TREND MICRO™

3.1

TREND MICRO™ Endpoint Encryption

Installationshandbuch

Umfassende Endpunktverschlüsselung für gespeicherte Daten

Endpoint Security

Trend Micro Incorporated behält sich das Recht vor, Änderungen an diesem Dokument und dem hierin beschriebenen Produkt ohne Vorankündigung vorzunehmen. Lesen Sie vor der Installation und Verwendung des Produkts die Readme-Dateien, die Anmerkungen zu dieser Version und/oder die neueste Version der verfügbaren Dokumentation durch:

http://docs.trendmicro.com/de-de/enterprise/endpoint-encryption.aspx

Trend Micro, das Trend Micro T-Ball-Logo, Endpoint Encryption, PolicyServer, Full Disk Encryption, FileArmor und KeyArmor sind Marken oder eingetragene Marken von Trend Micro Incorporated. Alle anderen Produkt- oder Firmennamen können Marken oder eingetragene Marken ihrer Eigentümer sein.

Copyright © 2012 Trend Micro Incorporated. Alle Rechte vorbehalten.

Dokument-Nr.: APGM35735/121016

Release-Datum: Dec 2012

Geschützt durch U.S. Patent-Nr.: Zum Patent angemeldet.

In dieser Dokumentation finden Sie eine Einführung in die Hauptfunktionen des Produkts und/oder Installationsanweisungen für eine Produktionsumgebung. Lesen Sie die Dokumentation vor der Installation und Verwendung des Produkts aufmerksam durch.

Ausführliche Informationen über die Verwendung bestimmter Funktionen des Produkts sind möglicherweise in der Trend Micro Online-Hilfe und/oder der Trend Micro Knowledge Base auf der Website von Trend Micro verfügbar.

Das Trend Micro Team ist stets bemüht, die Dokumentation zu verbessern. Bei Fragen, Anmerkungen oder Anregungen zu diesem oder anderen Dokumenten von Trend Micro wenden Sie sich bitte an docs@trendmicro.com.

Bewerten Sie diese Dokumentation auf der folgenden Website:

http://www.trendmicro.com/download/documentation/rating.asp

Inhaltsverzeichnis

Vorwort

Kapitel 1: Einführung in Trend Micro Endpoint Encryption

Kapitel 2: Überlegungen zur Verteilung

Kapitel 3: PolicyServer Installation

Kapitel 4: Endpoint Encryption Client-Installation

Kapitel 5: Upgrades, Migrationen und Deinstallationen

Kapitel 6: Unterstützung erhalten

Anhang A: Checkliste für das Endpoint Encryption Pilotprogramm

Anhang B: Checkliste für die Sicherheitsinfrastruktur

Anhang C: Installationsvoraussetzungen für Full Disk Encryption

Stichwortverzeichnis

Vorwort

Vorwort

Willkommen beim Installationshandbuch für Trend Micro™ Endpoint Encryption. Dieses Handbuch enthält eine Einführung in die Sicherheitsarchitektur und die Funktionen von Endpoint Encryption, um Administratoren die Installation und Einrichtung in kürzester Zeit zu ermöglichen. Folgende Themen werden behandelt: Systemvoraussetzungen, Vorbereitungsschritte für die Verteilung, Installation von PolicyServer und der Client-Software, Erläuterungen für Endbenutzer, Upgrade bzw. Migration von Server- und Client-Instanzen.

Das Vorwort umfasst folgende Themen:

Produktdokumentation

In der Dokumentation zu Trend Micro Endpoint Encryption sind folgende Dokumente enthalten:

TABELLE 1. Produktdokumentation

DOKUMENT	BESCHREIBUNG
Installationshandbuch	Im Installationshandbuch werden die Systemvoraussetzungen beschrieben. Es enthält zudem detaillierte Anweisungen zur Einrichtung, Installation und Migration sowie zum Upgrade von PolicyServer und den Endpunkt-Clients.
Administratorhandbuch	Im Administratorhandbuch werden die Produktkonzepte und -funktionen erläutert. Außerdem enthält es ausführliche Informationen zur Konfiguration und Verwaltung von PolicyServer und den Endpunkt-Clients.
Readme-Datei	Die Readme-Datei enthält aktuelle Produktinformationen, die in der Online-Hilfe oder im Benutzerhandbuch noch nicht erwähnt sind. Zu den Themen gehören die Beschreibung neuer Funktionen, Lösungen bekannter Probleme und eine Liste bereits veröffentlichter Produktversionen.
Knowledge Base	Eine Online-Datenbank mit Informationen zur Problemlösung und Fehlerbehebung. Sie enthält aktuelle Hinweise zu bekannten Softwareproblemen. Die Knowledge Base finden Sie im Internet unter folgender Adresse: http://esupport.trendmicro.com

Hinweis

Die Dokumentation steht unter folgender Adresse zum Download bereit:

http://docs.trendmicro.com/de-de/home.aspx

Dokumentationskonventionen

In der Dokumentation werden die folgenden Konventionen verwendet:

TABELLE 2. Dokumentationskonventionen

KONVENTION	BESCHREIBUNG
GROSSSCHREIBUNG	Akronyme, Abkürzungen und die Namen bestimmter Befehle sowie Tasten auf der Tastatur
Fettdruck	Menüs und Menübefehle, Schaltflächen, Registerkarten und Optionen
Kursivdruck	Referenzen auf andere Dokumente
`Schreibmaschinenschrift`	Beispiele für Befehlszeilen, Programmcode, Internet-Adressen, Dateinamen und Programmanzeigen
Navigation > **Pfad**	Navigationspfad für den Zugriff auf ein bestimmtes Fenster Beispiel: **Datei** > **Speichern** bedeutet, auf der Benutzeroberfläche auf **Datei** und dann auf **Speichern** zu klicken
 **Hinweis**	Konfigurationshinweise
 **Tipp**	Empfehlungen oder Vorschläge
 **Wichtig**	Informationen zu erforderlichen oder standardmäßigen Konfigurationseinstellungen und Produkteinschränkungen
 **Warnung!**	Kritische Aktionen und Konfigurationsoptionen

Zielgruppe

Dieses Handbuch wurde für IT-Administratoren geschrieben, die Trend Micro Endpoint Encryption in mittleren bis großen Unternehmen einsetzen. Es richtet sich zudem an Helpdesk-Mitarbeiter, die Benutzer, Gruppen, Richtlinien und Geräte

verwalten. In dieser Dokumentation werden grundlegende Kenntnisse zu Geräten, Netzwerken und Sicherheit vorausgesetzt. Dazu gehören:

- Setup und Konfiguration der Geräte-Hardware
- Partitionierung, Formatierung und Wartung der Festplatte
- Client-Server-Architektur

Begriffe

Die folgende Tabelle enthält die Terminologie, die innerhalb der Dokumentation verwendet wird:

TABELLE 3. Endpoint Encryption Terminologie

BEGRIFF	BESCHREIBUNG
Authentifizierung	Der Prozess des Identifizierens eines Benutzers.
ColorCode™	Ein Kennwort mit einer Farbfolge.
Command Line Helper	Mit dem Command Line Helper können verschlüsselte Werte erzeugt werden, die als sichere Anmeldedaten beim Erstellen von Installationsskripts verwendet werden können.
Command Line Installer Helper	Mit dem Command Line Installer Helper können verschlüsselte Werte erzeugt werden, die als sichere Anmeldedaten beim Erstellen von Skripts für automatisierte Installationen verwendet werden können.
Gerät	Computer, Laptop oder Wechselmedium (externes Laufwerk, USB-Laufwerk).
Domänenauthentifizierung	SSO (Single-Sign-On) mit Hilfe von Active Directory.
DriveTrust™	Hardware-basierte Verschlüsselungstechnologie von Seagate™.
Endpunkt-Client	Ein Gerät, auf dem eine Endpoint Encryption Anwendung installiert ist.

Begriff	Beschreibung
FileArmor	Der Endpoint Encryption Client für die Verschlüsselung von Dateien und Ordnern auf lokalen Laufwerken und Wechselmedien.
FIPS	Federal Information Processing Standard. Der Datenverarbeitungsstandard der US-Regierung.
Festes Kennwort	Ein Standardbenutzerkennwort, das aus Buchstaben und/oder Ziffern und/oder Sonderzeichen besteht.
Full Disk Encryption	Der Endpoint Encryption Client für die Verschlüsselung von Hardware und Software mit Preboot-Authentifizierung.
KeyArmor	Der Endpoint Encryption Client für ein durch ein Kennwort geschütztes verschlüsseltes USB-Laufwerk.
OCSP	Das OCSP (Online Certificate Status Protocol) ist ein für digitale X.509-Zertifikate verwendetes Internet-Protokoll.
OPAL	Die Subsystemklasse für Sicherheit der Trusted Computing Group für Client-Geräte.
Kennwort	Alle Arten von Authentifizierungsdaten, wie beispielsweise ein festes Kennwort, eine PIN und ein ColorCode.
PolicyServer	Der zentrale Verwaltungsserver, der die Verschlüsselungs- und Authentifizierungsrichtlinien an Endpunkt-Clients bereitstellt (Full Disk Encryption, FileArmor, KeyArmor).
SED	Secure Encrypted Device (sicher verschlüsseltes Gerät). Eine Festplatte oder ein anderes Gerät, das verschlüsselt wurde.
Smartcard	Eine physische Karte wird in Verbindung mit einer PIN oder einem festen Kennwort verwendet.
PIN	Eine persönliche Identifikationsnummer, die im Allgemeinen für Automatentransaktionen verwendet wird.
Wiederherstellungskonsole	Wiederherstellung eines Geräts beim Ausfall des primären Betriebssystems, beim Beheben von Netzwerkproblemen und beim Verwalten von Benutzern, Richtlinien und Protokollen.

BEGRIFF	BESCHREIBUNG
Remote-Hilfe	Interaktive Authentifizierung für Benutzer, die ihre Anmeldedaten vergessen haben, oder für Geräte, deren Richtlinien nicht innerhalb eines bestimmten Zeitraums synchronisiert wurden.
Reparatur-CD	Verwenden Sie diese startfähige CD, um das Laufwerk zu entschlüsseln, bevor Sie Full Disk Encryption im Falle einer Beschädigung der Festplatte entfernen.
RSA SecurID	Ein Mechanismus zum Ausführen der Zwei-Faktor-Authentifizierung für einen Benutzer bei einer Netzwerkressource.
Selbsthilfe	Kombinationen aus Fragen und Antworten, mit denen ein Benutzer ein vergessenes Kennwort zurücksetzen kann, ohne sich an den Support zu wenden.

Info über Trend Micro

Trend Micro, weltweit führend in der Internet-Content-Security und der Bewältigung von Bedrohungen, hat sich als Ziel gesetzt, den globalen Austausch von digitalen Informationen für Unternehmen und Endverbraucher sicher zu machen. Mit einer Erfahrung von über 20 Jahren bietet Trend Micro Client-, Server- und Cloud-basierte Lösungen, die neue Bedrohungen schneller unterbinden und die Daten in physischen, virtuellen und Cloud-Umgebungen schützen.

Da neue Bedrohungen und Schwachstellen immer wieder auftauchen, bleibt Trend Micro seiner Verpflichtung treu, seine Kunden beim Sichern von Daten, Einhalten der Konformität, Senken der Kosten und Wahren der Geschäftsintegrität zu unterstützen. Weitere Informationen finden Sie unter:

http://www.trendmicro.com

Trend Micro und das Trend Micro T-Ball-Logo sind Marken von Trend Micro Incorporated und in einigen Rechtsgebieten eingetragen. Alle anderen Marken- und Produktnamen sind Marken oder eingetragene Marken der entsprechenden Unternehmen.

Kapitel 1

Einführung in Trend Micro Endpoint Encryption

Bei der Prüfung des Nutzens eines Endpunktverschlüsselungsprojekts ist eine sorgfältige Planung ausschlaggebend.

In diesem Kapitel werden die folgenden Themen vorgestellt:

Info über Trend Micro Endpoint Encryption

Trend Micro Endpoint Encryption ist eine vollständig integrierte Hardware- und Software-basierte Verschlüsselungslösung zum Schutz für Laptops, Desktops, Dateien und Ordner, Wechselmedien und verschlüsselte ESB-Laufwerke mit eingebautem Antivirus-/Anti-Malware-Schutz. Mit Endpoint Encryption können Administratoren mit einer einzigen Management-Konsole flexibel eine Kombination aus Hardware- und Software-basierter Verschlüsselung mit voller Transparenz für Endbenutzer verwalten.

Trend Micro Endpoint Encryption stellt einen durchgängigen Datenschutz durch die Verschlüsselung gemäß FIPS 140-2 für folgende Daten bereit: Daten, die sich auf dem Verwaltungsserver befinden, alle Daten, die zum oder vom Server übertragen werden, alle Daten, die auf dem Endpunkt-Gerät gespeichert werden, sowie alle lokal gespeicherten Client-Protokolle.

Mit zertifizierter FIPS 140-2-Kryptographie bietet Endpoint Encryption die folgenden Vorteile:

- Umfassender Datenschutz durch vollständig integrierte Full Disk Encryption sowie durch Verschlüsselung von Dateien, Ordnern, USB-Laufwerken und Wechselmedien.
- Zentrale Richtlinienverwaltung und Schlüsselverwaltung über einen einzelnen Verwaltungsserver und eine einzelne Management-Konsole.
- Geräteverwaltung durch Sammeln von gerätespezifischen Informationen, Gerätesperre und Wiederherstellung sowie anhand der Möglichkeit zum Löschen aller Endpunktdaten.
- Erweiterte Berichtsfunktion und erweitertes Auditing in Echtzeit zur Einhaltung der Sicherheitsrichtlinien.

Komponenten von Endpoint Encryption

Endpoint Encryption besteht aus einem zentralen Verwaltungsserver (PolicyServer Web-Service), der die Richtlinien- und Protokolldatenbanken (MobileArmor DB), die LDAP-Authentifizierung mit Active Directory und alle Client-Server-Aktivitäten verwaltet. Endpoint Encryption Clients verfügen über keine direkte Schnittstelle zu PolicyServer und müssen die Verbindung über den Client-Web-Service herstellen. Eine

Darstellung dieser Architektur finden Sie unter *Abbildung 1-1: Endpoint Encryption Client-Server-Architektur auf Seite 1-3*.

Hinweis

Die Porteinstellungen für den gesamten HTTP-Datenverkehr können zum Zeitpunkt der Installation oder über Einstellungen auf dem Endpoint Encryption Client konfiguriert werden.

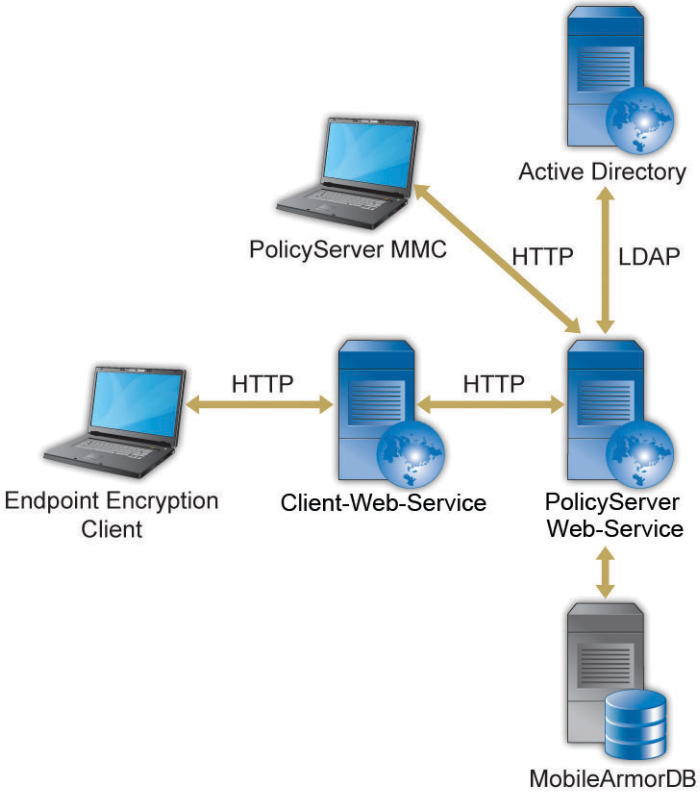


ABBILDUNG 1-1. Endpoint Encryption Client-Server-Architektur

In der folgenden Tabelle werden diese Komponenten beschrieben.

TABELLE 1-1. Komponenten von Endpoint Encryption

KOMPONENTE	BESCHREIBUNG
PolicyServer Web-Service	Der IIS-Web-Service für die zentrale Verwaltung der Administration, Authentifizierung und Berichterstellung im Zusammenhang mit Richtlinien.
PolicyServer MMC	Die PolicyServer Microsoft™ Management-Konsole (MMC) ist die Oberfläche zur Steuerung von PolicyServer.
Endpoint Encryption client	Ein Endpoint Encryption Client ist jedes Gerät, auf dem entweder Full Disk Encryption, FileArmor oder KeyArmor installiert ist. • Full Disk Encryption bietet Hardware- und Software-basierte Full Disk Encryption sowie Preboot-Authentifizierung. • FileArmor bietet Datei- und Ordnerverschlüsselung für Inhalte auf lokalen Festplatten und Wechselmedien. • KeyArmor ist ein robustes, verschlüsseltes USB-Laufwerk mit integriertem Virenschutz.
MobileArmorDB	Die Microsoft™ SQL Server Datenbank, in der alle Details zu Benutzern, Richtlinien und Protokollen gespeichert werden.
Active Directory	Der PolicyServer Web-Service synchronisiert Benutzerkontoinformationen durch Kommunikation mit Active Directory über LDAP. Die Kontoinformationen werden lokal in der MobileArmorDB zwischengespeichert. **Hinweis** Active Directory ist optional.
Client-Web-Service	Der IIS-Web-Service, den Endpoint Encryption Clients für die Kommunikation mit dem PolicyServer Web-Service verwenden.

Systemvoraussetzungen

Die unten stehenden Tabellen geben einen Überblick über die Systemvoraussetzungen für Endpoint Encryption.

TABELLE 1-2. Hardware-Voraussetzungen für PolicyServer

SEPARATE HOSTS		EINZELNER HOST
PolicyServer Host (3.000 Benutzer)	SQL-Server-Host (3.000 Benutzer)	PolicyServer und SQL-Server (1.500 Benutzer)
• 2 GHz Dual Quad Core Core2 Intel™ Xeon™ Prozessoren • 4GB RAM • 40 GB Festplattenspeicher	• 2 GHz Dual Quad Core Core2 Intel™ Xeon™ Prozessoren • 8GB RAM • 100GB Festplattenspeicher	• 2 GHz Quad Core Core2 Intel™ Xeon™ Prozessoren • 8GB RAM • 120GB Festplattenspeicher

TABELLE 1-3. Software-Mindestvoraussetzungen für PolicyServer

FUNKTION	VORAUSSETZUNG
Betriebssystem	• Windows Server 2003 SP2 32/64 Bit • Windows Server 2008 oder 2008 R2 64 Bit

Anwendungen und Einstellungen	• Anwendungsserver
	  • IIS
	  • ASP (Active Server Pages) zulassen
	  • ASP.NET zulassen
	• .Net Framework 2.0 SP2
	
	Hinweis
	PolicyServer 3.1.3 benötigt zwei IIS-Standorte. Die PolicyServer-Verwaltungsschnittstelle und die Client-Anwendungsschnittstelle müssen an verschiedenen IIS-Speicherorten installiert werden.

FUNKTION	VORAUSSETZUNG
Datenbank	• Microsoft SQL 2005/2008/2008 R2 • Microsoft SQL Express 2005(SP3)/2008 • Mixed Mode Authentication (SA-Kennwort) installiert • Berichtsdienste installiert

TABELLE 1-4. Full Disk Encryption Systemvoraussetzungen

VORGANG	VORAUSSETZUNG
Prozessor	Intel™ Core™ 2 oder kompatibler Prozessor.
Arbeitsspeicher	• Mindestens: 1GB
Festplattenspeicher	• Mindestens: 30GB • Erforderlich: 20% verfügbaren Festplattenspeicher • Erforderlich: 256 MB zusammenhängender freier Speicher
Netzwerkverbindung	Kommunikation mit PolicyServer 3.1.3 für verwaltete Installationen erforderlich
Betriebssysteme	• Windows 8™ (32/64 Bit) • Windows 7™ (32/64 Bit) • Windows Vista™ mit SP1 (32/64 Bit) • Windows XP™ mit SP3 (32 Bit)

VORGANG	VORAUSSETZUNG
Andere Software	Weitere Voraussetzungen für Windows 8: • Microsoft .NET Framework 3.5 ist aktiviert • Informationen zum Ändern der Startreihenfolge für Geräte mit UEFI finden Sie unter *Vorbereiten des Geräts auf Seite 4-5*. Weitere Voraussetzungen für Clients unter Windows XP: • Microsoft .NET Framework 2.0 SP1 oder höher • Microsoft Windows Installer 3.1
Festplatte	• Seagate DriveTrust-Laufwerke • Seagate OPAL- und OPAL 2-Laufwerke **Hinweis** • RAID- und SCSI-Festplatten werden nicht unterstützt. • Full Disk Encryption für Windows 8 unterstützt keine RAID-, SCSI-, eDrive- oder OPAL 2-Laufwerke.
Andere Hardware	ATA-, AHCI- oder IRRT-Festplattencontroller

TABELLE 1-5. Systemvoraussetzungen für FileArmor

VORGANG	VORAUSSETZUNG
Prozessor	Intel™ Core™ 2 oder kompatibler Prozessor.
Arbeitsspeicher	• Mindestens: 512MB • Empfohlen: 1GB
Festplattenspeicher	• Mindestens: 2GB • Erforderlich: 20% verfügbaren Festplattenspeicher
Netzwerkverbindung	Kommunikation mit PolicyServer für verwaltete Installationen erforderlich

VORGANG	VORAUSSETZUNG
Betriebssysteme	• Windows 8™ (32/64 Bit) • Windows 7™ (32/64 Bit) • Windows Vista™ mit SP1 (32/64 Bit) • Windows XP™ mit SP3 (32 Bit)
Andere Software	Weitere Voraussetzungen für Windows 8: • Microsoft .NET Framework 3.5 ist aktiviert • Informationen zum Ändern der Startreihenfolge für Geräte mit UEFI finden Sie unter *Vorbereiten des Geräts auf Seite 4-5*. Weitere Voraussetzungen für Clients unter Windows XP: • Microsoft .NET Framework 2.0 SP1 oder höher • Microsoft Windows Installer 3.1

TABELLE 1-6. Systemvoraussetzungen für KeyArmor

VORGANG	VORAUSSETZUNG
Hardware	USB-2.0-Port
Netzwerkverbindung	Kommunikation mit PolicyServer für verwaltete Installationen erforderlich
Betriebssysteme	• Windows 7™ (32/64 Bit) • Windows Vista™ mit SP1 (32/64 Bit) • Windows XP™ mit SP3 (32 Bit)
Andere Software	Weitere erforderliche Software bei der Installation auf Windows XP™: • Microsoft .NET Framework 2.0 SP1 oder höher

Wichtigste Funktionen und Vorteile

Endpoint Encryption umfasst die folgenden Funktionen und bietet die folgenden Vorteile:

TABELLE 1-7. Wichtigste Funktionen in Endpoint Encryption

FUNKTION	VORTEILE
Verschlüsselung	• Schutz durch Full Disk Encryption, einschließlich MBR (Master Boot Record), Betriebssystem und alle Systemdateien. • Hardware- und Software-basierte Verschlüsselung für gemischte Umgebungen.
Authentifizierung	• Flexible Authentifizierungsmethoden, einschließlich Einzel- und Multi-Faktor-Authentifizierung. • Richtlinienaktualisierungen vor der Authentifizierung und dem Systemstart. • Konfigurierbare Aktionen für den Schwellenwert für die Eingabe falscher Kennwörter.
Geräteverwaltung	• Richtlinien zum Schutz von Daten auf PCs, Laptops, Tablets, USB-Laufwerken, CDs und DVDs. • Möglichkeit zum Sperren, Löschen oder Auslöschen eines Geräts.
Zentrale Verwaltung	• Vollzugriff auf Verschlüsselung, Überwachung und Datenschutz. • Automatisierte Durchsetzung von Richtlinien mit Korrekturen an Sicherheitsereignissen.
Aufzeichnung von Protokollen, Berichten und Auditing	• Analysieren von Nutzungsstatistik mit geplanten Berichten und Warnmeldungen.

Verwaltung und Integration

Wenn Endbenutzer einen verstärkten Datenschutz auf verschiedenen Gerätetypen benötigen, von denen die meisten unterschiedliche Verschlüsselungstypen erfordern, senkt eine zentral verwaltete und integrierte Endpunktverschlüsselungslösung die Verwaltungs- und Wartungskosten. Endpoint Encryption ist eine zentral verwaltete Lösung, die folgende Datenschutzfunktionen ermöglicht:

- Zentrales und transparentes Aktualisieren der Endpunktverschlüsselungs-Clients, wenn neue Versionen veröffentlicht werden
- Verwalten und Nutzen von Sicherheitsrichtlinien für Einzelpersonen und Gruppen von einem einzigen Richtlinienserver aus
- Steuern der Kennwortstärke und Regelmäßigkeit von Kennwortänderungen
- Aktualisieren von Sicherheitsrichtlinien in Echtzeit vor der Authentifizierung, um Benutzer-Anmeldedaten vor dem Booten des Betriebssystems zu widerrufen

Verschlüsselung verstehen

Verschlüsselung bezeichnet den Vorgang, mit dem Daten unlesbar gemacht werden, wenn kein Zugriff auf den zur Verschlüsselung verwendeten Schlüssel besteht. Die Verschlüsselung kann durch eine Software- oder Hardware-basierte Verschlüsselung (oder eine Kombination aus beidem) vorgenommen werden, um sicherzustellen, dass Daten lokal auf einem Gerät, auf einem Wechselmedium, in bestimmten Dateien und Ordnern und beim Durchqueren von Netzwerken oder des Internets geschützt werden. Die Endpunktverschlüsselung ist das wichtigste Mittel, um die Datensicherheit zu gewährleisten und die Einhaltung gesetzlicher Vorschriften zum Datenschutz sicherzustellen.

Dateiverschlüsselung

FileArmor schützt einzelne Dateien und Ordner auf lokalen Festplatten und auf Wechselmedien (USB-Laufwerken). Administratoren können Richtlinien festlegen, die angeben, welche Ordner und Laufwerke auf dem Gerät verschlüsselt sind, und die

Richtlinien zu verschlüsselten Daten auf Wechselmedien festlegen. Die Datei- und Ordnerverschlüsselung wird durchgeführt, nachdem die Authentifizierung stattgefunden hat.

FileArmor kann auch verschiedene Dateien mit unterschiedlichen Schlüsseln schützen, was Administratoren ermöglicht, Zugriffsrichtlinien für ein Gerät und separate Richtlinien für den Zugriff auf bestimmte Dateien festzulegen. Dies ist in Umgebungen nützlich, in denen mehrere Benutzer auf einen Endpunkt zugreifen.

Full Disk Encryption

Full Disk Encryption ist die häufigste Verschlüsselungslösung, die heute auf Endpunkten eingesetzt wird, weil Sie alle Laufwerksdaten inkl. dem Betriebssystem, Programmdateien, temporäre Dateien und Endbenutzerdateien sichert. Viele Full Disk Encryption Anwendungen erhöhen zudem die Betriebssystemsicherheit, indem sie den Benutzer dazu auffordern, sich vor dem Starten bzw. Entsperren des Laufwerks und vor dem Zugriff auf das Betriebssystem zu authentifizieren.

Als eine Verschlüsselungslösung bietet Trend Micro Full Disk Encryption sowohl Software-basierte als auch Hardware-basierte Verschlüsselung. Während Hardware-basierte Verschlüsselung leichter auf neuer Hardware bereitgestellt und verwaltet werden kann und eine höhere Leistungsstufe bietet, ist für die Software-basierte Verschlüsselung keine Hardware erforderlich und die Bereitstellung auf vorhandenen Endpunkten ist billiger. Trend Micro PolicyServer kann Full Disk Encryption zentral verwalten und bietet Unternehmen die Flexibilität, Software-basierte oder Hardware-basierte verschlüsselte Geräte nach Bedarf einzusetzen.

Einzigartig an Endpoint Encryption ist eine netzwerkorientierte Funktion, die Richtlinien in Echtzeit aktualisiert, bevor die Authentifizierung zugelassen wird. Endpoint Encryption ermöglicht Administratoren, ein Laufwerk zu sperren oder per Wipe zu löschen, bevor auf das Betriebssystem (und auf vertrauliche Daten) zugegriffen werden kann.

Schlüsselverwaltung

Nicht verwaltete Verschlüsselungsprodukte erfordern, dass Administratoren oder Benutzer den Verschlüsselungsschlüssel auf einem USB-Gerät aufbewahren. Endpoint

Encryption sichert und hinterlegt Verschlüsselungsschlüssel transparent, während es einem Administrator ermöglicht, sich mit einem Administratorschlüssel bei dem geschützten Gerät anzumelden, um geschützte Daten wiederherzustellen.

KeyArmor USB-Geräte schützen Daten mit ständig verfügbarer Hardware-Verschlüsselung und integriertem Antivirus-/Anti-Malware-Schutz, um strenge gesetzliche Vorschriften und Richtlinien zu erfüllen. Mit KeyArmor haben Administratoren vollständige Transparenz und Kontrolle darüber, wer USB-Geräte zu welchem Zeitpunkt, an welchem Ort im Unternehmen und auf welche Weise einsetzt.

Info über FIPS

Die *Federal Information Processing Standard (FIPS) Publication 140-2* ist ein Gerätesicherheitsstandard der US-amerikanischen Regierung, der die Sicherheitsstandards für Verschlüsselungsmodule vorgibt. FIPS 140-2 beinhaltet vier Sicherheitsstufen:

TABELLE 1-8. FIPS 140-2-Sicherheitsstufen

STUFE	BESCHREIBUNG
Stufe 1	Alle Verschlüsselungskomponenten müssen sich auf der Produktionsstufe befinden und dürfen keine Sicherheitslücken aufweisen.
Stufe 2	Beinhaltet alle Anforderungen von Stufe 1 und fügt physischen Manipulationsbeweis und rollenbasierte Authentifizierung hinzu.
Stufe 3	Beinhaltet alle Anforderungen von Stufe 2 und fügt physischen Manipulationswiderstand und identitätsbasierte Authentifizierung hinzu.
Stufe 4	Beinhaltet alle Anforderungen von Stufe 3 und fügt weitere physische Sicherheitsanforderungen hinzu.

Endpoint Encryption stellt einen durchgängigen Datenschutz durch die Verschlüsselung gemäß FIPS 140-2 für Daten auf dem Policy Server bereit: alle Daten, die zwischen dem PolicyServer und Endpunkt-Clients übertragen werden, alle Daten, die auf dem Endpunkt-Gerät gespeichert werden sowie alle lokal gespeicherten Client-Protokolle.

Kapitel 2

Überlegungen zur Verteilung

Wenn ein Verschlüsselungsprojekt umgesetzt werden sUnternehmen, die explizite Anforderungen hinsichtlich der Einhaltung gesetzlicher Bestimmungen erfüllen müssen, benötigen häufig weiter gefasste Verschlüsselungslösungen mit einem Schwerpunkt auf der Berichterstellung, während Unternehmen, die die Datensicherheit erhöhen möchten, möglicherweise gezieltere Bedürfnisse für den Schutz spezifischer Daten-Assets haben.oll, ist es wichtig, die Implementierungsziele zu identifizieren. Unternehmen, die explizite Anforderungen hinsichtlich der Einhaltung gesetzlicher Bestimmungen erfüllen müssen, benötigen häufig weiter gefasste Verschlüsselungslösungen mit einem Schwerpunkt auf der Berichterstellung, während Unternehmen, die die Datensicherheit erhöhen möchten, möglicherweise gezieltere Bedürfnisse für den Schutz spezifischer Daten-Assets haben.

Ein einzelner Plan ist nicht für jedes Anwendungsszenario passend. Das Verständnis davon, was von einer Verschlüsselungslösung verlangt wird, verkürzt die Verteilungszeiten bedeutend, minimiert oder verhindert einen Leistungsabfall und stellt den Erfolg des Projekts sicher. Es ist eine sorgfältige Planung erforderlich, um die Verteilungsanforderungen und Einschränkungen für die Skalierung von Endpoint Encryptio für Endpunkte in einem großen Unternehmen zu verstehen. Die Planung ist besonders wichtig, wenn diese Änderung auf Tausenden von Endpunkten mit Auswirkungen auf alle Endbenutzer umgesetzt wird.

Dieses Kapitel umfasst folgende Themen:

Unterstützte Plattformen und Checkliste vor der Verteilung

In den folgenden Tabellen werden die unterstützten Betriebssysteme und Bereitstellungsvoraussetzungen für die einzelnen Trend Micro Endpoint Encryption Clients aufgeführt.

TABELLE 2-1. POLICYSERVER 3.1.3

UNTERSTÜTZTE PLATTFORMEN	CHECKLISTE VOR DER VERTEILUNG
Windows Server 2003 (32/64-Bit-Version) Windows Server 2008/2008 R2 (64-Bit-Version)	• Stellen Sie sicher, dass Microsoft .NET 2.0 SP2 oder höher auf dem Host-Computer installiert ist. • Verwenden Sie ein Admin-Konto für die Installation von PolicyServer MMC. • Zum Authentifizieren bei MMC ist eine Verbindung zum PolicyServer erforderlich.

TABELLE 2-2. Full Disk Encryption

UNTERSTÜTZTE PLATTFORMEN	CHECKLISTE VOR DER VERTEILUNG
Windows 8™ (32/64 Bit)	• Bei UEFI-kompatiblen Geräten muss die Startreihenfolge im BIOS auf "Legacy First" statt "UEFI First" festgelegt werden. • Vergewissern Sie sich, dass Microsoft .Net 3.5 aktiviert ist. • Führen Sie "scandisk" und "defrag" vor der Installation aus. • Bestätigen Sie, dass ein normaler Master Boot Record (MBR) vorliegt. • 20% verfügbaren Festplattenspeicher • Sichern Sie die Benutzerdaten. **Hinweis** Full Disk Encryption für Windows 8 unterstützt keine RAID-, SCSI-, eDrive- oder OPAL 2-Laufwerke.
Windows 7™ (32/64 Bit) Windows Vista™ mit SP1 (32/64 Bit) Windows XP™ mit SP3 (32 Bit)	• Vergewissern Sie sich, dass Microsoft .NET 2.0 SP1 oder höher installiert ist. • Windows Installer 3.1 • Wenn verwaltet: Verbindung zu PolicyServer • Führen Sie "scandisk" und "defrag" vor der Installation aus. • Bestätigen Sie, dass ein normaler Master Boot Record (MBR) vorliegt. • 20% verfügbaren Festplattenspeicher • Sichern Sie die Benutzerdaten. **Hinweis** Full Disk Encryption unterstützt keine RAID- oder SCSI-Laufwerke.

TABELLE 2-3. FileArmor 3.1.3

UNTERSTÜTZTE PLATTFORMEN	CHECKLISTE VOR DER VERTEILUNG
Windows 8™ (32/64 Bit)	• Bei UEFI-kompatiblen Geräten muss die Startreihenfolge im BIOS auf "Legacy First" statt "UEFI First" festgelegt werden. • Vergewissern Sie sich, dass Microsoft .Net 3.5 aktiviert ist.
Windows 7™ (32/64 Bit)	• Vergewissern Sie sich, dass Microsoft .NET 2.0 SP1 oder höher installiert ist.
Windows Vista™ mit SP1 (32/64 Bit)	
Windows XP™ mit SP3 (32 Bit)	

TABELLE 2-4. KeyArmor

UNTERSTÜTZTE PLATTFORMEN	CHECKLISTE VOR DER VERTEILUNG
Windows 8™ (32/64 Bit)	• Windows 8 wird nicht unterstützt.
Windows 7™ (32/64 Bit)	• USB-Port ist verfügbar
Windows Vista™ mit SP1 (32/64 Bit)	
Windows XP™ mit SP3 (32 Bit)	

Anfängliche Fragen zur Verteilung

Der Fragebogen unterstützt Sie bei der Definition des Projektteams, der Dokumentation Ihrer Betriebsumgebung, der Bewertung der Architekturanforderungen, der Ermöglichung der Prüfung von Desktop-Hardware- und -Software-Profilen und der Definition von Sicherheitsfragen und administrativen bzw. Support-Prozessen.

Endbenutzer:

1. Für wie viele Benutzer soll die Verteilung insgesamt durchgeführt werden?

2. Wie viele davon sind:
    - Administratoren des Unternehmens
    - Gruppen-Administratoren
    - Authentifizierer (Helpdesk-Mitarbeiter)
    - Endbenutzer

Endpunkt-Geräte:

1. Gibt es auf der Hardware eine Standard-Anzahl von Partitionen?
2. Besitzen die Geräte mehrere physische Festplatten?
3. Gibt es Geräte mit Dual-Boot-Managern?
4. Welche Standard-Software ist installiert? Prüfen Sie Folgendes:
    a. Virenschutz
    b. Sicherheitsanwendungen, die Software-Installationen blockieren
    c. Frühere Verschlüsselungsprodukte

Unternehmensnetzwerke und -datenbanken:

1. Wie viele PolicyServer werden zur Unterstützung der Benutzerbasis erforderlich sein?
    a. Schätzen Sie die maximale Benutzeranzahl für die nächsten drei Jahre.
    b. Falls die Domänenauthentifizierung verwendet wird, ist ein PolicyServer für jede Active Directory-Domäne erforderlich.
2. Ist eine Lastverteilung auf den Servern erforderlich?
    a. Die Lastverteilung wird für Installationen empfohlen, die Redundanz und hohe Verfügbarkeit für PolicyServer verlangen.
    b. Es kann Clustering verwendet werden, um Redundanz und hohe Verfügbarkeit für die Datenbankserver zu bieten.
3. Wie lauten die Schätzungen für die Datenbankgröße?

a. Schätzen Sie die maximale Benutzeranzahl für die nächsten drei Jahre.

b. Der Speicherplatzbedarf beträgt etwa 1 GB pro Jahr je 1.000 Endbenutzer.

4. Werden Endpunkt-Clients erforderlich sein, um über das Internet mit dem PolicyServer zu kommunizieren?

   a. Fragen Sie beim internen Netzwerk-/Sicherheits-Team nach, um die Anforderungen für das Verfügbarmachen eines Webservers im Internet zu verstehen.

   b. Folgendes wird mit einem von außen erreichbaren PolicyServer vollständig unterstützt:

   - Domänenauthentifizierung/Single-Sign-On kann über das Internet verwendet werden
   - Richtlinien-Updates über das Internet
   - Geräte-Auditing über das Internet
   - Online-Kennwortzurücksetzung

Projektteam zuweisen

Zu der erfolgreichen Implementierung eines Produkts gehören die Gewährleistung der Kontinuität sowie das Erzielen der Akzeptanz durch die internen Benutzer. Wenn das Team so strukturiert wird, dass es ein oder mehrere strategische Mitglieder aus den von der Software-Verteilung betroffenen Abteilungen umfasst, kann dies das Erzielen eine Akzeptanz unterstützen und die Führungsstärke des Projektteams erhöhen. Es wird empfohlen, dass Ihr Projektteam ein oder mehrere Mitglieder aus jeder der folgenden Gruppen umfassen sollte:

- Geschäftsleitung
- Anwendungsserver des Unternehmens
- Datenbank-Administratoren des Unternehmens
- Datensicherheit

- Desktop-Unterstützung
- Notfall-Wiederherstellung

Checkliste für die Sicherheitsinfrastruktur

Überprüfen Sie die bestehende Sicherheitsinfrastruktur, bevor Sie einen neuen IT-Dienst in der Produktionsumgebung verteilen. Trend Micro bietet eine Checkliste für die Sicherheitsinfrastruktur, die die Punkte enthält, die in folgenden Bereichen überprüft werden sollten:

- Endbenutzer
- Reaktion auf Vorfälle
- Risikobewertung
- Personalabteilung
- Einhaltung von Richtlinien

Weitere Informationen finden Sie unter *Checkliste für die Sicherheitsinfrastruktur auf Seite B-1*.

Richtlinien und Sicherheitsprofile erstellen

Trend Micro Endpoint Encryption verfügt über Standard-Sicherheitsrichtlinien, die im Hinblick auf die Verteilungs- und Schutzziele geprüft werden sollten. Neben weiteren Standard-Richtlinieneinstellungen gibt es Standard-Richtlinien für den Benutzernamen, die Kennwortkomplexität und Änderungsanforderungen, die Gerätesteuerung, die Richtliniensynchronisierung, die Gerätesperre und den Geräte-Wipe. Standard-Richtlinien können abhängig von den Sicherheitszielen und den Anforderungen hinsichtlich der Einhaltung von Gesetzesvorschriften zum Datenschutz einfach geändert werden.

Wenn Endpoint Encryption verwendet wird, um die Nutzung von USB-Medien und Wechselmedien zu steuern, sollte im Voraus entschieden werden, welche USB-Medien zugelassen werden und wann und wo diese verwendet werden können (innerhalb oder

außerhalb des Netzwerks; jederzeit), um sicherzustellen, dass die Benutzer Ihre Sicherheitsrichtlinien und -ziele einhalten.

Im Administratorhandbuch finden Sie eine vollständige Beschreibung der Richtlinien, Standardwerte und konfigurierbaren Optionen.

Hinweis

Wenn Endpoint Encryption zum Verwalten von Richtlinien und Wechselmedien verwendet wird:

- Testen und validieren Sie vor der Verteilung die Richtlinienvorlagen.
- Entscheiden Sie, welche USB-Geräte und Wechselmedien erlaubt sind und wann und wo diese verwendet werden können (im Netzwerk, außerhalb des Netzwerks oder beides), um sicherzustellen, dass die Benutzer die Sicherheitsvorgaben einhalten.

Die Wichtigkeit eines Pilotprogramms

Trend Micro empfiehlt das Ausführen eines Pilotprogramms und die Durchführung einer Testverteilung an eine kleine Gruppe von Benutzern, bevor die Verteilung an ein größeres Publikum erfolgt. Ein Pilotprogramm ermöglicht einem Unternehmen, die Installationsmethode, die bei der Installation von Endpoint Encryption angewendet werden soll, endgültig festzulegen. Die effektivsten Pilotprogramme schließen verschiedene Abteilungen, Zielbenutzer und Geräte ein. Wenn das Unternehmen beispielsweise zehn verschiedene Laptop-Hersteller unterstützt, sollte jedes dieser Geräte in das Pilotprogramm aufgenommen werden. Ebenso sollten, wenn bestimmte wichtige Gruppen speziell betroffen sind, ein oder zwei Mitglieder der Gruppe(n) am Pilotprogramm teilnehmen.

Weitere Informationen finden Sie unter *Checkliste für das Endpoint Encryption Pilotprogramm auf Seite A-1*.

Überlegungen zur Änderungsverwaltung

PolicyServer und die dazugehörigen Datenbanken sind unternehmenskritische Dienste. Überlegungen zur Änderungsverwaltung sind wichtig, um die Verfügbarkeit für

Endbenutzer, die sich im Netzwerk authentifizieren möchten, zu jeder Zeit sicherzustellen. Wenn Änderungen erforderlich sind:

- Überwachen Sie aktiv die CPU-Auslastung und legen Sie einen Schwellenwert dafür fest, wann der PolicyServer Windows-Dienst neu gestartet werden sollte.
- Starten Sie den Dienst regelmäßig gemäß einem Zeitplan entsprechend neu, der in etablierten Wartungsfenster des Unternehmens passt (täglich, wöchentlich, monatlich).
- Starten Sie den PolicyServer Windows Dienst immer dann neu, wenn Wartungsmaßnahmen für die Active Directory-Umgebung, den Server, die Datenbank oder zugehörige Kommunikation durchgeführt werden.
- Sichern Sie regelmäßig die PolicyServer Datenbanken, genau wie alle anderen unternehmenskritischen Datenbanken.
- Es wird empfohlen, primäre Datenbanken und Protokolldatenbanken nachts zu sichern und die Sicherungen in einem anderen Gebäude aufzubewahren.

Warnung!

Alle Änderungen an den Active Directory- oder Datenbank-Umgebungen können die Verbindung zum PolicyServer beeinträchtigen.

Endbenutzer-Kommunikation

Endbenutzer müssen im Rahmen eines gut durchdachten Kommunikationsplans vorab benachrichtigt werden, um unerwünschte Auswirkungen zu beschränken und den Übergang zu vereinfachen. Die Kommunikation nach der Verteilung spielt ebenfalls eine wichtige Rolle für den reibungslosen Einstieg in die Verwendung von Trend Micro Endpoint Encryption.

Zu beantwortende Fragen

Ein häufiges Hindernis für die Akzeptanz im Unternehmen ist mangelnde Kommunikation. Für eine erfolgreiche Implementierung sind klare Informationen für Endbenutzer erforderlich. Dabei müssen drei Fragen beantwortet werden:

1. Warum benötigen wir Endpoint Encryption?
2. Wie unterstützt Endpoint Encryption mich und das Unternehmen?
3. Was wird sich ändern?

Strategie eines schrittweisen Rollouts implementieren

Wenn Ihr Pilotprogramm erfolgreich war, beginnen Sie mit dem Verteilen des Programms, indem Sie schrittweise auf jeweils 25 bis 50 Endpunkt-Clients mit der Produktionsverteilung der Lösung beginnen. Stellen Sie sicher, dass sich einen Tag nach der Installation der neuen Lösung die Entwicklungsingenieure bei der ersten Bereitstellungsgruppe vor Ort befinden, damit unmittelbar Hilfe geleistet werden kann. Verteilen Sie die Lösung aufbauend auf den Erfahrungen der anfänglichen Gruppe von Endpunkt-Clients auf 100 bis 200 Endpunkt-Clients pro Nacht. Während Ihre Verteilungsmethode weiter in der Produktionsumgebung validiert wird und wenn Ihre internen IT- und Helpdesk-Teams zustimmen, können Tausende von Geräten für die gleichzeitige Verteilung festgelegt werden.

Erklären Sie den Benutzern die Aktionen, Termine und Gründe

Trend Micro empfiehlt, dass die leitende Person des Datenschutzprojekts eine Nachricht an die Endbenutzer schickt, in der die Bedeutung des Projekts für das Unternehmen und die Vorteile für die Benutzer herausgestellt wird. In unserer Knowledge Base befinden sich mehrere Vorlagen für die Endbenutzer-Kommunikation, die vor der Verteilung von Endpoint Encryption benutzt und an Ihre Kommunikationsanforderungen angepasst werden können.

Einführung der Änderung

1. Einen Monat vor dem Rollout sollte eine Person aus dem Management beschreiben, warum die neue Software-/Hardware-Verschlüsselung eingeführt wird und welche Vorteile für die Endbenutzer und das Unternehmen durch die Einhaltung der neuen Prozesse entstehen.

2. Teilen Sie den Benutzern einen Zeitplan für den Rollout mit und informieren Sie sie darüber, wie es nach Tag 1 weitergeht und wie sie Hilfe zur neuen Software erhalten können.

Kommunikation eine Woche vor dem Rollout

1. Wiederholen Sie, welche Änderungen kommen und was die Benutzer am Umstellungstag erwarten können, wenn neue Authentifizierungsverfahren für ihre PCs, mobilen Geräte und Wechseldatenträger erforderlich sind.
2. Fügen Sie Screenshots und detaillierte Anweisungen zum Benutzernamen, zu Kennwortkonventionen und zu anderen internen Support-Diensten hinzu.

Kommunikation am Tag vor dem Rollout

1. Bekräftigen Sie das Timing des Rollout-Zeitplans, welche Erwartungen erfüllt werden und an wen man sich zur Unterstützung wenden kann.
2. Verteilen Sie Merkzettel und Helpdesk-Informationen und geben Sie Kontaktinformationen für den Ansprechpartner vor Ort an, der verfügbar ist, um am nächsten Tag die Benutzer zu unterstützen.

Kommunikation nach dem Rollout

1. Wiederholen Sie die Helpdesk-Informationen und geben Sie die Kontaktinformationen für den Ansprechpartner vor Ort an, der verfügbar ist, um am nächsten Tag die Benutzer zu unterstützen.
2. Stellen Sie Tools zur Unterstützung der Fehlerbehebung bereit.

Skalierung: Anforderungen für PolicyServer und die SQL Datenbank

Nachfolgend finden Sie Empfehlungen für die Skalierung an einem einzelnen Standort, die verschiedene Hardware-Optionen für die Systemredundanz und keinen "Single Point of Failure" bietet.

TABELLE 2-5. Skalierung ohne Redundanz

GERÄTE	MINDESTSYSTEMVORAUSSETZUNGEN	
	POLICYSERVER FRONTEND	POLICYSERVER SQL DATENBANK
1,500	• PolicyServer und Datenbank-Mehrzweck-Server • 2 GHz Quad Core Core2 Intel™ Xeon™ Prozessoren • 8GB RAM • 120GB RAID 5 Festplattenspeicher	• Installiert auf PolicyServer Frontend-Host
3,000	• 1 PolicyServer Frontend-Host • 2 GHz Dual Quad Core Core2 Intel™ Xeon™ Prozessoren • 4GB RAM • 40GB RAID 1 Festplattenspeicher	• 1 PolicyServer SQL Datenbank-Host • 2 GHz Quad Core Core2 Intel™ Xeon™ Prozessoren • 8GB RAM • 100GB RAID 5 Festplattenspeicher

TABELLE 2-6. Skalierung mit Redundanz und hoher Verfügbarkeit

GERÄTE	MINDESTSYSTEMVORAUSSETZUNGEN	
	POLICYSERVER FRONTEND	POLICYSERVER SQL DATENBANK
10,000	• 2 PolicyServer Frontend-Hosts • 2 GHz Dual Quad Core Core2 Intel™ Xeon™ Prozessoren • 4GB RAM • 40GB RAID 1 Festplattenspeicher	• 1 PolicyServer SQL Datenbank-Hosts • 2 GHz Quad Core Core2 Intel™ Xeon™ Prozessoren • 8GB RAM • 120GB RAID 5 Festplattenspeicher

Geräte	Mindestsystemvoraussetzungen	
	PolicyServer Frontend	PolicyServer SQL Datenbank
20,000	• 4 PolicyServer Frontend-Hosts • 2 GHz Dual Quad Core2 Intel™ Xeon™ Prozessoren • 4GB RAM • 40GB RAID 1 Festplattenspeicher	• 1 PolicyServer SQL Datenbank-Hosts • 2 GHz Quad Core2 Intel™ Xeon™ Prozessoren • 16GB RAM • 160GB RAID 5 Festplattenspeicher
40,000	• 8 PolicyServer Frontend-Hosts • 2 GHz Dual Quad Core Core2 Intel™ Xeon™ Prozessoren • 4GB RAM • 40GB RAID 1 Festplattenspeicher	• 2 PolicyServer SQL Datenbank-Cluster-Hosts • 2 GHz Quad Core Core2 Intel™ Xeon™ Prozessoren • 16GB RAM • 320GB RAID 5 Festplattenspeicher

TABELLE 2-7. Skalierung ohne "Single Point of Failure"

GERÄTE	MINDESTSYSTEMVORAUSSETZUNGEN	
	POLICYSERVER FRONTEND	POLICYSERVER SQL DATENBANK
10,000	• 2 PolicyServer Frontend-Hosts • 2 GHz Quad Core Core2 Intel™ Xeon™ Prozessoren • 4GB RAM • 40GB RAID 1 Festplattenspeicher **Hinweis** Virtualisierte Hardware wird unter VMware Virtual Infrastructure unterstützt.	• 2 PolicyServer SQL Datenbank-Hosts • 2 GHz Dual Quad Core Core2 Intel™ Xeon™ Prozessoren • 8GB RAM • 60GB RAID 5 Festplattenspeicher • 130GB Festplattenspeicher auf gemeinsam genutzten RAID 5 SAN **Hinweis** Microsoft oder VMware auf virtualisierter Hardware bietet keine Unterstützung für den Microsoft Cluster Service.

Geräte	Mindestsystemvoraussetzungen	
	PolicyServer Frontend	PolicyServer SQL Datenbank
20,000	• 4 PolicyServer Frontend-Hosts • 2 GHz Dual Quad Core Core2 Intel™ Xeon™ Prozessoren • 4GB RAM • 40GB RAID 1 Festplattenspeicher **Hinweis** Virtualisierte Hardware wird unter VMware Virtual Infrastructure unterstützt.	• 2 PolicyServer SQL Datenbank-Hosts • 2 GHz Dual Quad Core Core2 Intel™ Xeon™ Prozessoren • 8GB RAM • 60GB RAID 5 Festplattenspeicher • 180GB Festplattenspeicher auf gemeinsam genutzten RAID 5 SAN **Hinweis** Microsoft oder VMware auf virtualisierter Hardware bietet keine Unterstützung für den Microsoft Cluster Service.

Geräte	Mindestsystemvoraussetzungen	
	PolicyServer Frontend	PolicyServer SQL Datenbank
40,000	• 8 PolicyServer Frontend-Hosts • 2 GHz Dual Quad Core Core2 Intel™ Xeon™ Prozessoren • 4GB RAM • 40GB RAID 1 Festplattenspeicher **Hinweis** Virtualisierte Hardware wird unter VMware Virtual Infrastructure unterstützt.	• 4 PolicyServer SQL Datenbank-Hosts • 2 GHz Dual Quad Core Core2 Intel™ Xeon™ Prozessoren • 16GB RAM • 60GB RAID 5 Festplattenspeicher • 350GB Festplattenspeicher auf gemeinsam genutzten RAID 5 SAN **Hinweis** Microsoft oder VMware auf virtualisierter Hardware bietet keine Unterstützung für den Microsoft Cluster Service.

Skalierungsbeispiel

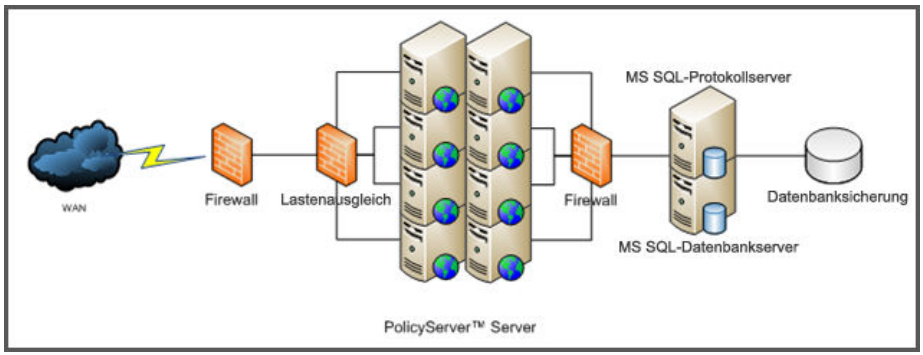


Abbildung 2-1. PolicyServer für die Unterstützung von 40.000 Benutzern skaliert

Kapitel 3

PolicyServer Installation

Dieses Kapitel gibt einen Überblick über die Installation von PolicyServer sowie über die Dateien und Konten, die hierfür benötigt werden.

In diesem Kapitel werden die folgenden Themen erläutert:

Einführung in PolicyServer

PolicyServer verwendet eine Microsoft Management-Konsole (MMC). PolicyServer hat eine hierarchische Struktur, die administrativen Verantwortlichkeiten verteilt und eine zentralisierte Steuerung aufrecht erhält, wenn:

- Parameter für Sicherheitsrichtlinien definiert werden
- Benutzer, Geräte und Gruppen (Offline-Gruppen) verwaltet werden
- Endpunktanwendungen aktiviert/deaktiviert werden

Verwenden Sie die Audit- und Berichterstellungsfunktionen von PolicyServer MMC, um die Sicherheitsinfrastruktur zu überwachen und die Einhaltung von Bestimmungen zu gewährleisten.

Inhalt des Installationsordners

Der Installationsordner für Trend Micro PolicyServer enthält die folgenden Installationsprogramme:

- `PolicyServerMMCSnapinSetup.msi`
- `PolicyServerInstaller.exe`
- `LDAProxyInstaller.exe`
- Tools

Außerdem wird folgende Datei benötigt:

- Die von Trend Micro erhaltene Lizenztextdatei und der Code zum Entsperren (Kennwort). Verwenden Sie die Lizenzdatei und den Code zum Entsperren, wenn Sie sich das erste Mal bei der PolicyServer MMC anmelden.

Hinweis

PolicyServer 3.1.3 enthält eine Testlizenz für 30 Tage. Weitere Informationen über die Testlizenz finden Sie unter *PolicyServer Datenbank und Web-Services installieren auf Seite 3-7*.

Voraussetzungen für PolicyServer

In diesem Abschnitt werden die Voraussetzungen für PolicyServer beschrieben, darunter die Hardware- und Software-Voraussetzungen, die zum Ausführen der Installationen erforderlichen Dateien sowie die zum Einrichten der Datenbank- und Windows-Server-Umgebungen benötigten Konten.

Hardware-Voraussetzungen

Für die Installation von PolicyServer wird empfohlen, dass mindestens zwei dedizierte Server zur Verfügung stehen:

1. Ein Server für die Datenbank. Alternativ können Sie die Datenbank zu einem vorhandenen SQL-Cluster hinzufügen.
2. Ein Server für den PolicyServer Service/Web-Service.

Hinweis

Virtualisierte Hardware wird unter VMware Virtual Infrastructure unterstützt.

TABELLE 3-1. Hardware-Voraussetzungen für PolicyServer

SEPARATE HOSTS		EINZELNER HOST
PolicyServer Host (3.000 Benutzer)	SQL-Server-Host (3.000 Benutzer)	PolicyServer und SQL-Server (1.500 Benutzer)
• 2 GHz Dual Quad Core Core2 Intel™ Xeon™ Prozessoren • 4GB RAM • 40 GB Festplattenspeicher	• 2 GHz Dual Quad Core Core2 Intel™ Xeon™ Prozessoren • 8GB RAM • 100GB Festplattenspeicher	• 2 GHz Quad Core Core2 Intel™ Xeon™ Prozessoren • 8GB RAM • 120GB Festplattenspeicher

Software-Voraussetzungen

TABELLE 3-2. Software-Mindestvoraussetzungen für PolicyServer

FUNKTION	VORAUSSETZUNG
Betriebssystem	• Windows Server 2003 SP2 32/64 Bit • Windows Server 2008 oder 2008 R2 64 Bit

Anwendungen und Einstellungen	• Anwendungsserver
	  ◦ IIS
	  ◦ ASP (Active Server Pages) zulassen
	  ◦ ASP.NET zulassen
	• .Net Framework 2.0 SP2
	
	Hinweis
	PolicyServer 3.1.3 benötigt zwei IIS-Standorte. Die PolicyServer-Verwaltungsschnittstelle und die Client-Anwendungsschnittstelle müssen an verschiedenen IIS-Speicherorten installiert werden.

Datenbank	• Microsoft SQL 2005/2008/2008 R2 • Microsoft SQL Express 2005(SP3)/2008 • Mixed Mode Authentication (SA-Kennwort) installiert • Berichtsdienste installiert

TABELLE 3-3. Überlegungen zur Software für Windows Server 2008 und 2008 R2

Server OS	2008	2008 R2

Rollen	• Anwendungsserverrolle installieren • IIS-Unterstützung hinzufügen • Webserverrolle installieren	• Anwendungsserverrolle installieren • IIS-Unterstützung hinzufügen • Webserverrolle installieren
Funktionen	• SMTP hinzufügen	• SMTP hinzufügen
Weitere Voraussetzungen	• .NET 3.5 SP1	• Zum Ausführen von SQL 2008 muss SQL 2008 SP1 installiert werden • Kein .NET-Upgrade erforderlich

Erforderliche Installationsdateien

TABELLE 3-4. Dateien, die für die Installation von PolicyServer benötigt werden

DATEI	ZWECK
`PolicyServerInstaller.exe`	Installiert PolicyServer Datenbanken und Dienste
`PolicyServerMMCSnapinSetup.msi`	Installiert die PolicyServer Management-Konsole als MMC-Snap-In
Lizenz	Wird von Trend Micro zur Verfügung gestellt. Für die erstmalige Authentifizierung bei der PolicyServer MMC erforderlich

Wichtig

Kopieren Sie vor der Installation alle Installationsdateien auf die lokale Festplatte.

Erforderliche Konten

Zum Installieren von PolicyServer müssen bestimmte Konten verfügbar sein. In der folgenden Tabelle werden die Konten und die Services, denen sie zugeordnet sind,

aufgeführt. Darüber hinaus wird erläutert, zu welchem Zweck PolicyServer die einzelnen Konten verwendet.

TABELLE 3-5. Konten, die für die Installation von PolicyServer benötigt werden

KONTO	DIENST	ZWECK
SQL SA	PolicyServer Installationsprogramm	Dieses Konto wird NUR zum Erstellen der PolicyServer Datenbanken verwendet.
SQL MADB	PolicyServer Windows-Dienst	Das Konto wird während der Installation zum Authentifizieren bei den PolicyServer Datenbanken erstellt.
Dienstkonto	PolicyServer Windows-Dienst und IIS	Über dieses Konto werden der PolicyServer Windows-Dienst und der Web-Service ausgeführt.
PolicyServer Enterprise Administrator	PolicyServer MMC	Dieses Konto wird von Trend Micro bereitgestellt (aus der Lizenzdatei). Es ist erforderlich, um PolicyServer MMC zum ersten Mal zu authentifizieren.

PolicyServer Installationsvorgang

Installieren Sie Microsoft SQL Server™, bevor Sie eine beliebige PolicyServer Installationsdatei ausführen. Die Installationsprogramme für die einzelnen PolicyServer Anwendungen sind so konfiguriert, dass die Installation unkompliziert und einfach ist.

Der Installationsvorgang:

1. Installieren Sie die Microsoft SQL Datenbank.

   Hinweis

   In diesem Dokument wird die Installation von Microsoft SQL nicht erläutert.

2. Installieren Sie die PolicyServer Datenbank und Dienste.

3. Installieren Sie PolicyServer MMC.

PolicyServer Datenbank und Web-Services installieren

Vorbereitungen

Microsoft SQL Server ist bereits eingerichtet.

Das PolicyServer Installationsprogramm konfiguriert Datenbankeinstellungen und installiert Windows Web-Services. Neu in PolicyServer 3.1.3 ist die Möglichkeit, eine Portnummer für den PolicyServer Web-Service anzugeben. Für den Client-Web-Service wird jetzt außerdem ein zweiter Port benötigt. Wenn kein zweiter Port vorhanden ist, wird während der Installation ein neuer Port erstellt. Weitere Informationen zur neuen Architektur finden Sie unter *Komponenten von Endpoint Encryption auf Seite 1-2*.

Um Endpoint Encryption testweise für eine begrenzte Zeit zu verwenden, können der Unternehmensname und das Konto für den Unternehmensadministrator zum Zeitpunkt der Installation konfiguriert werden. PolicyServer funktioniert normal mit allen Client-Anwendungen, einer unbegrenzten Zahl von Geräten und bis zu 100 Benutzern für einen Testzeitraum von 30 Tagen. Wenden Sie sich nach 30 Tagen an den Technischen Support, um eine Lizenzdatei zu erhalten. Nach Ablauf der Testzeitraums können sich Benutzer und Geräte weiterhin anmelden.

Prozedur

1. Führen Sie `PolicyServerInstaller.exe` aus.
2. Lesen Sie sich die Endbenutzer-Lizenzvereinbarung aufmerksam durch. Wenn Sie einverstanden sind, klicken Sie auf **Zustimmen**.
3. Überprüfen Sie im Fenster **PolicyServer Services** die PolicyServer Version und klicken Sie dann auf **Installieren**.
4. Die Standardeinstellungen im **Dienstanmeldungsfenster von Windows** sind für die meisten Installationen geeignet. Klicken Sie auf **Fortfahren**.
5. Geben Sie im **Datenbankadministrator-Anmeldefenster** den Host-Namen oder die IP-Adresse des Microsoft SQL Server sowie die Anmeldedaten eines Kontos mit der Sysadmin-Rolle für die angegebene SQL-Instanz an.

Hinweis

Bei Umgebungen mit mehreren SQL Server-Instanzen fügen Sie die SQL-Instanz ans Ende des PolicyServer Hostnamens oder die verwendete IP-Adresse an. Verwenden Sie zur Angabe einer Instanz die folgende Syntax:

```
<Hostname oder IP-Adresse>\<Datenbankinstanz>
```

Das Installationsprogramm überprüft die Datenbankverbindung.

6. Geben Sie im Fenster **Datenbankanmeldung** die Anmeldedaten eines Kontos für den Windows-Dienst PolicyServer an, das für alle Datentransaktionen verwendet werden soll. Wenn PolicyServer zum ersten Mal installiert wird, wird das angegebene Konto erstellt.

7. Geben Sie im Fenster **Web Service - Installationsspeicherort** den IIS-Standort an, den PolicyServer MMC und der Client-Web-Service für die Kommunikation mit PolicyServer verwenden sollen. Die Standardportnummer ist 8080. Ist Port 8080 bereits belegt, wird der nächste verfügbare Port zugewiesen.

   a. Wählen Sie eine Site aus dem Listenfeld **Ziel-Site** aus.

   b. Überprüfen Sie den aktuell zugewiesenen Port und geben Sie, falls erforderlich, im Feld **Neuer Port** eine andere Portnummer an.

   Hinweis

   Trend Micro empfiehlt, Port 80 für den Client-Web-Service zu reservieren.

   c. Klicken Sie auf **Fortfahren**.

8. Mit dem nächsten Schritt wird der Client-Web-Service - der IIS-Standort, den alle Endpoint Encryption Clients für die Kommunikation mit PolicyServer nutzen - konfiguriert. Abhängig davon, ob ein zweiter IIS-Standort verfügbar ist, wird eines der folgenden Fenster angezeigt:

   - Wenn ein zweiter IIS-Standort verfügbar ist, wird das Fenster **Speicherort für Client-Web-Service** angezeigt.

     a. Wählen Sie eine Site aus dem Listenfeld **Ziel-Site** aus.

     b. Überprüfen Sie die Standardportzuweisung für den Client-Web-Service.

Hinweis

Trend Micro empfiehlt, Port 80 beizubehalten. Falls erforderlich, können Sie jedoch im Feld **Neuer Port** eine andere Portnummer angeben. Die Portnummer muss eine positive Ganzzahl zwischen 1 und 65535 sein.

c. Klicken Sie auf **Fortfahren**.

- Wenn kein zweiter IIS-Standort verfügbar ist, wird das Fenster **Speicherort für Client-Web-Service erstellen** angezeigt, um einen neuen IIS-Standort erstellen zu können.

  a. Geben Sie im Feld **Name der Site** einen Namen für den IIS-Speicherort an.

  b. Suchen Sie nach dem Speicherort für die Site. Wenn noch kein Ordner vorhanden ist, erstellen Sie einen neuen.

  c. Geben Sie die IP-Adresse und Portnummer für den neuen IIS-Speicherort an.

  Hinweis

  Trend Micro empfiehlt, Port 80 beizubehalten. Falls erforderlich, können Sie jedoch eine andere Portnummer angeben. Die Portnummer muss eine positive Ganzzahl zwischen 1 und 65535 sein.

  d. Klicken Sie auf **Fortfahren**.

9. Überprüfen Sie die Einstellungen im Fenster **Mobile Web Service - Installationsspeicherort**, und klicken Sie dann auf **Fortfahren**.

10. Geben Sie im Fenster **Unternehmensnamen und Administrator-Anmeldung erstellen** den neuen Unternehmensnamen und die Anmeldedaten für ein neues Unternehmensadministrator-Konto an, das während des anfänglichen Testzeitraums zum Verwalten von PolicyServer verwendet wird.

11. Klicken Sie auf **Fortfahren**.

    Der Installationsvorgang wird gestartet.

12. Klicken Sie in der **PolicyServer Installation**-Meldung auf **OK**.

13. Klicken Sie auf **Beendet**.

14. Klicken Sie im Fenster des PolicyServer Installationsprogramms auf **Beenden**.

15. Starten Sie den Server neu.

PolicyServer MMC

Die PolicyServer Microsoft Management-Konsole (MMC) ist die grafische Benutzeroberfläche, über die Administratoren auf die Funktionen von PolicyServer zugreifen. Der PolicyServer MMC kombiniert eine hierarchische Struktur mit separaten Administrator- und Authentifiziererrollen. Unternehmen können so die administrativen Verantwortlichkeiten verteilen und weiterhin eine zentralisierte Steuerung aufrecht erhalten.

Über die PolicyServer MMC können Sie Folgendes verwalten:

- Alle Trend Micro Endpoint Encryption Anwendungen
- PolicyServer Benutzer und Gruppen (einschließlich Offline-Gruppen)
- Client-Geräte, z. B. Laptops, Desktop-Computer, PDAs, Smartphones und USB-Speichergeräte
- Alle Verschlüsselungs-, Kennwortkomplexitäts- und Authentifizierungsrichtlinien
- Ereignisprotokolle zum Anzeigen von Authentifizierungsereignissen, Verwaltungsereignissen und Sicherheitsverstößen sowie dem Geräteverschlüsselungsstatus
- Remote-Hilfe zum Zurücksetzen des Kennworts
- Funktion zum Sperren/Auslöschen des Geräts

Zudem bietet PolicyServer messbare Vorteile dank der Audit- und Berichterstellungsoptionen. Dadurch können Führungskräfte aus dem Unternehmen und andere Personen den Erfolg messen.

Eine detaillierte Beschreibung der Funktionen der PolicyServer MMC finden Sie im Endpoint Encryption Administratorhandbuch.

PolicyServer MMC installieren

Prozedur

1. Starten Sie `PolicyServerMMCSnapinSetup.msi`.

   Die Installation beginnt.

2. Klicken Sie auf **Weiter**, um den Setup-Assistenten für PolicyServer MMC zu öffnen.

3. Lesen Sie die Lizenzvereinbarung sorgfältig durch und wählen Sie anschließend **Ich stimme zu**, um den Bedingungen zuzustimmen. Klicken Sie dann auf **Weiter**.

4. Wählen Sie den Installationsordner aus oder verwenden Sie den vorgegebenen Speicherort, und klicken Sie auf **Weiter**.

5. Klicken Sie auf **Weiter**, um die Installation zu bestätigen.

   Der Installationsvorgang wird gestartet. Auf dem Desktop wird die Verknüpfung "PolicyServer MMC" erstellt.

6. Klicken Sie auf **Schließen**, um die Installation abzuschließen.

7. Klicken Sie auf **Ja**, um den Server neu zu starten.

8. Melden Sie sich wieder beim Server an und öffnen Sie PolicyServer MMC über die Desktop-Verknüpfung.

9. Nachdem PolicyServer MMC geöffnet wurde, führen Sie einen der folgenden Schritte aus:

   - Anmeldung mit Hilfe des Unternehmensnamens und Kontos für den Unternehmensadministrator, die bei der Installation der PolicyServer-Datenbanken und -Dienste erstellt wurden. Der 30-Tage-Testzeitraum ermöglicht unbegrenzte Geräte und bis zu 100 Benutzer.
   - Lizenzdatei importieren:

     Hinweis

     Nehmen Sie Kontakt mit den Support von Trend Micro, um eine Lizenzdatei zu erhalten.

a. Navigieren Sie zu **Datei** > **Lizenz importieren**.

b. Geben Sie den Code zum Entsperren ein und wählen Sie die Lizenzdatei aus. Klicken Sie anschließend auf **Update**.

c. Klicken Sie auf **OK**, wenn das Fenster **Lizenz aktualisiert** angezeigt wird.

Die PolicyServer Installation ist abgeschlossen. Authentifizieren Sie sich bei PolicyServer MMC. Verwenden Sie hierzu die Anmeldedaten des Unternehmensadministrators, die Sie von Trend Micro erhalten haben.

Nächste Maßnahme

1. Erstellen Sie ein Ersatzkonto des Typs "Unternehmensadministrator", und ändern Sie das Standardkennwort.
2. Aktivieren Sie alle Anwendungen, die innerhalb des Unternehmens verwendet werden, bevor Sie Testgruppen oder Gruppen für die endgültige Verteilung einrichten.
3. Eine Liste der empfohlenen Aufgaben nach der Installation, z. B. Geräte und Benutzer erstellen sowie Richtlinien festlegen, finden Sie im Endpoint Encryption Administratorhandbuch.

PolicyServer AD-Synchronisierung

PolicyServer unterstützt die Active Directory (AD)-Synchronisierung für eine konfigurierte PolicyServer Gruppe. Durch die Synchronisierung werden AD-Benutzer automatisch zu konfigurierten PolicyServer Gruppen hinzugefügt bzw. aus diesen entfernt.

Active Directory-Überblick

Für die PolicyServer AD-Synchronisierung sind drei Komponenten erforderlich:

1. Eine konfigurierte AD-Domäne.

2. Eine PolicyServer Gruppe, die so konfiguriert ist, dass sie auf eine gültige AD-Organisationseinheit (Organizational Unit, OU) verweist.

3. Entsprechende Anmeldedaten für den Zugriff auf die AD-Domäne, die mit dem eindeutigen Namen der PolicyServer Gruppe übereinstimmen.

Wenn die Synchronisierung ordnungsgemäß konfiguriert ist, erstellt sie automatisch neue PolicyServer Benutzer und verschiebt diese in die zugeordneten Gruppen auf dem PolicyServer. Während der Synchronisierung wird der PolicyServer aktualisiert, so dass die Benutzer und die Gruppenzuweisungen der zugeordneten Gruppen übereinstimmen.

Wenn ein neuer Benutzer zur Domäne hinzugefügt und in der Organisationseinheit platziert wird, wird dieser Benutzer markiert, so dass AD diesen Benutzer während der nächsten Synchronisierung in PolicyServer erstellt und anschließend in die zugeordnete PolicyServer Gruppe verschiebt.

Wenn ein Benutzer aus AD gelöscht wird, wird er automatisch aus der zugeordneten PolicyServer Gruppe und dem Unternehmen entfernt.

PolicyServer Administratoren können eigene Benutzer erstellen und sie zu den zugeordneten PolicyServer Gruppen hinzuzufügen, ohne dass diese Benutzer vom Synchronisierungssystem geändert werden. Dies ermöglicht den Administratoren, Nicht-Domänenbenutzer Gruppen hinzuzufügen, die mit der Domäne synchronisiert werden.

Wenn ein PolicyServer Administrator einen Benutzer manuell aus einer zugeordneten Gruppe auf dem PolicyServer entfernt, wird dieser Domänenbenutzer nicht wieder vom Synchronisierungssystem automatisch hinzugefügt. Dies verhindert das Überschreiben der Administratoraktion für diesen Benutzer. Wenn ein Administrator einen synchronisierten Domänenbenutzer manuell wieder in eine zugeordnete Gruppe verschiebt, beginnt das Synchronisierungssystem automatisch wieder damit, den Benutzer in der Gruppe zu verwalten.

Active Directory konfigurieren

Für diese Aufgabe wird vorausgesetzt, dass der Domänencontroller auf Windows Server 2003 eingerichtet wurde und AD installiert ist.

Prozedur

1. Navigieren Sie zu **Start** > **Programme** > **Verwaltung** > **Active Directory-Benutzer und -Computer**.

   Das Fenster "Active Directory-Benutzer und -Computer" wird geöffnet.

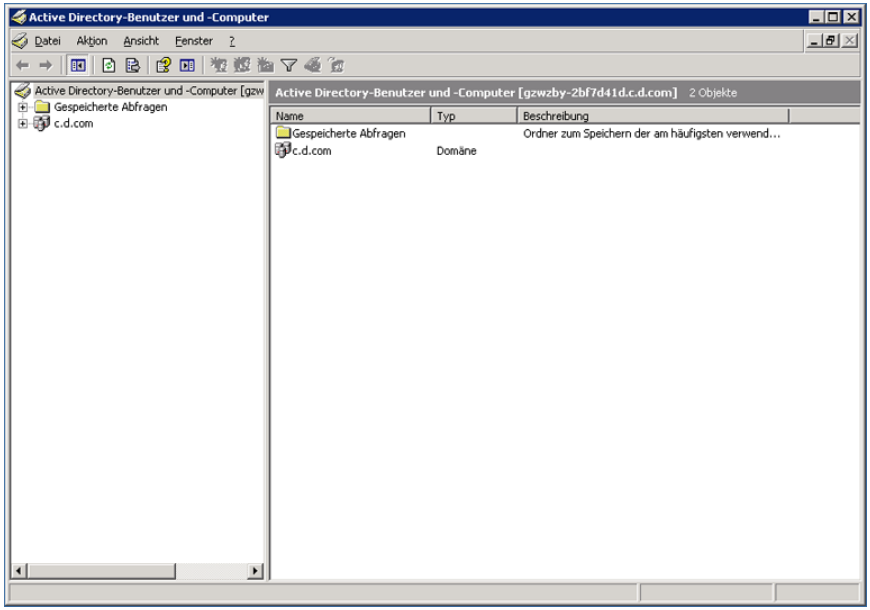


ABBILDUNG 3-1. Active Directory-Benutzer und -Computer

2. Klicken Sie mit der rechten Maustaste auf die neue Domäne, die bei der Installation von AD erstellt wurde, und wählen Sie **Neu** aus.

3. Wählen Sie **Organisationseinheit** aus.

4. Klicken Sie auf **Weiter**.

5. Geben Sie im Fenster **Neues Objekt - Organisationseinheit** den neuen Namen an und klicken Sie auf **OK**.

   Die neue Gruppe wird in der linken Navigation unter der Domäne angezeigt.

Die neue Gruppe wird zur Synchronisierung mit einer PolicyServer Gruppe verwendet. Zunächst müssen jedoch Benutzer zur Gruppe hinzugefügt werden.

6. Klicken Sie mit der rechten Maustaste auf die neue Gruppe und wählen Sie **Neuer Benutzer** aus.

7. Geben Sie im Fenster **Neues Objekt - Benutzer** die Kontoinformationen des neuen Benutzers an und klicken Sie auf **Weiter**.

8. Geben Sie das Domänenkennwort des neuen Benutzers an, und bestätigen Sie es. Klicken Sie auf **Weiter**, um fortzufahren.

Hinweis

Deaktivieren Sie die Option **Benutzer muss Kennwort bei nächster Anmeldung ändern** und aktivieren Sie die Option **Kennwort läuft nie ab**, um weitere Tests zu einem späteren Zeitpunkt zu vereinfachen.

9. Wenn die Installation abgeschlossen ist, klicken Sie auf **Fertig stellen**.

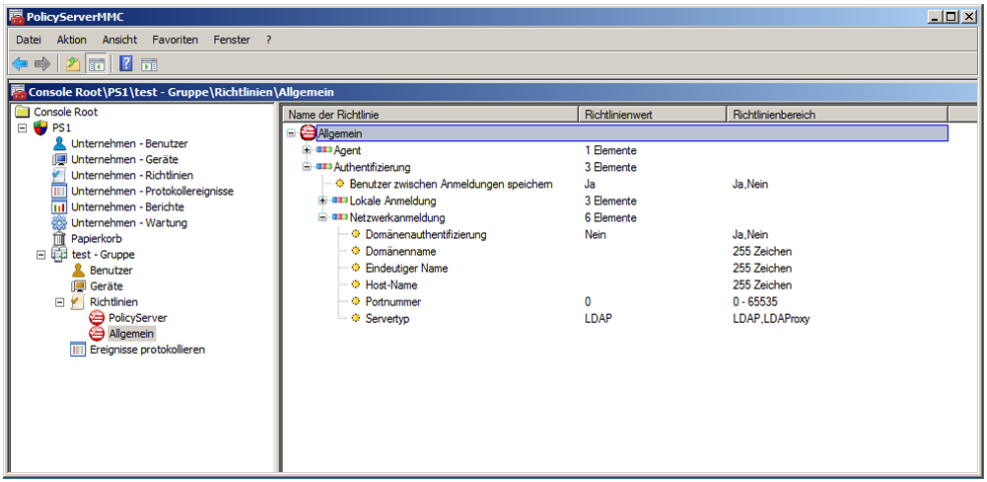
   Der Domänencontroller ist mit einer neuen Organisationseinheit und einem Benutzer in dieser Gruppe konfiguriert. Um diese Gruppe mit PolicyServer zu synchronisieren, installieren Sie PolicyServer, und erstellen Sie eine Gruppe für die Synchronisierung. Für den nächsten Abschnitt wird vorausgesetzt, dass PolicyServer bereits installiert ist.

10. Melden Sie sich bei PolicyServer MMC an.

11. Klicken Sie mit der rechten Maustaste auf das Unternehmen und wählen Sie **Top-Gruppe hinzufügen**.

12. Geben Sie den Namen und die Beschreibung für die Gruppe an und klicken Sie anschließend auf **Anwenden**.

13. Um die Synchronisierungsrichtlinie zu konfigurieren, öffnen Sie die Gruppe und navigieren Sie zu **Allgemein** > **Authentifizierung** > **Netzwerkanmeldung**.



14. Öffnen Sie **Eindeutiger Name**, und geben Sie den vollständig qualifizierten eindeutigen Namen aus der konfigurierten AD-Organisation an, die mit dieser Gruppe synchronisiert werden soll. Klicken Sie anschließend auf **OK**.

Hinweis

Das Format für den eindeutigen Namen einer Organisationseinheit namens "Engineering" auf der Domäne "test.home" ist:
`OU=Engineering,DC=TEST,DC=HOME`

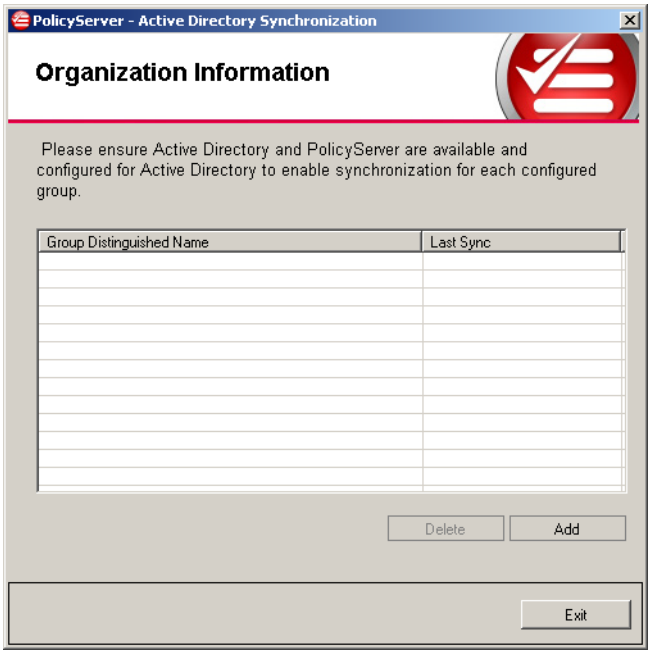
---

15. Öffnen Sie **Domänenname**, und geben Sie den NetBIOS-Domänennamen an, der zum Konfigurieren des AD-Servers verwendet wurde.

    Nachdem die PolicyServer Richtlinie konfiguriert wurde, ist als letzter Konfigurationsvorgang die Erstellung der Synchronisierungskonfiguration über das AD Synchronization Configuration Tool erforderlich. Dieses Tool ermöglicht den Administratoren, für jede synchronisierte Organisationseinheit und jeden Domänencontroller separate AD-Anmeldedaten zu erstellen.

16. Um auf das **AC Synchronization Configuration** Tool zuzugreifen, navigieren Sie zum Installationsordner von PolicyServer und öffnen Sie **ADSyncConfiguration.exe**.

    Das Fenster "PolicyServer - AD Synchronization Tool" wird geöffnet.



17. Klicken Sie auf **Add**, um die Anmeldedaten für die AD-Organisationseinheit anzugeben.

Hinweis

Für Server, die zusätzliche Anmeldedaten erfordern, können die Benutzer den entsprechenden Administrator-Benutzernamen und das Administrator-Kennwort eingeben, um über dieses Tool eine Verbindung zum Domänencontroller herzustellen.

---

18. Beenden Sie das **ADSyncConfiguration** Tool.

Die Synchronisierung zwischen dem AD und PolicyServer ist abgeschlossen. Die Synchronisierung erfolgt automatisch alle 45 Minuten (dies ist das standardmäßig von Microsoft Domänencontrollern verwendete Synchronisierungsintervall). Sie können eine Synchronisierung erzwingen, indem Sie den PolicyServer Windows-Dienst anhalten und

neu starten. Die Domänensynchronisierung wird kurz nach dem Start des PolicyServer Windows-Dienstes und anschließend alle 45 Minuten ausgeführt.

LDAP-Proxy (optional)

Die optionale Funktion LDAP-Proxy ermöglicht die Domänenauthentifizierung bzw. das Single-Sign-On (SSO) über einen externen Proxy-Server in der DMZ des Kunden.

Hinweis

- Die LDAP-Proxy-Installation ist in gehosteten Umgebungen, die Domänenauthentifizierung/Single-Sign-On (SSO) verwenden, erforderlich.
- LDAP-Proxy-Versionen vor 3.1 werden nicht mehr unterstützt.
- Kunden, die eine ältere LDAP-Proxy-Version verwenden, müssen ein Upgrade auf Version 3.1 durchführen.

LDAP-Voraussetzungen

TABELLE 3-6. Hardware- und Softwarespezifikationen für LDAP

VORGANG	VORAUSSETZUNG
Prozessor	Intel™ Core™ 2 oder kompatibler Prozessor.
Arbeitsspeicher	• Mindestens: 2GB
Festplattenspeicher	• Mindestens: 30GB • Erforderlich: 20% verfügbaren Festplattenspeicher

Vorgang	Voraussetzung
Netzwerkverbindung	• Der Server muss sich in der Domäne befinden und Zugriff auf AD haben. • Die Serveradresse muss über das Internet zugänglich sein. • Eingehende Proxy-Verbindungen müssen zugelassen werden. • PolicyServer muss Zugriff auf den IIS-Server dieses Servers haben.
Betriebssysteme	• Windows Server 2003 32/64 Bit • Windows Server 2008 oder 2008 R2 32/64 Bit

Anwendungen und Einstellungen	• Anwendungsserverrolle
	  • IIS
	  • ASP (Active Server Pages) zulassen
	  • ASP.NET zulassen
	• .Net Framework 2.0 SP2

Checkliste für LDAP-Proxy-Hardware

Tabelle 3-7. Checkliste für LDAP-Proxy-Hardware

LDAP-Proxy-Server		Anmerkungen
Angaben zu Windows Server	Betriebssystemversion	
	Service-Pack-Version	
Angaben zur Hardware	Marke	
	RAM	
	Modell	
	CPU	

LDAP-Proxy-Server		Anmerkungen
Installierte Software auf dem Server	IIS	
	Microsoft .NET SP 2.0 Sp1 oder höher	
Angaben zum Netzwerk	IP-Adresse	
	Subnetzmaske	
	Host-Name	
	Domänenname	
	Verfügbare Anmeldedaten der Domäne (nur für SSO)	

Kapitel 4

Endpoint Encryption Client-Installation

Jede Endpoint Encryption-Anwendung hat eigene Installations- und Systemanforderungen. Detaillierte Erläuterungen zur Konfiguration und Verwendung von Endpunkt-Anwendungen finden Sie im Endpoint Encryption Administratorhandbuch.

In diesem Kapitel werden die folgenden Themen erläutert:

Überlegungen zur Installationsvorbereitung

Bevor Sie mit der Installation beginnen, beachten Sie Folgendes:

- Kopieren Sie alle Endpunkt-Client-Installationsdateien auf das Gerät.
- Für alle Endpunkt-Client-Anwendungen wird Microsoft .NET Framework 2.0 SP1 oder höher benötigt.

  Hinweis

  Zum Installieren von Endpunkt-Clients unter Windows 8 ist Kompatibilität mit Microsoft .NET Framework 3.5 erforderlich.

- Die Installation von Full Disk Encryption und FileArmor kann automatisiert werden.
- Für alle Produkinstallationen werden Administratorrechte benötigt.

Weitere Informationen zu unterstützten Plattformen und anderen Überlegungen vor der Verteilung finden Sie unter *Unterstützte Plattformen und Checkliste vor der Verteilung auf Seite 2-3*.

Installieren von Full Disk Encryption

Full Disk Encryption wurde dafür entwickelt, mit Hilfe von obligatorischer starker Authentifizierung und Full Disk Encryption eine umfassende Endpunkt-Datensicherheit zu bieten. Full Disk Encryption sichert nicht nur die Datendateien, sondern darüber hinaus alle Anwendungen, Registrierungseinstellungen, temporären Dateien, Auslagerungsdateien, Druck-Spooler und gelöschten Dateien. Eine starke Preboot-Authentifizierung beschränkt den Zugriff auf das anfällige Host-Betriebssystem, bis der Benutzer validiert wird.

Optionen vor der Verteilung

Um die Auswirkungen auf den Endbenutzer auf ein Minimum zu reduzieren und die Verteilung auf viele Geräte zu vereinfachen, deaktivieren Sie die

Laufwerkverschlüsselung vorübergehend. Sobald die Kompatibilität bestätigt ist, kann die Verschlüsselung im Rahmen des Standard-Produkt-Rollouts wieder aktiviert werden.

TABELLE 4-1. Geräteverschlüsselung aktivieren/deaktivieren

KONFIGURATIONSEINSTELLUNG	OPTIONEN	POLICYSERVER PFAD
Geräteverschlüsselung	Ja/Nein	**Full Disk Encryption** > **PC** > **Verschlüsselung** > **Gerät verschlüsseln**

Installationsvoraussetzungen

Das Installationsprogramm von Full Disk Encryption überprüft das Zielsystem, um sicherzustellen, dass alle erforderlichen Systemvoraussetzungen vor der Installation der Anwendung erfüllt sind. Weitere Informationen finden Sie in der Datei `PreInstallCheckReport.txt`, die nach der Ausführung des Installationsprogramms im Installationsverzeichnis abgelegt wird.

Ausführliche Informationen über die Systemüberprüfung und die Voraussetzungen finden Sie unter *Installationsvoraussetzungen für Full Disk Encryption auf Seite C-1*

Full Disk Encryption Systemvoraussetzungen

In diesem Abschnitt werden die minimalen und empfohlenen Systemanforderungen zur Installation von Full Disk Encryption beschrieben.

TABELLE 4-2. Full Disk Encryption Systemvoraussetzungen

VORGANG	VORAUSSETZUNG
Prozessor	Intel™ Core™ 2 oder kompatibler Prozessor.
Arbeitsspeicher	• Mindestens: 1GB
Festplattenspeicher	• Mindestens: 30GB • Erforderlich: 20% verfügbaren Festplattenspeicher • Erforderlich: 256 MB zusammenhängender freier Speicher

VORGANG	VORAUSSETZUNG
Netzwerkverbindung	Kommunikation mit PolicyServer 3.1.3 für verwaltete Installationen erforderlich
Betriebssysteme	• Windows 8™ (32/64 Bit) • Windows 7™ (32/64 Bit) • Windows Vista™ mit SP1 (32/64 Bit) • Windows XP™ mit SP3 (32 Bit)
Andere Software	Weitere Voraussetzungen für Windows 8: • Microsoft .NET Framework 3.5 ist aktiviert • Informationen zum Ändern der Startreihenfolge für Geräte mit UEFI finden Sie unter *Vorbereiten des Geräts auf Seite 4-5*. Weitere Voraussetzungen für Clients unter Windows XP: • Microsoft .NET Framework 2.0 SP1 oder höher • Microsoft Windows Installer 3.1
Festplatte	• Seagate DriveTrust-Laufwerke • Seagate OPAL- und OPAL 2-Laufwerke **Hinweis** • RAID- und SCSI-Festplatten werden nicht unterstützt. • Full Disk Encryption für Windows 8 unterstützt keine RAID-, SCSI-, eDrive- oder OPAL 2-Laufwerke.
Andere Hardware	ATA-, AHCI- oder IRRT-Festplattencontroller

Festplatte vorbereiten

Full Disk Encryption verschlüsselt jeden Sektor auf dem physischen Laufwerk. Da viele Anwendungen, inkl. dem Betriebssystem, nicht den vollständigen physischen

Festplattenspeicher verwenden, können Sektoren beschädigt sein. Eventuell ist auch das Laufwerk extrem fragmentiert.

Hinweis

Trend Micro empfiehlt, ein kleines Pilotprojekt mit Neuinstallationen und Upgrades durchführen, bevor der neueste Full Disk Encryption Build verteilt wird. Wenn Sie Fragen haben oder technische Unterstützung benötigen, wenden Sie sich an den Support von Trend Micro.

Vorbereiten des Geräts

Prozedur

1. Trennen Sie alle USB-Speichergeräte. Sie können sie nach der Installation wieder anschließen.
2. Vergewissern Sie sich, dass das Laufwerk mit dem Betriebssystem nicht bereits verschlüsselt wurde und BitLocker ausgeschaltet ist.
3. Ändern Sie für Windows 8-Geräte, die UEFI BIOS unterstützen, die Startreihenfolge in **Legacy First**.
   a. Halten Sie in Windows 8 die UMSCHALTTASTE gedrückt und starten Sie das Gerät neu.

      Das Gerät wird neu gestartet und UEFI BIOS wird geladen.

   b. Klicken Sie auf die Kachel **Problembehandlung**.

      Das Fenster **Erweiterte Optionen** wird angezeigt.

   c. Klicken Sie auf die Kachel **UEFI-Firmwareeinstellungen**.

      Wenn die Kachel **UEFI-Firmwareeinstellungen** nicht vorhanden ist, verwendet das Gerät kein UEFI und es ist keine Änderung erforderlich.

   d. Legen Sie **UEFI/Legacy Boot Priority** auf **Legacy First** fest.

   e. Starten Sie das Gerät neu.

Laufwerk vorbereiten

Prozedur

1. Führen Sie das Defragmentierungs-Dienstprogramm von Windows auf dem Systemlaufwerk aus.
2. Überprüfen Sie, ob auf dem Systemlaufwerk mindestens 256MB an zusammenhängendem freiem Speicher zur Verfügung stehen.
3. Führen Sie das Dienstprogramm für die Prüfung der Datenträger-Integrität von Windows aus (erfordert einen Neustart).
   a. Rufen Sie mit einem Skript oder über eine Befehlszeile `chkdsk /f /r` auf, und planen Sie die Überprüfung der Festplatte nach dem nächsten Systemneustart.
   b. Starten Sie das Gerät neu.
   c. Tauschen Sie das Laufwerk aus, wenn chkdsk mehrere fehlerhafte Sektoren meldet.
4. Überprüfen Sie, ob bei der Festplatte ein normaler Master Boot Record (MBR) vorliegt, und bestätigen Sie, dass ein normaler Bootsektor auf der Bootpartition vorhanden ist. Beispiel: Auf einem Computer mit zwei bootfähigen Betriebssystemen befindet sich ein modifizierter Bootsektor.

   Hinweis

   GPT wird derzeit nicht unterstützt.

5. Kopieren Sie die Full Disk Encryption Installations-Software auf das Systemlaufwerk von Windows.

Wichtige Hinweise für DataArmor SP7 und frühere Versionen

- SP6 und früher:
  - Überprüfen Sie im BIOS, ob der Festplatten-Controller auf ATA- oder AHCI-Modus eingestellt ist.
  - Bei Laptops mit einer Docking-Station installieren Sie die Software, während das Gerät nicht an ein Multi-Bay-Gehäuse angeschlossen ist.
- Intel™Rapid Recovery Technology (IRRT):
  - Einige neuere Systeme unterstützen IRRT im BIOS.
  - Wenn für den BIOS-Festplattencontroller der IRRT-Modus festgelegt ist, müssen Sie diesen vor der Installation von Full Disk Encryption in den AHCI-Modus ändern.
  - IRRT muss vom Betriebssystem unterstützt werden.
- Intel™ Matrix Manager-Software:
  - Standardmäßig ist unter Window XP die Intel Matrix Manager-Software nicht installiert. Die Einstellungen müssen im BIOS ohne eine erneute Neuinstallation des Betriebssystems vorgenommen werden.
  - Unter Windows Vista ist die Intel Matrix Manager-Software standardmäßig installiert.

Hinweis

Wenn die Einstellung für den SATA-Betrieb unter Windows VISTA geändert und Full Disk Encryption installiert wird, wird Windows nicht gestartet. Ändern Sie die Einstellung wieder in IRRT, und Vista wird normal geladen.

Full Disk Encryption Installation

In diesem Abschnitt wird die Installation von Full Disk Encryption unter Windows beschrieben.

Installationstypen

Abhängig von den spezifischen Anforderungen des Unternehmens kann Full Disk Encryption als verwalteter oder nicht verwalteter Client installiert werden.

Typ	Details
Verwaltet	• Authentifizierungs- und Verschlüsselungsrichtlinien werden von PolicyServer verwaltet. • Häufigster Installationstyp für Geräte, die normalerweise mit PolicyServer verbunden sind.
Nicht verwaltet	• Die Authentifizierungs- und Verschlüsselungsrichtlinien werden direkt innerhalb von Full Disk Encryption und der Wiederherstellungskonsole verwaltet. • Geeignet für Geräte, die nicht zentral von PolicyServer verwaltet werden.

Installationsoptionen

Installieren Sie Full Disk Encryption manuell oder erstellen Sie Skripts, um die Installationsaufgaben zu automatisieren.

Tabelle 4-3. Full Disk Encryption Installationsoptionen

Optionen	Details
Automatisiert	• Erfordert Systemverwaltungs-Software: Tivoli, SCCM/SMS oder LANDesk sowie ein Installationsskript. • Empfohlene Methode für Unternehmen mit vielen Endpunkten.
Manuell	• Einfache Installation direkt aus Windows, entweder über ein grafisches Installationsprogramm oder eine Befehlszeile. • Eignet sich für kleine Unternehmen, Testverteilungen oder individuelle Installationen.

Automatisierte Installation

Die Installation von Full Disk Encryption mit Hilfe von Skripts automatisiert den Prozess und vereinfacht die Verteilung der Software im gesamten Unternehmen. Weitere Informationen finden Sie unter *Skripts zur Automatisierung von Installationen verwenden auf Seite 4-21*.

Verwaltete Installation

Eine verwaltete Installation von Full Disk Encryption ist der häufigste Installationstyp für Geräte, die normalerweise mit PolicyServer verbunden sind. Authentifizierungs- und Verschlüsselungsrichtlinien werden von PolicyServer verwaltet. In diesem Abschnitt werden die grundlegenden Installationsschritte für einen verwalteten Endpunktclient beschrieben.

Führen Sie das Folgende aus, bevor Sie fortfahren:

- Lesen Sie *Full Disk Encryption Systemvoraussetzungen auf Seite 4-3*.
- Prüfen Sie die *Festplatte vorbereiten auf Seite 4-4*

Warnung!

Eine unzureichende Einrichtung des Systems oder Vorbereitung der Festplatte kann zu irreversiblen Datenverlusten führen.

Voraussetzungen

Folgendes ist für verwaltete Installationen erforderlich:

- Client ist während der Installation mit PolicyServer verbunden.
- PolicyServer muss mit einem Unternehmen, einem Host-Namen und einer IP-Adresse konfiguriert sein.

Hinweis

Trend Micro empfiehlt die Verwendung des vollqualifizierten Domänennamens des PolicyServer. Wenn sich die IP-Adresse oder der Host-Name des PolicyServers ändert, muss nicht jeder Client manuell aktualisiert werden.

- Das Benutzerkonto muss zu einer PolicyServer Gruppe gehören und über die Berechtigung verfügen, Geräte zu dieser Gruppe hinzuzufügen.

Warnung!

PolicyServer Enterprise Administrator- oder Authentifiziererkonten können nicht zur Installation von Full Disk Encryption verwendet werden.

- Das installierende Konto benötigt lokale Administratorrechte.
- Wenn Domänenauthentifizierung/Single-Sign-On aktiviert ist, muss der Benutzername mit Active Directory übereinstimmen. Stattdessen wird das Active Directory Kennwort verwendet.

Installieren von Full Disk Encryption als ein verwalteter Client

Überprüfen Sie die Systemvoraussetzungen, bevor Sie Full Disk Encryption als einen verwalteten Client installieren. Weitere Informationen finden Sie unter *Full Disk Encryption Systemvoraussetzungen auf Seite 4-3*. Nach der Installation von Full Disk Encryption wird der Computer für Software-basierte Verschlüsselung neu gestartet oder für Hardware-basierte Verschlüsselung heruntergefahren.

Hinweis

Bei dem installierenden Benutzer darf es sich nicht um ein Enterprise Administrator- oder Authentifiziererkonto handeln.

Prozedur

1. Kopieren Sie das Installationspaket von Full Disk Encryption auf die lokale Festplatte.
2. Starten Sie `TMFDEInstall.exe`.

Hinweis

Wenn das Fenster **Benutzerkontensteuerung** angezeigt wird, klicken Sie auf **Ja**, damit das Installationsprogramm Änderungen am Gerät vornehmen kann.

Der Begrüßungsbildschirm für die Installation wird angezeigt.

3. Wählen Sie die Option **Verwaltete Installation** aus und klicken Sie auf **Weiter**.

   Das Fenster **Verwaltete Installation** wird angezeigt.

4. Geben Sie die Anmeldedaten für das Benutzerkonto, die PolicyServer Adresse und das Unternehmen ein und klicken Sie anschließend auf **Weiter**.

   Die Installation von Full Disk Encryption wird gestartet. Das Programm wird nach Abschluss der Installation geschlossen. Dies dauert u. U. mehrere Minuten.

Tipp

Wenn die verwaltete Installation fehlschlägt, verwenden Sie die Geräte-ID, die sich unten rechts auf dem Bildschirm des Installationsprogramms befindet, um zu prüfen, ob das Gerät bereits in PolicyServer vorhanden ist. Die Geräte-ID wird nur angezeigt, nachdem ein Installationsfehler aufgetreten ist.

---

5. Klicken Sie im Bestätigungsfenster auf **Ja**, um das Gerät neu zu starten oder herunterzufahren.

   Die Installation von Full Disk Encryption ist abgeschlossen, sobald Preboot angezeigt wird. Die Verschlüsselung der Festplatte beginnt nach dem Starten von Windows.

Nächste Maßnahme

Wenn Full Disk Encryption Preboot geladen wird, muss sich der Benutzer anmelden, bevor er auf Windows zugreifen kann. Wenn die Richtlinie festgelegt ist, wird der Benutzer möglicherweise aufgefordert, das Kennwort nach der Anmeldung zu ändern.

Nicht verwaltete Installation

Eine nicht verwaltete Full Disk Encryption Installation ist mit einer verwalteten Installation vergleichbar, abgesehen davon, dass die Benutzer-Anmeldedaten und -Richtlinien nur für das Client-Gerät gelten.

Full Disk Encryption als nicht verwalteten Client installieren

Überprüfen Sie die Systemvoraussetzungen, bevor Sie Full Disk Encryption als einen verwalteten Client installieren. Weitere Informationen finden Sie unter *Full Disk Encryption Systemvoraussetzungen auf Seite 4-3*. Nach der Installation von Full Disk Encryption wird der Computer für Software-basierte Verschlüsselung neu gestartet oder für Hardware-basierte Verschlüsselung heruntergefahren.

Prozedur

1. Kopieren Sie das Installationspaket von Full Disk Encryption auf die lokale Festplatte.
2. Starten Sie `TMFDEInstall.exe`.

   Hinweis

   Wenn das Fenster **Benutzerkontensteuerung** angezeigt wird, klicken Sie auf **Ja**, damit das Installationsprogramm Änderungen am Gerät vornehmen kann.

   Der Begrüßungsbildschirm für die Installation wird angezeigt.
3. Wählen Sie die Option **Nicht verwaltete Installation** aus und klicken Sie auf **Weiter**.

   Das Fenster **Nicht verwaltete Installation** wird angezeigt.

4. Geben Sie den Benutzernamen und das Kennwort für ein neues Konto zur Anmeldung beim nicht verwalteten Client ein und klicken Sie auf **Weiter**.

   Die Installation beginnt.

5. Klicken Sie im Fenster **Installation abgeschlossen** auf **Schließen**.

6. Klicken Sie im Bestätigungsfenster auf **Ja**, um das Gerät neu zu starten oder herunterzufahren.

   Die Installation von Full Disk Encryption ist abgeschlossen, sobald Preboot angezeigt wird. Die Verschlüsselung der Festplatte beginnt nach dem Starten von Windows.

Nächste Maßnahme

Wenn Full Disk Encryption Preboot geladen wird, muss sich der Benutzer anmelden, bevor er auf Windows zugreifen kann.

FileArmor installieren

Mit der FileArmor Verschlüsselung können Sie die Dateien und Ordner auf nahezu jedem Gerät, das als Laufwerk im Host-Betriebssystem angezeigt wird, schützen.

Überblick über die FileArmor Verteilung

Prozedur

1. Aktivieren Sie FileArmor in PolicyServer MMC.
2. Konfigurieren Sie die FileArmor Richtlinien:
   a. Verwendeter Verschlüsselungsschlüssel
   b. Zu verschlüsselnde Ordner
   c. Verwendung von Wechselmedien
   d. Authentifizierungsmethode

3. Richten Sie Benutzer und Gruppen ein.
4. Erstellen und testen Sie das Installationspaket.
5. Überprüfen Sie, ob die festgelegten Richtlinieneinstellungen erzwungen werden.
6. Bereiten Sie die Endbenutzer-Kommunikation vor.

Erforderliche FileArmor Richtlinieneinstellungen

Prozedur

1. Die wichtigste Entscheidung vor der Verteilung von FileAmor ist es, den richtigen Verschlüsselungsschlüssel auszuwählen:
   - **Benutzerschlüssel:** Nur der Benutzer kann auf die verschlüsselte Datei zugreifen.
   - **Gruppenschlüssel:** Alle Benutzer innerhalb der Richtliniengruppe können auf die Datei zugreifen.
   - **Unternehmensschlüssel:** Alle Benutzer innerhalb aller Gruppen können auf die Datei zugreifen.
2. Die zweite Entscheidung betrifft die FileArmor Richtlinien für Wechselmedien. Alle Richtlinien befinden sich unter: **FileArmor** > **Verschlüsselung** > **Wechselmedien**.

TABELLE 4-4. Zu konfigurierende FileArmor Richtlinien

RICHTLINIE	BESCHREIBUNG
Wechselmedien	Aktiviert den Schutz für USB-Speichergeräte.
Zulässige USB-Geräte	Sie können alle USB-Speichergeräte oder nur KeyArmor Geräte zulassen.
Gerät vollständig verschlüsseln	FileAmor verschlüsselt automatisch alle Dateien, die auf das USB-Speichergerät kopiert werden.

Richtlinie	Beschreibung
USB-Laufwerk deaktivieren	Geben Sie an, ob das USB-Laufwerk immer, nie oder nur, wenn nicht angemeldet, deaktiviert werden soll.

3. Legen Sie fest, ob Ordner auf dem Host mit FileArmor automatisch verschlüsselt werden sollen. Dateien, die in einen geschützten Ordner kopiert werden, werden automatisch verschlüsselt. In der Standardeinstellung wird ein von FileArmor verschlüsselter Ordner auf dem Desktop erstellt.

   - Verwenden Sie **Verschlüsselung** > **Ordner zum Verschlüsseln angeben**, um geschützte Ordner auf dem Host zu erstellen.
   - Verwenden Sie **Verschlüsselung** > **Wechselmedien** > **Zu verschlüsselnde Ordner auf Wechselmedien**, um geschützte Ordner auf einem USB-Speichergerät zu erstellen.

FileArmor Installation

FileArmor kann mit einer der folgenden Methoden installiert werden:

- Mit einem Automatisierungs-Tool, z. B. Microsoft SCCM oder SMS
- Manuell auf einem lokalen Computer

Systemvoraussetzungen für FileArmor

Tabelle 4-5. Systemvoraussetzungen für FileArmor

Vorgang	Voraussetzung
Prozessor	Intel™ Core™ 2 oder kompatibler Prozessor.
Arbeitsspeicher	• Mindestens: 512MB • Empfohlen: 1GB

VORGANG	VORAUSSETZUNG
Festplattenspeicher	• Mindestens: 2GB • Erforderlich: 20% verfügbaren Festplattenspeicher
Netzwerkverbindung	Kommunikation mit PolicyServer für verwaltete Installationen erforderlich
Betriebssysteme	• Windows 8™ (32/64 Bit) • Windows 7™ (32/64 Bit) • Windows Vista™ mit SP1 (32/64 Bit) • Windows XP™ mit SP3 (32 Bit)
Andere Software	Weitere Voraussetzungen für Windows 8: • Microsoft .NET Framework 3.5 ist aktiviert • Informationen zum Ändern der Startreihenfolge für Geräte mit UEFI finden Sie unter *Vorbereiten des Geräts auf Seite 4-5*. Weitere Voraussetzungen für Clients unter Windows XP: • Microsoft .NET Framework 2.0 SP1 oder höher • Microsoft Windows Installer 3.1

Weitere Voraussetzungen

- Der die Installation durchführende Benutzer muss über Administratorrechte auf dem Gerät verfügen.
- Kopieren Sie das Installationspaket auf den lokalen Computer, und führen Sie es dort aus.
- Legen Sie ein festes Kennwort für alle PolicyServer Benutzer fest.
- Das Benutzerkonto muss zu einer PolicyServer Gruppe gehören und über die Berechtigung verfügen, Geräte zu dieser Gruppe hinzuzufügen.

Hinweis

PolicyServer Enterprise Administrator- oder Authentifiziererkonten können nicht zur Installation von FileArmor verwendet werden.

Manuelle FileArmor Installation

Der manuelle Installationsvorgang besteht aus dem Ausführen eines Installationsprogramms auf dem Client und dem Durchführen der schrittweisen Anweisungen. FileArmor kann von PolicyServer Gruppenadministratoren, Authentifizierern oder Standardbenutzern installiert werden.

Prozedur

1. Führen Sie `FASetup.msi` für ein 32-Bit-Betriebssystem oder `FASetup(x64).msi` für ein 64-Bit-Betriebssystem aus.

   Der FileArmor Setup-Assistent beginnt mit dem FileArmor Installationsvorgang.

2. Klicken Sie auf **Weiter**.

   Hinweis

   Wenn Sie eine Nachfrage von der Benutzerkontensteuerung erhalten, klicken Sie auf **Ja**.

3. Wenn die Installation abgeschlossen ist, klicken Sie auf **Schließen**.

4. Klicken Sie auf **Ja**, um Windows neu zu starten.

   Nach dem Neustart des Geräts wird die FileArmor Software installiert und zwei FileArmor Symbole werden angezeigt – eine Verknüpfung auf dem Desktop und ein Symbol in der Task-Leiste.

Automatische FileArmor Installation

Die Installation von FileArmor mit Hilfe von Skripts automatisiert den Prozess und vereinfacht die Verteilung der Software im gesamten Unternehmen. Weitere

Informationen finden Sie unter *Skripts zur Automatisierung von Installationen verwenden auf Seite 4-21*.

KeyArmor

KeyArmor USB-Geräte schützen Daten mit ständig verfügbarer Hardware-Verschlüsselung und integriertem Antivirus-/Anti-Malware-Schutz, um strenge gesetzliche Vorschriften und Richtlinien zu erfüllen. Mit KeyArmor haben Administratoren vollständige Transparenz und Kontrolle darüber, wer USB-Geräte zu welchem Zeitpunkt, an welchem Ort im Unternehmen und auf welche Weise einsetzt.

Systemvoraussetzungen für KeyArmor

In der folgenden Tabelle werden die Mindestanforderungen für die Verwendung von KeyArmor USB-Sticks erläutert.

TABELLE 4-6. Systemvoraussetzungen für KeyArmor

VORGANG	VORAUSSETZUNG
Hardware	USB-2.0-Port
Netzwerkverbindung	Kommunikation mit PolicyServer für verwaltete Installationen erforderlich
Betriebssysteme	• Windows 7™ (32/64 Bit) • Windows Vista™ mit SP1 (32/64 Bit) • Windows XP™ mit SP3 (32 Bit)
Andere Software	Weitere erforderliche Software bei der Installation auf Windows XP™: • Microsoft .NET Framework 2.0 SP1 oder höher

Gerätekomponenten

KeyArmor stellt zwei Laufwerke bereit, wenn Sie das Gerät an einen USB-Port anschließen.

ABBILDUNG 4-1. KeyArmor Geräte

- **KeyArmor (E:)** enthält die Programmdateien von KeyArmor.
- **SECURE DATA (F:)** ist das Benutzerspeichergerät von KeyArmor. KeyArmor verschlüsselt alle auf diesem Laufwerk gespeicherten Dateien.

Überblick über die KeyArmor Verteilung

Ähnlich wie für Full Disk Encryption und FileArmor sind für die KeyArmor Verteilung folgende Schritte erforderlich:

1. Aktivieren Sie KeyArmor in PolicyServer.
2. Konfigurieren Sie die entsprechenden KeyArmor Richtlinien:
    - Authentifizierungsmethode
    - Muss mit dem Server verbunden sein
    - Nur ein Benutzer pro Gerät
    - Aktion bei fehlgeschlagener Anmeldung
    - Antivirus-Update-Optionen
3. Richten Sie Benutzer und Gruppen ein.
4. Bereiten Sie die Geräteauthentifizierung und die Kennwörter vor.

5. Bereiten Sie die Endbenutzer-Kommunikation vor.

KeyArmor Richtlinien für Endbenutzer

- Das Gerät wird beim Anschluss an einen USB-2.0-Port von Windows automatisch erkannt und konfiguriert.
- Wenn der Endbenutzer ein neues Gerät erhält, muss er den Setup-Vorgang einmal ausführen.
- Anschließend benötigt er nur einen gültigen Benutzernamen und ein Kennwort.
- KeyArmor verschlüsselt automatisch alle Dateien, die auf dem KeyAmor Gerät gespeichert werden.
- Das Öffnen, Anzeigen, Verschieben oder Kopieren von Dateien auf einen Host sind Benutzeraktivitäten, die nur nach ordnungsgemäßer Authentifizierung am KeyArmor Gerät durchgeführt werden können.

KeyArmor Dateien schützen

- Auf dem KeyArmor Gerät gespeicherte Dateien und Ordner werden automatisch verschlüsselt. Zum Zugriff auf die Dateien und Ordner ist die Anmeldung am Gerät mit einem gültigen Benutzernamen und einem Kennwort erforderlich.
- Die Dateien bleiben verschlüsselt, solange sie auf KeyArmor gespeichert sind.
- Um sicherzustellen, dass die Antivirusdefinitionen aktuell sind, empfiehlt Trend Micro, Dateien erst auf das KeyArmor Gerät zu kopieren, nachdem die ersten Antivirus-Updates durchgeführt wurden.

Warnung!

Führen Sie immer die folgenden Schritte für das sichere Entfernen von KeyArmor Geräten aus:

1. Wählen Sie **Abmelden** in der KeyArmor Anwendung aus.
2. Klicken Sie mit der rechten Maustaste auf das KeyArmor Symbol in der Task-Leiste, und wählen Sie **Abmelden** aus.

Durch das sichere Entfernen des KeyArmor Geräts beugen Sie vorzeitiger Abnutzung und Datenverlusten vor.

Skripts zur Automatisierung von Installationen verwenden

Die skriptgesteuerte Installationsmethode wird bei großen Verteilungen mit Hilfe von automatischen Tools wie Microsoft SMS oder Active Directory am häufigsten verwendet. Command Line Installer Helper (weitere Details unter *Command Line Installer Helper auf Seite 4-23*) ist ein Tool zum Erstellen von Skripts. Die verfügbaren Argumente unterstützen vollständig oder teilweise unbeaufsichtigte Installationen.

Warnung!

Eine unzureichende Einrichtung des Systems oder Vorbereitung der Festplatte kann zu irreversiblen Datenverlusten führen.

Voraussetzungen

- Alle Installationsskripts sollten lokal ausgeführt werden, nicht von einem freigegebenen Netzwerklaufwerk oder USB-Laufwerk.
- Skripts müssen als "lokaler Administrator" ausgeführt werden.
- Installationsskripts sollten in einem Pilotprogramm getestet werden.

Skriptargumente

In der nachfolgenden Tabelle werden die Argumente zum Aufbau von Skripts zur automatischen Installation von Endpunkt-Clients erläutert.

TABELLE 4-7. Skript-Argumente für automatisierte Full Disk Encryption Installationen

ARGUMENT	WERT	HINWEISE
ENTERPRISE	Der Name des Unternehmens.	Sie finden den Namen des Unternehmens mit Hilfe Ihrer Lizenzdatei.
HOST	DNS-Host-Name oder IP-Adresse	Der Name oder Standort von PolicyServer.
USERNAME	• Gruppenadministrator • Gruppenauthentifizierer • Gruppenbenutzer (wenn die Richtlinie zum Erlauben der Installation aktiviert ist)	Ein Administrator- oder Authentifiziererkonto auf Unternehmensebene kann nicht zur Installation von Full Disk Encryption verwendet werden.
PASSWORD	Kennwort für den angegebenen Benutzernamen	Das feste Kennwort, das in PolicyServer für den Benutzer konfiguriert wurde, oder ein Domänenkennwort.

TABELLE 4-8. Skript-Argumente für automatisierte FileArmor Installationen

ARGUMENT	WERT	HINWEISE
PSENTERPRISE	Der Name des Unternehmens.	Sie finden den Namen des Unternehmens mit Hilfe Ihrer Lizenzdatei.
PSHOST	DNS-Host-Name oder IP-Adresse	Der Name oder Standort von PolicyServer.

Argument	Wert	Hinweise
FAUSERNAME	• Gruppenadministrator • Gruppenauthentifizierer • Gruppenbenutzer (wenn die Richtlinie zum Erlauben der Installation aktiviert ist)	Ein Administrator- oder Authentifiziererkonto auf Unternehmensebene kann nicht zur Installation von FileArmor verwendet werden.
FAPASSWORD	Kennwort für den angegebenen Benutzernamen	Das feste Kennwort, das in PolicyServer für den Benutzer konfiguriert wurde, oder ein Domänenkennwort.

Command Line Installer Helper

Der Command Line Installer Helper (`CommandLineInstallerHelper.exe`) kann Skripts generieren, um Full Disk Encryption, FileArmor und PolicyServer zu installieren. Über die Optionen können die Installationskontodaten verschlüsselt und verborgen sowie verschiedene Optionen für die Eingabe ausgewählt werden. Skriptergebnisse können zum Exportieren auf einfache Weise in die Zwischenablage kopiert werden. Das Tool hat zwei Registerkarten: eine für Clients und eine für PolicyServer.

Hinweis

Die Befehlszeileninstallation von PolicyServer wird von den Versionen 3.1.2 und höher unterstützt.

Beim Verwenden von Command Line Installer Helper:

- Führen Sie Installationsskripts nur auf einem Endpunkt-Client aus, nicht über das Netzwerk.
- Führen Sie Skripts als lokaler Administrator aus.
- Testen Sie Installationsskripts zunächst in einem Pilotprogramm.
- Überprüfen Sie, ob alle Installationsvoraussetzungen von Full Disk Encryption und FileArmor erfüllt sind, bevor Sie eine Massenverteilung der Software ausführen.

Full Disk Encryption und FileArmor sind mit Tools zur automatischen Software-Verteilung kompatibel, beispielsweise mit SMS, SCCM, Tivoli, GPO und LANDesk.

PolicyServer Installationsskripts erstellen

Die folgenden Informationen sind mindestens erforderlich, um ein Skript zu erstellen:

- Adresse der primären Datenbank und Anmeldedaten des Administrators
- Pfad zum Installationsprogramm von PolicyServer

Wichtig

Eine skriptgesteuerte Installation wird nur von PolicyServer Version 3.1.2 oder neuer unterstützt.

Prozedur

1. Geben Sie alle erforderlichen Informationen ein.
2. Geben Sie ggf. zusätzliche Informationen ein.
3. Klicken Sie auf **Generate Command**.

   Das Codefeld **Policy Server Install Command** wird ausgefüllt.
4. Klicken Sie auf **Copy to Clipboard**.

   Das resultierende Skript wird in die Zwischenablage kopiert.

Client-Installationsskripts erstellen

Die folgenden Informationen sind erforderlich, um ein Skript für die unbeaufsichtigte Installation zu generieren: Host-Name oder IP-Adresse des PolicyServer, Name des Unternehmens, Benutzername, Kennwort sowie Pfad und Versionsnummer des Endpunkt-Client-Installationsprogramms.

Prozedur

1. Geben Sie die erforderlichen Informationen in die entsprechenden Textfelder ein.
2. Wählen Sie die Optionen aus, die im Skript enthalten sein sollen.
3. Klicken Sie auf **Generate Command**.

   Die Skripts werden generiert.
4. Klicken Sie auf **Copy Full Disk Encryption Command** oder **Copy FileArmor Command**.

   Das resultierende Skript wird in die Zwischenablage kopiert.

Command Line Helper

Mit Command Line Helper können verschlüsselte Werte erzeugt werden, die als sichere Anmeldedaten beim Erstellen von Installationsskripts oder für DAAutoLogin verwendet werden können. Command Line Helper befindet sich im Ordner "FileArmor Tools".

Hinweis

Command Line Helper kann nur auf Systemen ausgeführt werden, auf denen PolicyServer, Full Disk Encryption oder FileArmor installiert ist, da die Kryptographie von Mobile Armor genutzt wird.

Das Programm akzeptiert eine einfache Zeichenfolge als einziges Argument und gibt einen verschlüsselten Wert zurück, der im Installationsskript verwendet werden kann. Die vorangestellten und nachgestellten “=”-Zeichen sind Teil der gesamten verschlüsselten Zeichenfolge und müssen auf der Befehlszeile angegeben werden. Wenn der verschlüsselte Wert kein vorangestelltes "="-Zeichen enthält, müssen Sie es in das Skript einfügen.

Über die Optionen können die Installationskontodaten verschlüsselt und verborgen sowie verschiedene Optionen für die Eingabe ausgewählt werden. Skriptergebnisse können zum Exportieren auf einfache Weise in die Zwischenablage kopiert werden.

TABELLE 4-9. Argumente für Command Line Helper

FUNKTION	ARGUMENTE		
	FULL DISK ENCRYPTION	FULL DISK ENCRYPTION VERSCHLÜSSELT	FILEARMOR
Unternehmen	ENTERPRISE	eENTERPRISE	PSENTERPRISE
PolicyServer	HOST	eHOST	PSHOST
Benutzername	USERNAME	eUSERNAME	FAUSERNAME
Kennwort	PASSWORD	ePASSWORD	FAPASSWORD

Hinweis

Das Installationsprogramm von FileArmor kann verschlüsselte Werte automatisch verarbeiten.

Full Disk Encryption Skriptbeispiel

Nur ein Wert kann an Command Line Helper übergeben werden. Dieser kann jedoch so oft wie nötig ausgeführt werden, um alle erforderlichen verschlüsselten Werte zu sammeln.

```
Speicherort der Software = C:\Programme\Trend Micro\Full Disk
Encryption\TMFDEInstaller.exe

ENTERPRISE = MyCompany

HOST = PolicyServer.mycompany.com

eUSERNAME = GroupAdministrator

ePASSWORD = 123456
```

Hinweis

In diesem Beispiel werden der Benutzername und das Kennwort verschlüsselt.

Ausgabe zum Installieren von Full Disk Encryption:

```
C:\Program Files\Trend Micro\Full Disk Encryption
\TMFDEInstaller.exe ENTERPRISE=MyCompany HOST=
PolicyServer.mycompany.com eUSERNAME==jJUJC/Lu4C/
Uj7yYwxubYhAuCrY4f7AbVFp5hKo2PR4O
ePASSWORD==5mih67uKdy7T1VaN2ISWGQQ=
```

FileArmor Skript-Beispiel

Dies ist ein Beispiel eines FileArmor-Installationsskripts für ein Gerät, auf dem ein 32-Bit-Betriebssystem ausgeführt wird. Verwenden Sie für 64-Bit-Geräte stattdessen `FASetup(x64).msi`.

```
Software location = C:\Programme\Trend Micro\FileArmor
\FASetup.msi

PSEnterprise = MyCompany

PSHost = PolicyServer.mycompany.com

FAUser = GroupAdministrator

FAPassword = 123456
```

Hinweis

In diesem Beispiel werden der Benutzername und das Kennwort verschlüsselt.

Ausgabe für die Installation von FileArmor:

```
C:\Programme\Trend Micro\FileArmor\FASetup.msi
PSEnterprise=MyCompany PSHost= PolicyServer.mycompany.com
FAUser==jJUJC/Lu4C/Uj7yYwxubYhAuCrY4f7AbVFp5hKo2PR4O=
FAPassword==5mih67uKdy7T1VaN2ISWGQQ=
```

Kapitel 5

Upgrades, Migrationen und Deinstallationen

In diesem Kapitel werden die verschiedenen Aspekte der Aktualisierung, Verwaltung, Migration und Deinstallation von Trend Micro Endpoint Encryption erläutert.

Dieses Kapitel enthält folgende Themen:

Upgrade des Servers und der Client-Software

In diesem Abschnitt wird beschrieben, wie Sie ein Upgrade von PolicyServer und Endpoint Encryption Client-Software durchführen.

Upgrade von PolicyServer

Bevor Sie PolicyServer upgraden, beachten Sie Folgendes:

- Vor der Durchführung des Datenbank-Upgrades müssen alle PolicyServer Frontend-Server oder -Dienste gestoppt werden.
- Wenn Sie mehrere PolicyServer, die mit derselben Datenbank verbunden sind, upgraden:
  1. Stellen Sie sicher, dass nur ein PolicyServer das Datenbank-Upgrade durchführt.
  2. Beenden Sie den PolicyServer Windows-Dienst auf allen PolicyServern bis auf einen.
  3. Führen Sie das Upgrade auf dem aktiven Server durch.
  4. Nachdem das Upgrade abgeschlossen und die Datenbank repliziert ist, führen Sie das Upgrade auf den anderen Servern aus.
- Wenn Trend Micro LDAP Proxy verwendet wird, führen Sie erst das Upgrade von LDAP Proxy durch und dann das Upgrade auf PolicyServer 3.1.3.

Hinweis

Trend Micro unterstützt gehostete PolicyServer Umgebungen zurzeit nicht.

Upgrade von PolicyServer Datenbanken und Diensten

Das PolicyServer Installationsprogramm konfiguriert Datenbankeinstellungen und installiert Windows Web-Services. Neu in PolicyServer 3.1.3 ist die Möglichkeit, eine Portnummer für den PolicyServer Web-Service anzugeben. Für den Client-Web-Service wird jetzt außerdem ein zweiter Port benötigt. Wenn kein zweiter Port vorhanden ist,

wird während der Installation ein neuer Port erstellt. Weitere Informationen zur neuen Architektur finden Sie unter *Komponenten von Endpoint Encryption auf Seite 1-2*.

Um Endpoint Encryption testweise für eine begrenzte Zeit zu verwenden, können der Unternehmensname und das Konto für den Unternehmensadministrator zum Zeitpunkt der Installation konfiguriert werden. PolicyServer funktioniert normal mit allen Client-Anwendungen, einer unbegrenzten Zahl von Geräten und bis zu 100 Benutzern für einen Testzeitraum von 30 Tagen. Wenden Sie sich nach 30 Tagen an den Technischen Support, um eine Lizenzdatei zu erhalten. Nach Ablauf der Testzeitraums können sich Benutzer und Geräte weiterhin anmelden.

Prozedur

1. Führen Sie `PolicyServerInstaller.exe` aus.
2. Lesen Sie sich die Endbenutzer-Lizenzvereinbarung aufmerksam durch. Wenn Sie einverstanden sind, klicken Sie auf **Zustimmen**.
3. Überprüfen Sie die PolicyServer Version und klicken Sie anschließend auf **Upgrade**.
4. Die Standardeinstellungen im **Dienstanmeldungsfenster von Windows** sind für die meisten Installationen geeignet. Klicken Sie auf **Fortfahren**.
5. Geben Sie im Fenster **Datenbankadministrator-Anmeldung** den Host-Namen (localhost) oder die IP-Adresse des Microsoft SQL Server sowie den Benutzernamen und das Kennwort eines Kontos mit der Sysadmin-Rolle für die angegebene SQL Instanz an.

Hinweis

Bei Umgebungen mit mehreren SQL Server-Instanzen fügen Sie die SQL-Instanz ans Ende des PolicyServer Hostnamens oder die verwendete IP-Adresse an. Verwenden Sie zur Angabe einer Instanz die folgende Syntax:

```
<Hostname oder IP-Adresse>\<Datenbankinstanz>
```

Das Installationsprogramm überprüft die Datenbankverbindung.

6. Klicken Sie im Fenster **PolicyServer Frage** auf **Ja**, wenn die vorhandenen Datenbanken gesichert werden sollen. Klicken Sie auf **Nein**, um die vorhandenen Daten zu überschreiben.

ABBILDUNG 5-1. Meldung zur Datenbanksicherung

7. Geben Sie im Fenster **Datenbankanmeldung** die Anmeldedaten für das Konto an, das zuvor von PolicyServer zur Verwaltung von Datentransaktionen verwendet wurde (PolicyServer Windows-Dienst).

   Wenn dieses Konto nicht verfügbar ist, geben Sie Anmeldedaten zum Erstellen eines neuen Kontos ein.

8. Geben Sie im Fenster **Web Service - Installationsspeicherort** den IIS-Standort an, den PolicyServer MMC und der Client-Web-Service für die Kommunikation mit PolicyServer verwenden sollen. Die Standardportnummer ist 8080. Ist Port 8080 bereits belegt, wird der nächste verfügbare Port zugewiesen.

   a. Wählen Sie eine Site aus dem Listenfeld **Ziel-Site** aus.

   b. Überprüfen Sie den aktuell zugewiesenen Port und geben Sie, falls erforderlich, im Feld **Neuer Port** eine andere Portnummer an.

   Hinweis

   Trend Micro empfiehlt, Port 80 für den Client-Web-Service zu reservieren.

   c. Klicken Sie auf **Fortfahren**.

9. Mit dem nächsten Schritt wird der Client-Web-Service - der IIS-Standort, den alle Endpoint Encryption Clients für die Kommunikation mit PolicyServer nutzen - konfiguriert. Abhängig davon, ob ein zweiter IIS-Standort verfügbar ist, wird eines der folgenden Fenster angezeigt:

- Wenn ein zweiter IIS-Standort verfügbar ist, wird das Fenster **Speicherort für Client-Web-Service** angezeigt.

  a. Wählen Sie eine Site aus dem Listenfeld **Ziel-Site** aus.

  b. Überprüfen Sie die Standardportzuweisung für den Client-Web-Service.

  Hinweis

  Trend Micro empfiehlt, Port 80 beizubehalten. Falls erforderlich, können Sie jedoch im Feld **Neuer Port** eine andere Portnummer angeben. Die Portnummer muss eine positive Ganzzahl zwischen 1 und 65535 sein.

  c. Klicken Sie auf **Fortfahren**.

- Wenn kein zweiter IIS-Standort verfügbar ist, wird das Fenster **Speicherort für Client-Web-Service erstellen** angezeigt, um einen neuen IIS-Standort erstellen zu können.

  a. Geben Sie im Feld **Name der Site** einen Namen für den IIS-Speicherort an.

  b. Suchen Sie nach dem Speicherort für die Site. Wenn noch kein Ordner vorhanden ist, erstellen Sie einen neuen.

  c. Geben Sie die IP-Adresse und Portnummer für den neuen IIS-Speicherort an.

  Hinweis

  Trend Micro empfiehlt, Port 80 beizubehalten. Falls erforderlich, können Sie jedoch eine andere Portnummer angeben. Die Portnummer muss eine positive Ganzzahl zwischen 1 und 65535 sein.

  d. Klicken Sie auf **Fortfahren**.

10. Überprüfen Sie die Einstellungen im Fenster **Mobile Web Service - Installationsspeicherort**, und klicken Sie dann auf **Fortfahren**.

11. Geben Sie im Fenster **Unternehmensnamen und Administrator-Anmeldung erstellen** den neuen Unternehmensnamen und die Anmeldedaten für ein neues

Unternehmensadministrator-Konto an, das während des anfänglichen Testzeitraums zum Verwalten von PolicyServer verwendet wird.

12. Klicken Sie auf **Fortfahren**.

    Der Installationsvorgang wird gestartet.

13. Klicken Sie in der **PolicyServer Installation**-Meldung auf **OK**.

14. Klicken Sie auf **Beendet**.

15. Klicken Sie im Fenster des PolicyServer Installationsprogramms auf **Beenden**.

16. Starten Sie den Server neu.

Upgrade von PolicyServer MMC

Entfernen Sie zunächst PolicyServer MMC mit Hilfe der Windows-Funktion "Software", bevor Sie die neue Version installieren.

Prozedur

1. Navigieren Sie zu **Start** > **Systemsteuerung** > **Software**.

2. Wählen Sie "PolicyServer MMC Snapin" aus der Liste aus und klicken Sie auf **Entfernen**.

3. Klicken Sie auf **Ja**, um PolicyServer MMC zu entfernen.

4. Starten Sie `PolicyServerMMCSnapinSetup.msi`.

5. Klicken Sie auf **Weiter**, um den Setup-Assistenten für PolicyServer MMC zu öffnen.

6. Lesen Sie die Lizenzvereinbarung sorgfältig durch und wählen Sie anschließend **Ich stimme zu**, um den Bedingungen zuzustimmen. Klicken Sie dann auf **Weiter**.

7. Wählen Sie den Installationsordner aus oder verwenden Sie den vorgegebenen Speicherort, und klicken Sie auf **Weiter**.

8. Klicken Sie auf **Weiter**, um die Installation zu bestätigen.

Der Upgrade-Vorgang wird gestartet.

9. Klicken Sie auf **Schließen**, um die Installation abzuschließen.

10. Klicken Sie auf **Ja**, um das Gerät neu zu starten (optional).

11. Melden Sie sich wieder beim Server an und öffnen Sie PolicyServer MMC über die Desktop-Verknüpfung.

    Das Upgrade von PolicyServer MMC ist abgeschlossen. Authentifizieren Sie sich bei PolicyServer MMC. Verwenden Sie hierzu die Anmeldedaten des Unternehmensadministrators.

Hinweis

Eine Liste der empfohlenen Aufgaben nach der Installation, z. B. Anwendungen aktivieren, Geräte und Benutzer erstellen sowie Richtlinien festlegen, finden Sie im Endpoint Encryption Administratorhandbuch.

Upgrade von Full Disk Encryption

Das Installationsprogramm von Full Disk Encryption Upgrade (`TMFDEUpgrade.exe`) unterstützt DataArmor SP7g (3.0.12.861) und DataArmor 3.1.2. Für ein Upgrade von DataArmor SP7g muss das Gerät mit PolicyServer verbunden sein. Für ältere Versionen von DataArmor und DriveArmor deinstallieren Sie die Anwendung und starten Sie das Gerät neu, bevor Sie Full Disk Encryption installieren.

Hinweis

Nicht-englische Betriebssysteme, auf denen aktuell eine ältere Version von Full Disk Encryption (DataArmor 3.0.12 oder 3.1.2) ausgeführt wird, verwenden nach dem Upgrade weiterhin Englisch. Um ein Upgrade auf eine unterstützte Sprache durchzuführen, deinstallieren Sie zuerst die bisherige Anwendung und installieren Sie Full Disk Encryption 3.1.3. Informationen zum Deinstallieren von Full Disk Encryption finden Sie unter *Full Disk Encryption deinstallieren auf Seite 5-18*.

Prozedur

1. Kopieren Sie das Installationspaket von Full Disk Encryption auf die lokale Festplatte.
2. Führen Sie `TMFDEUpgrade.exe` aus.

Hinweis

Falls die Windows Benutzerkontensteuerung geöffnet wird, klicken Sie auf **Ja**, um fortzufahren.

3. Wenn die Meldung, dass das Upgrade abgeschlossen ist, angezeigt wird, starten Sie das Gerät neu.

Upgrade von FileArmor

Verwenden Sie `FA_313_Upgrade.exe`, um für ein Gerät ein Upgrade von FileArmor 3.0.13 oder FileArmor 3.0.14 durchzuführen. `FA_313_Upgrade.exe`befindet sich im Ordner "Tools" des FileArmor Installationsverzeichnisses.

Hinweis

`FA_313_Upgrade.exe` umgeht die Richtlinie "Deinstallation durch Benutzer zulassen" und führt ein Upgrade durch, ohne zu berücksichtigen, ob die Richtlinie auf **Ja** oder auf **Nein** gesetzt ist.

Prozedur

1. Führen Sie `FA_313_Upgrade.exe` aus.

   Windows Installer deinstalliert die ältere FileArmor Version und installiert dann FileArmor 3.1.3. Wenn der Vorgang abgeschlossen ist, wird Windows neu gestartet.

2. Melden Sie sich nach dem Neustart von Windows an und prüfen Sie den neuen FileArmor Ordner. Verschlüsselte Dateien und Ordner werden beibehalten.

Auf Windows 8 upgraden

Endpoint Encryption unterstützt kein Upgrade auf Windows 8. Ist ein Upgrade erforderlich, empfiehlt Trend Micro diese Vorgehensweise, um Datenverlust zu vermeiden, wenn Full Disk Encryption oder FileArmor bereits auf dem Endpunkt-Client installiert ist. KeyArmor unterstützt die Windows 8-Umgebung nicht.

Prozedur

1. Befolgen Sie die Anweisungen im Endpoint Encryption Administratorhandbuch zum Entschlüsseln des Geräts.
2. Deinstallieren Sie Endpunkt-Client-Anwendungen:
   - Informationen über das Deinstallieren von Full Disk Encryption finden Sie unter *Full Disk Encryption deinstallieren auf Seite 5-18*.
   - Informationen über das Deinstallieren von FileArmor finden Sie unter *FileArmor deinstallieren auf Seite 5-19*.
3. Upgraden Sie das Betriebssystem auf Windows 8 bzw. installieren Sie Windows 8.

   Hinweis

   In diesem Dokument wird die Installation der Windows 8-Umgebung nicht erläutert. Anweisungen dazu finden Sie in der entsprechenden Benutzerdokumentation von Microsoft.

4. Stellen Sie sicher, dass die Windows 8-Umgebung stabil ist und dass das Upgrade erfolgreich durchgeführt wurde.
5. Installieren Sie Endpunkt-Client-Anwendungen neu:
   - Informationen über das Installieren von Full Disk Encryption finden Sie unter *Installieren von Full Disk Encryption auf Seite 4-2*.
   - Informationen über das Installieren von FileArmor finden Sie unter *FileArmor installieren auf Seite 4-13*.

Patch-Verwaltung mit Full Disk Encryption

Verwenden Sie **Command Line Helper** zusammen mit **DAAutoLogin** zur Ausführung der Windows Patch-Verwaltung auf Geräten, auf denen Full Disk Encryption installiert ist. Command Line Helper erstellt verschlüsselte Werte für Skripts und DAAutoLogin ermöglicht das einmalige Umgehen von Full Disk Encryption Preboot.

DAAutoLogin bietet je nach Anforderung mehrere Anwendungsmöglichkeiten. Sie können Patches per Push-Verfahren senden, gefolgt von einem Skript mit DAAutoLogin, das einen Befehl zum Neustarten an das Gerät sendet. Auf dem Gerät wird dann Windows GINA angezeigt und die erfolgreiche Durchführung des Patching bestätigt oder es können weitere Patches bereitgestellt werden.

DAAutoLogin akzeptiert die folgenden Switches:

```
DAAutoLogin <Preboot-Benutzername> <Preboot-Kennwort>
[<Domänenname> <Domänenbenutzername> <Domänenkennwort>]
```

Sie können alle erforderlichen Werte übergeben und durch ein Leerzeichen trennen. Wenn Sie die Parameter zur Domäne hinzufügen, ermöglichen Sie die Windows Authentifizierung.

Hinweis

- Führen Sie beide Tools auf einem Gerät aus, auf dem Full Disk Encryption installiert ist.
- Beide Tools befinden sich im Ordner "Tools" in der ZIP-Datei, die Sie von Trend Micro erhalten haben. Wenn Sie Hilfe benötigen, wenden Sie sich an den Trend Micro Support.

Command Line Helper

Die Verwendung von Command Line Helper zusammen mit DAAutoLogin ermöglicht eine problemlose Patch-Verwaltung mit Full Disk Encryption. Mit Command Line Helper können Sie über Ihr Skript verschlüsselte Werte an Full Disk Encryption Preboot übergeben. DAAutoLogin lässt das einmalige Umgehen von Full Disk Encryption Preboot zu.

Prozedur

1. Kopieren Sie `CommandLineHelper.exe` auf die lokale Festplatte des Computers, auf dem Full Disk Encryption installiert ist. (In diesem Beispiel wird `CommandLineHelper.exe` nach `C:\` kopiert.)
2. Öffnen Sie ein Eingabeaufforderungsfenster, und geben Sie `C:\CommandLineHelper.exe` sowie den zu verwendenden Benutzernamen oder das Kennwort ein. Wenn der Benutzername SMSUser ist. lautet der Befehl `C:\CommandLineHelper.exe SMSUser.`
3. Drücken Sie die **Eingabetaste**, um den verschlüsselten Wert anzuzeigen.
4. Führen Sie Command Line Helper erneut aus, um den zweiten Wert zu verschlüsseln. Falls Sie zunächst den Benutzernamen verschlüsselt haben, verschlüsseln Sie im zweiten Durchgang das Kennwort.

Patching-Verfahren für Full Disk Encryption

Prozedur

1. Senden Sie die Patches per Push-Verfahren an die Zielgeräte.
2. Senden Sie ein Skript, das DAAutoLogin ausführt.
3. Senden Sie einen Befehl zum Neustarten, so dass das Gerät Windows GINA lädt und die erfolgreiche Durchführung des Patching bestätigt oder um weitere Patches per Push-Verfahren zu senden.

Installiertes Verschlüsselungsprodukt ersetzen

Sie können Full Disk Encryption auf einem Gerät installieren, das vorher mit einer anderen Software zur Full Disk Encryption verschlüsselt wurde. Da die meisten Full Disk Encryption-Programme jeden Sektor der Festplatte ändern, ist es sehr wichtig, dass Sie Ihr Verfahren zur Vorbereitung der Festplatte und Ihre Verteilungsmethode testen. Je nachdem, wie lange es dauert, ein Gerät zu entschlüsseln und mit Full Disk

Encryption zu verschlüsseln, ist es ggf. sinnvoll, vor der Installation von Full Disk Encryption einfach die Benutzerdaten zu sichern und ein neues Image des Computers aufzuspielen.

Möglichkeit 1: Installiertes Verschlüsselungsprodukt entfernen

Prozedur

1. Entschlüsseln Sie die Festplatte gemäß der vom Softwareanbieter angegebenen Methode.
2. Deinstallieren Sie die Software des Anbieters (oder stellen Sie sicher, dass die BitLocker-Verschlüsselung deaktiviert ist).
3. Starten Sie das Gerät neu.
4. Führen Sie den Befehl `chkdsk` aus und defragmentieren Sie das Laufwerk.
5. Überprüfen Sie auf jedem Gerät, ob ein normaler Master Boot Record (MBR) vorliegt, und vergewissern Sie sich, dass ein normaler Bootsektor auf der Bootpartition vorhanden ist.

   Hinweis

   Das Gerät darf nicht über zwei bootfähige Betriebssysteme verfügen.

6. Sichern Sie die Benutzerdateien.
7. Installieren Sie Full Disk Encryption. Weitere Informationen finden Sie unter *Installieren von Full Disk Encryption auf Seite 4-2*.

Möglichkeit 2: Sicherung durchführen und neues Image auf das Gerät aufspielen

Prozedur

1. Sichern Sie die Benutzerdateien.
2. Spielen Sie ein Image des Geräts auf:
   a. Führen Sie über eine Befehlszeile `DiskPart Clean All` aus.
   b. Erstellen Sie eine Partition.
   c. Formatieren Sie das Laufwerk.
   d. Spielen Sie ein Image des Laufwerks auf.
3. Installieren Sie Full Disk Encryption und verschlüsseln Sie das Gerät.
4. Stellen Sie die Benutzerdateien wieder her.

Endpunkt-Clients auf einen neuen PolicyServer migrieren

In diesem Abschnitt wird beschrieben, wie Sie den PolicyServer, der die Richtlinien eines Endpunkt-Clients steuert, wechseln. Dies ist sinnvoll, wenn ein Endbenutzer in eine Abteilung oder einen Geschäftsbereich wechselt, die bzw. der von einer anderen PolicyServer Instanz verwaltet wird.

Full Disk Encryption PolicyServer wechseln

Sie können die Full Disk Encryption PolicyServer Einstellungen konfigurieren, indem Sie von Full Disk Encryption Preboot aus die Wiederherstellungskonsole öffnen oder indem Sie die Datei `C:\Programme\Trend Micro\Full Disk Encryption \RecoveryConsole.exe` ausführen.

PolicyServer Einstellungen verwalten

Prozedur

1. Öffnen Sie die Registerkarte **PolicyServer**. Die Registerkarte enthält zwei Textfelder: **Aktueller Server** und **Aktuelles Unternehmen**.

   - Das aktuelle Unternehmen wechseln:

     a. Klicken Sie auf **Unternehmen wechseln**.

     b. Klicken Sie auf **Ja**, wenn die Warnmeldung angezeigt wird.

     c. Geben Sie den Benutzernamen, das Kennwort, das Unternehmen und den Servernamen für den neuen Server ein und klicken Sie anschließend auf **Speichern**.

     Warnung!

     Wenn Sie das Unternehmen wechseln, müssen Sie die Richtlinien erneut konfigurieren und die Gruppen neu erstellen. Die gespeicherten Kennwörter, der Kennwortverlauf und die Audit-Protokolle werden gelöscht.

   - Den aktuellen Server wechseln:

     a. Klicken Sie auf **Server wechseln**.

     b. Klicken Sie auf **Ja**, wenn die Warnmeldung angezeigt wird.

     c. Geben Sie die Adresse des neuen Servers ein und klicken Sie auf **Speichern**.

2. Klicken Sie auf **Abbrechen**, um zum Fenster mit den Menüoptionen für die Wiederherstellungskonsole zurückzukehren.

Full Disk Encryption einem anderen Unternehmen zuordnen

Warnung!

Wenn Sie das Unternehmen wechseln, müssen Sie die Richtlinien erneut konfigurieren und die Gruppen neu erstellen. Die gespeicherten Kennwörter, der Kennwortverlauf und die Audit-Protokolle werden gelöscht.

Prozedur

1. Öffnen Sie die Wiederherstellungskonsole. Die Wiederherstellungskonsole kann auf zwei Arten geöffnet werden:
   - Aus Full Disk Encryption Preboot:
     a. Aktivieren Sie das Kontrollkästchen **Wiederherstellungskonsole**.
     b. Geben Sie die Anmeldedaten ein und klicken Sie auf **Anmelden**.
   - Aus Windows:
     a. Navigieren Sie zu `C:\Programme\Trend Micro\Full Disk Encryption\`.
     b. Führen Sie `RecoveryConsole.exe` aus.
     c. Geben Sie die Anmeldedaten ein und klicken Sie auf **Anmelden**.
2. Klicken Sie auf **Netzwerk-Setup**.
3. Wählen Sie die Registerkarte **PolicyServer**.
4. Klicken Sie auf **Unternehmen wechseln**.

   Das Fenster **Unternehmen wechseln** wird angezeigt.

ABBILDUNG 5-2. Wiederherstellungskonsole – Unternehmen wechseln

5. Geben Sie den Benutzernamen, das Kennwort, die PolicyServer IP-Adresse (oder den PolicyServer Host-Namen) für den neuen Server ein.

6. Klicken Sie auf **Speichern**.

   Full Disk Encryption validiert den Server und gibt eine Bestätigungsmeldung aus.

7. Wenn die Bestätigungsmeldung angezeigt wird, klicken Sie auf **OK**.

FileArmor PolicyServer wechseln

Prozedur

1. Klicken Sie mit der rechten Maustaste auf das FileArmor Symbol in der Task-Leiste, und wählen Sie **Info über FileArmor**.

2. Klicken Sie auf **PolicyServer bearbeiten**.

3. Geben Sie die IP-Adresse oder den Host-Namen für den neuen PolicyServer an und klicken Sie dann auf **OK**.

KeyArmor einem anderen Unternehmen zuordnen

Prozedur

1. Melden Sie sich mit den aktuellen Endpoint Encryption Administrator-Anmeldedaten am Gerät an.
2. Klicken Sie mit der rechten Maustaste auf das KeyArmor Symbol in der Task-Leiste, und wählen Sie **Info über KeyArmor** aus.
3. Klicken Sie auf den **Bearbeiten**-Link neben dem Feld **Serveradresse** und geben Sie die neue Serveradresse ein.
4. Klicken Sie auf **OK**.
5. Melden Sie sich von KeyArmor ab.
6. Stellen Sie das Gerät wieder bereit, und melden Sie sich mit den Administrator-Anmeldedaten wieder an.
7. Klicken Sie mit der rechten Maustaste auf das KeyArmor Symbol in der Task-Leiste, und wählen Sie **Info über KeyArmor** aus.
8. Klicken Sie auf den **Bearbeiten**-Link neben dem Feld **Unternehmen** und geben Sie den neuen Namen des Unternehmens ein.
9. Klicken Sie auf **OK**.
10. Klicken Sie auf **Schließen**.
11. Melden Sie sich von KeyArmor ab.
12. Melden Sie sich beim KeyArmor Gerät mit dem Benutzernamen und Kennwort eines Gruppenadministrators des neu festgelegten Unternehmens an.

13. Prüfen Sie die Protokollereignisse zu dieser neuen Unternehmensgruppe, und vergewissern Sie sich, dass das Gerät zur korrekten Gruppe hinzugefügt wurde.

Client-Anwendungen deinstallieren

In diesem Abschnitt wird die Deinstallation von Endpoint Encryption Client-Anwendungen beschrieben.

Full Disk Encryption deinstallieren

Zum Deinstallieren von Full Disk Encryption muss der Benutzer über die entsprechenden Deinstallationsrechte für die Gruppe verfügen und zudem lokale Administratorrechte unter Windows haben.

Tipp

Jeder Benutzer oder Gruppen-Authentifizierer kann das Deinstallationsprogramm unter Windows ausführen, wenn folgende Richtlinieneinstellung gilt: **Full Disk Encryption** > **Allgemein** > **Client** > **Deinstallation durch Benutzer zulassen** = **Ja**.

Prozedur

1. Melden Sie sich bei erst bei Full Disk Encryption an und dann bei Windows.
2. Wechseln Sie unter Windows zu `C:\Programme\Trend Micro\Full Disk Encryption` und führen Sie `TMFDEUninstall.exe` aus.

   Hinweis

   Wenn Sie eine Nachfrage von der **Benutzerkontensteuerung** erhalten, klicken Sie auf **Ja**.

   Das Fenster zum Deinstallieren von Full Disk Encryption wird geöffnet.
3. Klicken Sie auf **Weiter**.

Full Disk Encryption wird deinstalliert.

4. Klicken Sie zur Bestätigung der Laufwerksentschlüsselung auf **OK**.

> **Hinweis**
>
> Um den Status der Entschlüsselung anzuzeigen, öffnen Sie Full Disk Encryption von der Task-Leiste aus.

5. Wenn die Entschlüsselung abgeschlossen ist, klicken Sie auf **OK**.

6. Führen Sie `TMFDEUninstall.exe` erneut aus, um die Deinstallation abzuschließen.

7. Starten Sie das Gerät neu.

> **Hinweis**
>
> Der Gerätedatensatz wird nicht automatisch gelöscht. Er muss manuell aus PolicyServer entfernt werden.

FileArmor deinstallieren

Deinstallieren Sie FileAmor über die Windows-Funktion "Software".

> **Hinweis**
>
> - Setzen Sie **Richtlinien** > **FileArmor** > **Computer** > **Deinstallation durch Benutzer zulassen** auf **Ja**, um allen Benutzern oder Gruppen-Authentifizierern die Ausführung des Deinstallationsprogramms unter Windows zu erlauben.
> - Entschlüsseln Sie manuell alle verschlüsselten Dateien, bevor Sie FileArmor deinstallieren. Anderenfalls sind diese nicht mehr lesbar.
> - Speichern und schließen Sie alle Dokumente, bevor Sie die Deinstallation durchführen. Nachdem die Deinstallation abgeschlossen ist, müssen Sie einen Neustart durchführen.

Prozedur

1. Melden Sie sich bei FileArmor mit einem Konto an, das über die Berechtigung zum Deinstallieren von FileArmor verfügt.
2. Öffnen Sie das **Windows Startmenü** und navigieren Sie zu **Systemsteuerung** > **Programme** > **Programm deinstallieren**.
3. Wählen Sie "FileArmor" aus der Liste aus und klicken Sie dann auf **Deinstallieren**.

Kapitel 6

Unterstützung erhalten

Je nach dem, welche Art von Support benötigt wird, gibt es verschiedene Möglichkeiten, Hilfe zu erhalten.

Dieses Kapitel umfasst folgende Themen:

Trend Community

Hier erhalten Sie Hilfe, können Erfahrungen austauschen, Fragen stellen und Sicherheitsprobleme mit anderen Benutzern, Enthusiasten und Sicherheitsexperten diskutieren.

http://community.trendmicro.com/

Support-Portal

Über das Trend Micro Support-Portal können Sie rund um die Uhr auf Tausende von hilfreichen und einfach zu nutzenden Lösungsvorschlägen zu technischen Problemen mit Trend Micro Produkten und Diensten zugreifen. Täglich werden neue Lösungen hinzugefügt.

Prozedur

1. Gehen Sie zu http://esupport.trendmicro.com.
2. Wählen Sie ein Produkt oder einen Service aus dem entsprechenden Dropdown-Menü aus, und geben Sie weitere verwandte Informationen an, wenn Sie dazu aufgefordert werden.

   Die Produktseite für den Technischen Support wird angezeigt.
3. Geben Sie Suchkriterien an, z. B. eine Fehlermeldung, und klicken Sie anschließend auf das Suchsymbol.

   Eine Liste mit Lösungen wird angezeigt.
4. Wenn in der Liste keine Lösung für Ihr Problem enthalten ist, übermitteln Sie Ihr Problem als Fall. Ein Support-Mitarbeiter von Trend Micro wird sich dann um das Problem kümmern. Die Reaktionszeit beträgt in der Regel maximal 24 Stunden.

   Übermitteln Sie einen Support-Fall online unter:

   http://esupport.trendmicro.com/srf/SRFMain.aspx

Kontaktaufnahme mit dem technischen Support

Bei allen Produktlizenzen erhalten Sie ein Jahr lang technischen Support, Pattern-Downloads und Produkt/Service-Updates. Wenn Sie die Lizenz nach Ablauf des Jahres verlängern, erhalten Sie weiterhin Support von Trend Micro.

Anschriften/Telefonnummern weltweit

```
Weltweite Kontaktadressen für den asiatisch-pazifischen Raum, Australien
http://www.trendmicro.de/ueber-uns/kontakt/index.html
```

- Auf der folgenden Website finden Sie eine Liste unserer weltweiten Support-Büros: http://www.trendmicro.com/us/about-us/contact/index.html
- Auf dieser Website finden Sie die neuesten Dokumentationen von Trend Micro: http://docs.trendmicro.com/de-de/home.aspx

Probleme schneller lösen

Um das Lösen eines Problems zu beschleunigen, halten Sie die folgenden Informationen bereit:

- Schritte, um das Problem nachvollziehen zu können
- Informationen zu Gerät oder Netzwerk
- Marke und Modell des Computers sowie weitere, an den Endpunkt angeschlossene Hardware
- Größe des Arbeitsspeichers und des freien Festplattenspeichers
- Version und Service Pack des verwendeten Betriebssystems
- Endpunkt-Clientversion
- Seriennummer oder Aktivierungscode
- Ausführliche Beschreibung der Installationsumgebung

- Genauer Wortlaut eventueller Fehlermeldungen

TrendLabs

TrendLabs ist ein weltweites Netzwerk aus Forschungs-, Entwicklungs- und Lösungszentren, das rund um die Uhr Bedrohungen überwacht, Präventionsstrategien entwickelt sowie rasche und kontinuierliche Lösungen bereitstellt. TrendLabs bildet die Grundlage der Trend Micro Service-Infrastruktur und beschäftigt mehrere hundert Mitarbeiter und zertifizierte Support-Experten, die sich um die vielfältigen Anfragen zu Produkten und technischem Support kümmern.

TrendLabs überwacht die weltweite Bedrohungslage und liefert wirksame Sicherheitsmaßnahmen für die Erkennung, Vermeidung und Beseitigung von Angriffen. Die Kunden profitieren von diesen täglichen Bemühungen in Form von häufigen Viren-Pattern-Updates und Erweiterungen der Scan Engine.

Weitere Informationen über TrendLabs finden Sie unter:

http://cloudsecurity.trendmicro.com/us/technology-innovation/experts/index.html#trendlabs

Anhang A

Checkliste für das Endpoint Encryption Pilotprogramm

Checkliste für das Pilotprogramm	Datum	Hinweise
Erforderliche Konfiguration von PolicyServer durchgeführt • Richtlinien festgelegt • Gruppen erstellt • Benutzer erstellt/importiert		
Client-Software installiert (Full Disk Encryption und/oder FileArmor) • Software lokal auf den Computer kopiert und ausgeführt		
Administratoren, Authentifizierer und Endbenutzer können basierend auf den Richtlinieneinstellungen auf Geräte zugreifen • Festes Kennwort • Single-Sign-On • SmartCard		

Checkliste für das Pilotprogramm	Datum	Hinweise
Alle Computer sind mit der neuen Software kompatibel • Preboot-Authentifizierung und/ oder Verbindung bestätigt • Verschlüsselung wird abgeschlossen • Computer funktioniert normal • Dateien/Ordner gemäß Richtlinie verschlüsselt • USB-Port wird gemäß der Richtliniendefinition gesteuert • Warnungen, Ereignisprotokolle und Berichte von PolicyServer bestätigen die Administrator- und Endbenutzer-Aktivität		
Endbenutzer können Aktivitäten des Tagesgeschäfts durchführen • Mit dem bestehenden Benutzernamen/Kennwort oder SSO aus Preboot auf Windows zugreifen • Der Computer funktioniert innerhalb und außerhalb des Netzwerks normal • Der Benutzer kann auf alle Benutzerdaten, Anwendungen und Netzwerkressourcen zugreifen		

Checkliste für das Pilotprogramm	Datum	Hinweise
Systemadministratoren testen Support-Prozesse • Backup-Administratoren erstellen • Berichterstellung und Warnungen testen • Full Disk Encryption Recovery Console zum Sichern und Wiederherstellen von Dateien verwenden • Full Disk Encryption Recovery CD zum Entschlüsseln des Geräts und Entfernen des • Preboot-Authentifizierungsprozesses für die Remote-Hilfe verwenden • Gerätesperre und Geräte-Wipe testen. **Warnung!** Löschen Sie ein KeyArmor-Gerät nicht per Wipe. Das Gerät kann nicht wiederhergestellt werden.		

Anhang B

Checkliste für die Sicherheitsinfrastruktur

TABELLE B-1. Checkliste für die Sicherheitsinfrastruktur

PRÜFEN	FRAGEN
Endbenutzer	1. Enthält die Endbenutzerschulung die neuen Funktionen von Endpoint Encryption? 2. Wurde die Richtlinie zur akzeptablen Nutzung (Acceptable Use Policy, AUP) aktualisiert, so dass sie Verschlüsselungsdienste einschließt, insbesondere Strafen für die Nichtverwendung oder Umgehung der Verschlüsselung? 3. Werden Benutzer benachrichtigt, wenn sie sich bei einem Computer anmelden, der auf die AUP hinweist? 4. Wurden alle Benutzer umfassend darin geschult, wie man den Verlust oder Diebstahl eines Geräts meldet? 5. Wurden die Benutzer in den Verfahren hinsichtlich fehlgeschlagener Anmeldeversuche und der Kennwortwiederherstellung geschult? 6. Gibt es eine Richtlinie für die Verschlüsselung vertraulicher Dokumente, die aus dem Unternehmen hinaus gesendet werden? 7. Wurden der AUP neue Kennwortrichtlinien hinzugefügt?

Prüfen	Fragen
Reaktion auf Vorfälle	1. Wurde die Richtlinie für die Reaktion auf Vorfälle (Incident Response, IR) aktualisiert, so dass sie die bei Verlust oder Diebstahl eines Geräts durchzuführenden Aktionen einschließt? 2. Wurde für die PolicyServer Protokolle ein Zeitplan für die Prüfung der Audit-Protokolle festgelegt? 3. Wurden die E-Mail-Warnungen einschließlich der Empfänger und der erwarteten Reaktion beim Empfang eines Alarms zur IR-Richtlinie hinzugefügt? 4. Wurden bestimmte Kriterien dafür entwickelt, dass ein Gerät ausgelöscht oder per Wipe gelöscht werden darf, einschließlich der Audit-Trail-Dokumentation nach der Durchführung der Aktion?
Risikobewertung	1. Wurde eine neue Risikobewertung durchgeführt, um die von Endpoint Encryption gebotene Änderung des Risikoprofils zu zeigen? 2. Wurden die Risikobewertungsverfahren aktualisiert, so dass sie die vom PolicyServer bereitgestellten Audit-Daten einschließen?
Notfall-Wiederherstellung	1. Wurde der PolicyServer zur Liste der kritischen Dienste hinzugefügt? 2. Wurde der Plan zur Notfall-Wiederherstellung aktualisiert, so dass er die Wiederherstellung des PolicyServer Dienstes einschließt? 3. Wurde ein Verfahren entwickelt, das die Wiederherstellung der auf einem Gerät gespeicherten Benutzerdaten ermöglicht?
Personalabteilung	1. Wurde die Checkliste für neue Mitarbeiter aktualisiert, so dass sie alle neuen Prozesse für Endpoint Encryption enthält? 2. Wurden die Prozesse bei Beendigung des Arbeitsverhältnisses aktualisiert, so dass sie alle neuen Prozesse für Endpoint Encryption enthalten – insbesondere das Auslöschen/Wipe von Geräten?

PRÜFEN	FRAGEN
Einhaltung von Richtlinien	1. Wurde das Konformitätsprofil aktualisiert, so dass es die von Endpoint Encryption gebotenen Vorteile enthält? 2. Wurde eine Konformitätsprüfung für alle Aspekte der Implementierung und Verteilung von Endpoint Encryption durchgeführt?

Anhang C

Installationsvoraussetzungen für Full Disk Encryption

Vor der Installation von Full Disk Encryption startet das Installationsprogramm von Full Disk Encryption das Zielgerät und überprüft dieses, um sicherzustellen, dass alle erforderlichen Systemvoraussetzungen erfüllt sind. Das Installationsprogramm wird geschlossen, wenn diese nicht erfüllt werden.

Verwenden Sie die Prüfliste, um fehlende Voraussetzungen zu ermitteln. Einzelheiten finden Sie in der Datei `PreInstallCheckReport.txt`. `PreInstallCheckReport.txt` ist in demselben Ordner wie die Full Disk Encryption Installationsdateien gespeichert.

TABELLE C-1. Vom Installationsprogramm überprüfte Bedingungen

SYSTEMÜBERPRÜFUNG	VORAUSSETZUNG	HINWEISE
Feste Medien	Interne Festplatte	Full Disk Encryption kann nicht auf Wechseldatenträgern installiert werden, auf denen Windows ausgeführt wird. Verwenden Sie FileArmor für Datei- und Ordnerverschlüsselung auf Wechselmedien.
Freier Speicher	Mindestens 256MB	
Arbeitsspeicher	Mindestens 1GB	

SYSTEMÜBERPRÜFUNG	VORAUSSETZUNG	HINWEISE
Partitionsanzahl	Weniger als 25 Partitionen	Partitionen mit erweiterten MBRs sind nicht verfügbar.
Partitionstyp	Nur MBR wird unterstützt	GPT (erforderlich für Festplatten, die größer als 2 TB sind) wird gegenwärtig nicht unterstützt.
Physisches Laufwerk ist bootfähig	Eine bootfähige Partition ist erforderlich.	Full Disk Encryption muss auf einer bootfähigen Partition installiert werden.
SCSI-Festplatte	ATA-, AHCI- oder IRRT-Festplattencontroller. SCSI wird nicht unterstützt.	• Die Prüfung gibt nur eine Warnung aus, da Windows ein SATA-Laufwerk möglicherweise als SCSI-Laufwerk meldet. • Wenn es sich bei der Festplatte nicht um echtes SCSI-Laufwerk handelt, kann Full Disk Encryption installiert werden. Wenn Sie sich nicht sicher sind, nehmen Sie eine physische Überprüfung des Laufwerks vor.
.Net Framework	Für Windows XP oder höher ist .Net 2.0 SP1 oder neuer erforderlich.	Wird für Windows Vista oder neuere Betriebssysteme weggelassen.
SED-Hardwarekompatibilität	Hardware-Verschlüsselung ist aktiviert, falls vorhanden.	Full Disk Encryption unterstützt Seagate™ DriveTrust-™, OPAL- und OPAL 2-Laufwerke.
BitLocker ist nicht installiert	BitLocker kann nicht auf dem Gerät installiert werden.	Wenn BitLocker installiert ist, muss es entfernt werden, bevor Full Disk Encryption installiert werden kann.

Hinweis

Wenn die Präinstallationsprüfung aus einem dieser Gründe fehlschlägt, wenden Sie sich für weitere Hilfe an den Support von Trend Micro.

Stichwortverzeichnis

TREND MICRO INCORPORATED

10101 North De Anza Blvd. Cupertino, CA., 95014, USA

Tel:+1(408)257-1500/1-800 228-5651 Fax:+1(408)257-2003 info@trendmicro.com

www.trendmicro.com

Item Code: APGM35735/121016