App-Management-Lösungen (MAM) ohne Geräteregistrierung als sicher eingestuft wurden. Unaufgeklärte apps, die für WIP ohne Registrierung vorgesehen sind, werden unter persönlicher Modus ausgeführt.

Liste der optimierten Microsoft-Apps

Microsoft hat alle Anstrengungen unternommen, einige der beliebtesten Apps zu optimieren, beispielsweise:

- Microsoft 3D Viewer
- Microsoft Edge
- Internet-Explorer11
- Microsoft Kontakte
- Mobile Office-Apps, einschließlich Word, Excel, PowerPoint, OneNote sowie Outlook-Mail und -Kalender
- Office 365 ProPlus-Apps, einschließlich Word, Excel, PowerPoint, OneNote sowie Outlook Mail und Kalender
- OneDrive-App
- OneDrive-Synchronisierungsclient („OneDrive.exe", der Synchronisierungsclient der nächsten Generation)

- Microsoft Fotos
- Groove-Musik
- Editor
- Microsoft Paint
- Microsoft Filme & TV
- Microsoft-Nachrichten
- Microsoft-Remotedesktop

> **NOTE**
> Microsoft Visio, Microsoft Office Access und Microsoft Project sind keine enlightended-apps und müssen von der WIP-Richtlinie ausgenommen werden. Wenn Sie zulässig sind, besteht das Risiko eines Datenverlusts. Wenn beispielsweise ein Gerät am Arbeitsplatz verbunden und verwaltet wird und der Benutzer das Unternehmen verlässt, bleiben Metadatendateien, auf die die apps Vertrauen, weiterhin verschlüsselt, und die apps beenden functioining.

Liste der nur mit WIP kompatiblen Apps von Microsoft

Microsoft verfügt weiterhin über nicht optimierte Apps. Sie wurden jedoch getestet und werden für die Verwendung in einem Unternehmen mit WIP- und MAM-Lösungen als sicher eingeschätzt.

- Skype for Business

Hinzufügen von optimierten Microsoft-Apps zur Liste zugelassener Apps

> **NOTE**
> Ab Januar 2019 ist es nicht mehr notwendig, das InTune-Unternehmens Portal als ausgeschlossene App hinzuzufügen, da es jetzt in der Standardliste der geschützten Apps enthalten ist.

Sie können einige oder alle der optimierten Microsoft-Apps zu Ihrer Liste zugelassener Apps hinzufügen. Hier finden Sie den **Namen des Herausgebers**, den **Produkt-oder Dateinamen**sowie Informationen zu **App-Typen** sowohl für Microsoft InTune als auch für Microsoft Endpoint Configuration Manager.

PRODUKTNAME	APP-INFORMATIONEN
Microsoft 3D Viewer	**Herausgeber:** `CN=Microsoft Corporation, O=Microsoft Corporation, L=Redmond, S=Washington, C=US` **Produkt Name:** Microsoft. Microsoft3DViewer **App-Typ:** Universelle App
Microsoft Edge	**Herausgeber:** `CN=Microsoft Corporation, O=Microsoft Corporation, L=Redmond, S=Washington, C=US` **Produktname:** Microsoft.MicrosoftEdge **App-Typ:** Universelle App

PRODUKTNAME	APP-INFORMATIONEN
Microsoft Kontakte	**Herausgeber:** `CN=Microsoft Corporation, O=Microsoft Corporation, L=Redmond, S=Washington, C=US` **Produktname:** Microsoft.People **App-Typ:** Universelle App
Word Mobile	**Herausgeber:** `CN=Microsoft Corporation, O=Microsoft Corporation, L=Redmond, S=Washington, C=US` **Produktname:** Microsoft.Office.Word **App-Typ:** Universelle App
Excel Mobile	**Herausgeber:** `CN=Microsoft Corporation, O=Microsoft Corporation, L=Redmond, S=Washington, C=US` **Produktname:** Microsoft.Office.Excel **App-Typ:** Universelle App
PowerPoint Mobile	**Herausgeber:** `CN=Microsoft Corporation, O=Microsoft Corporation, L=Redmond, S=Washington, C=US` **Produktname:** Microsoft.Office.PowerPoint **App-Typ:** Universelle App
OneNote	**Herausgeber:** `CN=Microsoft Corporation, O=Microsoft Corporation, L=Redmond, S=Washington, C=US` **Produktname:** Microsoft.Office.OneNote **App-Typ:** Universelle App
Outlook-Mail und -Kalender	**Herausgeber:** `CN=Microsoft Corporation, O=Microsoft Corporation, L=Redmond, S=Washington, C=US` **Produktname:** microsoft.Windowscommunicationsapps **App-Typ:** Universelle App
Office 365 ProPlus und Office 2019 Professional Plus	Office 365 ProPlus und Office 2019 Professional Plus-apps sind als Suite eingerichtet. Sie müssen die im ZIP-Archiv enthaltenen Allow- und Exempt AppLocker-Richtliniendateien für O365 ProPlus verwenden, um die Suite für WIP zu aktivieren. Es wird nicht empfohlen, Office mithilfe einzelner Pfade oder Herausgeberregeln einzurichten.
Microsoft Fotos	**Herausgeber:** `CN=Microsoft Corporation, O=Microsoft Corporation, L=Redmond, S=Washington, C=US` **Produktname:** Microsoft.Windows.Photos **App-Typ:** Universelle App
Groove-Musik	**Herausgeber:** `CN=Microsoft Corporation, O=Microsoft Corporation, L=Redmond, S=Washington, C=US` **Produktname:** Microsoft.ZuneMusic **App-Typ:** Universelle App

PRODUKTNAME	APP-INFORMATIONEN
Microsoft Filme & TV	**Herausgeber:** `CN=Microsoft Corporation, O=Microsoft Corporation, L=Redmond, S=Washington, C=US` **Produktname:** Microsoft.ZuneVideo **App-Typ:** Universelle App
Microsoft-Nachrichten	**Herausgeber:** `CN=Microsoft Corporation, O=Microsoft Corporation, L=Redmond, S=Washington, C=US` **Produktname:** Microsoft.Messaging **App-Typ:** Universelle App
IE11	**Herausgeber:** `O=Microsoft Corporation, L=Redmond, S=Washington, C=US` **Name der Binärdatei:** iexplore.exe **App-Typ:** Desktop-App
OneDrive-Synchronisierungsclient	**Herausgeber:** `O=Microsoft Corporation, L=Redmond, S=Washington, C=US` **Name der Binärdatei:** onedrive.exe **App-Typ:** Desktop-App
OneDrive-App	**Herausgeber:** `CN=Microsoft Corporation, O=Microsoft Corporation, L=Redmond, S=Washington, C=US` **Produktname:** Microsoft.Microsoftskydrive **Produktversion:**Produktversion: 17.21.0.0 (und höher) **App-Typ:** Universelle App
Windows-Editor	**Herausgeber:** `O=Microsoft Corporation, L=Redmond, S=Washington, C=US` **Name der Binärdatei:** notepad.exe **App-Typ:** Desktop-App
Microsoft Paint	**Herausgeber:** `O=Microsoft Corporation, L=Redmond, S=Washington, C=US` **Name der Binärdatei:** mspaint.exe **App-Typ:** Desktop-App
Microsoft-Remotedesktop	**Herausgeber:** `O=Microsoft Corporation, L=Redmond, S=Washington, C=US` **Name der Binärdatei:** mstsc.exe **App-Typ:** Desktop-App
Microsoft MAPI-Reparatur Tool	**Herausgeber:** `O=Microsoft Corporation, L=Redmond, S=Washington, C=US` **Binärer Name:** Fixmapi. exe **App-Typ:** Desktop-App

NOTE

Tragen Sie dazu bei, dieses Thema zu verbessern, indem Sie uns Bearbeitungen, Ergänzungen und Feedback bereitstellen. Informationen dazu, wie Sie zu diesem Thema beitragen können, finden Sie unter Bearbeiten der Windows IT Professional-Dokumentation.

Verhalten nicht optimierter und optimierter Apps bei Verwendung von Windows Information Protection (WIP)

04.01.2020 • 3 minutes to read

Betrifft:

- Windows10, Version 1607 und höher
- Windows10 Mobile, Version 1607 und höher

Windows Information Protection (WIP) unterteilt Apps in zwei Kategorien: Optimierte und nicht optimierte Apps. Optimierte Apps können zwischen geschäftlichen und privaten Daten unterscheiden und auf Grundlage interner Richtlinien korrekt bestimmen, welche zu schützen sind. Unternehmensdaten werden auf dem verwalteten Gerät verschlüsselt. Versuche, sie zu kopieren und einzufügen oder mit nicht zum Unternehmen gehörenden Apps oder Personen zu teilen, schlagen fehl. Nicht optimierte Apps, die als vom Unternehmen verwaltet markiert sind, betrachten alle Daten als Unternehmensdaten und verschlüsseln sie standardmäßig.

Um die automatische Verschlüsselung von Daten zu verhindern, können Entwickler Apps optimieren, indem sie über die Anwendungsprogrammierschnittstellen von Windows Information Protection Code hinzufügen und kompilieren. Die wahrscheinlichsten Kandidaten für eine Optimierung sind Apps, die:

- keine allgemeinen Steuerelemente zum Speichern von Dateien verwenden;
- keine allgemeinen Steuerelemente für Textfelder verwenden;
- gleichzeitig private und geschäftliche Daten verarbeiten (z.B. Kontakt-Apps, die private und geschäftliche Daten in einer Ansicht anzeigen, oder ein Browser, der private und geschäftliche Webseiten auf Registerkarten in derselben Instanz anzeigt).

Es wird dringend empfohlen, der Liste zulässiger Apps keine nicht optimierten Apps hinzuzufügen. Einzige Ausnahme sind Branchen-Apps.

> **IMPORTANT**
> Nach dem Widerruf von WIP müssen unaufgeklärte apps deinstalliert und neu installiert werden, da ihre Einstellungsdateien verschlüsselt bleiben.

> **NOTE**
> Weitere Informationen zum Erstellen optimierter Apps finden Sie im Windows Dev Center im Thema Windows Information Protection (WIP).

Verhalten nicht optimierter Apps

Diese Tabelle enthält Informationen dazu, wie sich nicht optimierte Apps abhängig von Ihren WIP (Windows Information Protection)-Netzwerkrichtlinien und der App-Konfiguration verhalten können. Das Verhalten hängt außerdem davon ab, ob die App über IP-Adressen eine Direktverbindung mit Netzwerkressourcen herstellt oder ob sie Hostnamen für die Verbindungsherstellung verwendet.

APP-REGELEINSTELLUNG	NETZWERKRICHTLINIENKONFIGURATION

	NAMENBASIERTE RICHTLINIEN OHNE DIE ZEICHENFOLGE /*APPCOMPAT*/	NAMENBASIERTE RICHTLINIEN MIT DER ZEICHENFOLGE /*APPCOMPAT*/ ODER PROXYBASIERTE RICHTLINIEN
Nicht erforderlich. Die App stellt direkt mithilfe einer IP-Adresse eine Verbindung mit Unternehmenscloudressourcen her.	• Private und geschäftliche Cloudressourcen sind für die App vollständig gesperrt. • Es wird keine Verschlüsselung angewendet. • Die App kann nicht auf lokale Arbeitsdateien zugreifen.	• Die App kann sowohl auf private als auch auf geschäftliche Cloudressourcen zugreifen. Möglicherweise stoßen Sie vielleicht auf Apps mit Richtlinien, die den Zugriff auf Unternehmenscloudressourcen einschränken. • Es wird keine Verschlüsselung angewendet. • Die App kann nicht auf lokale Arbeitsdateien zugreifen.
Nicht erforderlich. Die App stellt mithilfe eines Hostnamens eine Verbindung mit Unternehmenscloudressourcen her.	• Der Zugriff auf Unternehmenscloudressourcen durch die App ist gesperrt. Sie kann jedoch auf andere Netzwerkressourcen zugreifen. • Es wird keine Verschlüsselung angewendet. • Die App kann nicht auf lokale Arbeitsdateien zugreifen.	
Zulassen Die App stellt mithilfe einer IP-Adresse oder eines Hostnamens eine Verbindung mit Unternehmenscloudressourcen her.	• Die App kann sowohl auf private als auch auf geschäftliche Cloudressourcen zugreifen. • Die automatische Verschlüsselung wird angewendet. • Die App kann auf lokale Arbeitsdateien zugreifen.	
Ausnahme. Die App stellt mithilfe einer IP-Adresse oder eines Hostnamens eine Verbindung mit Unternehmenscloudressourcen her.	• Die App kann sowohl auf private als auch auf geschäftliche Cloudressourcen zugreifen. • Es wird keine Verschlüsselung angewendet. • Die App kann auf lokale Arbeitsdateien zugreifen.	

Verhalten optimierter Apps

Diese Tabelle enthält Informationen dazu, wie sich optimierte Apps abhängig von Ihren WIP (Windows Information Protection)-Netzwerkrichtlinien und der App-Konfiguration verhalten können. Das Verhalten hängt außerdem davon ab, ob die App über IP-Adressen eine Direktverbindung mit Netzwerkressourcen herstellt oder ob sie Hostnamen für die Verbindungsherstellung verwendet.

APP-REGELEINSTELLUNG	NETZWERKRICHTLINIENKONFIGURATION FÜR NAMENBASIERTE RICHTLINIEN, WOMÖGLICH UNTER VERWENDUNG DER ZEICHENFOLGE /*APPCOMPAT*/, ODER PROXYBASIERTE RICHTLINIEN
Nicht erforderlich. Die App stellt mithilfe einer IP-Adresse oder eines Hostnamens eine Verbindung mit Unternehmenscloudressourcen her.	• Der Zugriff auf Unternehmenscloudressourcen durch die App ist gesperrt. Sie kann jedoch auf andere Netzwerkressourcen zugreifen. • Es wird keine Verschlüsselung angewendet. • Die App kann nicht auf lokale Arbeitsdateien zugreifen.
Zulassen Die App stellt mithilfe einer IP-Adresse oder eines Hostnamens eine Verbindung mit Unternehmenscloudressourcen her.	• Die App kann sowohl auf private als auch auf geschäftliche Cloudressourcen zugreifen. • Die App schützt geschäftliche Daten. Private Daten werden nicht geschützt. • Die App kann auf lokale Arbeitsdateien zugreifen.

Ausnahme. Die App stellt mithilfe einer IP-Adresse oder eines Hostnamens eine Verbindung mit Unternehmenscloudressourcen her.	• Die App kann sowohl auf private als auch auf geschäftliche Cloudressourcen zugreifen. • Die App schützt geschäftliche Daten. Private Daten werden nicht geschützt. • Die App kann auf lokale Arbeitsdateien zugreifen.

NOTE

Tragen Sie zur Verbesserung dieses Themas bei, indem Sie uns Änderungsvorschläge, Ergänzungen und Feedback senden. Informationen dazu, wie Sie zu diesem Thema beitragen können, finden Sie unter Bearbeiten der Windows IT Professional-Dokumentation.

Empfohlene Netzwerkeinstellungen für Unternehmenscloudressourcen und neutrale Ressourcen mit Windows Information Protection (WIP)

21.02.2020 • 2 minutes to read

Betrifft:

- Windows10, Version 1607 und höher
- Windows10 Mobile, Version 1607 und höher

> Unter Vergleichen von Windows10-Editionen erfahren Sie, welche Features und Funktionen von den einzelnen Windows-Editionen unterstützt werden.

Wenn Sie eine WIP-Richtlinie erstellen, empfehlen wir, die folgenden URLs zu den Netzwerkeinstellungen für Enterprise-Cloud-Ressourcen und neutrale Ressourcen hinzuzufügen. Wenn Sie InTune verwenden, können die SharePoint-Einträge automatisch hinzugefügt werden.

Empfohlene Enterprise Cloud Resources

Diese Tabelle enthält die empfohlenen URLs, die Sie den Netzwerkeinstellungen für Ihre Enterprise Cloud Resources hinzufügen sollten, basierend auf den Apps, die Sie in Ihrer Organisation verwenden.

WENN IHRE ORGANISATION DIESES PRODUKT VERWENDET...	DANN FÜGEN SIE DIESE EINTRÄGE DEN NETZWERKEINSTELLUNG FÜR IHRE ENTERPRISE CLOUD RESOURCES HINZU. (ERSETZEN SIE "CONTOSO" DURCH IHRE DOMÄNENNAMEN.)
SharePoint Online	• contoso.sharepoint.com • contoso-my.sharepoint.com • contoso-files.sharepoint.com
Yammer	• www.yammer.com • yammer.com • persona.yammer.com
Outlook Web Access (OWA)	• outlook.office.com • outlook.office365.com • attachments.office.net
Microsoft Dynamics	contoso.crm.dynamics.com
Visual Studio Online	contoso.visualstudio.com
Power BI	contoso.powerbi.com
Microsoft Teams	teams.microsoft.com

WENN IHRE ORGANISATION DIESES PRODUKT VERWENDET...	DANN FÜGEN SIE DIESE EINTRÄGE DEN NETZWERKEINSTELLUNG FÜR IHRE ENTERPRISE CLOUD RESOURCES HINZU. (ERSETZEN SIE "CONTOSO" DURCH IHRE DOMÄNENNAMEN.)
Andere Office 365-Dienste	• tasks.office.com • protection.office.com • meet.lync.com • project.microsoft.com

Sie können der Liste der Cloud-Ressourcen andere nur-Arbeit-apps hinzufügen, oder Sie können eine verpackte APP-Regel für die exe-Datei erstellen, um jede Datei zu schützen, die von der App erstellt oder geändert wird. Je nachdem, wie auf die App zugegriffen wird, möchten Sie möglicherweise beides hinzufügen.

Informationen zu Office 365-Endpunkten finden Sie unter Office 365-URLs und IP-Adressbereiche. Office 365-Endpunkte werden monatlich aktualisiert. Zulassen, dass die Domänen, die Unterabschnitts Nummer 46 aufgeführt sind, erforderlich sind, und fügen Sie auch die apps hinzu. Beachten Sie, dass apps von officeapps.Live.com auch persönliche Daten speichern können.

Wenn mehrere Dateien aus SharePoint Online oder OneDrive ausgewählt werden, werden die Dateien aggregiert, und die URL kann geändert werden. Fügen Sie in diesem Fall einen Eintrag für eine Domäne der zweiten Ebene hinzu, und verwenden Sie einen Platzhalter wie svc.ms.

Empfohlene Neutral Resources

Es wird empfohlen, diese URLs hinzuzufügen, wenn Sie die Netzwerkeinstellungen für Neutral Resources mit Windows Information Protection (WIP) verwenden.

- login.microsoftonline.com
- login.Windows.net

Verwenden von Outlook im Web mit Windows Information Protection (WIP)

04.12.2019 • 2 minutes to read

Betrifft:

- Windows10, Version 1607 und höher
- Windows10 Mobile, Version 1607 und höher

> Unter Vergleichen von Windows10-Editionen erfahren Sie, welche Features und Funktionen von den einzelnen Windows-Editionen unterstützt werden.

Da Outlook im Web sowohl privat als auch von Unternehmen verwendet werden kann, stehen Ihnen folgende Optionen für dessen Konfigurierung mit Windows Information Protection (WIP) zur Verfügung:

OPTION	VERHALTEN VON OUTLOOK IM WEB
Deaktivieren Sie Outlook im Web. Mitarbeiter können nur Microsoft Outlook2016 oder die App „Mail für Windows10" verwenden.	Deaktiviert.
Konfigurieren Sie „outlook.office.com" in keiner Ihrer Netzwerkeinstellungen.	Alle Postfächer werden automatisch als persönlich markiert. Das bedeutet, dass Mitarbeiter, die versuchen, Arbeitsinhalte zu Outlook im Web zu kopieren, entsprechende Meldungen erhalten und dass aus Outlook im Web heruntergeladene Dateien nicht automatisch als Unternehmensdaten geschützt werden.
Fügen Sie Outlook.Office.com und Outlook.office365.com dem Cloud Resources-Netzwerkelement in ihrer WIP-Richtlinie hinzu.	Alle Postfächer werden automatisch als Unternehmenspostfächer markiert. Das bedeutet, dass alle in Office365 gehosteten persönlichen Postfächer auch automatisch als Unternehmensdaten gekennzeichnet werden.

NOTE

Diese Einschränkungen gelten nicht für Outlook2016, die Mail für Windows10-App oder die Kalender für Windows10-App. Diese Apps funktionieren ordnungsgemäß und markieren das Postfach eines Mitarbeiters als Unternehmensdaten, unabhängig davon, wie Sie „outlook.office.com" in den Netzwerkeinstellungen konfiguriert haben.

Optimieren von Windows Information Protection (WIP) mit WIP-Learning

20.12.2019 • 3 minutes to read

Betrifft

- Windows10, Version 1703 und höher
- Windows10 Mobile, Version 1703 und höher

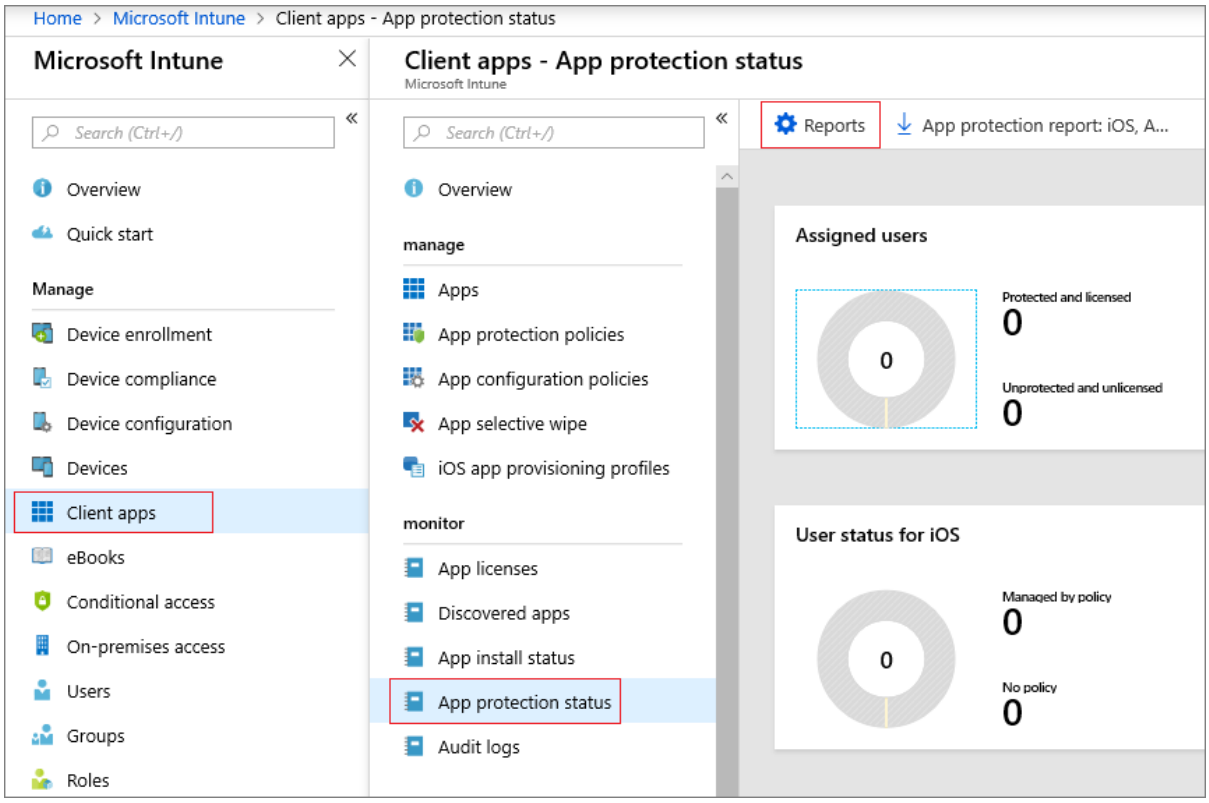
Mit WIP-lernen können Sie intelligent abstimmen, welche apps und Websites in ihrer WIP-Richtlinie enthalten sind, um unterbrechungsfreie Eingabeaufforderungen zu verringern und Sie exakt und relevant zu halten. WIP-lernen generiert zwei Berichte: den **App Learning-Bericht** und den **Website lernbericht**. Auf beide Berichte kann über Microsoft Azure InTune zugegriffen werden.

Der **App-lernbericht** überwacht Ihre apps, nicht die Richtlinie, die versuchen, auf Arbeitsdaten zuzugreifen. Sie können diese apps mithilfe des Berichts identifizieren und ihren WIP-Richtlinien hinzufügen, um Produktivitäts Unterbrechungen zu vermeiden, bevor Sie WIP mit dem Modus "blockieren" vollständig erzwingen. Das häufige Überwachen des Berichts hilft Ihnen, die Zugriffsversuche kontinuierlich zu identifizieren, damit Sie Ihre Richtlinie entsprechend aktualisieren können.

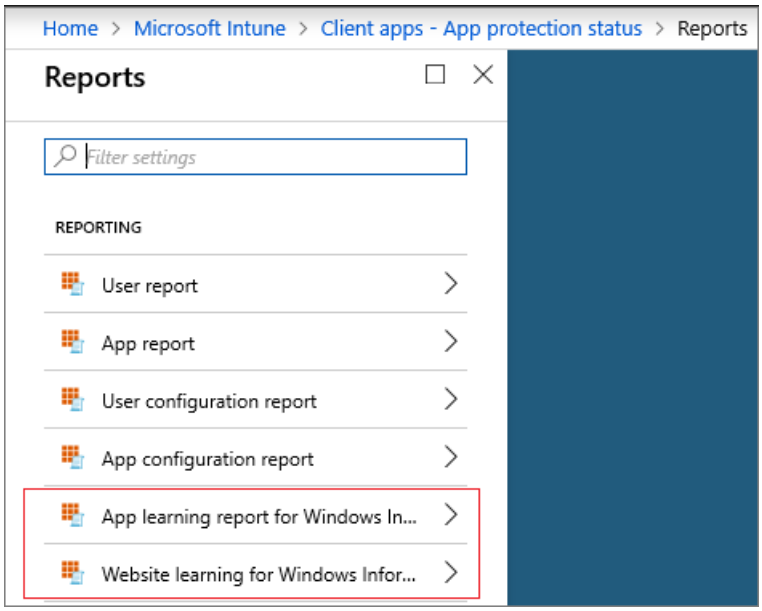
Im **Website lernbericht**können Sie eine Zusammenfassung der Geräte anzeigen, die über freigegebene Arbeitsdaten mit Websites verfügen. Mithilfe dieser Informationen können Sie ermitteln, welche Websites zu Gruppen-und Benutzer-WIP-Richtlinien hinzugefügt werden sollen. In der Zusammenfassung wird angezeigt, auf welche Website-URLs von WIP-aktivierten apps zugegriffen wird, damit Sie entscheiden können, welche Websites in der Cloud oder in der persönlichen Liste enthalten sind, und diese der Ressourcenliste hinzufügen.

Zugreifen auf die WIP-lernberichte

1. Öffnen Sie das Azure-Portal.
2. Klicken Sie auf **alle Dienste**, geben Sie **InTune** in den Text Feld Filter ein, und klicken Sie auf den Stern, um ihn zu den **Favoriten**hinzuzufügen.
3. Klicken Sie auf **InTune** > -**Client-apps** > -**App-Schutzstatus** > **Berichte**.



4. Wählen Sie entweder **App Learning Report für Windows Information Protection** oder **Website Learning Report für Windows Information Protection**aus.



Nachdem Sie die apps und Websites in den Berichten zur WIP-lernprotokollierung angezeigt haben, können Sie entscheiden, ob Sie Sie Ihren app-Schutzrichtlinien hinzufügen möchten.

Verwenden des WIP-Abschnitts des Gerätestatus

Sie können die Geräte Integrität verwenden, um Ihre WIP-Schutzrichtlinie anzupassen. Weitere Informationen finden Sie unter Verwenden des Gerätezustands .

Wenn Sie Ihre Umgebung für Windows Analytics konfigurieren möchten: Gerätestatus, lesen Sie Erste Schritte mit dem Gerätestatus , um weitere Informationen zu erhalten.

Nachdem Sie WIP-Richtlinien eingerichtet haben, können Sie über den Abschnitt WIP des Gerätezustands Folgendes ausführen:

- Reduzieren Sie Unterbrechungs Aufforderungen durch Hinzufügen von Regeln, um die Datenfreigabe von genehmigten apps zu ermöglichen.
- Optimieren Sie WIP-Regeln, indem Sie bestätigen, dass bestimmte Apps durch die aktuelle Richtlinie zugelassen oder verweigert werden.

Verwenden von Gerätestatus und InTune zum Anpassen von WIP-Schutzrichtlinien

Die für die folgenden Schritte erforderlichen Informationen finden Sie unter Gerätestatus, den Sie zunächst einrichten müssen. Erfahren Sie mehr darüber, wie Sie den Zustand von Geräten mit Gerätestatus überwachenkönnen.

1. Klicken Sie unter **Gerätestatus** auf die APP, die Sie zu Ihrer Richtlinie hinzufügen möchten, und kopieren Sie die **WipAppId**.

   Wenn es sich bei der APP beispielsweise um Google Chrome handelt, lautet der WipAppId wie folgt:

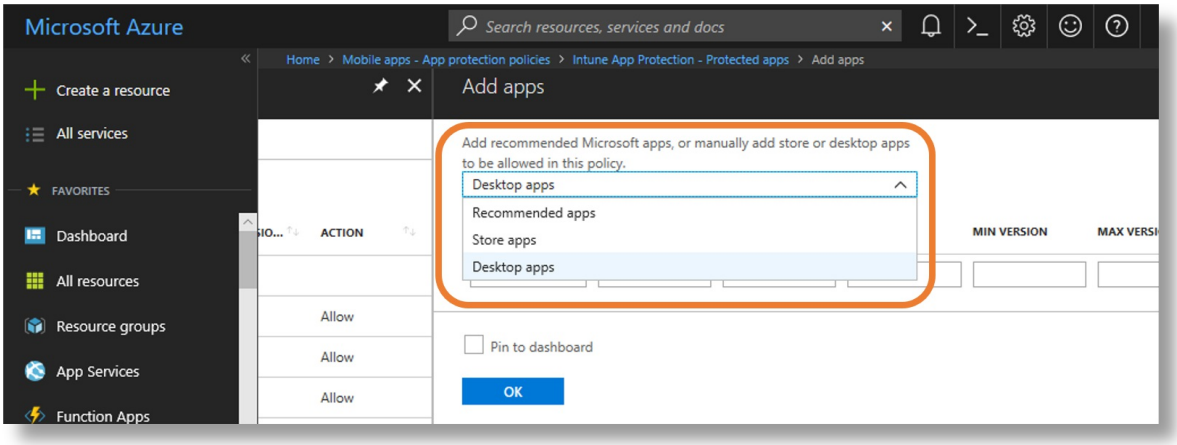
   ```
   O=GOOGLE LLC, L=MOUNTAIN VIEW, S=CA, C=US\GOOGLE CHROME\CHROME.EXE\74.0.3729.108
   ```

   In den nachstehenden Schritten trennen Sie die WipAppId durch umgekehrte Schrägstriche in die Felder **Publisher**, **Product Name**und **File** .

2. Klicken Sie in InTune auf **App-Schutzrichtlinien** , und wählen Sie dann die APP-Richtlinie aus, der Sie eine Anwendung hinzufügen möchten.

3. Klicken Sie auf **geschützte apps**, und klicken Sie dann auf **apps hinzufügen**.

4. Wählen Sie im Dropdownmenü **Empfohlene apps** entweder Store- **apps** oder **Desktop-Apps**aus, je nachdem, welche app Sie ausgewählt haben (beispielsweise ist eine ausführbare Datei (exe) eine Desktop-App).



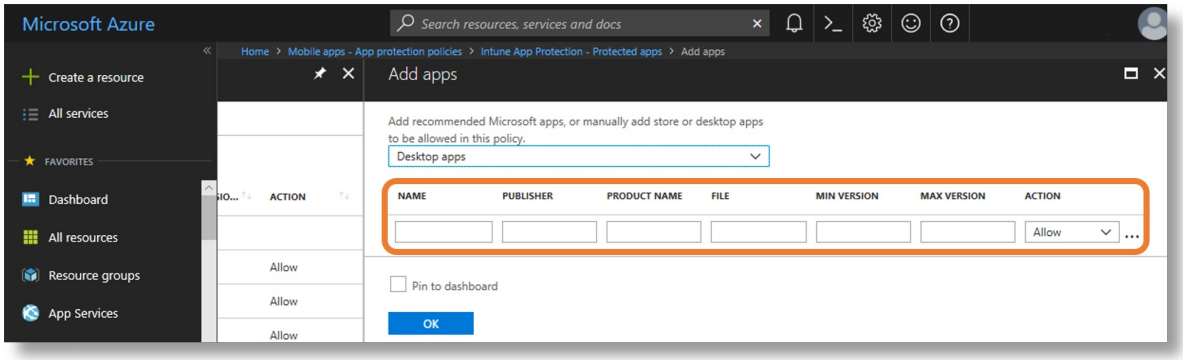
5. Geben Sie in **Name** (optional) den Namen der APP ein, und fügen Sie dann in **Publisher** (erforderlich) die Herausgeberinformationen ein, die Sie in Schritt 1 oben kopiert haben.

   Wenn beispielsweise die WipAppId

   ```
   O=GOOGLE LLC, L=MOUNTAIN VIEW, S=CA, C=US\GOOGLE CHROME\CHROME.EXE\74.0.3729.108
   ```

   der Text vor dem ersten umgekehrten Schrägstrich ist der Herausgeber:

   ```
   O=GOOGLE LLC, L=MOUNTAIN VIEW, S=CA, C=US
   ```



6. Geben Sie den Namen des Produkts in **Product Name** (erforderlich) ein (Dies ist wahrscheinlich mit dem übereinstimmen, was Sie für den **Namen**eingegeben haben).

   Wenn beispielsweise die WipAppId

   ```
   O=GOOGLE LLC, L=MOUNTAIN VIEW, S=CA, C=US\GOOGLE CHROME\CHROME.EXE\74.0.3729.108
   ```

   der Text zwischen dem ersten und zweiten umgekehrten Schrägstrich ist der Produktname:

   ```
   GOOGLE CHROME
   ```

7. Kopieren Sie den Namen der ausführbaren Datei (beispielsweise "snippingtool. exe"), und fügen Sie Sie in die **Datei** ein (erforderlich).

   Wenn beispielsweise die WipAppId

   ```
   O=GOOGLE LLC, L=MOUNTAIN VIEW, S=CA, C=US\GOOGLE CHROME\CHROME.EXE\74.0.3729.108
   ```

   der Text zwischen dem zweiten und dritten umgekehrten Schrägstrich ist die Datei:

   ```
   CHROME.EXE
   ```

8. Geben Sie die Versionsnummer der app in die **Min-Version** in InTune ein (Alternativ können Sie die Max-Version angeben, aber die eine oder andere ist erforderlich), und wählen Sie dann die **Aktion**aus: **zulassen** oder **ablehnen** .

Beim Arbeiten mit WIP-aktivierten apps und WIP-unbekannten apps wird empfohlen, dass Sie mit **Silent** beginnen oder **Außerkraftsetzungen zulassen** , während Sie mit einer kleinen Gruppe überprüfen, ob Sie die richtigen apps in der Liste der zulässigen Apps verwenden. Nachdem Sie fertig sind, können Sie zu ihrer endgültigen Erzwingungsrichtlinie wechseln, **blockieren**. Weitere Informationen zu WIP-Modi finden Sie unter Schützen von Unternehmensdaten mithilfe von WIP: WIP-Modi .

> **NOTE**
>
> Tragen Sie dazu bei, dieses Thema zu verbessern, indem Sie uns Bearbeitungen, Ergänzungen und Feedback schicken. Informationen dazu, wie Sie zu diesem Thema beitragen können, finden Sie unter Bearbeiten der Windows IT Professional-Dokumentation.

So schützt Windows Information Protection (WIP) eine Datei mit einer Vertraulichkeits Bezeichnung

11.02.2020 • 4 minutes to read

Betrifft

- Windows Defender Advanced Threat Protection (Windows Defender ATP)
- Windows10, Version1903
- Windows10, Version1809

> **IMPORTANT**
> Einige Informationen beziehen sich auf die Vorabversion, an der bis zur kommerziellen Veröffentlichung unter Umständen noch grundsätzliche Änderungen vorgenommen werden. Microsoft übernimmt keine Garantie, weder ausdrücklich noch stillschweigend, für die hier bereitgestellten Informationen.

In diesem Thema wird erläutert, wie der Windows-Informationsschutz mit anderen Microsoft-Informationsschutz Technologien funktioniert, um Dateien mit einer Vertraulichkeits Bezeichnung zu schützen. Microsoft-Informationsschutz Technologien arbeiten als integrierte Lösung zusammen, um Unternehmen zu unterstützen:

- Ermitteln von Unternehmensdaten auf endpunktgeräten
- Klassifizieren und Beschriften von Informationen basierend auf Inhalt und Kontext
- Schützen von Unternehmensdaten vor unbeabsichtigtem verlassen in Umgebungen außerhalb des Unternehmens
- Aktivieren von Überwachungsberichten für Benutzerinteraktionen mit Unternehmensdaten auf endpunktgeräten

Zu den Microsoft-Informationsschutz Technologien gehören:

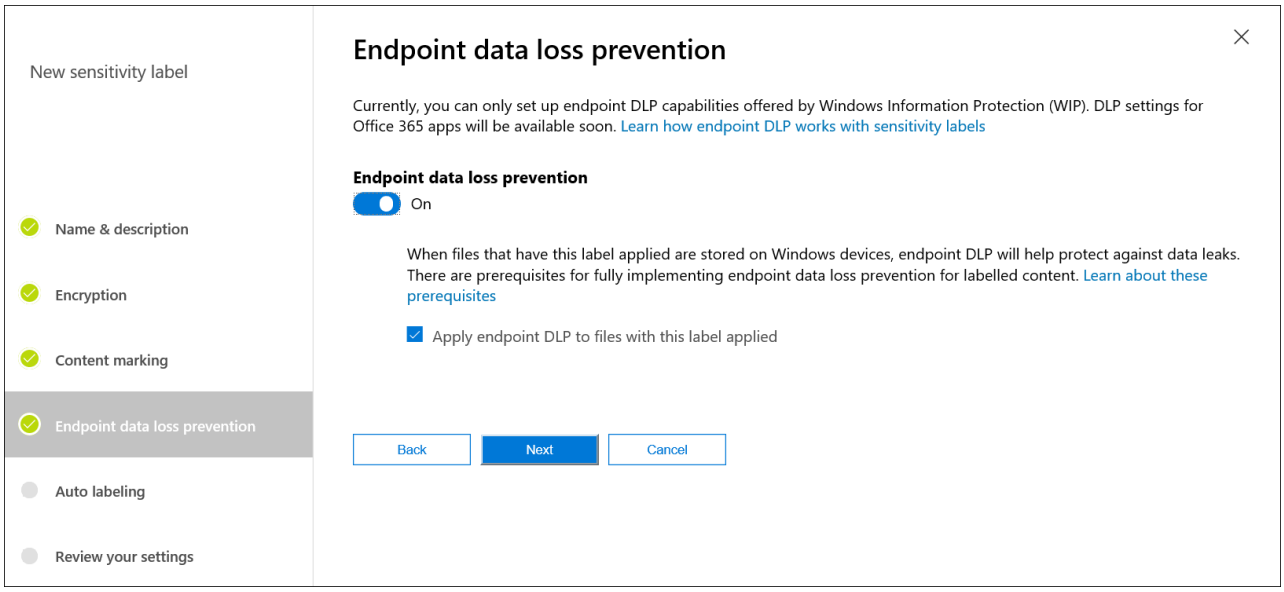
- Windows Information Protection (WIP) ist in Windows 10 integriert und schützt lokale Daten, die sich auf Endgeräten befinden, und verwaltet apps, um die verwendeten lokalen Daten zu schützen. Daten, die das Endpunktgerät verlassen, wie etwa eine e-Mail-Anlage, sind nicht durch WIP geschützt.

- Azure Information Protection ist eine Cloud-basierte Lösung, die entweder eigenständig oder als Teil von Microsoft 365 Enterprise erworben werden kann. Es hilft einer Organisation, Ihre Dokumente und e-Mails durch Anwenden von Etiketten zu klassifizieren und zu schützen. Der Azure-Informationsschutz wird direkt auf Inhalte angewendet und mit dem Inhalt durchwandert, während er Zwischenspeicher Orten und Cloud-Diensten verschoben wird.

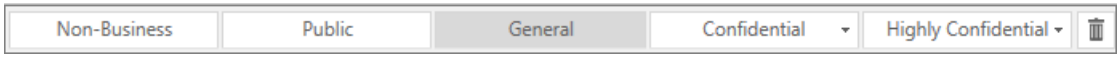
- Die Microsoft-Cloud-App-Sicherheit ist eine Cloud Access Security Broker-Lösung (CASB), mit der Sie Benutzerdaten in Software-as-a-Service (SaaS)-apps von Drittanbietern, die von Ihrer Organisation verwendet werden, ermitteln, klassifizieren, schützen und überwachen können.

So schützt WIP Vertraulichkeits Beschriftungen mit der Vermeidung von Endpunkt Datenverlust

Sie können Vertraulichkeits Beschriftungen im Microsoft 365 Compliance Center erstellen und verwalten. Wenn Sie eine Vertraulichkeits Beschriftung erstellen, können Sie angeben, dass die Verhinderung von Endpunkt Datenverlust für Inhalte mit diesem Etikett gelten soll.



Benutzer von Office-Apps können eine Vertraulichkeits Beschriftung aus einem Menü auswählen und auf eine Datei anwenden.



WIP erzwingt den Standardendpunkt Schutz wie folgt:

- Wenn die Verhinderung von Endpunkt Datenverlust aktiviert ist, erzwingt das Gerät den Arbeitsschutz für jede Datei mit der Bezeichnung.
- Wenn die Verhinderung von Endpunkt Datenverlust nicht aktiviert ist:
  - Das Gerät erzwingt den Arbeitsschutz für eine Datei, die von einer Arbeitswebsite heruntergeladen wurde.
  - Das Gerät erzwingt keinen Arbeitsschutz für eine Datei, die von einer persönlichen Website heruntergeladen wurde.

Hier sehen Sie ein Beispiel, in dem eine Datei ohne Arbeitskontext außerhalb der Vertraulichkeits Beschriftung geschützt bleibt:

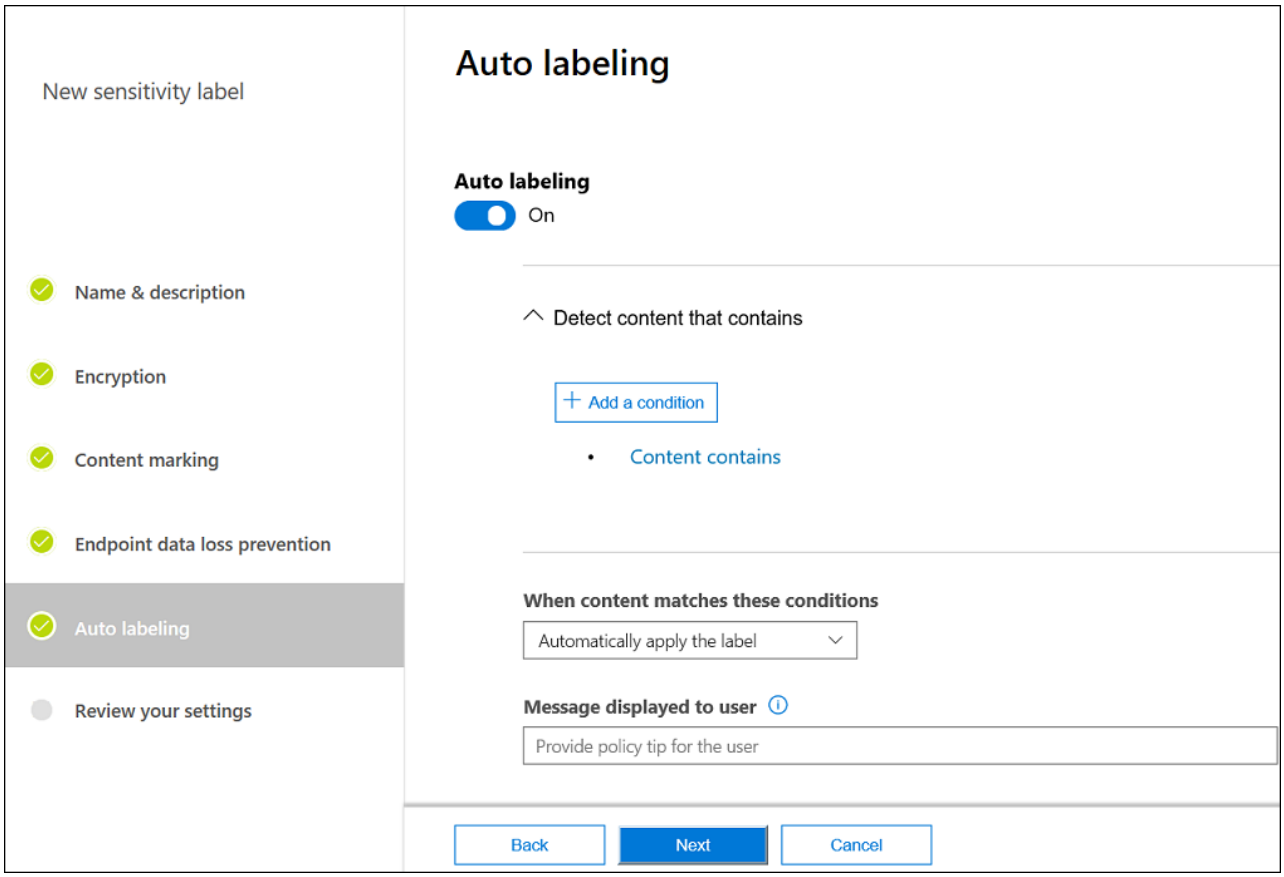
1. Sara erstellt eine PDF-Datei auf einem Mac und kennzeichnet Sie als **vertraulich**.
2. Sie sendet die PDF-Datei von Ihrem Gmail-Konto an Laura.
3. Laura öffnet die PDF-Datei auf Ihrem Windows 10-Gerät.
4. Windows Defender Advanced Threat Protection (Windows Defender ATP) scannt Windows 10 auf jede Datei, die geändert oder erstellt wird, einschließlich Dateien, die auf einer persönlichen Website erstellt wurden.
5. Windows Defender ATP löst die WIP-Richtlinie aus.
6. WIP-Richtlinie schützt die Datei, obwohl Sie von einer persönlichen Website stammen.

So schützt WIP automatisch klassifizierte Dateien

In den nächsten Abschnitten wird erläutert, wie Windows Defender ATP die Erkennung und den Schutz vertraulicher Informationen durch Verbesserungen in Windows 10, Version 1903, erweitert.

Entdeckung

Windows Defender ATP kann den Inhalt der Datei selbst extrahieren und auswerten, ob vertrauliche Informationstypen wie Kreditkartennummern oder Mitarbeiter-ID-Nummern enthalten sind. Wenn Sie eine Vertraulichkeits Beschriftung erstellen, können Sie angeben, dass die Beschriftung jeder Datei hinzugefügt werden soll, die einen vertraulichen Informationstyp enthält.

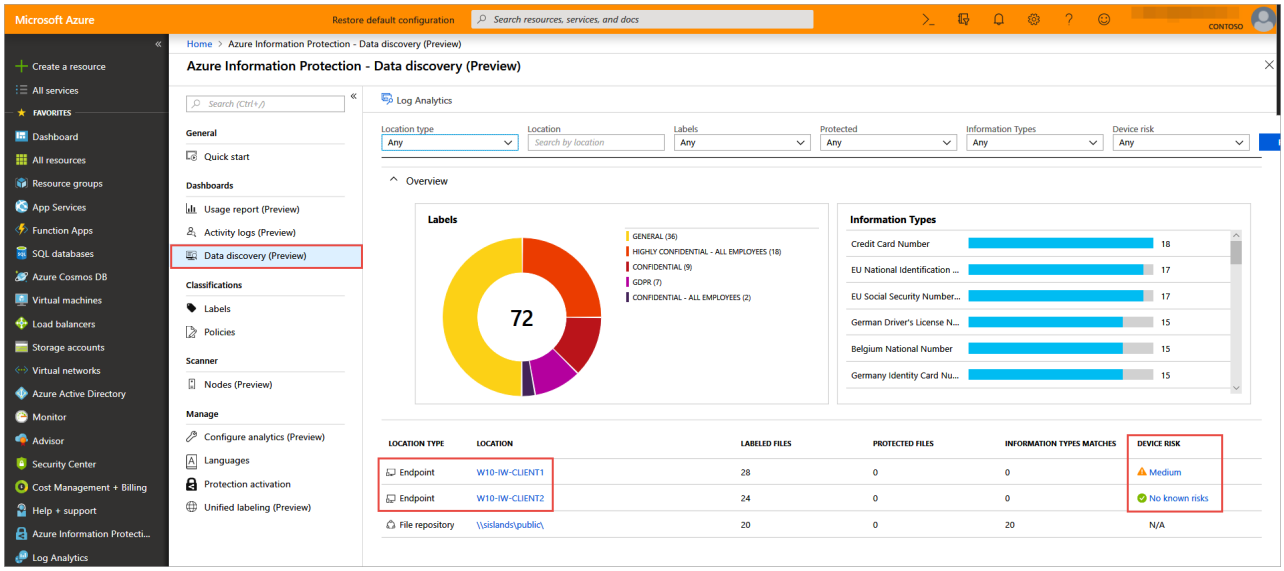


Ein Standardsatz vertraulicher Informationstypen im Microsoft 365 Compliance Center umfasst Kreditkartennummern, Telefonnummern, Führerscheinnummern usw. Sie können auch einen benutzerdefinierten vertraulichen Informationstyp erstellen, der ein beliebiges Stichwort oder einen Ausdruck enthalten kann, den Sie auswerten möchten.

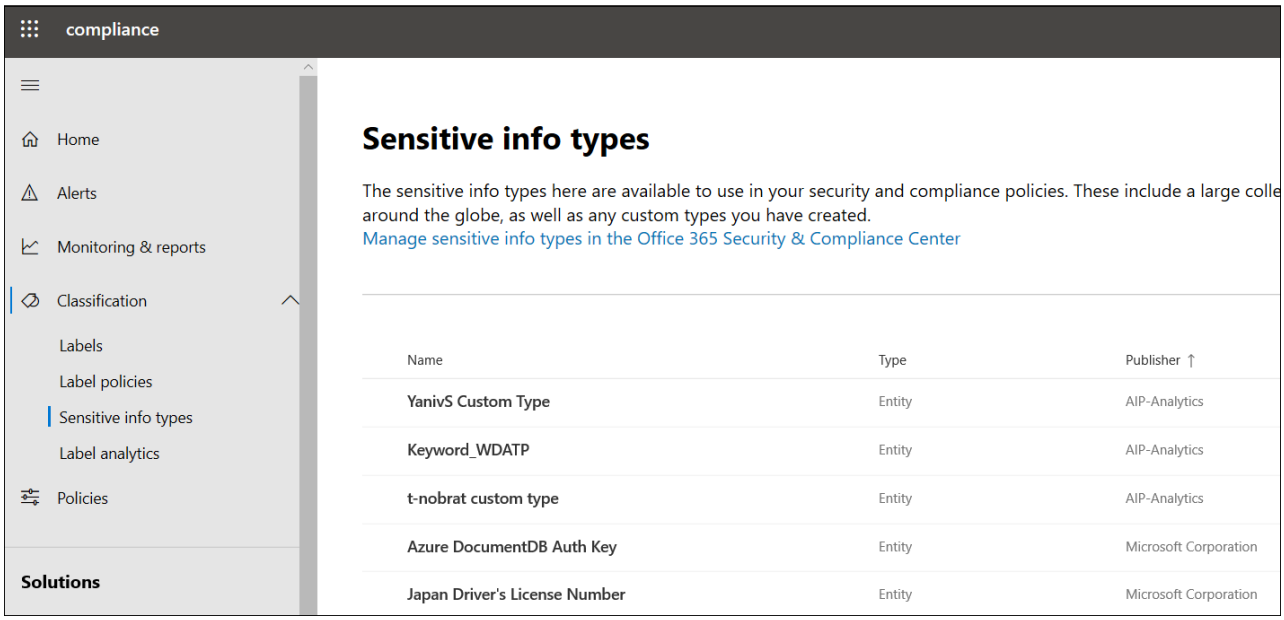
Schutz

Wenn eine Datei auf einem Windows 10-Endpunkt erstellt oder bearbeitet wird, extrahiert Windows Defender ATP den Inhalt, und es wird ausgewertet, ob er Standard-oder benutzerdefinierte vertrauliche Informationstypen enthält, die definiert wurden. Wenn die Datei übereinstimmt, wendet Windows Defender ATP die Verhinderung von Endpunkt Datenverlust an, auch wenn die Datei zuvor keine Bezeichnung aufwies.

Windows Defender ATP ist in Azure Information Protection für die Datenerkennung integriert und meldet vertrauliche Informationstypen, die gefunden wurden. Azure Information Protection aggregiert die Dateien mit Vertraulichkeits Beschriftungen und den vertraulichen Informationstypen, die im gesamten Unternehmen enthalten sind.



Sie können vertrauliche Informationstypen in der Microsoft 365-Compliance unter **Klassifizierungen**anzeigen. Standardmäßige vertrauliche Informationstypen haben Microsoft als Publisher. Der Herausgeber für benutzerdefinierte Typen ist der Name des Mandanten.



> **NOTE**
>
> Bei der automatischen Klassifizierung wird die Datei selbst nicht geändert, Sie wird jedoch auf der Grundlage des Labels geschützt. WIP schützt eine Datei, die einen vertraulichen Informationstyp enthält, als Arbeitsdatei. Der Azure-Informationsschutz funktioniert anders, da er eine Datei mit einem neuen Attribut erweitert, damit der Schutz beibehalten wird, wenn die Datei kopiert wird.

Voraussetzungen

- Verhinderung von Endpunkt Datenverlust erfordert Windows 10, Version 1809
- Für die automatische Kennzeichnung ist Windows 10, Version 1903, erforderlich.
- Geräte müssen an Windows Defender ATPübermittelt werden, die Inhalte für ein Etikett scannt und die WIP-Richtlinie anwendet
- Vertraulichkeits Bezeichnungen müssen im Microsoft 365 Compliance Center konfiguriert werden.
- Die WIP-Richtlinie muss mithilfe von InTune oder Microsoft Endpoint Configuration Manager auf Endpunktgeräte angewendet werden.

Sichern des Startvorgangs von Windows10

04.12.2019 • 8 minutes to read

Betrifft:

- Windows 10
- Windows8.1

Das Windows-Betriebssystem verfügt über zahlreiche Funktionen zum Schutz vor Malware, und es ist erstaunlich gut. Mit Ausnahme von Apps, die von Unternehmen entwickelt und intern verwendet werden, müssen alle Microsoft Store-Apps eine Reihe von Anforderungen erfüllen, um zertifiziert zu sein und im Microsoft Store aufgenommen zu werden. Dieser Zertifizierungsprozess überprüft verschiedene Kriterien, einschließlich der Sicherheit und ist eine effektive Möglichkeit um zu verhindert, dass Schadsoftware im Microsoft Store auftritt. Auch wenn eine böswillige App durchkommt, umfasst das Windows10-Betriebssystem eine Reihe von Sicherheitsfeatures, die die Auswirkungen verringern können. Microsoft Store-Apps befinden sich beispielsweise im Sandkasten und verfügen nicht über die erforderlichen Rechte, um auf Benutzerdaten zuzugreifen oder Systemeinstellungen zu ändern.

Windows10 verfügt auch über mehrere Schutzebenen für Desktop-Apps und-Daten. Windows Defender verwendet Signaturen zum Erkennen und Isolieren von Apps, die bekanntermaßen schädlich sind. Windows Defender-SmartScreen warnt Benutzer vor dem Ausführen einer nicht vertrauenswürdigen APP, selbst wenn Sie als Schadsoftware erkannt wird. Bevor eine App Systemeinstellungen ändern kann, müssen Benutzer der App mit der Benutzerkontensteuerung Administratorrechte gewähren.

Das sind nur einige der Möglichkeiten, wie Windows10 Sie vor Malware schützt. Diese Sicherheitsfeatures schützen Sie jedoch erst nach dem Start von Windows10. Moderne Schadsoftware – und besonders Bootkits – können sogar vor dem Start von Windows durchgeführt werden und so die Sicherheit des Betriebssystems umgehen, und dabei vollständig verborgen bleiben.

Beim Ausführen von Windows10 auf einem PC oder einem beliebigen PC, der Unified Extensible Firmware Interface (UEFI) unterstützt, schützt der vertrauenswürdige Start Ihren PC vor Schadsoftware von dem Moment an, in dem Sie Ihren PC einschalten, bis die Anti-Malware beginnt. Im unwahrscheinlichen Fall, dass Schadsoftware einen PC infiziert, kann sie nicht versteckt bleiben. Der vertrauenswürdige Start kann die Integrität des Systems auf eine Weise belegen, damit Malware kann nicht versteckt durchgeführt werden kann. Selbst auf PCs ohne UEFI bietet Windows10 noch bessere Startsicherheit als frühere Windows-Versionen.

Zunächst betrachten wir, was Rootkits sind und wie sie funktionieren. Dann zeigen wir Ihnen, wie Sie Windows10 schützen können.

Die Bedrohung: Rootkits

Rootkits sind ausgefeilte, gefährliche Schadsoftware, die im Kernelmodus ausgeführt wird und die gleichen Berechtigungen wie das Betriebssystem ausnutzt. Da Rootkits dieselben Berechtigungen wie das Betriebssystem haben und vor dem Start ausgeführt werden, können sie sich selbst und andere Anwendungen vollständig verstecken. Rootkits sind häufig Bestandteil einer ganzen Schadsoftware-Suite, die lokale Anmeldedaten umgehen, Kennwörter und Tastaturanschlägen aufzeichnen, private Dateien übertragen und kryptografische Daten erfassen kann.

Verschiedene Arten von Rootkits werden in verschiedenen Phasen des Startvorgangs geladen:

- **Firmware-Rootkits.** Diese Kits überschreiben die Firmware des NetBIOS des PCs oder andere Hardware, damit das Rootkit vor Windows gestartet werden kann.

- **Bootkits.** Diese Kits ersetzen Sie das Startladeprogramm des Betriebssystems (der kleiner Teil der Software, der das Betriebssystem startet), damit der PC den Bootkit vor dem Betriebssystem lädt.
- **Kernel-Rootkits.** Diese Kits ersetzt einen Teil des Kernels des Betriebssystems, damit das Rootkit automatisch gestartet werden kann, wenn das Betriebssystem geladen wird.
- **Treiber-Rootkits.** Diese Kits geben sich als vertrauenswürdiger Treiber aus, den Windows zum Kommunizieren mit der PC-Hardware verwendet.

Die Gegenmaßnahmen

Windows10 unterstützt vier Features, mit denen verhindert wird, dass Rootkits und Bootkits während des Startvorgangs geladen werden:

- **Sicherer Start.** PCs mit UEFI-Firmware und einem Trusted Platform Module (TPM) können so konfiguriert werden, dass nur vertrauenswürdige Betriebssystem-Startladeprogramme geladen werden.
- **Vertrauenswürdiger Start.** Windows überprüft die Integrität jeder Komponente des Startvorgangs, bevor diese geladen wird.
- **Antischadsoftware-Frühstart (Early Launch Antimalware, ELAM).** ELAM testet alle Treiber vor dem Laden und verhindert, dass nicht genehmigte Treiber geladen werden.
- **Kontrollierter Start.** Die Firmware des PCs protokolliert den Startvorgang, und Windows kann die Informationen an einen vertrauenswürdigen Server senden, der die Integrität des PCs objektiv prüfen und bewerten kann.

Abbildung1 zeigt den Windows10-Startvorgang an.

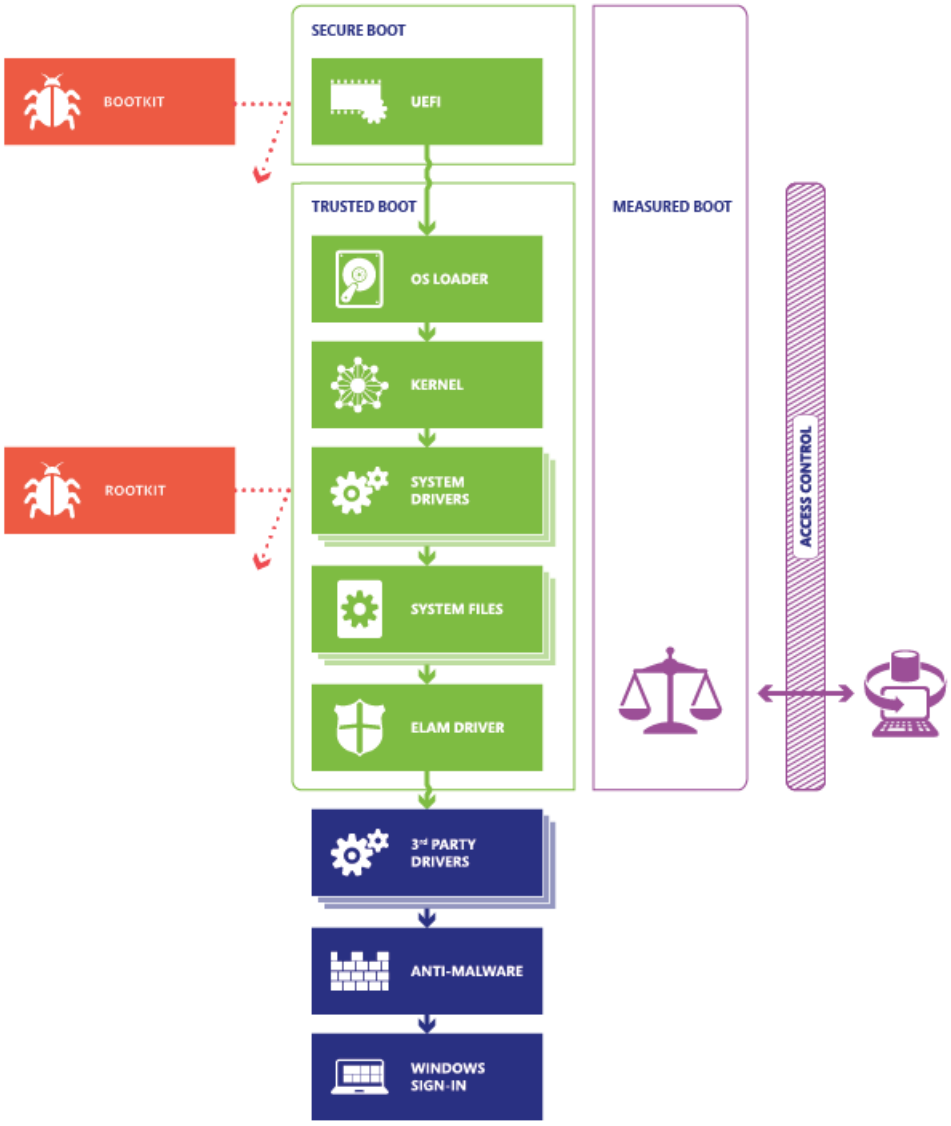


Abbildung1. Sicherer Start, vertrauenswürdiger Start und kontrollierter Start, der Malware in jeder Phase blockiert

Sicheres Booten und gemessenes Booten sind nur auf PCs mit UEFI 2.3.1 und einem TPM-Chip möglich. Glücklicherweise verfügen alle Windows10-PCs, die das Windows-Hardware-Kompatibilitätsprogramm erfüllen, diese Anforderungen und viele PCs, die für frühere Versionen von Windows entwickelt wurden, ebenfalls.

Den folgenden Abschnitten wird der sichere Start, der vertrauenswürdige Start, ELAM und der kontrollierte Start beschrieben.

Sicherer Start

Beim Starten eines PCs findet dieser zuerst das Startladeprogramm des Betriebssystems. PCs ohne sicheren Start führen Sie einfach das Startladeprogramms aus, das sich auf der PC-Festplatte befindet. Es gibt keine Möglichkeit für den PC, um festzustellen, ob es sich um ein vertrauenswürdiges Betriebssystem oder einen Rootkit handelt.

Wenn ein PC mit UEFI gestartet wird, überprüft der PC zunächst, ob die Firmware digital signiert ist und reduziert so das Risiko der Firmware Rootkits. Wenn der sichere Start aktiviert ist, überprüft die Firmware die digitale Signatur des Startladeprogramms, um sicherzustellen, dass es nicht geändert wurde. Wenn das Startladeprogramm intakt ist, beginnt die Firmware nur dann das Startladeprogramm, wenn eine der folgenden Bedingungen zutrifft:

- **Das Startladeprogramm wurde mit einem vertrauenswürdigen Zertifikat signiert.** Im Fall von PCs, die für Windows10 zertifiziert sind, wird das Microsoft®-Zertifikat als vertrauenswürdig eingestuft.
- **Der Benutzer hat die digitale Signatur des Startladeprogramms manuell genehmigt.** Dadurch kann der Benutzer Nicht-Microsoft-Betriebssysteme laden.

Alle x86-basierten zertifizierten für Windows10-PCs müssen verschiedene Anforderungen im Zusammenhang mit dem sicheren Booten erfüllen:

- Der sichere Start muss standardmäßig aktiviert sein.
- Sie müssen dem Zertifikat von Microsoft (und damit alle von Microsoft signierten Bootloadern) vertrauen.
- Sie müssen dem Benutzer erlauben, den sicheren Start so zu konfigurieren, dass anderen Startladeprogrammen vertraut wird.
- Sie müssen dem Benutzer erlauben, den sicheren Start vollständig zu deaktivieren.

Diese Anforderungen bieten Schutz gegen Rootkits und erlauben Ihnen gleichzeitig, jedes beliebige Betriebssystem auszuführen. Sie haben drei Optionen zum Ausführen nicht von Microsoft stammender Betriebssysteme:

- **Verwenden Sie ein Betriebssystem mit einem zertifizierten Startladeprogramm.** Da alle zertifizierten für Windows10-PCs dem Microsoft-Zertifikat vertrauen müssen, bietet Microsoft einen Dienst zum Analysieren und Signieren eines nicht von Microsoft bereitgestellten Bootloaders, damit dieser von allen zertifizierten für Windows10-PCs als vertrauenswürdig eingestuft wird. Ein Open-Source-Startladeprogramm, das Linux laden ist, steht bereits zur Verfügung. Wenn Sie mit dem Verfahren zum Erhalt eines Zertifikats beginnen möchten https://partner.microsoft.com/dashboard, wechseln Sie zu.
- **Konfigurieren Sie UEFI, um Ihrem benutzerdefinierten Startladeprogramm zu vertrauen.** Mit allen zertifizierten für Windows10-PCs können Sie einem nicht zertifizierten Bootloader Vertrauen, indem Sie der UEFI-Datenbank eine Signatur hinzufügen, die es Ihnen ermöglicht, ein beliebiges Betriebssystem einschließlich selbst gemachter Betriebssysteme auszuführen.
- **Deaktivieren Sie den sicheren Start.** Alle zertifizierten für Windows10-PCs ermöglichen Ihnen, das sichere Booten zu deaktivieren, damit Sie jede beliebige Software ausführen können. Dies hilft Ihnen aber nicht beim Schutz gegen Bootkits.

Um zu verhindern, dass Schadsoftware diese Optionen missbraucht, muss der Benutzer die UEFI-Firmware manuell so konfigurieren, dass sie einem nicht zertifizierten Startladeprogramm vertraut, oder er muss den sicheren Start deaktivieren. Software kann die Einstellungen für den sicheren Start nicht ändern. Weitere Informationen zum sicheren Start finden Sie im Blog Schützen der Umgebung vor dem Betriebssystemstart mit UEFI.

Wie die meisten mobilen Geräte sind arm-based Certified für WindowsRT-Geräte wie das Microsoft Surface RT-Gerät so konzipiert, dass nur Windows 8.1 ausgeführt werden kann. Aus diesem Grund kann der sichere Start nicht deaktiviert werden, und ein anderes Betriebssystem kann nicht geladen werden. Es gibt allerdings viele ARM-Geräte, die andere Betriebssysteme ausführen können.

Vertrauenswürdiger Start

Der vertrauenswürdige Start fängt dort an, wo der sichere Start aufhört. Der Bootloader überprüft die digitale Signatur des Windows10-Kernels, bevor er geladen wird. Der Windows10-Kernel überprüft wiederum jede andere Komponente des Windows-Startvorgangs, einschließlich der Start Treiber, Startdateien und Elam. Wenn eine Datei geändert wurde, erkennt das Startladeprogramm das Problem und weigert sich, die beschädigte Komponente zu laden. Häufig kann Windows10 die beschädigte Komponente automatisch reparieren, die Integrität von Windows wiederherstellen und es dem PC ermöglichen, normal zu starten.

Antischadsoftware-Frühstart

Da der sichere Start das Startladeprogramm und der vertrauenswürdige Start den Windows-Kernel geschützt hat, ist die nächste Angriffsgelegenheit für die Schadsoftware die Infizierung eines nicht von Microsoft stammenden Starttreibers. Herkömmliche Antischadsoftware-Apps starten erst, nachdem die Starttreiber geladen wurden. Dadurch kann ein als Treiber maskiertes Rootkit zu wirken beginnen.

Antischadsoftware-Frühstart (Early Launch Antimalware, ELAM) kann vor dem Laden von nicht von Microsoft stammenden Starttreibern und Anwendungen einen Antischadsoftware-Treiber von Microsoft oder einem Drittanbieter laden und so die durch „Sicherer Start" und „Vertrauenswürdiger Start" erstellte Vertrauenskette fortsetzen. Da das Betriebssystem noch nicht gestartet wurde, und da Windows so schnell wie möglich zu starten muss, hat ELAM eine einfache Aufgabe: alle Startgerätetreiber untersuchen und bestimmen, ob sie auf der Liste der vertrauenswürdigen Treiber stehen. Wenn er nicht als vertrauenswürdig eingestuft wird, lädt Windows ihn nicht.

Ein ELAM-Treiber ist keine vollwertige Antischadsoftware-Lösung, die später im Startprozess geladen wird. Windows Defender (im Lieferumfang von Windows10 enthalten) unterstützt Elam, ebenso wie Microsoft System Center2012-Endpunktschutz und verschiedene Antimalware-apps, die nicht von Microsoft verwendet werden.

Kontrollierter Start

Wenn ein PC in Ihrer Organisation mit einem Rootkit infiziert wird, müssen Sie darüber Bescheid wissen. Enterprise Antischadsoftware-Apps können Schadsoftwareinfektionen an die IT-Abteilung melden, dies gilt allerdings nicht für Rootkits, die ihre Anwesenheit verdecken. Anders ausgedrückt, können nicht dem Kunden nicht vertrauen, festzustellen, ob alles fehlerfrei ist.

Daher erscheinen mit Rootkits infizierte PCs fehlerfrei, auch wenn Antischadsoftware ausgeführt wird. Infizierten PCs stellen auch weiterhin eine Verbindung mit dem Netzwerk des Unternehmens her und geben so dem Rootkit Zugriff auf große Mengen an vertraulichen Daten und lassen potenziell zu, dass das Rootkit auf dem internen Netzwerk verteilt wird.

Wenn Sie mit der TPM-und nicht-Microsoft-Software arbeiten, ermöglicht der gemessene Start in Windows10 einem vertrauenswürdigen Server im Netzwerk, die Integrität des Windows-Startvorgangs zu überprüfen. Der kontrollierte Start verwendet folgenden Prozess:

1. Die UEFI-Firmware des PCs speichert im TPM einen Hash der Firmware, des Startladeprogramm, Starttreibers und aller Elemente, die vor der Antischadsoftware-App geladen werden.
2. Am Ende des Startvorgangs startet Windows den Nicht-Microsoft-Client für dem Remotenachweis. Der vertrauenswürdige Integritätsnachweis-Server sendet dem Client einen eindeutigen Schlüssel.
3. Das TPM verwendet den eindeutigen Schlüssel, um das von der UEFI aufgezeichnete Protokoll digital zu signieren.
4. Der Client sendet das Protokoll an den Server, eventuell zusammen mit anderen Sicherheitsinformationen.

Je nach Implementierung und Konfiguration kann der Server ermitteln, ob der Client fehlerfrei ist und dem Client Zugriff auf ein beschränktes Quarantänenetzwerk oder das vollständige Netzwerk gewähren.

Bild2 veranschaulicht den gemessenen Start-und Remote-Bestätigungsprozess.

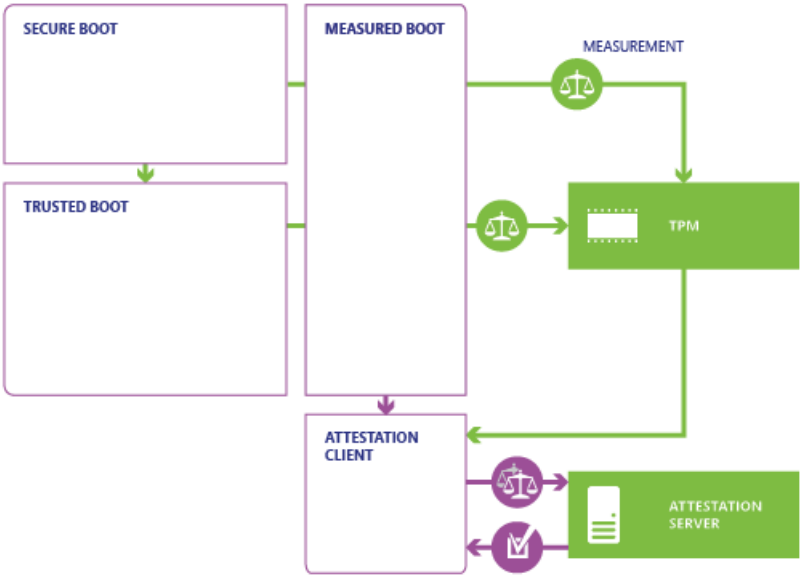


Abbildung2. Der kontrollierte Start garantiert dem Remoteserver die Integrität des PCs

Windows10 enthält die Anwendungsprogrammierschnittstellen zur Unterstützung des gemessenen Starts, aber Sie benötigen nicht-Microsoft-Tools, um einen Remote Bestätigungs Client und einen vertrauenswürdigen Bestätigungs Server zu implementieren, um ihn zu nutzen. Ein Beispiel eines solchen Tools kann als TPM-Plattform-Kryptografieanbieter-Toolkit von Microsoft Research oder Microsoft Enterprise Security MVP Dan Griffin als kontrolliertes Starttool heruntergeladen werden.

Der gemessene Start verwendet die Leistungsfähigkeit von UEFI, TPM und Windows10, um Ihnen eine Möglichkeit zu geben, die Vertrauenswürdigkeit eines Client-PCs über das Netzwerk sicher zu bewerten.

Zusammenfassung

Sicherer Start, vertrauenswürdiger Start und kontrollierter Start erstellen eine Architektur, die grundsätzlich widerstandsfähiger gegen Bootkits und Rootkits ist. In Windows10 haben diese Features das Potenzial, Malware auf Kernelebene aus Ihrem Netzwerk zu entfernen. Dies ist die bahnbrechendste Antischadsoftware-Lösung, die Windows jemals entwickelt hat. Sie sprengt alle vorher bekannten Grenzen. Mit Windows10 können Sie der Integrität Ihres Betriebssystems wirklich vertrauen.

Zusätzliche Ressourcen

- Windows 10 Enterprise Evaluation

Trusted Platform Module

12.09.2019 • 2 minutes to read

Betrifft

- Windows 10
- Windows Server 2016

Die TPM-Technologie stellt hardwarebasierte, sicherheitsbezogene Funktionen bereit. Ein TPM-Chip ist ein sicherer Krypto-Prozessor, der Sie u.a. beim Erstellen und Speichern kryptografischer Schlüssel sowie beim Beschränken der Nutzung kryptografischer Schlüssel unterstützt. Die folgenden Themen enthalten ausführlichere Informationen:

THEMA	BESCHREIBUNG
Trusted Platform Module – Übersicht	Hier finden Sie eine Übersicht über das Trusted Platform Module (TPM) und erfahren, wie Windows es für die Zugriffssteuerung und Authentifizierung verwendet.
Grundlagen zu Trusted Platform Module	Enthält Hintergrundinformationen zur Funktionsweise von einem TPM mit kryptografischen Schlüsseln. Darüber hinaus werden Technologien beschrieben, die mit dem TPM verwendet werden können, beispielsweise TPM-basierte virtuelle Smartcards.
Gruppenrichtlinieneinstellungen für TPM-Dienste	Beschreibt die TPM-Dienste, die mithilfe von Gruppenrichtlinieneinstellungen zentral gesteuert werden können.
Sichern der TPM-Wiederherstellungsinformationen in AD DS	Gilt nur für Windows 10, Version 1511, und Windows 10, Version 1507. Es wird beschrieben, wie die TPM-Informationen eines Computers in Active Directory Domain Services gesichert werden.
Behandeln von Problemen mit dem TPM	Hier werden die Aktionen beschrieben, die Sie über das TPM-Snap-In „TPM.msc" ausführen können: Anzeigen des TPM-Status, Beheben von Problemen bei der TPM-Initialisierung und Löschen von Schlüsseln aus dem TPM. Darüber hinaus wird für TPM1.2 und Windows10, Version 1507 oder 1511, erläutert, wie Sie das TPM aktivieren bzw. deaktivieren.
Grundlegendes zu PCR-Bänken auf TPM2.0-Geräten	Enthält Hintergrundinformationen darüber, was geschieht, wenn Sie PCR-Bänke auf TPM 2.0-Geräten wechseln.
TPM-Empfehlungen	Hier werden verschiedene Aspekte des TPMs, beispielsweise der Unterschied zwischen TPM1.2 und 2.0, sowie die Windows10-Features erläutert, für die ein TPM erforderlich ist oder empfohlen wird.

Trusted Platform Module – Technologieübersicht

12.09.2019 • 4 minutes to read

Betrifft

- Windows10
- Windows Server 2016
- Windows Server 2019

In diesem Thema für IT-Experten wird das Trusted Platform Module (TPM) beschrieben. Außerdem wird erläutert, wie es von Windows für die Zugriffssteuerung und Authentifizierung verwendet wird.

Featurebeschreibung

Die TPM-Technologie stellt hardwarebasierte, sicherheitsbezogene Funktionen bereit. Ein TPM-Chip ist ein sicherer Krypto-Prozessor, der für die Ausführung kryptografischer Vorgänge ausgelegt ist. Der Chip umfasst mehrere physische Sicherheitsmechanismen, die ihn manipulationssicher machen, und Schadsoftware ist nicht in der Lage, die Sicherheitsfunktionen des TPMs zu manipulieren. Die wichtigsten Vorteile der TPM-Technologie bestehen in ihren Möglichkeiten. Sie können:

- Kryptografieschlüssel generieren, speichern und deren Einsatz beschränken.
- TPM-Technologie für die Plattformgeräteauthentifizierung nutzen. Sie verwenden dazu den eindeutigen RSA-Schlüssel des TPMs, der in sich selbst geschrieben ist.
- Plattformintegrität gewährleisten, indem Sicherheitsmessungen vorgenommen und gespeichert werden.

Die häufigsten TPM-Funktionen werden für Messungen der Systemintegrität sowie für die Erstellung und Verwendung von Schlüsseln verwendet. Während des Systemstarts kann der geladene Startcode (einschließlich Firmware- und Betriebssystemkomponenten) gemessen und im TPM aufgezeichnet werden. Mithilfe der Integritätsmessungen kann nachgewiesen werden, wie ein System gestartet wurde. Darüber hinaus stellen sie sicher, dass ein TPM-basierter Schlüssel erst verwendet wurde, nachdem das System mit der richtigen Software gestartet wurde.

TPM-basierte Schlüssel können auf verschiedene Weisen konfiguriert werden. Beispielsweise können Sie dafür sorgen, dass ein TPM-basierter Schlüssel nicht außerhalb des TPMs verfügbar ist. Auf diese Weise lassen sich Phishingangriffe verringern, da der Schlüssel nicht ohne das TPM kopiert und verwendet wird. TPM-basierte Schlüssel können auch so konfiguriert werden, dass zu ihrer Verwendung ein Autorisierungswert erforderlich ist. Wenn der Autorisierungswert zu häufig falsch geraten wird, aktiviert das TPM seine Logik gegen Wörterbuchangriffe und verhindert, dass weiter versucht wird, den Autorisierungswert zu erraten.

In den Spezifikationen der Trusted Computing Group (TCG) sind unterschiedliche TPM-Versionen definiert. Weitere Informationen finden Sie auf der TCG-Website.

Automatische Initialisierung des TPMs mit Windows10

Ab Windows10 wird das Betriebssystem automatisch initialisiert und die Inhaberschaft des TPMs übernommen. Daher empfiehlt es sich in den meisten Fällen, die Konfiguration des TPMs über die TPM-Verwaltungskonsole (**TPM.msc**) zu vermeiden. Es gibt einige Ausnahmen, die hauptsächlich mit dem Zurücksetzen oder einer Neuinstallation auf einem PC in Zusammenhang stehen. Weitere Informationen finden Sie unter Löschen aller Schlüssel aus dem TPM. Die TPM-Verwaltungskonsole wird ab Windows Server 2019 und Windows 10, Version 1809, nicht mehr aktiv entwickelt .

In bestimmten Unternehmensszenarios (nur Windows 10, Version 1507 und 1511) kann die Gruppenrichtlinie zum Sichern des TPM-Benutzerautorisierungswerts in Active Directory verwendet werden. Da der TPM-Zustand über Betriebssysteminstallationen hinweg erhalten bleibt, werden diese TPM-Informationen an einem von Computerobjekten getrennten Speicherort in Active Directory gespeichert.

Praktische Anwendungsfälle

Zertifikate können auf Computern installiert oder erstellt werden, die das TPM verwenden. Nachdem ein Computer bereitgestellt wurde, wird der private RSA-Schlüssel für ein Zertifikat an das TPM gebunden und kann nicht exportiert werden. Das TPM kann auch als Ersatz für Smartcards verwendet werden, wodurch die Kosten im Zusammenhang mit der Erstellung und Auszahlung von Smartcards reduziert werden.

Die automatische Bereitstellung im TPM reduziert die Kosten der TPM-Bereitstellung in einem Unternehmen. Neue APIs für die TPM-Verwaltung können bestimmen, ob für TPM-Bereitstellungsaktionen die physische Anwesenheit eines Servicetechnikers erforderlich ist, um während des Startvorgangs Anforderungen zur Änderung des TPM-Zustands zu genehmigen.

Antischadsoftware kann den beim Start des Betriebssystems gemessenen Zustand nutzen, um die Integrität eines Computers unter Windows 10 oder Windows Server 2016 zu bestätigen. Die Messungen umfassen den Start von Hyper-V, um sicherzustellen, dass in Rechenzentren, in denen Virtualisierung verwendet wird, keine nicht vertrauenswürdigen Hypervisoren ausgeführt werden. Mit der BitLocker-Netzwerkentsperrung können IT-Administratoren ein Pushupdate ausführen, ohne dass auf einem Computer eine PIN-Eingabe erforderlich ist.

Das TPM verfügt über verschiedene Gruppenrichtlinieneinstellungen, die in bestimmten Unternehmensszenarios nützlich sein können. Weitere Informationen finden Sie unter TPM-Gruppenrichtlinieneinstellungen.

Neue und geänderte Funktionalität

Weitere Infos zu neuen und geänderten TPM (Trusted Platform Module)-Funktionen in Windows 10 finden Sie unter Neues im Trusted Platform Module.

Nachweis über Geräteintegrität

Durch den Nachweis über Geräteintegrität können Unternehmen eine Vertrauensstellung basierend auf Hardware- und Softwarekomponenten eines verwalteten Geräts herstellen. Mit dem Nachweis der Geräteintegrität können Sie einen MDM-Server für die Abfrage eines Integritätsnachweisdiensts konfigurieren, der den Zugriff eines verwalteten Geräts auf eine sichere Ressource zulässt oder verweigert.

Folgendes können Sie für das Gerät überprüfen:

- Wird die Datenausführungsverhinderung unterstützt und ist sie aktiviert?
- Wird die BitLocker-Laufwerkverschlüsselung unterstützt und ist sie aktiviert?
- Wird SecureBoot unterstützt und ist es aktiviert?

> **NOTE**
> Windows 10, Windows Server 2016 und Windows Server 2019 unterstützen Geräte Integritäts Bescheinigungen mit TPM 2,0. Die Unterstützung für TPM 1,2 wurde ab Windows Version 1607 (RS1) hinzugefügt. TPM 2,0 erfordert UEFI-Firmware. Ein Computer mit Legacy-BIOS und TPM 2,0 funktioniert nicht erwartungsgemäß.

Unterstützte Versionen für die Geräte Integritäts Bescheinigung

TPM-VERSION	WINDOWS 10	WINDOWS SERVER 2016	WINDOWS SERVER 2019
TPM 1.2	>= ver 1607	>= ver 1607	Ja
TPM 2.0	Ja	Ja	Ja

Verwandte Themen

- Trusted Platform Module (Liste der Themen)
- Details zum TPM-Standard (enthält Links zu Features, die TPM verwenden)
- TPM-Basisdienste-Portal
- TPM-Basisdienste-API
- TPM-Cmdlets in Windows PowerShell
- Vorbereiten Ihrer Organisation für BitLocker: Planung und Richtlinien – TPM-Konfigurationen
- Bereitstellung von Azure Devices: Identitäts Bescheinigung mit TPM
- Bereitstellung von Azure Devices: eine Fertigungs Zeitachse für TPM-Geräte
- Windows 10: Aktivieren von vTPM (virtuelles TPM)
- So wird es gemacht: Multiboot mit BitLocker, TPM und einem nicht-Windows-Betriebssystem

Grundlagen zu Trusted Platform Module

06.03.2020 • 10 minutes to read

Betriff:

- Windows 10
- Windows Server 2016

In diesem Thema für den IT-Experten finden Sie eine Beschreibung der Komponenten des Trusted Platform Module (TPM 1.2 und TPM 2.0) und erläutern, wie Sie zum Verringern von Wörterbuchangriffen verwendet werden.

Bei einem Trusted Platform Module (TPM) handelt es sich um einen Mikrochip, der grundlegende sicherheitsrelevante Funktionen bereitstellen soll, in erster Linie mit Verschlüsselungsschlüsseln. Das TPM wird normalerweise auf der Hauptplatine eines Computers installiert, und es kommuniziert mit dem restlichen System mithilfe eines Hardware Busses.

Computer, die ein TPM integrieren, können kryptografische Schlüssel erstellen und verschlüsseln, sodass Sie nur vom TPM entschlüsselt werden können. Dieser Vorgang, der häufig als Umbruch oder Bindung eines Schlüssels bezeichnet wird, kann dazu beitragen, den Schlüssel vor Offenlegung zu schützen. Jedes TPM verfügt über einen Haupt umbruchschlüssel, den so genannten Speicherstammschlüssel, der im TPM selbst gespeichert ist. Der private Teil eines Speicher-root-Schlüssels oder Bestätigungs Schlüssels, der in einem TPM erstellt wird, wird niemals für andere Komponenten, Software, Prozesse oder Benutzer verfügbar gemacht.

Sie können angeben, ob vom TPM erstellte Verschlüsselungsschlüssel migriert werden können. Wenn Sie angeben, dass Sie migriert werden können, können die öffentlichen und privaten Teile des Schlüssels für andere Komponenten, Software, Prozesse oder Benutzer verfügbar gemacht werden. Wenn Sie angeben, dass Verschlüsselungsschlüssel nicht migriert werden können, wird der private Teil des Schlüssels niemals außerhalb des TPM verfügbar gemacht.

Computer, die ein TPM integrieren, können auch einen Schlüssel erstellen, der nicht nur umbrochen, sondern auch an bestimmte Plattformmaße gebunden ist. Diese Art von Schlüssel kann nur abgewickelt werden, wenn diese Plattformmaße dieselben Werte aufweisen, die Sie beim Erstellen des Schlüssels hatten. Dieser Vorgang wird als "Versiegeln des Schlüssels für das TPM" bezeichnet. Das Entschlüsseln des Schlüssels wird als Entsiegelung bezeichnet. Das TPM kann auch Daten versiegeln und entsiegeln, die außerhalb des TPM generiert werden. Mit diesem versiegelten Schlüssel und einer Software wie der BitLocker-Laufwerkverschlüsselung können Sie Daten Sperren, bis bestimmte Hardware-oder Softwarebedingungen erfüllt sind.

Bei einem TPM werden private Teile von Schlüsselpaaren getrennt vom Arbeitsspeicher aufbewahrt, der vom Betriebssystem gesteuert wird. Schlüssel können mit dem TPM versiegelt werden, und bestimmte Zusicherungen bezüglich des Zustands eines Systems (Zusicherungen, die die Vertrauenswürdigkeit eines Systems definieren) können erfolgen, bevor die Schlüssel entsiegelt und zur Verwendung freigegeben werden. Da das TPM seine eigenen internen Firmware-und Logikschaltkreise verwendet, um Anweisungen zu verarbeiten, ist es nicht auf das Betriebssystem angewiesen, und es ist nicht für Sicherheitslücken verfügbar, die im Betriebssystem oder in der Anwendungssoftware vorhanden sein können.

Informationen dazu, welche Versionen von Windows welche Versionen des TPMs unterstützen, finden Sie unter Übersicht über Trusted Platform Module Technology. Die in den Versionen verfügbaren Features werden in Spezifikationen von der Trusted Computing Group (TCG) definiert. Weitere Informationen finden Sie auf der Seite Trusted Platform Module auf der Website Trusted Computing Group: Trusted Platform Module.

Die folgenden Abschnitte enthalten eine Übersicht über die Technologien, die das TPM unterstützen:

- Gemessener Start mit Unterstützung für die Bescheinigung
- TPM-basierte virtuelle Smartcard
- TPM-basierter Zertifikatspeicher
- TPM-Cmdlets
- Physische Anwesenheitsschnittstelle
- TPM-1,2-Zustände und-Initialisierung
- Bestätigungsschlüssel
- TPM-Schlüsselnachweis
- Anti-hämmern

Im folgenden Thema werden die TPM-Dienste beschrieben, die mithilfe von Gruppenrichtlinieneinstellungen zentral gesteuert werden können: TPM-Gruppenrichtlinieneinstellungen.

Gemessener Start mit Unterstützung für die Bescheinigung

Das gemessene Start Feature bietet Antimalwaresoftware mit einem vertrauenswürdigen Protokoll (unempfindlich gegen Spoofing und Manipulation) aller Startkomponenten. Antimalware-Software kann das Protokoll verwenden, um zu ermitteln, ob Komponenten, die vor der Ausführung vertrauenswürdig sind, im Vergleich zu Malware infiziert sind. Sie kann auch die gemessenen Start Protokolle zur Auswertung an einen Remoteserver senden. Der Remoteserver kann Behebungsaktionen initiieren, indem er mit der Software auf dem Client oder über Out-of-Band-Mechanismen interagiert.

TPM-basierte virtuelle Smartcard

Die virtuelle Smartcard emuliert die Funktionalität herkömmlicher Smartcards, doch virtuelle Smartcards verwenden den TPM-Chip, der auf den Computern einer Organisation zur Verfügung steht, anstatt eine separate physische Smartcard und einen separaten Reader zu verwenden. Dies reduziert die Verwaltungs-und Bereitstellungskosten von Smartcards in einem Unternehmen erheblich. Für den Endbenutzer steht die virtuelle Smartcard immer auf dem Computer zur Verfügung. Wenn ein Benutzer mehr als einen Computer verwenden muss, muss eine virtuelle Smartcard für den Benutzer für jeden Computer ausgestellt werden. Ein Computer, der von mehreren Benutzern gemeinsam genutzt wird, kann mehrere virtuelle Smartcards hosten, eine für jeden Benutzer.

TPM-basierter Zertifikatspeicher

Das TPM kann zum Schützen von Zertifikaten und RSA-Schlüsseln verwendet werden. Der TPM-Schlüsselspeicheranbieter (KSP) bietet eine einfache, praktische Verwendung des TPM als Möglichkeit, um private Schlüssel stark zu schützen. Das TPM KSP kann zum Generieren von Schlüsseln verwendet werden, wenn eine Organisation für Zertifikate registriert, und der KSP wird von Vorlagen auf der Benutzeroberfläche verwaltet. Das TPM kann auch verwendet werden, um Zertifikate zu schützen, die aus einer externen Quelle importiert werden. TPM-basierte Zertifikate können genauso wie Standardzertifikate mit der hinzugefügten Funktion verwendet werden, dass das Zertifikat das TPM, aus dem die Schlüssel generiert wurden, nie belassen kann. Das TPM kann jetzt mithilfe der Kryptografie-API: Next Generation (CNG) für kryptografische Vorgänge verwendet werden. Weitere Informationen finden Sie unter Kryptographie-API: Next Generation.

TPM-Cmdlets

Sie können das TPM mithilfe von Windows PowerShell verwalten. Ausführliche Informationen finden Sie unter TPM-Cmdlets in Windows PowerShell.

Physische Anwesenheitsschnittstelle

Für TPM 1,2 erfordern die TCG-Spezifikationen für TPMs physische Anwesenheit (in der Regel durch Drücken einer Taste), um das TPM einzuschalten, zu deaktivieren oder zu löschen. Diese Aktionen können normalerweise nicht mit Skripts oder anderen Automatisierungstools automatisiert werden, es sei denn, der einzelne OEM liefert Sie.

TPM-1,2-Zustände und-Initialisierung

Für TPM 1,2 gibt es mehrere mögliche Zustände. Windows 10 initialisiert das TPM automatisch, wodurch es in einen aktivierten, aktivierten und im Besitz befindlichen Zustand versetzt wird.

Bestätigungsschlüssel

Damit ein TPM von einer vertrauenswürdigen Anwendung verwendet werden kann, muss es einen bestätigungsschlüssel enthalten, bei dem es sich um ein RSA-Schlüsselpaar handelt. Die private Hälfte des Schlüsselpaars wird im TPM gespeichert, und es wird niemals außerhalb des TPM offenbart oder darauf zugegriffen.

Schlüssel Bescheinigung

Mit der TPM-Schlüssel Bescheinigung kann eine Zertifizierungsstelle überprüfen, ob ein privater Schlüssel tatsächlich durch ein TPM geschützt ist und dass das TPM einer Zertifizierungsstelle vertraut. Nachweislich gültige bestätigungsschlüssel können verwendet werden, um die Benutzeridentität an ein Gerät zu binden. Darüber hinaus bietet das Benutzerzertifikat mit einem TPM-bestätigten Schlüssel eine höhere Sicherheit, die durch die nicht exportierbare, Anti-Hämmer-und Isolierung von Schlüsseln unterstützt wird, die von einem TPM bereitgestellt werden.

Anti-hämmern

Wenn ein TPM einen Befehl verarbeitet, erfolgt dies in einer geschützten Umgebung, beispielsweise einem dedizierten Microcontroller auf einem diskreten Chip oder einem speziellen Hardware geschützten Modus auf der Haupt-CPU. Ein TPM kann verwendet werden, um einen kryptografischen Schlüssel zu erstellen, der nicht außerhalb des TPM offen gelegt wird, aber im TPM verwendet werden kann, nachdem der richtige Autorisierungswert bereitgestellt wurde.

TPMs verfügen über einen Anti-hämmerschutz, der dazu dient, Brute-Force-Angriffe oder komplexere Wörterbuchangriffe zu verhindern, die versuchen, Autorisierungswerte für die Verwendung eines Schlüssels zu ermitteln. Der grundlegende Ansatz besteht darin, dass das TPM nur eine begrenzte Anzahl von Autorisierungsfehlern zulässt, bevor es weitere Versuche zur Verwendung von Schlüsseln und Sperren verhindert. Das Bereitstelleneiner Fehleranzahl für einzelne Schlüssel ist technisch nicht praktikabel, daher haben TPMs eine globale Sperrung, wenn zu viele Autorisierungsfehler auftreten.

Da viele Entitäten das TPM verwenden können, kann ein einzelner Autorisierungs Erfolg den Schutz vor dem Hämmern des TPM nicht zurücksetzen. Dadurch wird verhindert, dass ein Angreifer einen Schlüssel mit einem bekannten Autorisierungswert erstellt und dann zum Zurücksetzen des TPM-Schutzes verwendet. Im Allgemeinen sind TPMs dazu vorgesehen, Autorisierungsfehler nach einem bestimmten Zeitraum zu vergessen, damit das TPM nicht unnötig in einen Sperrzustand wechselt. Ein TPM-Besitzerkennwort kann verwendet werden, um die Sperrungs Logik des TPM zurückzusetzen.

TPM 2.0-Anti-hämmern

TPM 2.0 hat ein gut definiertes Anti-Hämmer-Verhalten. Dies steht im Gegensatz zu TPM 1.2, bei dem der Schutz vor dem hämmern vom Hersteller implementiert wurde, und die Logik ist in der gesamten Branche stark unterschiedlich.

Bei Systemen mit TPM 2.0 wird das TPM von Windows konfiguriert, um nach 32-Autorisierungsfehlern zu sperren und einen Autorisierungsfehler alle zwei Stunden zu vergessen. Dies bedeutet, dass ein Benutzer schnell versuchen kann, einen Schlüssel mit dem falschen Autorisierungswert 32-mal zu verwenden. Für jeden der 32-Versuche zeichnet das TPM auf, ob der Autorisierungswert richtig war oder nicht. Dies führt versehentlich dazu, dass das TPM nach 32 fehlgeschlagenen versuchen einen gesperrten Zustand eingibt.

Versuche, einen Schlüssel mit einem Autorisierungswert für die nächsten zwei Stunden zu verwenden, geben keinen Erfolg oder Misserfolg zurück. Stattdessen zeigt die Antwort an, dass das TPM gesperrt ist. Nach zwei Stunden wird ein Autorisierungsfehler vergessen, und die Anzahl der Autorisierungsfehler, die vom TPM gespeichert werden, sinkt auf 31, sodass das TPM den gesperrten Zustand verlässt und zum normalen Betrieb zurückkehrt. Mit dem korrekten Autorisierungswert können Schlüssel normal verwendet werden, wenn während der nächsten zwei Stunden keine Autorisierungsfehler auftreten. Wenn ein Zeitraum von 64 Stunden ohne Autorisierungsfehler verstreicht, erinnert das TPM an keine Autorisierungsfehler, und 32 fehlerhafte Versuche können erneut auftreten.

Bei der Windows8-Zertifizierung sind keine TPM 2.0-Systeme erforderlich, um Autorisierungsfehler zu vergessen, wenn das System vollständig ausgeschaltet ist oder wenn das System den Ruhezustand aufweist. Windowsdoes erfordern, dass Autorisierungsfehler vergessen werden, wenn das System normal ausgeführt wird, in einem Ruhemodus oder in einem anderen Zustand als "aus". Wenn ein Windows-System mit TPM 2.0 gesperrt ist, verlässt das TPM den Sperrmodus, wenn das System zwei Stunden lang eingeschaltet bleibt.

Der Schutz vor dem hämmern für TPM 2.0 kann vollständig zurückgesetzt werden, indem ein Befehl zum Zurücksetzen der Sperrung an das TPM gesendet und das TPM-Besitzerkennwort bereitgestellt wird. Standardmäßig stellt Windows TPM 2.0 automatisch zur Verfügung und speichert das TPM-Besitzerkennwort für die Verwendung durch Systemadministratoren.

In einigen Unternehmenssituationen ist der TPM-Besitzerautorisierungswert so konfiguriert, dass er zentral in Active Directory gespeichert wird und nicht auf dem lokalen System gespeichert ist. Ein Administrator kann die TPM-MMC starten und festlegen, dass die TPM-Sperr Zeit zurückgesetzt werden soll. Wenn das TPM-Besitzerkennwort lokal gespeichert wird, wird es verwendet, um die Sperrungszeit zurückzusetzen. Wenn das TPM-Besitzerkennwort nicht auf dem lokalen System verfügbar ist, muss es vom Administrator bereitgestellt werden. Wenn ein Administrator versucht, den TPM-Sperrzustand mit dem falschen TPM-Besitzerkennwort zurückzusetzen, lässt das TPM keinen weiteren Versuch zu, den Sperrzustand for24 Stunden zurückzusetzen.

Mit TPM 2.0 können einige Schlüssel erstellt werden, ohne dass Ihnen ein Autorisierungswert zugeordnet ist. Diese Schlüssel können verwendet werden, wenn das TPM gesperrt ist. Beispielsweise kann BitLocker mit einer standardmäßigen TPM-Konfiguration einen Schlüssel im TPM verwenden, um Windows zu starten, auch wenn das TPM gesperrt ist.

Begründung hinter den Standardeinstellungen

Ursprünglich war BitLocker für eine PIN von 4 bis 20 Zeichen zulässig. Windows Hello hat eine eigene PIN für die Anmeldung, die 4 bis 127 Zeichen umfassen kann. Sowohl BitLocker als auch Windows Hello verwenden das TPM, um Angriffe durch Brute-Force-Angriffe zu verhindern.

Das TPM kann so konfiguriert werden, dass Wörterbuchangriffs Verhütungs Parameter (Sperrschwelle und Sperrdauer) verwendet werden, um zu steuern, wie viele fehlerhafte Autorisierungsversuche zulässig sind, bevor das TPM gesperrt wird, und wie viel Zeit verstreichen muss, bevor ein weiterer Versuch ausgeführt werden kann.

Die Parameter für die Verhinderung von Wörterbuchangriffen bieten eine Möglichkeit, Sicherheitsanforderungen mit Usability auszugleichen. Wenn BitLocker beispielsweise mit einer TPM + PIN-Konfiguration verwendet wird, ist die Anzahl der PIN-Vermutungen im Laufe der zeitlimitiert. Ein TPM-2,0 in diesem Beispiel kann so konfiguriert werden, dass nur 32-Pin-Vermutungen sofort zulässig sind, und dann nur noch eine Vermutung alle zwei Stunden. Dies summiert sich auf maximal ungefähr 4415 Vermutungen pro Jahr. Wenn die Pin 4 Ziffern umfasst, können alle 9999 möglichen Pin-Kombinationen in etwas mehr als zwei Jahren versucht werden.

Das Erhöhen der PIN-Länge erfordert eine größere Anzahl von Vermutungen für einen Angreifer. In diesem Fall

kann die Sperrdauer zwischen den einzelnen Vermutungen verkürzt werden, damit legitime Benutzer einen fehlgeschlagenen Versuch schneller wiederholen können, während gleichzeitig ein ähnliches Schutzniveau beibehalten wird.

Ab Windows 10, Version 1703, wurde die Mindestlänge für die BitLocker-PIN auf 6 Zeichen erhöht, um besser mit anderen Windows-Features auszurichten, die TPM 2,0 nutzen, einschließlich Windows Hello. Um Organisationen beim Übergang zu unterstützen, beginnend mit Windows 10, Version 1709 und Windows 10, Version 1703, bei dem das kumulative Update vom Oktober 2017 installiert ist, ist die BitLocker-PIN-Länge standardmäßig 6 Zeichen, kann aber auf vier Zeichen reduziert werden. Wenn die minimale PIN-Länge vom Standardwert von sechs Zeichen reduziert wird, wird der TPM-2,0-Sperrzeitraum verlängert.

TPM-basierte Smartcards

Die Windows-TPM-basierte Smartcard, eine virtuelle Smartcard, kann so konfiguriert werden, dass die Anmeldung beim System zugelassen wird. Im Gegensatz zu physischen Smartcards verwendet der Anmeldevorgang einen TPM-basierten Schlüssel mit einem Autorisierungswert. Die folgende Liste zeigt die Vorteile virtueller Smartcards:

- Physische Smartcards können die Sperrung nur für die physische Smartcard-PIN erzwingen, und Sie können die Sperrung nach dem Eingeben der richtigen PIN zurücksetzen. Bei einer virtuellen Smartcard wird der Schutz vor dem Hämmern des TPM nach erfolgreicher Authentifizierung nicht zurückgesetzt. Die zulässige Anzahl von Autorisierungsfehlern, bevor das TPM in die Sperrung eintritt, umfasst viele Faktoren.
- Hardware Hersteller und Softwareentwickler haben die Möglichkeit, die Sicherheitsfeatures des TPM zu verwenden, um Ihre Anforderungen zu erfüllen.
- Der Zweck der Auswahl von 32-Fehlern als Sperrschwelle liegt darin, dass Benutzer das TPM nur selten Sperren (auch wenn Sie lernen, neue Kennwörter einzugeben oder wenn Sie Ihre Computer häufig Sperren und entsperren). Wenn Benutzer das TPM sperren, müssen Sie zwei Stunden warten oder andere Anmeldeinformationen verwenden, um sich anzumelden, beispielsweise einen Benutzernamen und ein Kennwort.

Verwandte Themen

- Trusted Platform Module (Liste der Themen)
- TPM-Cmdlets in Windows PowerShell
- TPM-WMI-Anbieter
- Vorbereiten Ihrer Organisation für BitLocker: Planung und Richtlinien – TPM-Konfigurationen

So verwendet Windows10 das Trusted Platform Module

12.09.2019 • 22 minutes to read

Das Betriebssystem Windows10 verbessert die meisten vorhandenen Sicherheitsfeatures im Betriebssystem und fügt bahnbrechende neue Sicherheitsfeatures wie Device Guard und Windows Hello for Business hinzu. Es platziert hardwarebasierte Sicherheit tiefer im Betriebssystem als frühere Windows-Versionen und maximiert so die Plattformsicherheit und gleichzeitig auch die Benutzerfreundlichkeit. Windows10 nutzt das Trusted Platform Module (TPM), um viele dieser Sicherheitsfunktionen bereitstellen zu können. Dieser Artikel bietet eine kurze Übersicht über das TPM, beschreibt, wie es funktioniert, erläutert die Vorteile, die TPM für Windows10 bietet, und beschreibt die kumulativen Auswirkungen auf die Sicherheit, wenn Windows10 auf einem PC mit TPM ausgeführt wird.

Siehe auch:

- Windows10-Spezifikationen
- TPM-Grundlagen
- TPM-Empfehlungen

TPM-Übersicht

Das TPM ist ein kryptografisches Modul, das Sicherheit und Datenschutz für Computer verbessert. Der Schutz von Daten durch Verschlüsselung und Entschlüsselung, der Schutz von Anmeldeinformationen für die Authentifizierung und der Nachweis, welche Software auf einem System ausgeführt wird, sind grundlegende Funktionen, um die Sicherheit von Computern zu gewährleisten. Das TPM hilft bei all diesen Szenarien und mehr.

Bisher wurden TPMs als diskrete Chips auf die Hauptplatine des Computers aufgelötet. Diese Implementierung ermöglichen es OEM-Herstellers, das TPM unabhängig vom Rest des Systems zu bewerten und zu zertifizieren. Obwohl diskrete TPM-Implementierungen nach wie vor häufig sind, können sie bei integrierten Geräten problematisch sein, wenn diese kleinformatig sind bzw. nur einen geringen Stromverbrauch haben. Einige neuere TPM-Implementierungen integrieren die TPM-Funktionalität in denselben Chipsatz wie andere Plattformkomponenten, behalten aber eine logische Trennung bei wie diskrete TPM-Chips.

TPMs sind passiv: Sie empfangen Befehle und geben Antworten zurück. Um alle Vorteile von TPM nutzen zu können, muss der OEM-Hersteller die Systemhardware und die Firmware sorgfältig integrieren in TPM integrieren, damit diese geeignete Befehle senden und auf die Antworten reagieren kann. TPMs wurden ursprünglich entwickelt, um Sicherheit und Datenschutzes für die Besitzer und Benutzer von Plattformen zu verbessern, aber neuere Versionen können diese Verbesserungen bereits über die Hardware selbst bereitstellen. Bevor TPMs für erweiterte Szenarios verwendet werden können, müssen sie jedoch bereitgestellt werden. Windows10 stellt TPMs automatisch bereit. Wenn der Benutzer das Betriebssystem erneut installiert, muss er jedoch möglicherweise das System anweisen, das TPM explizit erneut bereitzustellen, damit es die TPM Funktionen uneingeschränkt verwenden kann.

Die Trusted Computing Group (TCG) ist eine gemeinnützige Organisation, die die TPM-Spezifikation veröffentlicht und verwaltet. Zweck der TCG ist es, herstellerunabhängige, globale Branchenstandards zu entwickeln, zu definieren und zu propagieren, die eine hardwarebasierte vertrauenswürdige Stammzertifizierungsstelle für interoperable Trusted Computing-Plattformen unterstützen. Die TCG veröffentlicht auch die TPM-Spezifikation als Internationaler Standard ISO/IEC 11889, wobei der öffentlich zugängliche Prozess zur Einreichung der Spezifikation zugrunde gelegt wird, die das Joint Technical Committee 1 zwischen der International Organization

for Standardization (ISO) und der International Electrotechnical Commission (IEC) definiert.

OEM-Hersteller implementieren das TPM als Komponente in eine vertrauenswürdige Computerplattform wie einem PC, einem Tablet oder einem Telefon. Vertrauenswürdige Computerplattformen nutzen TPM, um Datenschutz- und Sicherheitsszenarios zu unterstützen, die mit Software allein nicht erreicht werden kann. Beispielsweise kann Software allein nicht zuverlässig angeben, ob während des Systemstartvorgangs Malware vorhanden ist. Die enge Integration zwischen TPM und Plattform erhöht die Transparenz des Startvorgangs und unterstützt eine Auswertung des Gerätezustands, weil die Integration eine zuverlässige Messung und Berichte zu der Software, unter der das Gerät gestartet wurde, ermöglichen. Eine Implementierung eines TPMs als Teil einer vertrauenswürdigen Computerplattform bietet einen Hardware-basierten Vertrauensanker, d. h. die Hardware verhält sich vertrauenswürdig. Wenn beispielsweise ein im TPM gespeicherter Schlüssel Eigenschaften hat, die nicht zulassen, dass er exportiert wird, kann der Schlüssel *das TPM nicht verlassen*.

Die TCG hat das TPM als kostengünstige Lösung für den Massenmarkt entwickelt, die die Anforderungen von unterschiedlichen Kundensegmente bedient. Es gibt in den verschiedenen TPM-Implementationen Unterschiede bei den Sicherheitseigenschaften und ebenfalls bei den kundenseitigen und behördlichen Anforderungen für die verschiedenen Sektoren. Im öffentlichen Beschaffungssektor haben beispielsweise einige Behörden klare Sicherheitsanforderungen für TPMs definiert, die es in anderen Sektoren möglicherweise nicht gibt.

-Zertifizierungsprogramme für TPMs – und Technologie im Allgemeinen – werden laufend weiterentwickelt, während Innovationen immer schneller eingeführt werden. Auch wenn es sicher besser ist, ein TPM zu besitzen, als kein TPM zu haben, empfiehlt Microsoft, die Sicherheitsanforderungen Ihrer Organisation zu ermitteln und alle Vorschriften zu analysieren, die es für Ihre Branche im Zusammenhang mit der Beschaffung gibt. Das Ergebnis ist ein ausgewogenes Verhältnis zwischen verwendeten Szenarien, Sicherheitsstufe, Kosten, Vereinfachung und Verfügbarkeit.

TPM in Windows10

Die Sicherheitsfeatures von Windows10 bieten zusammen mit den Vorteilen eines TPM praktische Sicherheits- und Datenschutzvorteile. Die folgenden Abschnitte beginnen mit wichtigen TPM-bezogenen Sicherheitsfeatures in Windows10 und fahren mit Beschreibungen der Verwendung des TPM durch Schlüsseltechnologien fort, um Sicherheit zu erzielen oder sie zu verbessern.

Plattformkryptografieanbieter

Windows enthält ein Kryptografie-Framework namens *Cryptographic API: Next Generation* (CNG). Das grundlegende Konzept besteht in der Implementierung kryptografischer Algorithmen auf unterschiedliche Arten, jedoch mit einer gemeinsamen Anwendungsprogrammierschnittstelle (API). Anwendungen, die Kryptografie verwenden, können die gemeinsame API verwenden, ohne die Details der Implementierung oder den Algorithmus selbst zu kennen.

Auch wenn CNG nach etwas sehr Banalem klingt, veranschaulicht das Konzept einige der Vorteile, die ein TPM bietet. Hinter der CNG-Schnittstelle stellen Windows oder Drittanbieter einen Kryptografiedienstanbieter (d.h. eine Implementierung eines Algorithmus) in Form von Softwarebibliotheken oder in Form einer Kombination von Software und verfügbarer Systemhardware oder Hardware von Drittanbietern bereit. Im Fall einer Hardwareimplementierung kommuniziert der Kryptografieanbieter mit der Hardware hinter der CNG-Softwareschnittstelle.

Der Plattformkryptografieanbieter wurde im Betriebssystem Windows8 eingeführt und stellt die folgenden speziellen TPM-Eigenschaften bereit, die ausschließlich softwarebasierte CNG-Anbieter entweder nicht anbieten oder nicht vergleichbar effektiv anbieten können:

• **Schlüsselschutz**. Der Plattformkryptografieanbieter kann im TPM Schlüssel mit Einschränkungen für ihre Verwendung erstellen. Das Betriebssystem kann die Schlüssel im TPM laden und verwenden, ohne die Schlüssel in den Systemspeicher zu kopieren, in dem sie anfällig für Malware sind. Der Plattformkryptografieanbieter kann

auch Schlüssel konfigurieren, die von einem TPM geschützt werden, sodass sie nicht entfernt werden können. Wenn ein TPM einen Schlüssel erstellt wird, ist der Schlüssel eindeutig und befindet sich nur in diesem TPM. Wenn das TPM einen Schlüssel importiert, kann der Plattformkryptografieanbieter den Schlüssel in diesem TPM verwenden. Dieses TPM ermöglicht jedoch keine zusätzlichen Kopien des Schlüssels oder die Verwendung von Kopien an anderer Stelle. Im Gegensatz hierzu unterliegen Softwarelösungen, die Schlüssel vor dem Kopieren schützen, Rückentwicklungsangriffen, bei denen jemand herausfindet, wie die Lösung Schlüssel speichert oder Kopien von Schlüsseln erstellt, während sie sich zur Verwendung im Arbeitsspeicher befinden.

• **Schutz vor Wörterbuchangriffen**. Schlüssel, die von einem TPM geschützt werden, können einen Autorisierungswert anfordern, z.B. eine PIN. Durch den Schutz vor Wörterbuchangriffen kann das TPM Angriffe verhindern, die eine große Zahl von Vermutungen anstellen, um die PIN zu ermitteln. Nach zu vielen Versuchen gibt das TPM einfach die Fehlermeldung zurück, dass für einen gewissen Zeitraum keine weiteren Vermutungen zulässig sind. Softwarelösungen können ähnliche Funktionen bereitstellen, aber nicht das gleiche Maß an Schutz bieten, insbesondere, wenn das System neu gestartet wird, die Systemuhr geändert wird oder Rollbacks für Dateien auf der Festplatte ausgeführt werden, die die Anzahl der fehlgeschlagenen Vermutungen zählen. Durch den Schutz vor Wörterbuchangriffen können Autorisierungswerte wie PINs außerdem kürzer und leichter zu merken sein, dabei jedoch den gleichen Grad an Schutz wie komplexere Werte bieten, die mit Softwarelösungen verwendet werden.

Diese TPM-Features stellen Plattformkryptografieanbietern wichtige Vorteile gegenüber softwarebasierten Lösungen bereit. Eine einfache Möglichkeit, diese Vorteile in Aktion zu sehen, besteht in der Verwendung von Zertifikaten auf einem Windows10-Gerät. Auf Plattformen, die ein TPM enthalten, kann Windows den Plattformkryptografieanbieter verwenden, um Zertifikatspeicher bereitzustellen. Zertifikatvorlagen können angeben, dass ein TPM den Plattformkryptografieanbieter verwendet, um den Schlüssel zu schützen, der mit einem Zertifikat verknüpft ist. In gemischten Umgebungen, in denen einige Computer möglicherweise nicht über ein TPM verfügen, könnte die Zertifikatvorlage einfach den Plattformkryptografieanbieter anstelle des standardmäßigen Windows-Softwareanbieter bevorzugen. Wenn ein Zertifikat als nicht exportierbar konfiguriert ist, ist der private Schlüssel für das Zertifikat eingeschränkt und kann nicht aus dem TPM exportiert werden. Wenn für das Zertifikat eine PIN erforderlich ist, wird die PIN durch das TPM automatisch vor Wörterbuchangriffen geschützt.

Virtuelle Smartcards

Smartcards sind äußerst sichere physische Geräte, die in der Regel ein einzelnes Zertifikat und den entsprechenden privaten Schlüssel speichern. Benutzer fügen eine Smartcard in einen integrierten oder USB-Kartenleser ein und geben eine PIN zum Entsperren ein. Windows kann dann auf das Zertifikat der Karte zugreifen und den privaten Schlüssel zur Authentifizierung oder zum Entsperren von durch BitLocker geschützten Datenvolumes verwenden. Smartcards sind verbreitet, da sie eine zweistufige Authentifizierung bereitstellen, für die sowohl etwas erforderlich ist, was der Benutzer besitzt (d.h. die Smartcard), als auch etwas, was der Benutzer weiß (z.B. die Smartcard-PIN). Smartcards sind jedoch schwer zu verwenden, da für sie der Kauf und die Bereitstellung von Smartcards und Smartcard-Lesern erforderlich sind.

In Windows ermöglicht das virtuelle Smartcard-Feature dem TPM, eine dauerhaft eingefügte Smartcard zu imitieren. Das TPM wird zu etwas, „was der Benutzer besitzt“, erfordert jedoch nach wie vor eine PIN. Physische Smartcards schränken die Anzahl der PIN-Eingabeversuche ein, bevor die Karte gesperrt und eine Zurücksetzung erforderlich werden. Virtuelle Smartcards verlassen sich auf den Schutz vor Wörterbuchangriffen durch das TPM, um die Zahl der PIN-Eingabeversuche einzuschränken.

Im Fall TPM-basierter virtueller Smartcards schützt das TPM die Verwendung und Speicherung des privaten Schlüssels des Zertifikats, sodass er nicht kopiert werden kann, wenn er verwendet oder gespeichert wird, oder an anderen Stellen verwendet werden kann. Die Verwendung einer Komponente, die Teil des Systems und nicht eine separate physische Smartcard ist, kann die Gesamtbetriebskosten senken, da Szenarien wie „Kartenverlust“ oder „Karte zu Hause gelassen“ vermieden werden, während weiterhin die Vorteile der Smartcard-basierten mehrstufigen Authentifizierung bereitgestellt werden. Für Benutzer sind virtuelle Smartcards einfach zu

verwenden. Es wird lediglich eine PIN zum Entsperren benötigt. Virtuelle Smartcards unterstützen die gleichen Szenarien wie physische Smartcards, einschließlich der Anmeldung bei Windows oder der Authentifizierung für den Zugriff auf Ressourcen.

Windows Hello for Business

Windows Hello for Business bietet Authentifizierungsmethoden, mit denen Kennwörter ersetzt werden sollen, die schwer zu merken sein können und leicht kompromittiert werden können. Darüber hinaus werden bei Verwendung von Kombinationen aus Benutzername und Kennwort häufig dieselben Kombinationen aus Benutzername und Kennwort für mehrere Geräte und Dienste verwendet. Wenn diese Anmeldeinformationen kompromittiert sind, sind sie an vielen Stellen gefährdet. Windows Hello for Business stellt Geräte einzeln bereit und kombiniert die Informationen, die auf den einzelnen Geräten bereitgestellt werden (d.h., den kryptografischen Schlüssel), mit zusätzlichen Informationen zum Authentifizieren von Benutzern. Auf einem System, das über ein TPM verfügt, kann das TPM den Schlüssel schützen. Wenn ein System nicht über ein TPM verfügt, wird der Schlüssel von softwarebasierten Techniken geschützt. Bei den zusätzlichen Informationen, die der Benutzer bereitstellt, kann es sich um einen PIN-Wert oder, wenn das System über die erforderliche Hardware verfügt, biometrische Informationen handeln, z.B. Fingerabdruck oder Gesichtserkennung. Um die Privatsphäre zu schützen, werden die biometrischen Informationen nur auf dem jeweiligen Gerät für den Zugriff auf den bereitgestellten Schlüssel verwendet. Sie werden nicht für mehrere Geräte verwendet.

Die Einführung neuer Technologien zur Authentifizierung erfordert, dass Identitätsanbieter und Organisationen diese Technologie bereitstellen und verwenden. Windows Hello for Business ermöglicht Benutzern die Authentifizierung mit ihrem vorhandenen Microsoft-Konto, einem Active Directory-Konto, einem Microsoft Azure Active Directory-Konto oder sogar mit nicht von Microsoft angebotenen Identitätsanbieterdiensten oder Diensten vertrauender Seiten, die Fast ID Online V2.0-Authentifizierung unterstützen.

Identitätsanbieter haben bei der Art der Bereitstellung von Anmeldeinformationen auf Client-Geräten Flexibilität. Eine Organisation kann z.B. nur Geräte bereitstellen, die über ein TPM verfügen, damit die Organisation weiß, dass ein TPM die Anmeldeinformationen geschützt. Die Fähigkeit, ein TPM von Schadsoftware zu unterscheiden, die sich wie ein TPM verhält, setzt die folgenden TPM-Funktionen voraus (siehe Abbildung1):

• **Endorsement key**. Der TPM-Hersteller kann einen speziellen Schlüssel im TPM erstellen, der als *Endorsement Key* bezeichnet wird. Ein vom Hersteller unterzeichneter bestätigungsschlüssel Zertifikat besagt, dass der bestätigungsschlüssel in einem vom Hersteller erstellten TPM vorhanden ist. Lösungen können das Zertifikat mit dem TPM verwenden, das den Endorsement Key enthält, um zu überprüfen, ob an einem Szenario wirklich ein TPM von einem bestimmten TPM-Hersteller beteiligt ist (anstelle einer Schadsoftware, die sich wie ein TPM verhält).

• **Attestation Identity Key**. Um die Privatsphäre zu schützen, verwenden die meisten TPM-Szenarien nicht direkt einen tatsächlichen Endorsement Key. Stattdessen verwenden sie Attestation Identity Keys. Eine Identitäts-Zertifizierungsstelle (Certificate Authority, CA) verwendet den Endorsement Key und dessen Zertifikat, um nachweisen, dass in einem echten TPM tatsächlich ein oder mehrere Attestation Identity Keys vorhanden sind. Die Identität-CA stellt Attestation Identity Key-Zertifikate aus. Dasselbe Endorsement Key-Zertifikat, mit dem das TPM eindeutig identifiziert werden kann, wird im Allgemeinen von mehr als einer Identitäts-CA gesehen. Es kann jedoch eine beliebige Zahl von Attestation Identity Key-Zertifikaten erstellt werden, um die Informationen zu begrenzen, die in anderen Szenarien freigegeben werden.

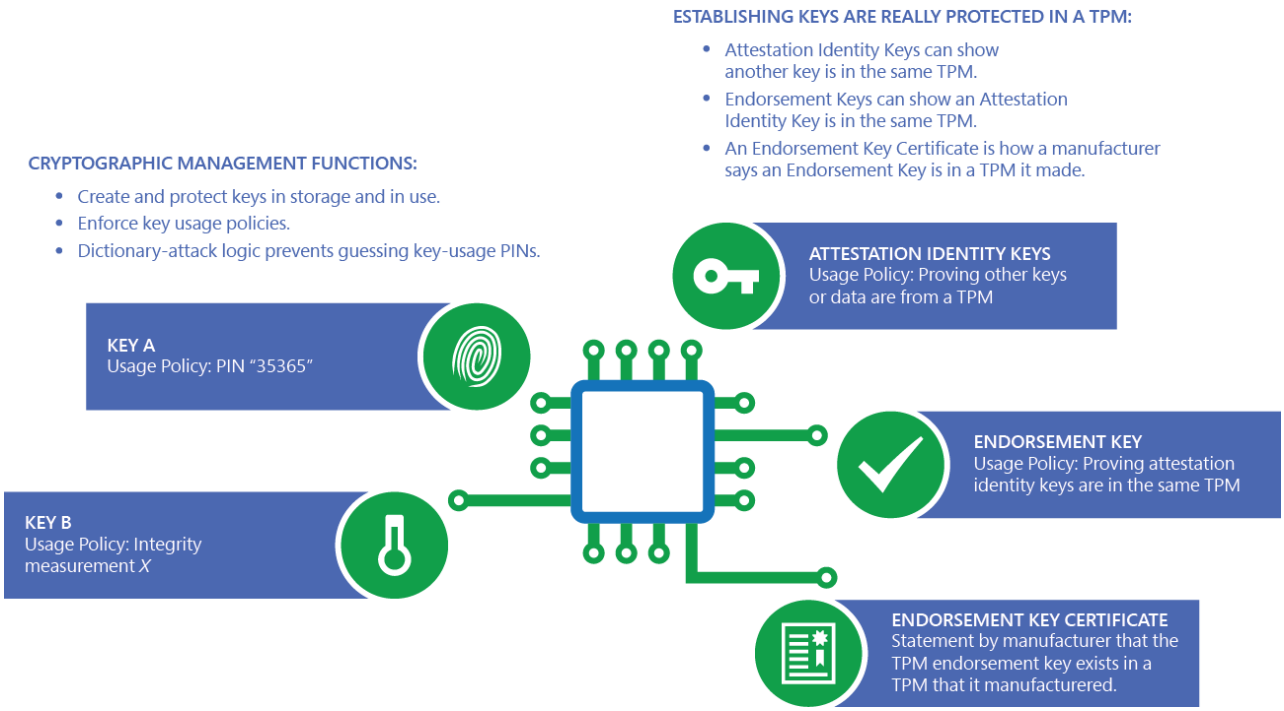


Abbildung 1: Verwalten von kryptografischen Schlüsseln im TPM

Für Windows Hello for Business kann Microsoft die Rolle der Identitäts-CA ausfüllen. Microsoft-Dienste können ein Attestation Identity Key-Zertifikat für jedes Gerät, jeden Benutzer und jeden Identitätsanbieter ausstellen, um die Privatsphäre zu schützen und Identitätsanbieter dabei zu unterstützen, sicherzustellen, dass die TPM-Geräteanforderungen erfüllt werden, bevor Windows Hello for Business-Anmeldeinformationen bereitgestellt werden.

BitLocker-Laufwerkverschlüsselung

BitLocker bietet eine vollständige Volumeverschlüsselung, um gespeicherte Daten zu schützen. Die am häufigsten verwendete Gerätekonfiguration teilt die Festplatte in mehrere Volumes auf. Das Betriebssystem und die Benutzerdaten befinden sich auf einem Volume, das vertrauliche Informationen enthält, und andere Volumes enthalten öffentliche Informationen wie Startkomponenten, Systeminformationen und Wiederherstellungstools. (Diese anderen Volumes werden selten genug verwendet, um nicht für Benutzer angezeigt zu werden.) Wenn das Volume mit Betriebssystem und Benutzerdaten nicht verschlüsselt ist und keine zusätzliche Schutzmaßnahmen angewendet werden, kann eine Person ein anderes Betriebssystem starten und die Dateiberechtigungen umgehen, die das ursprüngliche Betriebssystem zu erzwingen beabsichtigt, um Benutzerdaten zu lesen.

In der am häufigsten verwendeten Konfiguration verschlüsselt BitLocker das Betriebssystemvolume, sodass die Daten auf dem Volume weiter geschützt sind, wenn der Computer oder die Festplatte verloren gehen oder gestohlen werden, wenn sie ausgeschaltet sind. Wenn der Computer eingeschaltet wird, wird er normal gestartet und zeigt die Windows-Anmeldeaufforderung an. Die einzige Möglichkeit für Benutzer besteht darin, sich mit ihren Anmeldeinformationen anzumelden, sodass das Betriebssystem die normalen Dateiberechtigungen erzwingen kann. Wenn der Startvorgang jedoch geändert wird, beispielsweise, wenn über ein USB-Gerät ein anderes Betriebssystem gestartet wird, können das Betriebssystemvolume und die Benutzerdaten nicht gelesen werden und sind nicht zugänglich. Das TPM und die Systemfirmware arbeiten zusammen, um Daten darüber aufzuzeichnen, wie das System gestartet wird, einschließlich der geladenen Software und Konfigurationsdetails. Dazu gehören Informationen darüber, ob der Start von der Festplatte oder von einem USB-Gerät ausgeführt wurde. BitLocker verwendet das TPM, um die Verwendung eines Schlüssels nur dann zuzulassen, wenn der Start auf eine erwartete Weise erfolgt. Die Systemfirmware und das TPM wurden sorgfältig für eine Zusammenarbeit entwickelt, um die folgenden Funktionen bereitstellen:

• **Hardware-Vertrauensanker für Messungen**. Ein TPM ermöglicht Software das Senden von Befehlen, die Messungen von Software- oder Konfigurationsinformationen aufzeichnen. Diese Informationen können mithilfe

eines Hashalgorithmus verarbeitet werden, der im Wesentlichen eine große Datenmenge in einen kleinen, statistisch eindeutigen Hashwert umwandelt. Die Systemfirmware verfügt über eine Komponente mit dem Namen „Core Root of Trust für Measurement (CRTM)“, die implizit als vertrauenswürdig eingestuft wird. Die CRTM hasht die nächste Softwarekomponente ohne Bedingungen und zeichnet den Wert der Messung durch Senden eines Befehls an das TPM auf. Aufeinander folgende Komponenten, ob Systemfirmware- oder Betriebssystem-Ladeprogramme, setzen den Vorgang fort, indem sie alle von ihnen geladenen Softwarekomponenten messen, bevor sie ausgeführt werden. Da die Messung jeder Komponente an das TPM gesendet wird, bevor es ausgeführt wird, kann keine Komponente ihre Messung aus dem TPM löschen. (Messungen werden jedoch gelöscht, wenn das System neu gestartet wird.) Das Ergebnis ist, dass das TPM für jeden Schritt des Systemstartvorgangs Messungen von Informationen zu Software und Konfiguration beim Starten enthält. Alle Änderungen der Software oder Konfiguration beim Starten führen zu unterschiedlichen TPM-Messungen für diesen und spätere Schritte. Da die Systemfirmware die Messungskette ohne Bedingungen startet, stellt es eine vertrauenswürdige hardwarebasierte Stelle für die TPM-Messungen bereit. An einem bestimmten Punkt im Startvorgang nimmt der Wert der Aufzeichnung von Informationen zu allen geladenen Software- und Konfigurationskomponenten ab und die Kette der Messungen wird beendet. Das TPM ermöglicht das Erstellen von Schlüsseln, die nur verwendet werden können, wenn die Plattformkonfigurationregister, die die Messungen enthalten, spezifische Werte haben.

• **Verwendung des Schlüssels nur bei korrekten Startmessungen**. BitLocker erstellt einen Schlüssel im TPM, der nur verwendet werden kann, wenn die Startmessungen einem erwarteten Wert entsprechen. Der erwartete Wert wird für den Schritt im Startprozess berechnet, in dem der Windows-Start-Manager auf dem Betriebssystemvolume auf der Systemfestplatte ausgeführt wird. Der Windows-Start-Manager wird unverschlüsselt auf dem Startvolume gespeichert und muss den TPM-Schlüssel verwenden, damit er Daten entschlüsseln kann, die aus dem Betriebssystemvolume in den Arbeitsspeicher gelesen werden, und der Startvorgang mittels des verschlüsselten Betriebssystemvolumes fortgesetzt werden kann. Wenn ein anderes Betriebssystem gestartet oder die Konfiguration geändert wird, unterscheiden sich die Messwerte im TPM. Das TPM gestattet dem Windows-Start-Manager die Verwendung des Schlüssels nicht und der Startvorgang kann nicht normal fortgesetzt werden, weil die Daten im Betriebssystem nicht entschlüsselt werden können. Wenn jemand versucht, das System mit einem anderen Betriebssystem oder Gerät zu starten, sind die Software- oder Konfigurationsmessungen im TPM falsch und das TPM gestattet die Verwendung des Schlüssels nicht, der benötigt wird, um das Betriebssystemvolume zu entschlüsseln. Wenn sich die Messwerte unerwartet ändern, können Benutzer stets den BitLocker-Wiederherstellungsschlüssel verwenden, um auf Volumedaten zuzugreifen. Organisationen können BitLocker zum Speichern des Wiederherstellungsschlüssels in Active Directory Domain Services (AD DS) konfigurieren.

Die Merkmale von Gerätehardware sind für BitLocker und dessen Möglichkeit, Daten zu schützen, wichtig. Ein Aspekt ist, ob das Gerät Angriffsvektoren bietet, wenn das System den Anmeldebildschirm anzeigt. Wenn beispielsweise das Windows-Gerät über einen Anschluss verfügt, der einen direkten Arbeitsspeicherzugriff zulässt, sodass eine Person Hardware anschließen und den Arbeitsspeicher lesen kann, kann ein Angreifer den Entschlüsselungsschlüssel des Betriebssystemvolumes aus dem Arbeitsspeicher lesen, während der Windows-Anmeldebildschirm angezeigt wird. Um dieses Risiko zu verringern, können Organisationen BitLocker so konfigurieren, dass der TPM-Schlüssel sowohl die richtigen Softwaremessungen als auch einen Autorisierungswert erfordert. Der Systemstartvorgang hält beim Windows-Start-Manager an. Der Benutzer wird aufgefordert, den Autorisierungswert für den TPM-Schlüssel einzugeben oder ein USB-Gerät mit dem Wert anzuschließen. Dieser Vorgang verhindert, dass BitLocker den Schlüssel automatisch in den Arbeitsspeicher lädt, wo er gefährdet sein könnte, bietet jedoch eine weniger komfortable Benutzererfahrung.

Neuere Hardware und Windows10 arbeiten besser zusammen, um den direkten Arbeitsspeicherzugriff über Ports zu deaktivieren und Angriffsvektoren zu reduzieren. Das Ergebnis ist, dass Organisationen mehr Systeme bereitstellen können, ohne dass Benutzer zusätzliche Autorisierungsinformationen während des Startvorgangs eingeben müssen. Die richtige Hardware ermöglicht die Verwendung von BitLocker mit der „Nur TPM“-Konfiguration. So können sich Benutzer zentral anmelden, ohne während des Startvorgangs eine PIN oder einen USB-Stick verwenden zu müssen.

Device Encryption

Device Encryption ist die Verbraucherversion von BitLocker und verwendet die gleiche zugrunde liegende Technologie. Wenn sich Verbraucher mit einem Microsoft-Konto anmelden und das System die Modern Standby-Hardwareanforderungen erfüllt, wird BitLocker Drive Encryption in Windows10 automatisch aktiviert. Der Wiederherstellungsschlüssel wird in der Microsoft-Cloud gesichert und Verbraucher können über ihr Microsoft-Konto auf diesen zugreifen. Die Modern Standby-Hardwareanforderungen informieren Windows10, dass die Hardware für die Bereitstellung von Device Encryption geeignet ist und die Verwendung der „Nur TPM"-Konfiguration unterstützt, um eine einfache Verbrauchererfahrung zu ermöglichen. Zusätzlich wurde Modern Standby-Hardware dafür entwickelt, die Wahrscheinlichkeit zu verringern, dass sich Messwerte ändern und Verbraucher nach dem Wiederherstellungsschlüssel gefragt werden.

Für Softwaremessungen nutzt Device Encryption Messungen der Autorität, die die Softwarekomponenten bereitstellt (basierend auf Codesignaturen von Herstellern wie OEMs oder Microsoft), anstelle der genauen Hashes der Softwarekomponenten selbst. Dies ermöglicht die Wartung von Komponenten, ohne die Messwerte zu ändern. Für Konfigurationsmessungen basieren die verwendeten Werte auf der Startsicherheitsrichtlinie und nicht auf den zahlreichen weiteren Konfigurationseinstellungen, die während des Starts aufgezeichnet werden. Diese Werte ändern sich auch weniger häufig. Das Ergebnis ist, dass Device Encryption auf geeigneter Hardware auf benutzerfreundliche Weise aktiviert wird und gleichzeitig die Daten schützt.

Kontrollierter Start

Windows8 führte den kontrollierten Start als eine Möglichkeit ein, wie das Betriebssystem die Kette der Messungen von Softwarekomponenten und Konfigurationsinformationen im TPM bis zur Initialisierung des Windows-Betriebssystems aufzeichnen kann. In vorherigen Windows-Versionen endete die Messungskette mit dem Windows-Start-Manager und die Messungen im TPM waren für die Bewertung des Startzustands von Windows nicht nützlich.

Der Windows-Startvorgang erfolgt in Phasen und umfasst häufig Treiber von Drittanbietern, um mit herstellerspezifischer Hardware zu kommunizieren oder Lösungen zur Bekämpfung von Malware zu implementieren. Im Fall von Software zeichnet der kontrollierte Start Messungen des Windows-Kernels, von Treibern für den Antischadsoftware-Frühstart und von Starttreibern im TPM auf. Im Fall von Konfigurationseinstellungen zeichnet der kontrollierte Start sicherheitsrelevante Informationen wie Signaturdaten, die von Treibern für Antischadsoftware verwendet werden, und Konfigurationsdaten zu Windows-Sicherheitsfeatures auf (beispielweise, ob BitLocker aktiviert oder deaktiviert ist).

Der kontrollierte Start stellt sicher, dass TPM-Messungen den Startzustand der Windows-Software- und -Konfigurationseinstellungen vollständig widerspiegeln. Wenn Sicherheitseinstellungen und andere Schutzmaßnahmen korrekt eingerichtet sind, werden sie die Sicherheit des ausgeführten Betriebssystems anschließend zuverlässig sicherstellen. Andere Szenarien können den Startzustand des Betriebssystems verwenden, um festzustellen, ob das ausgeführte Betriebssystem vertrauenswürdig ist.

TPM-Messungen sind so konzipiert, dass Aufzeichnungen sensibler Informationen als Messungen vermieden werden. Als zusätzliche Datenschutzmaßnahme beendet der kontrollierte Start die Messungskette zu Beginn des Startzustands von Windows. Daher enthält die Gruppe von Messungen keine Detail darüber, welche Anwendungen verwendet werden oder wie Windows verwendet wird. Messwertinformationen können für externe Entitäten freigegeben werden, um zu zeigen, dass das Gerät angemessene Sicherheitsrichtlinien erzwingt und nicht mit Schadsoftware gestartet wurde.

Das TPM stellt die folgende Möglichkeit bereit, wie Szenarien die Messungen verwenden können, die im TPM während des Startvorgangs aufgezeichnet werden:

• **Remotenachweis**. Unter Verwendung eines Attestation Identity Key kann das TPM eine Anweisung (oder ein *Zitat*) der aktuellen Messungen im TPM generieren und kryptografisch signieren. Windows10 kann eindeutige Attestation Identity Keys für verschiedene Szenarien erstellen, um zu verhindern, dass separate Auswerter

zusammenarbeiten, um das gleiche Gerät nachzuverfolgen. Weitere Informationen im Zitat werden kryptografisch verschlüsselt, um die gemeinsame Nutzung von Informationen zu begrenzen und den Datenschutz zu verbessern. Indem das Zitat an eine Remoteentität gesendet wird, kann ein Gerät die Software- und Konfigurationseinstellungen bestätigen, die für das Starten des Geräts und das Initialisieren des Betriebssystems verwendet wurden. Ein Attestation Identity Key-Zertifikat kann zusätzlich Gewissheit bieten, dass das Zitat aus einem wirklich vorhandenen TPM stammt. Die Remotebestätigung ist ein Vorgang, bei dem Messungen im TPM aufgezeichnet werden, ein Zitat generiert wird und die Zitatinformationen an ein anderes System gesendet werden, das die Messungen auswertet, um ein Gerät als vertrauenswürdig einstufen zu können. Dieser Vorgang wird in Abbildung2 dargestellt.

Wenn neue Sicherheitsfeatures zu Windows hinzugefügt werden, fügt der kontrollierte Start den Messungen, die im TPM aufgezeichnet wurden, sicherheitsrelevante Informationen hinzu. Der kontrollierte Start unterstützt Remotebestätigungsszenarien, die die Systemfirmware und den Status der Windows-Initialisierung widerspiegeln.

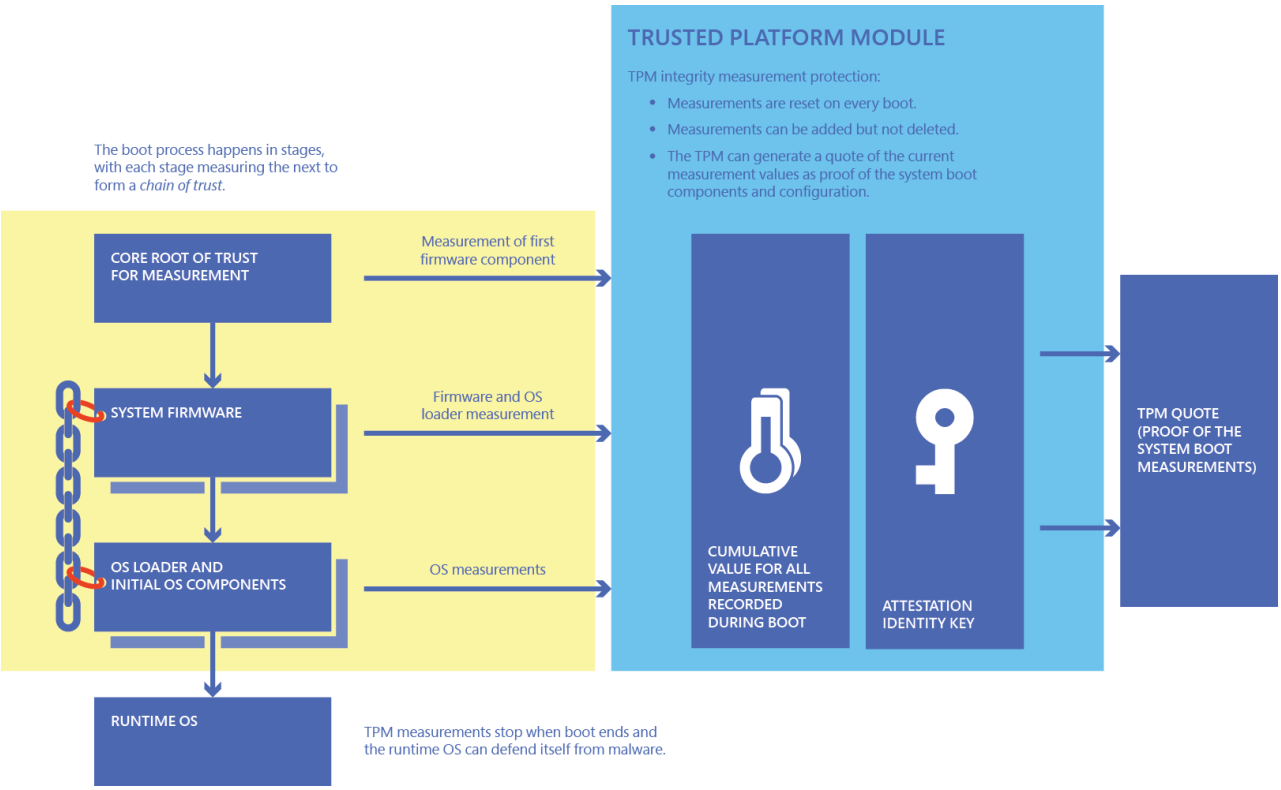


Abbildung2: Vorgang für die Erstellung von Nachweisen zu Startsoftware und -konfiguration mittels des TPM

Integritätsbestätigung für Geräte

Einige Verbesserungen in Windows10 unterstützen die Implementierung von Remotebestätigungsszenarien durch Sicherheitslösungen. Microsoft stellt einen Dienst für die Integritätsbestätigung bereit, der Attestation Identity Key-Zertifikate für TPMs von unterschiedlichen Herstellern erstellen sowie gemessene Startinformationen analysieren kann, um einfache Sicherheitsszenarien zu extrahieren, z.B., ob BitLocker aktiviert oder deaktiviert ist. Die einfachen Sicherheitsbestätigungen können verwendet werden, um die Geräteintegrität zu bewerten.

Lösungen für die mobile Geräteverwaltung (Mobile Device Management, MDM) können für einen Client einfache Sicherheitsbestätigungen vom Microsoft Health Attestation-Dienst empfangen, ohne sich mit der Komplexität des Zitats oder den Details der TPM-Messungen auseinandersetzen zu müssen. MDM-Lösungen können anhand der Sicherheitsinformationen Maßnahmen durchführen, indem fehlerhafte Geräte isoliert werden oder der Zugriff auf Clouddienste wie Microsoft Office365 gesperrt wird.

Credential Guard

Credential Guard ist ein neues Feature in Windows10, das zum Schutz von Windows-Anmeldeinformationen in

Organisationen beiträgt, die AD DS bereitgestellt haben. In der Vergangenheit wurden die Anmeldeinformationen eines Benutzers (z.B. das Anmeldekennwort) gehasht, um ein Autorisierungstoken zu generieren. Benutzer verwendeten das Token für den Zugriff auf Ressourcen, zu deren Verwendung sie berechtigt waren. Eine Schwachstelle des Token-Modells besteht darin, dass Schadsoftware, die Zugriff auf den Kernel des Betriebssystems hat, den Arbeitsspeicher des Computers durchsuchen und alle aktuell verwendeten Zugriffstoken extrahieren könnte. Der Angreifer könnte dann extrahierte Token verwenden, um sich an anderen Computern anzumelden und weitere Anmeldeinformationen zu sammeln. Diese Art von Angriff wird als „Hashweitergabe" bezeichnet und ist eine Schadsoftwaretechnik, mit der ein einzelner Computer infiziert wird, um viele weitere Computer in der Organisation zu infizieren.

Ähnlich wie Microsoft Hyper-V virtuelle Computer (VMs) voneinander trennt, verwendet auch Credential Guard die Virtualisierung, um den Vorgang, bei dem Anmeldeinformationen gehasht werden, in einem Arbeitsspeicherbereich zu isolieren, auf den der Betriebssystemkernel nicht zugreifen kann. Dieser isolierte Arbeitsspeicherbereich wird während des Startvorgangs initialisiert und geschützt, sodass Komponenten in der weiteren Betriebssystemumgebung ihn nicht manipulieren können. Credential Guard verwendet das TPM, um seine Schlüssel mit TPM-Messungen zu schützen damit nur während des Startvorgangs auf sie zugegriffen werden kann, wenn der getrennte Bereich initialisiert wurde. Sie sind für den normalen Betriebssystemkernel nicht verfügbar. Der lokale Sicherheitsautoritätscode im Windows-Kernel interagiert mit dem isolierten Arbeitsspeicherbereich, indem Anmeldeinformationen übergeben und Autorisierungstoken zur einmaligen Verwendung empfangen werden.

Die resultierende Lösung bietet einen umfassenden Schutz. Auch wenn Schadsoftware im Betriebssystemkernel ausgeführt wird, kann sie nicht auf die Geheimnisse innerhalb des isolierten Arbeitsspeicherbereichs zugreifen, der die Autorisierungstoken tatsächlich generiert. Die Lösung löst nicht das Keylogger-Problem, da die von diesen Tools erfassten Kennwörter tatsächlich über den normalen Windows-Kernel geleitet werden. In Verbindung mit anderen Lösungen wie der Smartcard-Authentifizierung verbessert Credential Guard den Schutz von Anmeldeinformationen in Windows10 jedoch erheblich.

Fazit

Das TPM fügt Windows10 hardwarebasierte Sicherheitsfunktionen hinzu. Bei der Installation von Hardware, die ein TPM umfasst, bietet Windows10 deutlich verbesserte Sicherheitsvorteile. In der folgenden Tabelle werden die wesentlichen Vorteile der TPM-Hauptfeatures zusammengefasst.

FEATURE	VORTEILE DER VERWENDUNG AUF EINEM SYSTEM MIT EINEM TPM
Plattformkryptografieanbieter	• Wenn der Computer gefährdet ist, kann der private Schlüssel nicht zusammen mit dem Zertifikat aus dem Gerät kopiert werden. • Der TPM-Mechanismus zum Schutz vor Wörterbuchangriffen schützt PIN-Werte, um Zertifikate verwenden zu können.
Virtuelle Smartcards	• Sie stellen einen Grad an Sicherheit bereit, der dem physischer Smartcards vergleichbar ist. Es müssen jedoch keine physischen Smartcards oder Kartenlesegeräte bereitgestellt werden.
Windows Hello for Business	• Anmeldeinformationen, die auf einem Gerät bereitgestellt sind, können nicht an andere Stellen kopiert werden. • Das TPM eines Geräts wird bestätigt, bevor Anmeldeinformationen bereitgestellt werden.

FEATURE	VORTEILE DER VERWENDUNG AUF EINEM SYSTEM MIT EINEM TPM
BitLocker-Laufwerkverschlüsselung	• Unternehmen stehen verschiedene Optionen für den Schutz gespeicherter Daten zur Verfügung, während Sicherheitsanforderungen und unterschiedliche Gerätehardware abgewogen werden.
Device Encryption	• Mit einem Microsoft-Konto und der richtigen Hardware können gespeicherte Daten auf Verbrauchergeräten umfassend geschützt werden.
Kontrollierter Start	• Ein Hardware-Vertrauensanker enthält Startmessungen, die helfen, Schadsoftware während der Remotebestätigung zu entdecken.
Integritätsbestätigung	• MDM-Lösungen können auf einfache Weise Remotebestätigungen ausführen und die Integrität von Clients bewerten, bevor Zugriff auf Ressourcen oder Clouddienste wie Office365 gewährt wird.
Credential Guard	• Die Verteidigung wird verbessert, sodass es deutlich schwieriger wird, zusätzliche Computer in einer Organisation zu kompromittieren, auch wenn Schadsoftware auf einem Rechner administrative Rechte besitzt.

Obwohl einige der oben genannten Features zusätzliche Anforderungen an die Hardware stellen (z.B. Virtualisierungsunterstützung), bildet das TPM einen Eckpfeiler der Windows10-Sicherheit. Microsoft und anderen Branchenmitglieder verbessern die globalen TPM-Standards weiter und fügen mehr und mehr Anwendungen hinzu, die es verwenden, um Kunden fassbare Vorteile zu bieten. Microsoft hat in seine Version von Windows für das Internet der Dinge (IoT) mit dem Namen Windows10 IoT Core Unterstützung für die meisten TPM-Features integriert. IoT-Geräte, die möglicherweise an unsicheren physischen Standorten bereitgestellt und zur Verwaltung mit Clouddiensten wie Azure IoT Hub verbunden werden, können das TPM auf innovative Weise verwenden, um die steigenden Sicherheitsanforderungen zu erfüllen.

Gruppenrichtlinieneinstellungen für TPM-Dienste

06.03.2020 • 8 minutes to read

Betriff:

- Windows 10
- Windows Server 2016 und höher

In diesem Thema werden die TPM-Dienste (Trusted Platform Module) beschrieben, die mithilfe von Gruppenrichtlinieneinstellungen zentral gesteuert werden können.

Die Gruppenrichtlinieneinstellungen für TPM-Dienste finden Sie unter:

Computer Configuration\Administrative Templates\System\Trusted Platform Module Services

Die folgenden Gruppenrichtlinieneinstellungen wurden in Windows 10 eingeführt.

Konfigurieren der Ebene der TPM-Besitzer Autorisierungsinformationen, die für das Betriebssystem verfügbar sind

> **IMPORTANT**
>
> Ab Windows 10, Version 1607 und Windows Server 2016, wird diese Richtlinieneinstellung nicht mehr von Windows verwendet, Sie wird jedoch weiterhin in gpedit. msc zur Kompatibilität mit früheren Versionen angezeigt. Ab Windows 10, Version 1703, ist der Standardwert 5. Dieser Wert wird während der Bereitstellung implementiert, damit eine andere Windows-Komponente Sie je nach Systemkonfiguration entweder löschen oder deren Besitz übernehmen kann. Bei TPM 2,0 bedeutet der Wert 5, die Sperrungs Autorisierung beizubehalten. Für TPM 1,2 bedeutet dies, die vollständige TPM-Besitzerautorisierung zu verwerfen und nur die Delegierte Autorisierung beizubehalten.

Diese Richtlinieneinstellung hat konfiguriert, welche TPM-Autorisierungswerte in der Registrierung des lokalen Computers gespeichert werden. Bestimmte Autorisierungswerte sind erforderlich, damit Windows bestimmte Aktionen ausführen kann.

TPM 1,2-WERT	TPM 2,0-WERT	ZWECK	AUF EBENE 0 AUFBEWAHRT?	AUF STUFE 2 AUFBEWAHRT?	AUF STUFE 4 AUFBEWAHRT?
OwnerAuthAdmin	StorageOwnerAuth	Erstellen von SRK	Nein	Ja	Ja
OwnerAuthEndorsement	EndorsementAuth	Erstellen oder Verwenden von EK (nur 1,2: Create AIK)	Nein	Ja	Ja
OwnerAuthFull	LockoutAuth	Zurücksetzen/ändern des Wörterbuchangriffs Schutzes	Nein	Nein	Nein

Es gibt drei TPM-Besitzer Authentifizierungseinstellungen, die vom Windows-Betriebssystem verwaltet werden. Sie können den Wert **Full**, **Delegat**oder **None**auswählen.

- **Vollständig**diese Einstellung speichert die vollständige TPM-Besitzerautorisierung, das BLOB für die TPM-Administrator Delegierung und das BLOB für die TPM-Benutzer Delegierung in der lokalen Registrierung. Mit dieser Einstellung können Sie das TPM verwenden, ohne dass der TPM-Besitzerautorisierungswert Remote oder extern gespeichert werden soll. Diese Einstellung ist für Szenarien geeignet, in denen Sie nicht die TPM-antihämmer-Logik zurücksetzen oder den TPM-Besitzerautorisierungswert ändern müssen. Einige TPM-basierte Anwendungen erfordern möglicherweise, dass diese Einstellung geändert wird, bevor Features verwendet werden können, die von der TPM-antihämmer-Logik abhängig sind. Die vollständige Besitzerautorisierung in TPM 1,2 ähnelt der Sperrungs Autorisierung in TPM 2,0. Die Besitzerautorisierung hat eine andere Bedeutung für TPM 2,0.
- **Delegierte**diese Einstellung speichert nur das BLOB für die TPM-administrative Delegierung und das BLOB für die TPM-Benutzer Delegierung in der lokalen Registrierung. Diese Einstellung ist für die Verwendung mit TPM-basierten Anwendungen geeignet, die von der TPM-antihämmer-Logik abhängen. Dies ist die Standardeinstellung in Windows vor Version 1703.
- **Keine**diese Einstellung bietet Kompatibilität mit früheren Betriebssystemen und Anwendungen. Sie können es auch für Szenarien verwenden, wenn die TPM-Besitzerautorisierung nicht lokal gespeichert werden kann. Bei Verwendung dieser Einstellung kann es zu Problemen mit einigen TPM-basierten Anwendungen kommen.

> **NOTE**
> Wenn die TPM-Authentifizierungseinstellung für das Betriebssystem von **vollständig** in **delegiert**geändert wurde, wird der vollständige TPM-Besitzerautorisierungswert erneut generiert, und alle Kopien des zuvor festgelegten TPM-Besitzer Autorisierungs Werts sind ungültig.

Registrierungsinformationen

Registrierungsschlüssel: HKEY \ _LOCAL \ _MACHINE \software\policies\microsoft\tpm

DWORD: OSManagedAuthLevel

In der folgenden Tabelle sind die TPM-Besitzer Autorisierungswerte in der Registrierung aufgeführt.

WERTDATEN	EINSTELLUNG
0	Keine
2	Delegierte
4	Vollständig

Wenn Sie diese Richtlinieneinstellung aktivieren, speichert das Windows-Betriebssystem die TPM-Besitzerautorisierung in der Registrierung des lokalen Computers entsprechend der von Ihnen ausgewählten TPM-Authentifizierungseinstellung.

Unter Windows 10 vor Version 1607, wenn Sie diese Richtlinieneinstellung deaktivieren oder nicht konfigurieren und die Richtlinieneinstellung **TPM-Sicherung in Active Directory-Domänendienste aktivieren** ebenfalls deaktiviert oder nicht konfiguriert ist, besteht die Standardeinstellung darin, den vollständigen TPM-Autorisierungswert in der lokalen Registrierung zu speichern. Wenn diese Richtlinie deaktiviert oder nicht konfiguriert ist und die Richtlinieneinstellung **TPM-Sicherung in Active Directory-Domänendienste aktivieren** aktiviert ist, werden nur die administrativen Delegierungs-und die Benutzer Delegierungs-BLOBs in der lokalen Registrierung gespeichert.

Standard Sperrungsdauer für Benutzer

Mit dieser Richtlinieneinstellung können Sie die Dauer in Minuten für das zählen von standardmäßigen Benutzer Autorisierungsfehlern für TPM-Befehle (Trusted Platform Module) verwalten, für die eine Autorisierung erforderlich ist. Ein Autorisierungsfehler tritt jedes Mal auf, wenn ein Standardbenutzer einen Befehl an das TPM sendet und eine Fehlerantwort erhält, die darauf hinweist, dass ein Autorisierungsfehler aufgetreten ist. Autorisierungsfehler, die älter als die von Ihnen festgelegte Dauer sind, werden ignoriert. Wenn die Anzahl der TPM-Befehle mit einem Autorisierungsfehler innerhalb der Sperrdauer einem Schwellenwert entspricht, wird ein Standardbenutzer daran gehindert, Befehle zu senden, für die eine Autorisierung für das TPM erforderlich ist.

Das TPM dient zum Schutz vor Kenn Wort erraten-Angriffen durch Eingabe eines Hardware-Lockout-Modus, wenn zu viele Befehle mit einem falschen Autorisierungswert empfangen werden. Wenn das TPM in einen Sperrmodus wechselt, ist es für alle Benutzer (einschließlich Administratoren) und für Windows-Features wie BitLocker-Laufwerkverschlüsselung Global.

Mit dieser Einstellung können Administratoren verhindern, dass die TPM-Hardware in einen Sperrmodus wechselt, indem Sie die Geschwindigkeit verlangsamen, mit der standardbenutzerbefehle senden können, für die eine Autorisierung für das TPM erforderlich ist.

Für jeden Standardbenutzer gelten zwei Schwellenwerte. Wenn Sie den Schwellenwert überschreiten, wird verhindert, dass der Benutzer einen Befehl sendet, der eine Autorisierung für das TPM erfordert. Verwenden Sie die folgenden Richtlinieneinstellungen zum Festlegen der Sperrdauer:

- Standard Benutzer einzelner Sperr SchwellenWert dieser Wert ist die maximale Anzahl von Autorisierungsfehlern, die jeder Standardbenutzer haben kann, bevor der Benutzer keine Befehle senden darf, die eine Autorisierung für das TPM erfordern.
- Standard Benutzer gesamt Sperrungs Schwelledieser Wert ist die maximale Gesamtzahl der Autorisierungsfehler, die alle Standardbenutzer aufweisen können, bevor alle standardbenutzerbefehle senden können, für die eine Autorisierung für das TPM erforderlich ist.

Ein Administrator mit dem TPM-Besitzerkennwort kann die Hardware-Lockout-Logik des TPM mithilfe des Windows Defender-Sicherheitscenters vollständig zurücksetzen. Jedes Mal, wenn ein Administrator die Hardware-Lockout-Logik des TPM zurücksetzt, werden alle vorherigen standardmäßigen TPM-Autorisierungsfehler ignoriert. Dies ermöglicht es Standardbenutzern, das TPM sofort normal zu verwenden.

Wenn Sie diese Richtlinieneinstellung nicht konfigurieren, wird ein Standardwert von 480 Minuten (8 Stunden) verwendet.

Standard Benutzer-individuelle Sperrschwelle

Mit dieser Richtlinieneinstellung können Sie die maximale Anzahl von Autorisierungsfehlern für jeden Standardbenutzer für das Trusted Platform Module (TPM) verwalten. Dieser Wert ist die maximale Anzahl von Autorisierungsfehlern, die jeder Standardbenutzer haben kann, bevor der Benutzer keine Befehle senden darf, die eine Autorisierung für das TPM erfordern. Wenn die Anzahl der Autorisierungsfehler des Benutzers innerhalb der Dauer, die für die Richtlinieneinstellung für die **standardmäßige Benutzer Sperrdauer** festgelegt ist, diesem Wert entspricht, wird dem Standardbenutzer das Senden von Befehlen verweigert, die eine Autorisierung für das Trusted Platform Module (TPM) erforderlich machen.

Mit dieser Einstellung können Administratoren verhindern, dass die TPM-Hardware in einen Sperrmodus wechselt, indem Sie die Geschwindigkeit verlangsamen, mit der standardbenutzerbefehle senden können, für die eine Autorisierung für das TPM erforderlich ist.

Ein Autorisierungsfehler tritt jedes Mal auf, wenn ein Standardbenutzer einen Befehl an das TPM sendet und eine Fehlerantwort erhält, die darauf hinweist, dass ein Autorisierungsfehler aufgetreten ist. Autorisierungsfehler, die älter als die Dauer sind, werden ignoriert.

Ein Administrator mit dem TPM-Besitzerkennwort kann die Hardware-Lockout-Logik des TPM mithilfe des Windows Defender-Sicherheitscenters vollständig zurücksetzen. Jedes Mal, wenn ein Administrator die Hardware-Lockout-Logik des TPM zurücksetzt, werden alle vorherigen standardmäßigen TPM-Autorisierungsfehler ignoriert. Dies ermöglicht es Standardbenutzern, das TPM sofort normal zu verwenden.

Wenn Sie diese Richtlinieneinstellung nicht konfigurieren, wird ein Standardwert von 4 verwendet. Der Wert 0 (null) bedeutet, dass das Betriebssystemstandard Benutzern nicht gestatten kann, Befehle an das TPM zu senden, was zu einem Autorisierungsfehler führen kann.

Standard Benutzer-gesamt Sperrungs Schwelle

Mit dieser Richtlinieneinstellung können Sie die maximale Anzahl von Autorisierungsfehlern für alle Standardbenutzer für das Trusted Platform Module (TPM) verwalten. Wenn die Gesamtzahl der Autorisierungsfehler für alle Standardbenutzer innerhalb der Dauer, die für die Richtlinie für die **standardmäßige Benutzer Sperrdauer** festgesetzt ist, diesem Wert entspricht, werden alle Standardbenutzer daran gehindert, Befehle zu senden, die eine Autorisierung für das Trusted Platform Module (TPM) erforderlich machen.

Mit dieser Einstellung können Administratoren verhindern, dass die TPM-Hardware in einen Sperrmodus wechselt, da Sie die Geschwindigkeit verlangsamt, mit der standardbenutzerbefehle senden können, die eine Autorisierung für das TPM erfordern.

Ein Autorisierungsfehler tritt jedes Mal auf, wenn ein Standardbenutzer einen Befehl an das TPM sendet und eine Fehlerantwort erhält, die darauf hinweist, dass ein Autorisierungsfehler aufgetreten ist. Autorisierungsfehler, die älter als die Dauer sind, werden ignoriert.

Ein Administrator mit dem TPM-Besitzerkennwort kann die Hardware-Lockout-Logik des TPM mithilfe des Windows Defender-Sicherheitscenters vollständig zurücksetzen. Jedes Mal, wenn ein Administrator die Hardware-Lockout-Logik des TPM zurücksetzt, werden alle vorherigen standardmäßigen TPM-Autorisierungsfehler ignoriert. Dies ermöglicht es Standardbenutzern, das TPM sofort normal zu verwenden.

Wenn Sie diese Richtlinieneinstellung nicht konfigurieren, wird ein Standardwert von 9 verwendet. Der Wert 0 (null) bedeutet, dass das Betriebssystemstandard Benutzern nicht gestatten kann, Befehle an das TPM zu senden, was zu einem Autorisierungsfehler führen kann.

Konfigurieren des Systems zur Verwendung von Legacy Dictionary Attack Prevention-Parametereinstellung für TPM 2,0

Diese Richtlinieneinstellung, die in Windows 10, Version 1703, eingeführt wurde, konfiguriert das TPM so, dass die Verhinderung von Wörterbuchangriffs Parametern (Sperrschwelle und Wiederherstellungszeit) auf die Werte angewendet wird, die für Windows 10, Version 1607 und darunter verwendet wurden.

> **IMPORTANT**
>
> Das Festlegen dieser Richtlinie wird nur in Kraft treten, wenn:
>
> - Das TPM wurde ursprünglich unter Verwendung einer Windows-Version nach Windows 10, Version 1607, bereitgestellt.
> - Das System verfügt über ein TPM 2,0.

> **NOTE**
>
> Das Aktivieren dieser Richtlinie wird erst wirksam, nachdem der TPM-Wartungstask ausgeführt wurde (was in der Regel nach einem Systemneustart geschieht). Nachdem diese Richtlinie auf einem System aktiviert wurde und (nach einem Neustart des Systems) wirksam wurde, hat eine Deaktivierung keine Auswirkungen, und das TPM des Systems bleibt unabhängig vom Wert dieser Gruppe mithilfe der Legacy-Wörterbuchangriffs Verhütungs Parameter konfiguriert. Richtlinie. Die einzige Möglichkeit für die deaktivierte Einstellung dieser Richtlinie, auf einem System wirksam zu werden, in dem Sie einmal aktiviert war, sind die folgenden:
>
> - Deaktivieren von Gruppenrichtlinien
> - Löschen des TPM auf dem System

TPM-Gruppenrichtlinieneinstellungen in der Windows-Sicherheits-App

Sie können in der Windows-Sicherheits-App ändern, was Benutzer über TPM sehen. Die Gruppenrichtlinieneinstellungen für den TPM-Bereich in der Windows-Sicherheits-App finden Sie unter:

Computer Configuration\Administrative Templates\Windows Components\Windows Security\Device-Sicherheit

Deaktivieren der Schaltfläche "TPM löschen"

Wenn Sie nicht möchten, dass Benutzer in der Windows-Sicherheits-App auf die Schaltfläche " **TPM löschen** " klicken können, können Sie Sie mit dieser Gruppenrichtlinieneinstellung deaktivieren. Wählen Sie **aktiviert** aus, damit die Schaltfläche **TPM löschen** für die Verwendung nicht verfügbar ist.

Ausblenden der TPM-Firmware-Update Empfehlung

Wenn Sie nicht möchten, dass Benutzer die Empfehlung zum Aktualisieren der TPM-Firmware sehen, können Sie Sie mit dieser Einstellung deaktivieren. Wählen Sie **aktiviert** aus, um zu verhindern, dass Benutzer eine Empfehlung zur Aktualisierung Ihrer TPM-Firmware sehen, wenn eine verwundbare Firmware erkannt wird.

Verwandte Themen

- Trusted Platform Module
- TPM-Cmdlets in Windows PowerShell
- Vorbereiten Ihrer Organisation für BitLocker: Planung und Richtlinien – TPM-Konfigurationen

Sichern der TPM-Wiederherstellungsinformationen in AD DS

12.09.2019 • 2 minutes to read

Betrifft

- Windows10, Version 1511
- Windows 10, Version 1507

Gilt nicht für

- Windows10, Version 1607 oder höher

Unter Windows 10, Versionen 1511 und 1507 können Sie die TPM-Informationen (Trusted Platform Module) eines Computers in Active Directory-Domänendienste (Adds) sichern. Auf diese Weise können Sie das TPM über einen Remotecomputer mit Adds verwalten. Das Verfahren ist mit Windows 8,1 identisch. Weitere Informationen finden Sie unter Sichern der TPM-Wiederherstellungsinformationen in AD DS.

Verwandte Themen

- Trusted Platform Module (Liste der Themen)
- Gruppenrichtlinieneinstellungen für TPM-Dienste

Behandeln von Problemen mit dem TPM

06.03.2020 • 7 minutes to read

Betriff:

- Windows 10
- Windows Server 2016

Dieses Thema enthält Informationen für IT-Experten zur Problembehandlung des Trusted Platform Module (TPM):

- Problembehandlung bei der TPM-Initialisierung
- Löschen aller Schlüssel aus dem TPM

Mit TPM 1,2 und Windows 10, Version 1507 oder 1511, können Sie auch die folgenden Aktionen ausführen:

- Aktivieren oder Deaktivieren des TPM

Informationen zu den TPM-Cmdlets finden Sie unter TPM-Cmdlets in Windows PowerShell.

Informationen zu TPM-Initialisierung und-Besitz

Ab Windows10 wird das Betriebssystem automatisch initialisiert und die Inhaberschaft des TPMs übernommen. Hierbei handelt es sich um eine Änderung gegenüber früheren Betriebssystemen, in der Sie das TPM initialisieren und ein Besitzerkennwort erstellen würden.

Problembehandlung bei der TPM-Initialisierung

Wenn Sie feststellen, dass Windows das TPM nicht automatisch initialisieren kann, überprüfen Sie die folgenden Informationen:

- Sie können versuchen, das TPM auf die werksseitigen Standardwerte zu löschen und es Windows zu ermöglichen, es erneut zu initialisieren. Wichtige Vorsichtsmaßnahmen für diesen Prozess und Anweisungen zum Abschließen des Vorgangs finden Sie unter Löschen aller Schlüssel aus dem TPMweiter unten in diesem Thema.
- Wenn es sich bei dem TPM um ein TPM-2,0 handelt, das von Windows nicht erkannt wird, überprüfen Sie, ob Ihre Computer Hardware eine Unified Extensible Firmware Interface (UEFI) enthält, die vertrauenswürdige Computing Group-kompatibel ist. Stellen Sie außerdem sicher, dass das TPM in den UEFI-Einstellungen nicht deaktiviert oder vom Betriebssystem ausgeblendet wurde.
- Wenn Sie über TPM 1,2 mit Windows 10, Version 1507 oder 1511 verfügen, ist das TPM möglicherweise deaktiviert und muss wieder aktiviert werden, wie es unter Aktivieren des TPMbeschrieben ist. Wenn Sie wieder aktiviert wird, wird Sie von Windows erneut initialisiert.
- Wenn Sie versuchen, BitLocker mit dem TPM einzurichten, überprüfen Sie, welcher TPM-Treiber auf dem Computer installiert ist. Wir empfehlen, immer einen der von Microsoft bereitgestellten TPM-Treiber zu verwenden und mit BitLocker geschützt zu sein. Wenn ein nicht-Microsoft-TPM-Treiber installiert ist, kann dies dazu führen, dass der standardmäßige TPM-Treiber nicht geladen wird und BitLocker meldet, dass kein TPM auf dem Computer vorhanden ist. Wenn Sie einen nicht von Microsoft installierten Treiber installiert haben, entfernen Sie ihn, und erlauben Sie dem Betriebssystem, das TPM zu initialisieren.

Behandeln von Problemen mit der Netzwerkverbindung für Windows 10, Versionen 1507 und 1511

Wenn Sie über Windows 10, Version 1507 oder 1511 verfügen, kann die Initialisierung des TPMs nicht

abgeschlossen werden, wenn Ihr Computer über Netzwerkverbindungsprobleme verfügt und beide der folgenden Bedingungen erfüllt sind:

- Ein Administrator hat Ihren Computer so konfiguriert, dass die TPM-Wiederherstellungsinformationen in aktiven DirectoryDomain-Diensten (Adds) gespeichert werden müssen. Diese Anforderung kann über Gruppenrichtlinien konfiguriert werden.
- Ein Domänencontroller kann nicht erreicht werden. Dies kann auf einem Computer auftreten, der derzeit vom Netzwerk getrennt ist, von der Domäne durch eine Firewall getrennt ist oder einen Netzwerkkomponenten Fehler (wie ein Unplugged-Kabel oder einen fehlerhaften Netzwerkadapter) aufweist.

Wenn diese Probleme auftreten, wird eine Fehlermeldung angezeigt, und Sie können den Initialisierungsprozess nicht abschließen. Um dieses Problem zu vermeiden, lassen Sie Windows das TPM initialisieren, während Sie mit dem Unternehmensnetzwerk verbunden sind, und wenden Sie sich an einen Domänencontroller.

Problembehandlung bei Systemen mit mehreren TPMs

Einige Systeme verfügen möglicherweise über mehrere TPMs, und das aktive TPM kann in UEFI umgeschaltet werden. Dieses Verhalten wird von Windows10 nicht unterstützt. Wenn Sie TPMs wechseln, wird Windows möglicherweise nicht ordnungsgemäß erkannt oder mit dem neuen TPM interagiert. Wenn Sie das TPMs wechseln möchten, wechseln Sie zum neuen TPM, deaktivieren Sie es, und installieren Sie Windows erneut. Weitere Informationen finden Sie weiter unten in diesem Thema unter Löschen aller Schlüssel aus dem TPM.

Durch das Umschalten von TPMs wird beispielsweise BitLocker zur Eingabe des Wiederherstellungsmodus veranlasst. Wir empfehlen dringend, auf Systemen mit zwei TPMs ein TPM auszuwählen, das verwendet werden soll, und die Auswahl wird nicht geändert.

Löschen aller Schlüssel aus dem TPM

Sie können die Windows Defender-Sicherheits Center-App verwenden, um das TPM als Schritt zur Problembehandlung oder als endgültige Vorbereitung vor einer sauberen Installation eines neuen Betriebssystems zu löschen. Wenn Sie sich auf diese Weise auf eine Neuinstallation vorbereiten, können Sie sicherstellen, dass das neue Betriebssystem alle TPM-basierten Funktionen, wie etwa die Bescheinigung, vollständig bereitstellen kann. Auch wenn das TPM nicht gelöscht wird, bevor ein neues Betriebssystem installiert wird, funktionieren die meisten TPM-Funktionen wahrscheinlich ordnungsgemäß.

Durch das Löschen des TPMs wird es auf einen nicht im Besitz befindlichen Zustand zurückgesetzt. Nachdem Sie das TPM gelöscht haben, wird es vom Windows 10-Betriebssystem automatisch neu initialisiert und wieder in Besitz übernommen.

> **WARNING**
> Das Löschen des TPMs kann zu Datenverlusten führen. Weitere Informationen finden Sie im nächsten Abschnitt "Vorsichtsmaßnahmen, die Sie ergreifen müssen, bevor Sie das TPM löschen."

Vorsichtsmaßnahmen vor dem Löschen des TPMs

Das Löschen des TPMs kann zu Datenverlusten führen. Wenn Sie sich gegen einen solchen Verlust schützen möchten, lesen Sie die folgenden Vorsichtsmaßnahmen:

- Wenn Sie das TPM löschen, verlieren Sie alle erstellten Schlüssel, die dem TPM zugeordnet sind, und die Daten, die durch diese Schlüssel geschützt werden, wie etwa eine virtuelle Smartcard oder eine Anmelde-PIN. Stellen Sie sicher, dass Sie über eine Sicherungs-und Wiederherstellungsmethode für alle Daten verfügen, die vom TPM geschützt oder verschlüsselt sind.
- Deaktivieren Sie das TPM nicht auf einem Gerät, das Sie nicht besitzen, beispielsweise einem Geschäfts-

oder Schulcomputer, ohne dass Sie von Ihrem IT-Administrator dazu aufgefordert werden.

- Wenn Sie TPM-Vorgänge vorübergehend anhalten und TPM 1,2 mit Windows 10, Version 1507 oder 1511 verwenden möchten, können Sie das TPM deaktivieren. Weitere Informationen finden Sie unter Deaktivieren des TPMweiter unten in diesem Thema.
- Verwenden Sie immer die Funktionalität im Betriebssystem (wie TPM. msc), um das TPM zu löschen. Löschen Sie das TPM nicht direkt aus UEFI.
- Da Ihre TPM-Sicherheitshardware ein physischer Teil Ihres Computers ist, sollten Sie vor dem Löschen des TPMs die Handbücher oder Anweisungen lesen, die mit Ihrem Computer geliefert wurden, oder die Website des Herstellers durchsuchen.

Zum Ausführen dieses Verfahrens müssen Sie mindestens Mitglied der lokalen Gruppe Administratoren oder einer entsprechenden Gruppe sein.

So löschen Sie das TPM

1. Öffnen Sie die Windows Defender Security Center-app.
2. Klicken Sie auf **Gerätesicherheit**.
3. Klicken Sie auf **Details zum Sicherheitsprozessor**.
4. Klicken Sie auf **Problembehandlung des Sicherheits Prozessors**.
5. Klicken Sie auf **TPM löschen**.
6. Sie werden aufgefordert, den Computer neu zu starten. Während des Neustarts werden Sie möglicherweise vom UEFI aufgefordert, eine Taste zu drücken, um zu bestätigen, dass Sie das TPM löschen möchten.
7. Nachdem der PC neu gestartet wurde, wird Ihr TPM automatisch für die Verwendung durch Windows10 vorbereitet.

Aktivieren oder Deaktivieren des TPMs (nur für TPM 1,2 mit Windows 10, Version 1507 oder 1511 verfügbar)

Normalerweise ist das TPM im Rahmen des TPM-Initialisierungsprozesses aktiviert. Sie müssen das TPM normalerweise nicht aktivieren oder deaktivieren. Falls erforderlich, können Sie dies jedoch mithilfe der TPM-MMC tun.

Aktivieren des TPM

Wenn Sie das TPM nach dem deaktivieren verwenden möchten, können Sie das TPM mithilfe des folgenden Verfahrens aktivieren.

So aktivieren Sie das TPM (nur TPM 1,2 mit Windows 10, Version 1507 oder 1511)

1. Öffnen Sie die TPM-MMC (TPM. msc).
2. Klicken Sie im Bereich " **Aktion** " auf **TPM aktivieren** , um die Seite **TPM-Sicherheits Hardware aktivieren** anzuzeigen. Lesen Sie die Anweisungen auf dieser Seite.
3. Klicken Sie auf **Herunterfahren** (oder **neu starten**), und folgen Sie dann den Anweisungen im UEFI-Bildschirm.

   Nachdem der Computer neu gestartet wurde, aber bevor Sie sich bei Windows anmelden, werden Sie aufgefordert, die Neukonfiguration des TPM zu akzeptieren. Dadurch wird sichergestellt, dass der Benutzer physischen Zugriff auf den Computer hat und dass bösartige Software nicht versucht, Änderungen am TPM vorzunehmen.

Deaktivieren des TPM

Wenn Sie die Verwendung der Dienste, die vom TPM bereitgestellt werden, beenden möchten, können Sie die TPM-MMC verwenden, um das TPM zu deaktivieren.

So deaktivieren Sie das TPM (nur TPM 1,2 mit Windows 10, Version 1507 oder 1511)

1. Öffnen Sie die TPM-MMC (TPM. msc).
2. Klicken Sie im Bereich " **Aktion** " auf **TPM** deaktivieren, um die Seite **TPM-Sicherheitshardware deaktivieren** anzuzeigen.
3. Wählen Sie im Dialogfeld **TPM-Sicherheitshardware deaktivieren** eine Methode aus, um Ihr Besitzerkennwort einzugeben und das TPM zu deaktivieren:
   - Wenn Sie Ihr TPM-Besitzerkennwort auf einem Wechselmediengerät gespeichert haben, fügen Sie es ein, und klicken Sie dann auf **Ich habe die Besitzerkennwort-Datei**. Klicken Sie im Dialogfeld **Sicherungsdatei mit TPM-Besitzerkennwort auswählen** auf **Durchsuchen** , um die TPM-Datei zu suchen, die auf Ihrem Wechselmediengerät gespeichert ist, klicken Sie auf **Öffnen**, und klicken Sie dann auf **TPM**deaktivieren.
   - Wenn Sie nicht über das Wechselmediengerät mit Ihrem gespeicherten TPM-Besitzerkennwort verfügen, klicken Sie auf **Ich möchte das Kennwort eingeben**. Geben Sie im Dialogfeld **TPM-Besitzerkennwort eingeben** Ihr Kennwort (einschließlich Bindestriche) ein, und klicken Sie dann auf **TPM deaktivieren**.
   - Wenn Sie Ihr TPM-Besitzerkennwort nicht gespeichert haben oder es nicht mehr kennen, klicken Sie auf **Ich habe nicht das TPM-Besitzerkennwort**, und befolgen Sie die Anweisungen, die im Dialogfeld und auf nachfolgenden UEFI-Bildschirmen bereitgestellt werden, um das TPM zu deaktivieren, ohne das Kennwort einzugeben.

Verwenden der TPM-Cmdlets

Sie können das TPM mithilfe von Windows PowerShell verwalten. Ausführliche Informationen finden Sie unter TPM-Cmdlets in Windows PowerShell.

Verwandte Themen

- Trusted Platform Module (Liste der Themen)

Grundlegendes zu PCR-Bänken auf TPM2.0-Geräten

12.09.2019 • 4 minutes to read

Betrifft

- Windows 10
- Windows Server 2016

Eine schrittweise Anleitung zum Wechseln von PCR-Banken auf TPM 2,0-Geräten auf Ihrem PC erhalten Sie von Ihrem OEM-oder UEFI-Anbieter. In diesem Thema wird der Hintergrund erläutert, was passiert, wenn Sie PCR-Banken auf TPM 2,0-Geräten wechseln.

Bei einem Platform Configuration Register (PCR) handelt es sich um einen Speicherplatz im TPM mit einigen eindeutigen Eigenschaften. Die Größe des Werts, der in einem PCR gespeichert werden kann, wird durch die Größe eines Digest bestimmt, der von einem zugeordneten Hashalgorithmus generiert wird. Ein SHA-1-PCR kann 20 Bytes (die Größe eines SHA-1-Digest) speichern. Mehrere PCRs, die dem gleichen Hashalgorithmus zugeordnet sind, werden als PCR-Bank bezeichnet.

Um einen neuen Wert in einem PCR zu speichern, wird der vorhandene Wert wie folgt um einen neuen Wert erweitert: PCR \ [n] = HASHalg (PCR \ [n] | | ArgumentOfExtend)

Der vorhandene Wert wird mit dem Argument des TPM-Extend-Vorgangs verkettet. Die resultierende Verkettung wird dann als Eingabe für den zugehörigen Hashalgorithmus verwendet, der einen Digest der Eingabe berechnet. Dieser berechnete Digest wird zum neuen Wert des PCR.

Die TPM-Profilspezifikation der TCG PC Client Platform definiert die Einbeziehung von mindestens einer PCR-Bank mit 24 Registern. Die einzige Möglichkeit zum Zurücksetzen der ersten 16 PCRs besteht darin, das TPM selbst zurückzusetzen. Mithilfe dieser Einschränkung wird sichergestellt, dass der Wert dieser PCRs nur über den TPM-Erweiterungsvorgang geändert werden kann.

Einige TPM-PCRs werden als Prüfsummen von Protokollereignissen verwendet. Die Protokollereignisse werden im TPM beim Auftreten der Ereignisse erweitert. Später kann ein Prüfer die Protokolle validieren, indem er die erwarteten PCR-Werte aus dem Protokoll berechnet und mit den PCR-Werten des TPM vergleicht. Da die ersten 16 TPM-PCRs nicht willkürlich geändert werden können, bietet eine Übereinstimmung zwischen einem erwarteten PCR-Wert in diesem Bereich und dem tatsächlichen TPM-PCR-Wert die Sicherheit eines ungeänderten Protokolls.

Wie verwendet Windows10 PCRs?

Um die Verwendung eines TPM-basierten Schlüssels an einen bestimmten Zustand des PCs zu binden, kann der Schlüssel mit einem erwarteten Satz von PCR-Werten versiegelt werden. Beispielsweise haben PCRs 0 bis 7 nach dem Startvorgang einen genau definierten Wert – wenn das Betriebssystem geladen wird. Wenn sich die Hardware, die Firmware oder der Bootloader des Computers ändert, kann die Änderung in den PCR-Werten erkannt werden. Windows10 verwendet diese Funktion, um bestimmte kryptografische Schlüssel nur zu bestimmten Zeiten während des Startvorgangs zur Verfügung zu stellen. Beispielsweise kann der BitLocker-Schlüssel an einer bestimmten Stelle im Start, aber nicht vor oder nach verwendet werden.

Es ist wichtig zu beachten, dass diese Bindung an PCR-Werte auch den für den PCR verwendeten Hashalgorithmus umfasst. So kann beispielsweise ein Schlüssel an einen bestimmten Wert des SHA-1-PCR \ [12] gebunden werden, wenn er SHA-256-PCR-Banken verwendet, sogar mit der gleichen Systemkonfiguration. Andernfalls Stimmen die PCR-Werte nicht überein.

Was passiert, wenn PCR-Banken gewechselt werden?

Wenn die PCR-Banken gewechselt werden, wird der Algorithmus, der zum Berechnen der in der PCRs während des Extend-Vorgangs gespeicherten Hashwerte verwendet wird, geändert. Jeder Hashalgorithmus gibt eine andere kryptografische Signatur für dieselben Eingaben zurück.

Wenn also die aktuell verwendete PCR-Bank gewechselt wird, funktionieren alle Schlüssel, die an die vorherigen PCR-Werte gebunden wurden, nicht mehr. Wenn beispielsweise ein Schlüssel an den SHA-1-Wert von PCR \ [12] gebunden und anschließend die PCR-Banken in SHA-256 geändert wurde, würden die Banken nicht übereinstimmen, und Sie können diesen Schlüssel nicht verwenden. Der BitLocker-Schlüssel wird mithilfe der PCR-Banken gesichert, und Windows10 kann die Versiegelung nicht aufheben, wenn die PCR-Banken gewechselt werden, während BitLocker aktiviert ist.

Was kann ich tun, um PCRs zu wechseln, wenn BitLocker bereits aktiv ist?

Bevor Sie PCR-Banken wechseln, sollten Sie BitLocker sperren oder deaktivieren oder den Wiederherstellungsschlüssel bereithalten. Eine schrittweise Anleitung zum Wechseln von PCR-Banken auf Ihrem PC erhalten Sie von Ihrem OEM-oder UEFI-Anbieter.

Wie kann ich feststellen, welche PCR-Bank verwendet wird?

Ein TPM kann so konfiguriert werden, dass mehrere PCR-Banken aktiv sind. Wenn das BIOS Messungen durchführt, erfolgt dies in allen aktiven PCR-Bänken, je nachdem, wie Sie diese Messungen durchführen können. Das BIOS hat möglicherweise entschieden, PCR-Banken zu deaktivieren, die nicht unterstützt werden, oder "Cap"-PCR-Banken, die durch das Erweitern eines Trennzeichens nicht unterstützt werden. Der folgende Registrierungswert gibt an, welche PCR-Banken aktiv sind.

- Registrierungsschlüssel: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\IntegrityServices
- DWORD: TPMActivePCRBanks
- Definiert, welche PCR-Banken aktuell aktiv sind. (Dieser Wert sollte als Bitmap interpretiert werden, für die die Bits in der Registrierungstabelle 21 der Version 1,27 des TCG-Algorithmus definiert sind.)

Windows überprüft, welche PCR-Banken aktiv sind und vom BIOS unterstützt werden. Windows überprüft auch, ob das gemessene Startprotokoll Messungen für alle aktiven PCR-Banken unterstützt. Windows bevorzugt die Verwendung der SHA-256-Bank für Messungen und wird auf die SHA1-PCR-Bank zurückgreifen, wenn eine der Voraussetzungen nicht erfüllt ist.

Sie können feststellen, welche PCR-Bank derzeit von Windows verwendet wird, indem Sie sich die Registrierung anschauen.

- Registrierungsschlüssel: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\IntegrityServices
- DWORD: TPMDigestAlgID
- Die Algorithmus-ID der PCR-Bank, die Windows zurzeit verwendet. (Dieser Wert stellt eine Algorithm-ID dar, wie Sie in der Registrierungstabelle des TCG-Algorithmus in der Revision 1,27 definiert ist.)

Windows verwendet nur eine PCR-Bank, um die Boot-Messungen fortzusetzen. Alle anderen aktiven PCR-Banken werden mit einem Trennzeichen erweitert, um anzugeben, dass Sie von Windows nicht verwendet werden, und Maße, die anscheinend aus Windows bestehen, sollten nicht als vertrauenswürdig eingestuft werden.

Verwandte Themen

- Trusted Platform Module (Liste der Themen)

TPM-Empfehlungen

24.10.2019 • 7 minutes to read

Betrifft

- Windows 10
- Windows Server 2016

Dieses Thema enthält Empfehlungen für die TPM-Technologie (Trusted Platform Module) für Windows10.

Eine allgemeine Featurebeschreibung von TPM finden Sie unter Trusted Platform Module – Technologieübersicht.

TPM-Entwurf und -Implementierung

Bisher wurden TPMs als diskrete Chips auf die Hauptplatine des Computers aufgelötet. Diese Implementierung ermöglichen es OEM-Herstellers, das TPM unabhängig vom Rest des Systems zu bewerten und zu zertifizieren. Obwohl diskrete TPM-Implementierungen nach wie vor häufig sind, können sie bei integrierten Geräten problematisch sein, wenn diese kleinformatig sind bzw. nur einen geringen Stromverbrauch haben. Einige neuere TPM-Implementierungen integrieren die TPM-Funktionalität in denselben Chipsatz wie andere Plattformkomponenten, behalten aber eine logische Trennung bei wie diskrete TPM-Chips.

TPMs sind passiv: Sie empfangen Befehle und geben Antworten zurück. Um alle Vorteile von TPM nutzen zu können, muss der OEM-Hersteller die Systemhardware und die Firmware sorgfältig integrieren in TPM integrieren, damit diese geeignete Befehle senden und auf die Antworten reagieren kann. TPMs wurden ursprünglich entwickelt, um Sicherheit und Datenschutzes für die Besitzer und Benutzer von Plattformen zu verbessern, aber neuere Versionen können diese Verbesserungen bereits über die Hardware selbst bereitstellen. Bevor TPMs für erweiterte Szenarios verwendet werden können, müssen sie jedoch bereitgestellt werden. Windows 10 stellt ein TPM automatisch bereit. Falls ein Benutzer das Betriebssystem jedoch neu installieren möchte, muss er unter Umständen das TPM vor der Neuinstallation löschen, damit Windows alle TPM-Features uneingeschränkt nutzen kann.

Die Trusted Computing Group (TCG) ist eine gemeinnützige Organisation, die die TPM-Spezifikation veröffentlicht und verwaltet. Zweck der TCG ist es, herstellerunabhängige, globale Branchenstandards zu entwickeln, zu definieren und zu propagieren, die eine hardwarebasierte vertrauenswürdige Stammzertifizierungsstelle für interoperable Trusted Computing-Plattformen unterstützen. Die TCG veröffentlicht auch die TPM-Spezifikation als Internationaler Standard ISO/IEC 11889, wobei der öffentlich zugängliche Prozess zur Einreichung der Spezifikation zugrunde gelegt wird, die das Joint Technical Committee 1 zwischen der International Organization for Standardization (ISO) und der International Electrotechnical Commission (IEC) definiert.

OEM-Hersteller implementieren das TPM als Komponente in eine vertrauenswürdige Computerplattform wie einem PC, einem Tablet oder einem Telefon. Vertrauenswürdige Computerplattformen nutzen TPM, um Datenschutz- und Sicherheitsszenarios zu unterstützen, die mit Software allein nicht erreicht werden kann. Beispielsweise kann Software allein nicht zuverlässig angeben, ob während des Systemstartvorgangs Malware vorhanden ist. Die enge Integration zwischen TPM und Plattform erhöht die Transparenz des Startvorgangs und unterstützt eine Auswertung des Gerätezustands, weil die Integration eine zuverlässige Messung und Berichte zu der Software, unter der das Gerät gestartet wurde, ermöglichen. Eine Implementierung eines TPMs als Teil einer vertrauenswürdigen Computerplattform bietet einen Hardware-basierten Vertrauensanker, d. h. die Hardware verhält sich vertrauenswürdig. Wenn beispielsweise ein im TPM gespeicherter Schlüssel eine Eigenschaften hat, die nicht zulassen, dass er exportiert wird, kann der Schlüssel das TPM effektiv nicht verlassen.

Die TCG hat das TPM als kostengünstige Lösung für den Massenmarkt entwickelt, die die Anforderungen von

unterschiedlichen Kundensegmente bedient. Es gibt in den verschiedenen TPM-Implementationen Unterschiede bei den Sicherheitseigenschaften und ebenfalls bei den kundenseitigen und behördlichen Anforderungen für die verschiedenen Sektoren. Im öffentlichen Beschaffungssektor haben beispielsweise einige Behörden klare Sicherheitsanforderungen für TPMs definiert, die es in anderen Sektoren möglicherweise nicht gibt.

Vergleich zwischen TPM 1.2 und 2.0

Microsoft ist seit jeher hinsichtlich Industriestandards Marktführer bezüglich der Fortentwicklung und Standardisierung auf TPM2.0, das viele wichtige anerkannte Vorteile hinsichtlich Algorithmen, Kryptografie, Hierarchie, Stammschlüsseln, Autorisierung und NV-RAM mit sich bringt.

Gründe für TPM 2.0

TPM 2.0-Produkte und -Systeme bieten wesentliche Sicherheitsvorteile gegenüber TPM 1.2. Einige Beispiele:

- Die TPM 1.2-Spezifikation lässt nur die Verwendung des RSA- und SHA-1-Hashalgorithmus zu.
- Aus Sicherheitsgründen rücken einige Entitäten inzwischen von SHA-1 ab. Insbesondere das NIST (National Institute of Standards and Technology) hat viele öffentliche Behörden 2014 dazu veranlasst, auf SHA-256 umzusteigen, und Technologieführer wie Microsoft und Google haben angekündigt, dass sie SHA-1-basierte Signaturen oder Zertifikate ab 2017 nicht mehr unterstützen werden.
- TPM 2.0 ermöglicht eine **höhere kryptografische Agilität** durch die flexiblere Unterstützung kryptografischer Algorithmen.
    - TPM2.0 unterstützt neuere Algorithmen, wodurch die Leistung bei der Signierung und Schlüsselgenerierung verbessert werden kann. Eine vollständige Liste der unterstützten Algorithmen finden Sie unter TCG-Algorithmusregistrierung. Einige TPMs unterstützen nicht alle Algorithmen.
    - Eine Liste der Algorithmen, die von Windows für den Plattform-Kryptografiespeicheranbieter unterstützt werden, finden Sie unter CNG-Kryptografiealgorithmusanbieter.
    - TPM 2.0 wurde nach ISO standardisiert (ISO/IEC 11889:2015).
    - TPM 2.0 kann Vorteile für OEMs bringen, das diese für bestimmte Länder und Regionen keine Ausnahmen von Standardkonfigurationen mehr bereitstellen müssen.
- TPM 2.0 bietet eine **einheitliche Benutzererfahrung** über verschiedene Implementierungen hinweg.
    - TPM1.2-Implementierungen weisen abweichende Richtlinieneinstellungen auf. Abweichende Sperrrichtlinien können die Unterstützung erschweren.
    - Die TPM2.0-Sperrrichtlinie wird von Windows konfiguriert. Auf diese Weise wird ein konsistenter Schutz vor Wörterbuchangriffen gewährleistet.
- Während es sich bei TPM 1.2 um separate Siliziumchips handelte, die in der Regel auf der Hauptplatine festgelötet waren, ist TPM 2.0 als **getrennte (dTPM)** Siliziumkomponente in einem einzelnen Halbleiterpaket, eine **integrierte** Komponente in einem oder mehreren Halbleiterpaketen (neben anderen Logikeinheiten in den gleichen Paketen) und als **firmwarebasierte (fTPM)** Komponente in einer vertrauenswürdigen Ausführungsumgebung (Trusted Execution Environment, TEE) in einem allgemeinen SoC erhältlich.

> **NOTE**
>
> TPM 2,0 wird im Legacy-und CSM-Modus des BIOS nicht unterstützt. Bei Geräten mit TPM 2,0 muss der BIOS-Modus nur als systemeigener UEFI konfiguriert sein. Die Optionen für Legacy-und Kompatibilitäts Unterstützungs Module (CSM) müssen deaktiviert sein. Für zusätzliche Sicherheit aktivieren Sie das Feature für sicheres Booten.
>
> Das installierte Betriebs System auf der Hardware im Legacy Modus verhindert das Booten des Betriebssystems, wenn der BIOS-Modus in UEFI geändert wird. Verwenden Sie das Tool MBR2GPT , bevor Sie den BIOS-Modus ändern, der das Betriebssystem und den Datenträger zur Unterstützung von UEFI vorbereitet.

Diskretes, integriertes oder firmwarebasiertes TPM?

Es gibt drei Implementierungsoptionen für TPMs:

- Diskreter TPM-Chip als separate Komponente in einem eigenen Halbleiterpaket
- Integrierte TPM-Lösung mit dedizierter Hardware, die zusammen mit anderen, logisch getrennten Komponenten in mindestens ein Halbleiterpaket integriert ist
- Firmware-TPM-Lösung, bei der das TPM in der Firmware in einem Modus für die vertrauenswürdige Ausführung einer allgemeinen Berechnungseinheit ausgeführt wird

Windows verwendet jedes kompatible TPM auf die gleiche Weise. Microsoft schreibt nicht vor, wie ein TPM implementiert werden sollte, und es gibt zahlreiche TPM-Lösungen, die verschiedenste Anforderungen erfüllen.

Ist TPM für Verbraucher relevant?

Für Endbenutzer agiert das TPM im Hintergrund, es ist aber dennoch von großer Bedeutung. Das TPM wird für Windows Hello und Windows Hello for Business verwendet und wird in Zukunft eine Komponente zahlreicher anderer Sicherheitsfeatures in Windows darstellen. Das TPM schützt die PIN, hilft, Kennwörter zu verschlüsseln, und baut auf unserer Windows10-Umgebung auf, in der Sicherheit eine zentrale Säule darstellt. Verwenden von Windows auf einem System mit TPM kann eine tiefgreifendere und umfassendere Abdeckung der Sicherheit.

TPM 2.0-Kompatibilität für Windows10

Windows10 für Desktop-Editionen (Home, pro, Enterprise und Education)

- Seit dem 28.Juli2016 müssen alle neuen Gerätemodelle, Produktlinien und Baureihen (oder bei Aktualisierung der Hardwarekonfiguration von bestehenden Gerätemodellen, Produktlinien und Baureihen mit einem wichtigen Upgrade, etwa bei CPU oder Grafikkarten) TPM 2.0 implementieren und standardmäßig aktivieren (Details finden Sie in Abschnitt3.7 der Seite Mindesthardwareanforderungen). Die Anforderung zum Aktivieren von TPM2.0 gilt nur für die Herstellung neuer Geräte. TPM-Empfehlungen für bestimmte Windows-Features finden Sie unter TPM und Windows-Features.

IoT Core

- TPM ist optional für IoT Core erhältlich.

Windows Server2016

- TPM ist optional für Windows Server-SKUs erhältlich, es sei denn, die SKU erfüllt die zusätzlichen Qualifizierungskriterien für das Host Guardian Services-Szenario, das TPM 2.0 erforderlich macht.

TPM und Windows-Features

In der folgenden Tabelle sind die Windows-Features aufgeführt, die TPM-Unterstützung erfordern.

WINDOWS-FEATURES	TPM ERFORDERLICH	UNTERSTÜTZT TPM 1.2	UNTERSTÜTZT TPM 2.0	DETAILS
Kontrollierter Start	Ja	Ja	Ja	Der kontrollierte Start erfordert TPM 1.2 oder 2.0 und den sicheren UEFI-Start.
BitLocker	Ja	Ja	Ja	TPM 1,2 oder 2,0 ist erforderlich, die Automatische Geräteverschlüsselung erfordert jedoch einen modernen Standby-Modus , einschließlich TPM 2,0-Unterstützung
Geräteverschlüsselung	Ja	–	Ja	Die Geräteverschlüsselung erfordert eine Modern Standby/Connected-Standbyzertifizierung, wozu TPM 2.0 erforderlich ist.
Windows Defender-Anwendungssteuerung (Geräteschutz)	Nein	Ja	Ja	
Windows Defender-Systemüberwachung	Ja	Nein	Ja	
Credential Guard	Nein	Ja	Ja	Windows10, Version 1507 (Einstellung im Mai2017), unterstützte nur TPM 2.0 für Credential Guard. Ab Windows10, Version 1511, werden TPM 1.2 und 2.0 unterstützt.
Nachweis über Geräteintegrität	Ja	Ja	Ja	

WINDOWS-FEATURES	TPM ERFORDERLICH	UNTERSTÜTZT TPM 1.2	UNTERSTÜTZT TPM 2.0	DETAILS
Windows Hello/Windows Hello for Business	Nein	Ja	Ja	Die Azure AD-Verknüpfung unterstützt beide TPM-Versionen, erfordert jedoch TPM mit dem Algorithmus für den Nachrichtenauthentifizierungscode mit Schlüsselhash (Hash Message Authentication Code, HMAC) sowie das Endorsement Key (EK)-Zertifikat für die Unterstützung des Schlüsselnachweises.
Sicherer UEFI-Start	Nein	Ja	Ja	
TPM-Plattformkryptografieanbieter/Schlüsselspeicheranbieter	Ja	Ja	Ja	
Virtuelle Smartcards	Ja	Ja	Ja	
Zertifikatspeicher	Nein	Ja	Ja	TPM ist nur erforderlich, wenn das Zertifikat im TPM gespeichert ist.
Autopilot	Ja	Nein	Ja	TPM 2,0-und UEFI-Firmware sind für weiße Handschuh und Self-Deploying-Szenarien erforderlich.
SecureBIO	Ja	Nein	Ja	TPM 2,0-und UEFI-Firmware sind erforderlich.
DRTM	Ja	Nein	Ja	TPM 2,0-und UEFI-Firmware sind erforderlich.

OEM-Status zu TPM 2.0-Systemverfügbarkeit und zertifizierten Komponenten

Regierungsbehörden und Unternehmenskunden in regulierten Branchen unterliegen möglicherweise Erwerbsstandards, die die Nutzung gängiger zertifizierter TPM-Komponenten voraussetzen. Die OEM-Lieferanten von Geräten können deshalb verpflichtet werden, kommerziell nutzbare Systeme nur mit zertifizierten TPM-Komponenten auszuliefern. Weitere Informationen erhalten Sie vom OEM oder Hardwarehersteller.

Verwandte Themen

- Trusted Platform Module (Liste der Themen)