TREND MICRO

6.0

TREND MICRO™ Endpoint Encryption

Administratorhandbuch

Umfassende Endpunktverschlüsselung für gespeicherte Daten

Endpoint Security

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

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

Trend Micro, das Trend Micro T-Ball-Logo, OfficeScan und Control Manager sind Marken oder eingetragene Marken von Trend Micro Incorporated. Alle anderen Produkt- oder Firmennamen können Marken oder eingetragene Marken ihrer Eigentümer sein.

Copyright © 2017. Trend Micro Incorporated. Alle Rechte vorbehalten.

Dokument-Nr.: APGM68099/171128

Release-Datum: Mai 2017

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

In dieser Dokumentation finden Sie eine Einführung in die Hauptfunktionen von Produkt und/oder Installationsanweisungen für eine Produktionsumgebung. Lesen Sie die Dokumentation vor der Installation und Verwendung von Produkt.

Ausführliche Informationen über die Verwendung bestimmter Funktionen innerhalb von Produkt 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

Kapitel 1: Einführung

Kapitel 2: Info über Trend Micro Endpoint Encryption

Funktionen und Vorteile 2-3

Neues 2-4

Info über PolicyServer 2-6

Management-Konsolen 2-7
- Trend Micro Control Manager 2-8
- Info über PolicyServer MMC 2-9

Endpoint Encryption Agents 2-9

Authentifizierungsmethode 2-11
- ColorCode 2-12
- Domänenauthentifizierung 2-12
- Festes Kennwort 2-13
- PIN 2-13
- Remote-Hilfe 2-14
- Selbsthilfe 2-14
- SmartCard 2-15

Kapitel 3: Erste Schritte

Systemvoraussetzungen 3-2
- Systemvoraussetzungen für PolicyServer 3-2
- Systemvoraussetzungen für PolicyServer MMC 3-9
- Full Disk Encryption Systemvoraussetzungen 3-9
- Systemvoraussetzungen für File Encryption 3-13
- Systemvoraussetzungen für die Encryption Management for Microsoft BitLocker 3-14
- Systemvoraussetzungen für die Encryption Management for Apple FileVault 3-16

Control Manager einrichten 3-17
Control Manager Architektur 3-18
PolicyServer als verwaltetes Produkt zu Control Manager hinzufügen 3-21
Verzeichnisverwaltung für PolicyServer konfigurieren 3-23
Proxy-Einstellungen konfigurieren 3-24

Active Directory-Synchronisierung 3-25
Active Directory-Überblick 3-26
Active Directory konfigurieren 3-27
Active Directory-Benutzer importieren 3-29
Kennworteinstellungsobjekte aus Active Directory verwalten 3-30

Kapitel 4: Dashboard

Registerkarten 4-2
Standardregisterkarten 4-2
Neue Registerkarte hinzufügen 4-2
Registerkarteneinstellungen ändern 4-3
Eine Registerkarte löschen 4-4

Widgets 4-4
Widgets zu einer Registerkarte hinzufügen 4-5
Widget-Optionen 4-6

Endpoint Encryption Benutzer 4-7
Benutzereinstellungen - Optionen 4-9
Optionen zum Hinzufügen neuer Benutzer 4-10
Richtlinienmitgliedschaft 4-11
Benutzer aus einer CSV-Datei importieren 4-12
Active Directory-Benutzer importieren 4-13

Endpoint Encryption - Geräte 4-14
Geräteaktionen 4-16
Geräteattribute 4-18

Full Disk Encryption Status 4-21
Bericht "Full Disk Encryption Status" 4-22

Erfolglose Anmeldeversuche am Endpoint Encryption Gerät 4-24
Bericht "Erfolglose Anmeldeversuche am Gerät" 4-25

Erfolglose Anmeldeversuche des Endpoint Encryption Benutzers 4-26
Bericht "Erfolglose Anmeldeversuche des Benutzers" 4-27

Endpoint Encryption - Gerätesperrung 4-28
Bericht zur Gerätesperrung 4-29

Endpoint Encryption Bericht zu Sicherheitsverstößen 4-31
Bericht zu aufeinanderfolgenden erfolglosen Anmeldeversuchen am Gerät 4-32
Bericht zu Richtlinienmanipulationen 4-33
Bericht zur Protokollintegrität 4-33

Kapitel 5: Richtlinien

Authentifizierungsübersicht 5-2
Geräte 5-2
Benutzer 5-3
Gruppen 5-5

Richtlinien in Control Manager 5-6
Richtlinienoptionen 5-8
Richtlinientypen 5-10

Eine Richtlinie erstellen 5-11
Richtlinienziele angeben 5-13

Endpoint Encryption Benutzerregeln konfigurieren 5-14

Full Disk Encryption Regeln konfigurieren 5-17

File Encryption Regeln konfigurieren 5-21

Allgemeine Regeln für Richtlinien konfigurieren 5-24
Sperraktionen 5-27

Gruppen auf Control Manager migrieren 5-29

Kapitel 6: Full Disk Encryption

Full Disk Encryption Tools 6-3

Kontextmenü von Full Disk Encryption 6-4

Full Disk Encryption Preboot 6-5
Menüoptionen 6-6

Netzwerkverbindung 6-6
Netzwerkinformationen 6-9
Bildschirmtastatur 6-10
Tastaturbelegung ändern 6-10
Authentifizierungsmethode ändern 6-11
Kennwörter ändern 6-13
Remote-Hilfe 6-16
Smartcard 6-17
Selbsthilfe 6-19

Synchronisierung der Full Disk Encryption Richtlinien 6-21
Full Disk Encryption Konnektivitätsanforderungen 6-22
Full Disk Encryption Agents manuell aktualisieren 6-23
Full Disk Encryption Festplatten verschieben 6-24

Patch-Verwaltung mit Full Disk Encryption 6-25
Command Line Helper verwenden 6-26
Patching-Verfahren für Full Disk Encryption 6-27

Kapitel 7: File Encryption

File Encryption registrieren 7-2

File Encryption-Aktionen 7-3
Datei oder Ordner verschlüsseln 7-4
Funktion "Sicheres Löschen" von File Encryption verwenden 7-10

File Encryption - Kontextmenü 7-11
Kennwort in File Encryption ändern 7-13
Mit Remote-Hilfe ein File Encryption Gerät entsperren 7-13

File Encryption Authentifizierung 7-15
Voraussetzungen für die Domänenauthentifizierung 7-16
Erzwungene Kennwortzurücksetzung 7-16
Richtlinienregeln für Endpoint Encryption Geräte 7-17

Synchronisierung von Richtlinien 7-18

Kapitel 8: Encryption Management für Fremdprodukte

Info über Agents zur Encryption Management 8-2

Einschränkungen der Agent-Richtlinie der Encryption Management ... 8-2

Encryption Management for Microsoft BitLocker 8-5
Status der Verschlüsselung anzeigen 8-6
Grundlegendes zum Verschlüsselungsstatus 8-6
Grundlegendes zu Agent-Informationen 8-8
Richtlinien mit PolicyServer synchronisieren 8-9

Encryption Management for Apple FileVault 8-11
Status der Verschlüsselung anzeigen 8-12
Grundlegendes zum Verschlüsselungsstatus 8-12
Grundlegendes zu Agent-Informationen 8-14
Richtlinien mit PolicyServer synchronisieren 8-15
Mobiles Konto für Active Directory unter Mac OS erstellen 8-17
Fehlerbehebung bei Kennwort- und Verschlüsselungsproblemen 8-18

Kapitel 9: Recovery

Preboot-Fehler nach der Installation 9-2

Full Disk Encryption Wiederherstellungsmethoden 9-4

Wiederherstellungskonsole 9-6
Optionen der Wiederherstellungskonsole 9-7
Von Full Disk Encryption Preboot auf die Wiederherstellungskonsole zugreifen 9-8
Auf die Wiederherstellungskonsole von Windows aus zugreifen ... 9-9
Festplattenoptionen verwalten 9-10
Verschlüsseln von Festplatten 9-11
Festplatten entschlüsseln 9-12
Partit. bereitst. 9-15
Boot wiederherst. 9-15
Full Disk Encryption Benutzer verwalten 9-17
Richtlinien verwalten 9-19
Protokolle anzeigen 9-19
Netzwerk 9-20

Recovery-Tool 9-26
Recovery-Tool vorbereiten 9-27
Eine Festplatte überprüfen und reparieren 9-28
Verwenden von Umfangreiche Reparatur 9-30

Optionen des Recovery-Tools 9-32
Erweiterte Funktionen 9-33

Unterstützung durch Remote-Hilfe 9-36

Kapitel 10: Behobene und bekannte Probleme

Behobene Probleme 10-2
Behobene Probleme in Endpoint Encryption 6.0 10-2
Behobene Probleme in Endpoint Encryption 6.0 Update 1 10-3

Bekannte Probleme 10-4
Probleme in Verbindung mit PolicyServer MMC 10-4
Probleme bei der Integration von Control Manager 10-5
Probleme mit dem Plug-in des Endpoint Encryption Verteilungstools 10-6
Probleme von Full Disk Encryption 10-6
Probleme mit File Encryption 10-11
Probleme bei Encryption Management for Microsoft BitLocker 10-12
Probleme bei Encryption Management for Apple FileVault 10-12

Kapitel 11: Technischer Support

Ressourcen zur Fehlerbehebung 11-2
Support-Portal verwenden 11-2
Bedrohungsenzyklopädie 11-2

Kontaktaufnahme mit Trend Micro 11-3
Problemlösung beschleunigen 11-4

Verdächtige Inhalte an Trend Micro senden 11-4
E-Mail-Reputation-Dienste 11-5
File-Reputation-Dienste 11-5
Web-Reputation-Dienste 11-5

Sonstige Ressourcen 11-6
Download Center 11-6
Anregungen und Kritik 11-6

Anhänge

Anhang A: Wartungstools

Diagnostics Monitor verwenden A-2
Das Protokollserver-Tool verwenden A-5
Das Tool zum Ändern von Einstellungen für PolicyServer verwenden A-6

Anhang B: PolicyServer Nachrichten-IDs

Administratorwarnungen B-2
Audit-Protokoll-Warnungen B-6
Zertifikatswarnungen B-8
Gerätewarnungen B-8
Fehlerwarnungen B-10
Warnungen bei Full Disk Encryption B-11
Installationswarnungen B-14
Anmelde-/Abmeldewarnungen B-14
Mobilgerätewarnungen B-18
OCSP-Warnungen B-19
OTA-Warnungen B-19
Kennwortwarnungen B-20
PIN-Änderungswarnungen B-23
Smartcard-Warnungen B-24

Anhang C: Endpoint Encryption Dienste

Anhang D: Richtlinienzuordnung zwischen Management-Konsolen

Anhang E: Glossar

Stichwortverzeichnis

Stichwortverzeichnis IN-1

Kapitel 1

Einführung

Dieses Handbuch soll Sicherheitsadministratoren und IT-Fachkräfte bei der Verwaltung von Benutzern, Geräten, Richtlinien, Protokollen und Berichten in Endpoint Encryption durch Verwendung der PolicyServer MMC (Microsoft Management Console) unterstützen. Diese Dokumentation setzt allgemeine Kenntnisse über Verschlüsselungsmethoden, Geräteformatierung und -partitionierung und Client-Server-Architektur voraus.

Diese Hilfe ist ein ergänzender Leitfaden für Administratoren, die ein erweitertes Richtliniensetup benötigen. Allgemeine Information zur Verwaltung von Endpoint Encryption und Hilfe bei der Verwendung von Trend Micro Control Manager finden Sie im *Endpoint Encryption Administratorhandbuch*.

Kapitel 2

Info über Trend Micro Endpoint Encryption

Trend Micro™ Endpoint Encryption™ ist ein Garant für den Datenschutz, indem auf Endpunkten gespeicherte Daten, Dateien und Ordner sowie Wechselmedien auf vielen verschiedenen Plattformen verschlüsselt werden. Endpoint Encryption bietet eine granulare Steuerung von Richtlinien und lässt sich flexibel in andere Verwaltungstools von Trend Micro integrieren, einschließlich Control Manager und OfficeScan. Die innovativen Verteilungsfunktionen unterstützen Sie dabei, Agent-Software ohne großen Aufwand mit FIPS-konformer hardwarebasierter oder softwarebasierter Verschlüsselung zu verteilen, die für Endbenutzer völlig transparent ist und die Produktivität nicht beeinträchtigt. Nach der Verteilung wird die Sicherheitsverwaltung für Endpunkte durch automatisierte Berichterstellung, Audits und Richtliniensynchronisierung mit Endpoint Encryption PolicyServer vereinfacht.

Endpoint Encryption unterstützt Funktionen, um Remote-Befehle zu verteilen, verlorene Daten wiederherzustellen und die Identität der Benutzer zu schützen, während die Richtliniensynchronisierung in Echtzeit beibehalten wird. Wenn ein Endpunkt verloren geht oder gestohlen wird, können Sie von einem entfernten Standort aus einen Befehl zum Zurücksetzen oder „Auslöschen“ geben, um unverzüglich die unternehmensinternen Informationen zu schützen. Es gibt ebenfalls viele Wiederherstellungstools, die Endbenutzer bei der Datenrettung in dem Fall unterstützen, dass die Festplatte beschädigt wird. Endpoint Encryption fügt sich nahtlos in die vorhandenen unternehmensinternen Kontrollfunktionen ein und unterstützt eine

Vielzahl von Authentifizierungsmethoden, einschließlich der Integration in Active Directory und Ressourcen für Endbenutzer, die ihre Anmeldedaten vergessen haben.

Es werden folgende Themen behandelt:

- *Funktionen und Vorteile auf Seite 2-3*
- *Neues auf Seite 2-4*
- *Info über PolicyServer auf Seite 2-6*
- *Management-Konsolen auf Seite 2-7*
- *Endpoint Encryption Agents auf Seite 2-9*
- *Authentifizierungsmethode auf Seite 2-11*

Funktionen und Vorteile

In der folgenden Tabelle werden die Hauptfunktionen und Vorteile von Endpoint Encryption erläutert.

TABELLE 2-1. Endpoint Encryption Die wichtigsten Funktionen

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 • Umfassender Schutz von Dateien, Ordnern und Wechselmedien
Authentifizierung	• Flexible Authentifizierungsmethoden, einschließlich Einzel- und Multi-Faktor-Authentifizierung • Steuern der Kennwortstärke und Regelmäßigkeit von Kennwortänderungen • Richtlinienaktualisierungen vor der Authentifizierung und dem Systemstart • Konfigurierbare Aktionen für den Schwellenwert für die Eingabe falscher Kennwörter
Geräteverwaltung	• Richtlinien zum Schutz von Daten auf Endpunkten und Wechselmedien • Möglichkeit zum Sperren, Zurücksetzen, Löschen oder Auslöschen eines Geräts

Funktion	Vorteile
Zentrale Verwaltung	• Flexible Verwendung entweder von PolicyServer MMC oder Control Manager zur Verwaltung von PolicyServer • Verteilen von Endpoint Encryption Agents auf bereits von OfficeScan verwaltete Endpunkte • Durchsetzung von Sicherheitsrichtlinien für Einzelpersonen oder Richtliniengruppen von einem einzigen Richtlinienserver aus • Unmittelbarer Schutz von Endbenutzerdaten durch Senden von Sperr- oder Löschbefehlen an verlorene oder gestohlene Endpoint Encryption Geräte • Automatisierte Durchsetzung von Richtlinien mit Korrekturen an Sicherheitsereignissen • Aktualisieren von Sicherheitsrichtlinien in Echtzeit vor der Authentifizierung, um Benutzer-Anmeldedaten vor dem Booten des Betriebssystems zu widerrufen
Aufzeichnung von Protokollen, Berichten und Auditing	• Erweiterte Berichtsfunktion und erweitertes Auditing in Echtzeit zur Einhaltung der Sicherheitsrichtlinien • Analysieren von Nutzungsstatistik mit geplanten Berichten und Warnmeldungen

Neues

Trend Micro Endpoint Encryption 6.0 bietet die folgenden Funktionen und Erweiterungen.

Tabelle 2-2. Neuigkeiten in Endpoint Encryption 6.0

Funktionen/ Verbesserungen	Beschreibung
Unterstützung für UEFI-Firmware	Endpoint Encryption unterstützt nun Starts auf Endpunkten mit UEFI-Firmware.

Funktionen/ Verbesserungen	Beschreibung
Verbesserte Laufwerkleistung mit dem Verschlüsselungsmodus AES-XTS	Bei neuen Installationen verwendet Endpoint Encryption standardmäßig die Methode AES-XTS. Vorhandene Agents, die auf diese Version aktualisiert wurden, verwenden jedoch weiterhin den vorhandenen Verschlüsselungsmodus AES-CBC. Außerdem kann Endpoint Encryption Endpunkte verwalten, auf denen beide Verschlüsselungsmodi, AES-XTS und AES-CBC, verwendet werden.
Unterstützung für Systeme mit mehr als einem physischen Laufwerk	Endpoint Encryption verschlüsselt alle Festplattenlaufwerke während der Installation. Darüber hinaus können Benutzer alle angeschlossenen Festplattenlaufwerke nach der Installation auch manuell verschlüsseln.
Richtlinien für WLAN-Preboot	WLAN-Einstellungen können mittels in PolicyServer verfügbarer neuer Richtlinien weiter angepasst werden. Mit diesen Richtlinieneinstellungen wird der Zugriff auf die WLAN-Einstellungen während des Preboots zugelassen oder eingeschränkt.
Anpassung des Preboot-Fensters	PolicyServer unterstützt nun Anpassungen des Preboot-Fensters.
Verschlüsselung des verwendeten Festplattenspeichers für Full Disk Encryption	Full Disk Encryption verschlüsselt nur den verwendeten Festplattenspeicher. Dies führt dazu, dass der Verschlüsselungsvorgang beschleunigt wird.
Sicherheitsprüfung	Endpoint Encryption führt nach der Installation eine Sicherheitsprüfung aus, um sicherzustellen, dass die Installation erfolgreich abgeschlossen wurde. War die Installation erfolgreich, lädt Endpoint Encryption das Preboot-Fenster und beginnt mit der Verschlüsselung. War die Installation hingegen nicht erfolgreich (oder wurde ein erzwungener Herunterfahrvorgang erkannt), lädt Endpoint Encryption das Preboot-Fenster nicht.
Synchronisierung mehrerer Active Directory-Domänen mit PolicyServer	Endpoint Encryption unterstützt die Synchronisierung mehrerer Active Directory-Domänen mit PolicyServer.

Info über PolicyServer

Trend Micro PolicyServer verwaltet Verschlüsselungsschlüssel und synchronisiert Richtlinien mit allen Endpunkten im Unternehmen. PolicyServer setzt ferner die sichere Authentifizierung durch und umfasst Echtzeit-Audits und Tools zur Berichterstellung, um die Einhaltung von gesetzlichen Bestimmungen sicherzustellen. Sie können PolicyServer mit PolicyServer MMC oder mit Trend Micro Control Manager flexibel verwalten. Andere Funktionen zur Datenverwaltung umfassen benutzerseitige Selbsthilfe-Optionen und Geräteaktionen, um ein verlorenes oder gestohlenes Gerät von einem entfernten Standort aus zurückzusetzen oder „auszulöschen“.

In der folgenden Tabelle werden die Komponenten von PolicyServer beschrieben, die Sie abhängig von den Anforderungen in der Umgebung auf einem oder mehreren Servern verteilen können.

TABELLE 2-3. Komponenten von PolicyServer

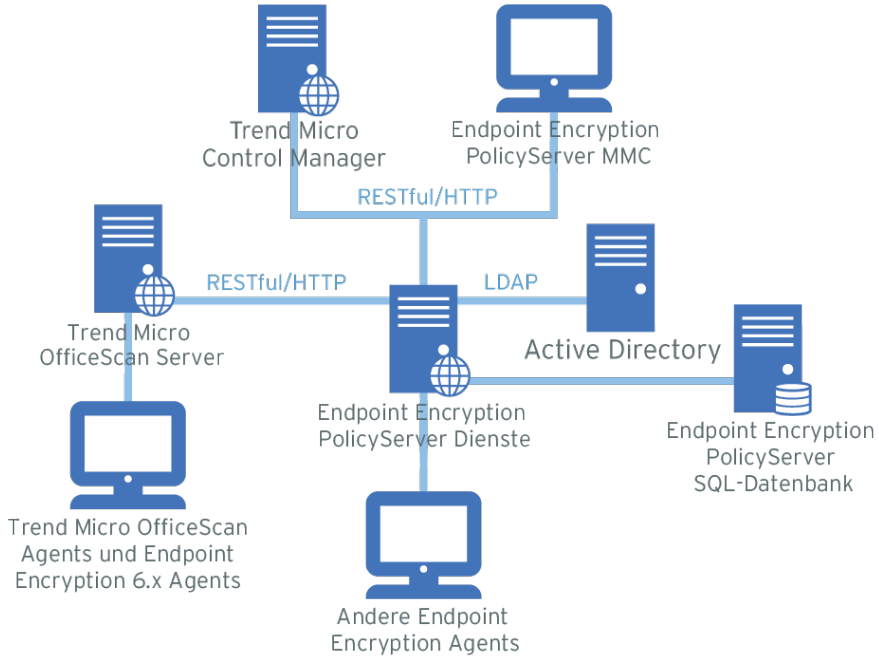
KOMPONENTE	BESCHREIBUNG
Unternehmen	Das Endpoint Encryption-Unternehmen ist der eindeutige Bezeichner für das Unternehmen in der PolicyServer Datenbank, der bei der Installation von PolicyServer konfiguriert wurde. In einer PolicyServer Datenbank darf es nur eine Unternehmenskonfiguration geben.
Datenbank	In der Microsoft SQL-Datenbank von PolicyServer werden alle Benutzer, Geräte und Protokolldaten sicher gespeichert. Die Datenbank ist entweder auf einem dedizierten Server konfiguriert oder wird einem vorhandenen SQL-Cluster hinzugefügt. Die Protokoll- und anderen Datenbanken können sich an unterschiedlichen Speicherorten befinden.
PolicyServer Windows-Dienst	Der PolicyServer Windows-Dienst verwaltet alle Kommunikationstransaktionen zwischen dem Host-Betriebssystem, Endpoint Encryption Dienst, Legacy Web Service, Client Web Proxy und SQL-Datenbanken.

Komponente	Beschreibung
Endpoint Encryption Dienst	Ab Endpoint Encryption 5.0 verwenden alle Agents den Endpoint Encryption Service zur Kommunikation mit PolicyServer. Der Endpoint Encryption Dienst verwendet eine Representational State Transfer Web-API (RESTful) mit einem AES-GCM-Verschlüsselungsalgorithmus. Nachdem sich ein Benutzer authentifiziert hat, generiert PolicyServer ein Token im Zusammenhang mit der spezifischen Richtlinienkonfiguration. Bis zur Authentifizierung durch den Endpoint Encryption Benutzer sperrt der Dienst alle Richtlinientransaktionen.
Legacy Web-Service	Alle Agents von Endpoint Encryption 3.1.3 und niedriger verwenden SOAP (Simple Object Access Protocol), um mit PolicyServer zu kommunizieren. In bestimmten Situationen erlaubt SOAP möglicherweise unsichere Richtlinientransaktionen ohne Benutzerauthentifizierung. Legacy Web Service filtert SOAP-Aufrufe, indem eine Authentifizierung erforderlich gemacht wird und die Befehle begrenzt werden, die SOAP akzeptiert. Dieser Dienst ist optional und kann auf demselben Endpunkt wie der Endpoint Encryption Service installiert werden, der das Endpoint Encryption-Proxy-Installationsprogramm verwendet.

Management-Konsolen

Administratoren können Endpoint Encryption nur mit PolicyServer MMC flexibel verwalten oder sie verwalten Endpoint Encryption mit Control Manager zur Verwaltung von Richtlinien, Benutzern und Geräten und setzen PolicyServer MMC für die erweiterte Protokollverwaltung und Berichterstellung ein.

Die folgende Darstellung zeigt, wie Endpoint Encryption mithilfe von Control Manager bereitgestellt werden muss, um PolicyServer zu verwalten. In einer Control Manager Installation setzen Administratoren Control Manager für alle Endpoint Encryption Richtlinien, Benutzer und Gerätefunktionen ein und verwenden PolicyServer MMC nur für die erweiterte Unternehmenswartung.



Hinweis

In Umgebungen, in denen Control Manager eingesetzt wird, werden Änderungen an PolicyServer Richtlinien immer von Control Manager gesteuert. Alle mit PolicyServer MMC durchgeführten Änderungen werden beim nächsten Mal überschrieben, wenn Control Manager die Richtlinien mit der PolicyServer Datenbank synchronisiert.

Trend Micro Control Manager

Trend Micro™ Control Manager™ ist eine zentrale Management-Konsole zur Verwaltung von Produkten und Diensten von Trend Micro auf Gateway-, Mailserver-, Dateiserver- und Corporate-Desktop-Ebene. Die webbasierte Management-Konsole von Control Manager bietet einen zentralen Überwachungspunkt für verwaltete Produkte und Dienste im gesamten Netzwerk.

Mit Control Manager können Systemadministratoren Aktivitäten wie beispielsweise auftretende Virenausbrüche, Sicherheitsverstöße oder mögliche Vireneintrittsstellen überwachen und aufzeichnen. Systemadministratoren können Komponenten herunterladen und im Netzwerk verteilen und somit einen einheitlichen und aktuellen Schutz gewährleisten. Mit Control Manager sind sowohl manuelle als auch zeitgesteuerte Updates möglich. Außerdem können Produkte als Gruppen oder einzeln konfiguriert und verwaltet werden.

Info über PolicyServer MMC

Das Plug-in PolicyServer Microsoft Management Console (PolicyServer MMC) ist die native Management-Konsole zur Verwaltung von Richtlinien, Benutzern und Geräten für Endpoint Encryption.

Sie können mit PolicyServer MMC Folgendes zentral verwalten:

- Alle Endpoint Encryption Benutzer, Geräte und Gruppen
- Alle Verschlüsselungs-, Kennwortkomplexitäts- und Authentifizierungsrichtlinien
- Remote-Aktionen zur Gerätemanipulation, inkl. Auslöschen eines Geräts, Löschen von Daten oder Verzögern der Authentifizierung
- Ereignisprotokolle über Authentifizierungsereignisse, Verwaltungsereignisse und Sicherheitsverstöße sowie den Geräteverschlüsselungsstatus
- Remote-Hilfe zum Zurücksetzen des Kennworts
- Optionen für Audits und Berichterstellung

Endpoint Encryption Agents

In der folgenden Tabelle werden die Endpoint Encryption Agents beschrieben, die für eine Vielzahl von Umgebungen verfügbar sind.

Agent	Beschreibung
Full Disk Encryption	Der Endpoint Encryption Agent für die Verschlüsselung von Hardware und Software mit Preboot-Authentifizierung. Full Disk Encryption sichert Datendateien, Anwendungen, Registrierungseinstellungen, temporäre Dateien, Auslagerungsdateien, Druck-Spooler und gelöschte Dateien auf allen Windows-Endpunkten. Eine starke Preboot-Authentifizierung beschränkt den Zugriff auf das anfällige System, bis der Benutzer validiert wird. Der Full Disk Encryption Agent kann auf demselben Endpunkt wie der File Encryption Agent installiert werden. Der Full Disk Encryption Agent darf nicht auf demselben Endpunkt wie entweder der Encryption Management for Microsoft BitLocker Agent oder der Encryption Management for Apple FileVault Agent installiert werden.
Encryption Management for Microsoft BitLocker	Der Endpoint Encryption Full Disk Encryption Agent für Microsoft Windows-Umgebungen, auf denen lediglich Microsoft BitLocker auf dem Hosting-Endpunkt aktiviert werden muss. Der Encryption Management for Microsoft BitLocker Agent kann auf demselben Endpunkt wie der File Encryption Agent installiert werden.
Encryption Management for Apple FileVault	Der Endpoint Encryption Full Disk Encryption Agent für Mac OS-Umgebungen, auf denen lediglich Apple FileVault auf dem Hosting-Endpunkt aktiviert werden muss.
File Encryption	Der Endpoint Encryption Agent für die Verschlüsselung von Dateien und Ordnern auf lokalen Laufwerken und Wechselmedien. Mit File Encryption können Sie die Dateien und Ordner auf nahezu jedem Gerät, das als Laufwerk im Host-Betriebssystem angezeigt wird, schützen. Der File Encryption Agent kann auf demselben Endpunkt wie entweder der Full Disk Encryption Agent oder der Encryption Management for Microsoft BitLocker Agent installiert werden.

Authentifizierungsmethode

Für Endpoint Encryption Administratoren und Benutzer stehen mehrere Authentifizierungsmethoden zur Anmeldung an den Endpoint Encryption Geräten zur Verfügung. Die verfügbaren Methoden werden vom PolicyServer Richtlinienkonfiguration bestimmt.

Hinweis

Sie müssen die für die Endpoint Encryption Benutzer verfügbaren Authentifizierungsmethoden mit PolicyServer MMC konfigurieren. Es ist nicht möglich, mit Control Manager die zulässigen Authentifizierungsmethoden zu konfigurieren. Sie können jedoch Control Manager für die Domänenauthentifizierung konfigurieren.

TABELLE 2-4. Unterstützte Authentifizierungsmethoden

AUTHENTIFIZIERUNGSMETHODE	BESCHREIBUNG
ColorCode auf Seite 2-12	Eine eindeutige Farbfolge.
Domänenauthentifizierung auf Seite 2-12	Active Directory LDAP-Synchronisierung für Single Sign-On (SSO).
Festes Kennwort auf Seite 2-13	Eine Zeichenfolge aus Zeichen, Ziffern und Symbolen.
PIN auf Seite 2-13	Eine herkömmliche PIN.
Remote-Hilfe auf Seite 2-14	Interaktive Authentifizierung für Benutzer, die ihre Anmeldedaten vergessen haben, oder für Geräte, deren Richtlinien nicht innerhalb eines bestimmten Zeitraums synchronisiert wurden.
Selbsthilfe auf Seite 2-14	Kombinationen aus Fragen und Antworten, mit denen ein Benutzer ein vergessenes Kennwort zurücksetzen kann, ohne sich an den technischen Support zu wenden.
SmartCard auf Seite 2-15	Eine physische Karte wird in Verbindung mit einer PIN oder einem festen Kennwort verwendet.

ColorCode

ColorCode™ ist eine einzigartige Authentifizierungsmethode, bei deren Entwicklung eine schnelle Eingabe und eine leichte Merkfähigkeit im Vordergrund standen. Die ColorCode-Authentifizierung besteht nicht aus alphanumerischen Zeichen oder Symbolen, sondern aus einer vom Benutzer erstellten Farbfolge (Beispiel: rot, rot, blau, gelb, blau, grün).

ABBILDUNG 2-1. Das Fenster "ColorCode-Authentifizierung"

Domänenauthentifizierung

Endpoint Encryption kann in Active Directory mit LDAP integriert werden, das in PolicyServer konfiguriert wird. Die Domänenauthentifizierung von Endpoint Encryption ermöglicht es Benutzern von Endpoint Encryption, SSO (Single Sign-On) zwischen dem Betriebssystem und dem Endpoint Encryption Agent einzusetzen. Benutzer von Endpoint Encryption mit Domänenauthentifizierung müssen beispielsweise nur einmal ihre Anmeldedaten für die Authentifizierung für Full Disk Encryption Preboot, Anmeldung bei Windows und den Zugriff auf die Dateien, die durch File Encryption geschützt werden, eingeben.

Vergewissern Sie sich, ob die folgenden Voraussetzungen erfüllt sind, damit die Active Directory-Integration nahtlos bewerkstelligt werden kann:

- PolicyServer ist der Domäne beigetreten.
- Alle Endpoint Encryption Geräte befinden sich im selben Active Directory und in derselben Domäne wie PolicyServer.
- Die in Active Directory konfigurierten Benutzernamen stimmen genau mit den Benutzernamen überein, die in PolicyServer (einschließlich Groß- oder Kleinschreibung) konfiguriert wurden.
- Die Benutzernamen befinden sich innerhalb einer PolicyServer Gruppe und die Richtlinie "Domänenauthentifizierung" ist aktiviert.
- Der Host-Name und der Domänenname sind auf Grundlage von LDAP oder den Servereinstellungen für Active Directory ordnungsgemäß konfiguriert.

Hinweis

Weitere Informationen zur Konfiguration von LDAP- und Active Directory-Einstellungen finden Sie im *Endpoint Encryption Installationshandbuch* auf:

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

Festes Kennwort

Die Authentifizierung mit festem Kennwort ist die gängigste Authentifizierungsmethode. Das feste Kennwort wird vom Benutzer angelegt. Dabei kann es sich fast um jede Zeichenfolge aus Ziffern, Buchstaben und Symbolen handeln. Sie können für feste Kennwörter Einschränkungen festlegen, um sicherzustellen, dass diese nicht leicht missbraucht werden können.

PIN

Eine PIN ist die gängigste Identifizierungsmethode, bei der die Eingabe einer eindeutigen Zahlenfolge erforderlich ist. Die PIN wird vom Benutzer angelegt und kann

fast alles sein. Wie bei festen Kennwörtern können Sie auch für PIN-Kombinationen Einschränkungen festlegen.

Remote-Hilfe

Mit der Remote-Hilfe können Gruppen- oder Unternehmensauthentifizierer ausgesperrte Endpoint Encryption Benutzer unterstützen, die sich nach zu vielen erfolglosen Versuchen oder, wenn zu viel Zeit seit der letzten PolicyServer Synchronisierung vergangen ist, nicht bei Endpoint Encryption Geräten anmelden können.

Hinweis

Die Remote-Hilfe-Authentifizierung wird durch die Richtlinienregeln des Endpoint Encryption Geräts ausgelöst. Die Richtlinienregeln für die Remote-Hilfe können sowohl mit PolicyServer MMC als auch mit Control Manager konfiguriert werden.

Selbsthilfe

Mit der Selbsthilfe-Authentifizierung können Endpoint Encryption Benutzer, die ihre Anmeldedaten vergessen haben, ohne die Hilfe durch den technischen Support Sicherheitsfragen beantworten und sich bei Endpoint Encryption Geräten anmelden. Die Endpoint Encryption Benutzer werden aufgefordert, die vordefinierten persönlichen Herausforderungsfragen der Selbsthilfe zu beantworten. Mit der Selbsthilfe kann ein festes Kennwort oder eine andere Authentifizierungsmethode ersetzt werden.

Beachten Sie bei der Auswahl Ihrer Authentifizierungsmethode oder bei der Konfiguration von der Selbsthilfe Folgendes:

- Die Selbsthilfe ist nicht für Administrator- und Authentifiziererkonten verfügbar.
- Die Selbsthilfe ist nicht für Konten verfügbar, die die Domänenauthentifizierung verwenden. PolicyServer kann vorherige Domänenkennwörter nicht ändern oder wiederherstellen.
- Die Selbsthilfe verfügt über maximal sechs Fragen für jedes Benutzerkonto. Benutzer können sich möglicherweise über die Selbsthilfe nicht anmelden, wenn mehr als sechs Fragen konfiguriert sind.

- Die Selbsthilfe kann nur mit PolicyServer MMC konfiguriert werden.

SmartCard

Die Smartcard-Authentifizierung erfordert sowohl eine PIN als auch ein physisches Token zur Bestätigung der Identität des Benutzers. Smartcard-Zertifikate sind mit dem Benutzerkonto und der zugewiesenen Gruppe des Benutzer verbunden. Nach der Registrierung kann der Benutzer die Smartcard-Authentifizierung von jedem Endpoint Encryption Gerät in der betreffenden Gruppe verwenden. Benutzer können nach Belieben jedes Endpoint Encryption Gerät in ihrer Gruppe verwenden und müssen kein Einmalkennwort anfordern.

Stellen Sie zur Verwendung der Smartcard-Authentifizierung sicher, dass die folgenden Anforderungen erfüllt werden:

- Das Smartcard-Lesegerät ist mit dem Endpunkt verbunden, wobei sich die Smartcard im Lesegerät befindet.
- ActivClient 6.2 ist mit allen Service Packs und Updates installiert.

Hinweis

ActivClient 7.0 und höher wird nicht unterstützt.

- Geben Sie die Smartcard-PIN in das Kennwortfeld ein.

Warnung!

Wenn kein gültiges Kennwort eingegeben wird, wird ein Kennwortfehler gesendet und die Smartcard kann gesperrt werden.

Hinweis

- Smartcard-Authentifizierung kann nur mit PolicyServer MMC konfiguriert werden.
- Die Änderung der Authentifizierungsmethode von Smartcard- in Domänenauthentifizierung kann bei Domänenbenutzern, die über ADSync oder Active Directory-Benutzerimport hinzugefügt wurden, zu Problemen führen. Zur Behebung dieses Problems entfernen Sie das Domänenbenutzerkonto aus dem Unternehmen und starten dann die PolicyServer-Dienste neu, um die Synchronisierung mit dem AD-Server zu starten. Während der Synchronisierung wird der Benutzer erneut mit Domänenauthentifizierung als Authentifizierungsmethode hinzugefügt. Alternativ können Sie das Domänenbenutzerkonto auch per Active Directory-Benutzerimport erneut hinzufügen.

Kapitel 3

Erste Schritte

In diesem Kapitel werden die ersten Schritte mit Trend Micro Control Manager zur Verwaltung von PolicyServer beschrieben.

Es werden folgende Themen behandelt:

- *Systemvoraussetzungen auf Seite 3-2*
- *Control Manager einrichten auf Seite 3-17*
- *Active Directory-Synchronisierung auf Seite 3-25*

Systemvoraussetzungen

In diesem Kapitel werden die Systemvoraussetzungen für Trend Micro Endpoint Encryption beschrieben.

Es werden folgende Themen behandelt:

- *Systemvoraussetzungen für PolicyServer auf Seite 3-2*
- *Systemvoraussetzungen für PolicyServer MMC auf Seite 3-9*
- *Full Disk Encryption Systemvoraussetzungen auf Seite 3-9*
- *Systemvoraussetzungen für File Encryption auf Seite 3-13*
- *Systemvoraussetzungen für die Encryption Management for Microsoft BitLocker auf Seite 3-14*
- *Systemvoraussetzungen für die Encryption Management for Apple FileVault auf Seite 3-16*

Systemvoraussetzungen für PolicyServer

Hardware- und Skalierungsvoraussetzungen

Im Folgenden werden die Verteilungs- und Skalierungsvoraussetzungen in mehreren Umgebungen unterschiedlicher Größe aufgeführt. Im Umgebungen mit einem kleinerem Netzwerk können PolicyServer SQL-Datenbanken auf demselben Server installiert werden. Für PolicyServer-Verteilungen in Umgebungen mit mehr als 1500 Geräten empfiehlt Trend Micro mindestens zwei dedizierte Server:

1. einen dedizierten Server für die PolicyServer-Dienste, auch als „Front-End-Server“ bekannt
2. einen dedizierten Server für die Datenbank, oder fügen Sie die Datenbank einem bestehenden SQL-Cluster hinzu

In der folgenden Tabelle werden die grundlegenden Anforderungen einer PolicyServer SQL-Datenbank für den jeweiligen Anwendungsfall angezeigt:

Geräte	Anforderungen des PolicyServer-Frontends	Anforderungen der PolicyServer SQL-Datenbank
1.000	• Ein Frontend- und SQL-Datenbankserver mit mehreren Rollen und einem Intel Xeon Quad-Core 2.2 GHz-Prozessor oder höher • 8 GB Arbeitsspeicher • Festplatte mit 120 GB	Installiert auf PolicyServer Frontend-Server
4.000	• Ein Frontend- und SQL-Datenbankserver mit mehreren Rollen und einem Intel Xeon Quad-Core 2.2 GHz-Prozessor oder höher • 8 GB Arbeitsspeicher • Festplatte mit 150 GB	Installiert auf PolicyServer Frontend-Server
8.000	• Zwei Frontend-Server mit jeweils einem Intel Xeon Quad-Core 2.2 GHz-Prozessor oder höher • 4 GB Arbeitsspeicher • Festplatte mit 40 GB	• Ein SQL-Datenbankserver mit einem Intel Xeon Quad-Core 2.2 GHz-Prozessor oder höher • 8 GB Arbeitsspeicher • Festplatte mit 150 GB
20.000	• Vier Frontend-Server mit jeweils einem Intel Xeon Quad-Core 2.2 GHz-Prozessor oder höher • 4 GB Arbeitsspeicher • Festplatte mit 40 GB	• Zwei SQL-Datenbankserver (einen für die Richtliniendatenbank und einen für die Protokolldatenbank) mit jeweils einem Intel Xeon Quad-Core 2.2 GHz-Prozessor oder höher • 8 GB Arbeitsspeicher • RAID-5-Festplatte mit 180 GB

Geräte	Anforderungen des PolicyServer-Frontends	Anforderungen der PolicyServer SQL-Datenbank
40.000	• Acht Frontend-Server mit jeweils einem Intel Xeon Quad-Core 2.2 GHz-Prozessor oder höher • 4 GB Arbeitsspeicher • Festplatte mit 40 GB	• Zwei SQL-Datenbankserver (einen für die Richtliniendatenbank und einen für die Protokolldatenbank) mit jeweils einem Intel Xeon Quad-Core 2.2 GHz-Prozessor oder höher • 16 GB Arbeitsspeicher • RAID-5-Festplatte mit 350 GB gemeinsam genutztem SAN

Hinweis

- Virtualisierte Hardware wird unter VMware Virtual Infrastructure unterstützt.
- Microsoft oder VMware auf virtualisierter Hardware bietet keine Unterstützung für den Microsoft Cluster Service.
- Basistests wurden auf einem Endpunkt mit einer Intel Xeon-CPU E5-2650 v4 2.20 GHz, 2200 MHz durchgeführt.

Anforderungen bezüglich der Redundanz

Bei größeren Umgebungen empfiehlt Trend Micro, zusätzliche Server hinzuzufügen, um das Vorhandensein einzelner Fehlerquellen zu vermeiden. In der folgenden Tabelle werden die Anforderungen für die PolicyServer SQL-Datenbank in einer Umgebung mit erhöhter Redundanz angezeigt:

Tipp

Trend Micro empfiehlt die Einrichtung von Redundanz in Umgebungen mit mehr als 8.000 Geräten.

Geräte	Anforderungen des PolicyServer-Frontends	PolicyServer SQL-Datenbank ohne einzelne Fehlerquellen
8.000	• Vier Frontend-Server mit jeweils einem Intel Xeon Quad-Core 2.2 GHz-Prozessor oder höher • 4 GB Arbeitsspeicher • Festplatte mit 40 GB	• Ein SQL-Server-Cluster mit zwei Knoten und Intel Xeon Quad-Core 2.2 GHz-Prozessoren oder höher • 8 GB Arbeitsspeicher • RAID-5-Festplatte mit 60 GB • RAID-5-Festplatte mit 150 GB gemeinsam genutztem SAN
20.000	• Sechs Frontend-Server mit jeweils Intel Xeon Quad-Core 2.2 GHz-Prozessoren oder höher • 4 GB Arbeitsspeicher • Festplatte mit 40 GB	• Zwei SQL-Server-Cluster mit zwei Knoten und Intel Xeon Quad-Core 2.2 GHz-Prozessoren oder höher • 8 GB Arbeitsspeicher • RAID-5-Festplatte mit 60 GB • RAID-5-Festplatte mit 180 GB gemeinsam genutztem SAN
40.000	• Zwölf Frontend-Server mit jeweils Intel Xeon Quad-Core 2.2 GHz-Prozessoren oder höher • 4 GB Arbeitsspeicher • Festplatte mit 40 GB	• Zwei SQL-Server-Cluster mit zwei Knoten und Intel Xeon Quad-Core 2.2 GHz-Prozessoren oder höher • 16 GB Arbeitsspeicher • RAID-5-Festplatte mit 60 GB • RAID-5-Festplatte mit 350 GB gemeinsam genutztem SAN

Hinweis

- Virtualisierte Hardware wird unter VMware Virtual Infrastructure unterstützt.
- Microsoft oder VMware auf virtualisierter Hardware bietet keine Unterstützung für den Microsoft Cluster Service.
- Basistests wurden auf einem Endpunkt mit einer Intel Xeon-CPU E5-2650 v4 2.20 GHz, 2200 MHz durchgeführt.

Software-Voraussetzungen

Spezifikation	Voraussetzungen
Betriebssystem	• Windows Server 2008/2008 R2 (64-Bit-Version) • Windows Server 2012/2012 R2 (64-Bit-Version) • Windows Server 2016 (64-Bit)
Datenbankserver	• Microsoft SQL Server 2008 / 2008 R2 / 2012 / 2012 R2 / 2014 / 2016 • Microsoft SQL Server Express 2008 / 2012 / 2014 / 2016 • Mixed Mode Authentication (SA-Kennwort) installiert • Berichtsdienste installiert **Hinweis** Für Windows Server 2008 R2 müssen Sie SQL Server 2008 SP1 installieren.

Anwendungsserver	PolicyServer 6.0 erfordert Microsoft-Internetinformationsdienste (IIS), wobei folgende Rollen installiert und aktiviert sein müssen:
	• Anwendungsbereitstellung
	  • ASP.NET
	  • ASP

Spezifikation	Voraussetzungen
	• ISAPI-Erweiterungen • ISAPI-Filter • Management-Tools • IIS-Verwaltungskonsole • IIS-Verwaltungsskripts und -tools • Verwaltungsdienst • IIS 6-Verwaltungskompatibilität • IIS 6-Metabasiskompatibilität Für Windows Server 2008 und 2008 R2 müssen Sie die Rolle „Anwendungsserver“ und die Rolle „Webserver“ installieren. Darüber hinaus müssen Sie Funktionen zur Unterstützung für SMTP und Microsoft IIS hinzufügen. Ältere Endpoint Encryption Umgebungen (Version 3.1.3 und früher) benötigen Client-Web-Service. Wenn Sie Client-Web-Service auf einem Remote-Endpunkt installieren, installieren Sie Microsoft IIS auf diesem Endpunkt.
Andere Software	• Sowohl Microsoft .NET Framework 2.0 SP2 (oder 3.5) als auch 4.0 • Windows Installer 4.5 (SQL Express)

Installationsdateien

Datei	Zweck
`PolicyServerInstaller.exe`	Installiert PolicyServer Datenbanken und Dienste. Optional kann PolicyServer MMC gleichzeitig installiert werden.
`PolicyServer MMCSnapinSetup.msi`	Installiert nur PolicyServer MMC.

Datei	Zweck
`TMEEProxyInstaller.exe`	Installiert den Client-Web-Service und den Traffic Forwarding Service. Diese Dienste fungieren als Web-Proxys und Kommunikationsprotokolle für Umgebungen, in denen sich PolicyServer und Endpoint Encryption Agents in unterschiedlichen LANs befinden. Client-Web-Service bietet Funktionen für Agents der Versionen 3.1.3 oder früher und Traffic Forwarding Service für Agents der Versionen 5.0 oder höher.

Hinweis

PolicyServer enthält eine Testlizenz für 30 Tage. Um ein Upgrade auf die vollständige Produktversion durchzuführen, registrieren Sie Ihr Produkt mit Ihrem Aktivierungscode in Control Manager oder PolicyServer MMC.

Erforderliche Konten

Konto	Funktion	Beschreibung
SQL SA	PolicyServer Installationsprogramm	Das 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.
Lokaler Administrator	PolicyServer Windows-Dienst und IIS	Über dieses Konto werden der PolicyServer Windows-Dienst und der Web-Service ausgeführt.

Systemvoraussetzungen für PolicyServer MMC

Hinweis

PolicyServer MMC kann auf dem PolicyServer Frontend-Server oder auf einem anderen Endpunkt, der über eine Netzwerkverbindung mit PolicyServer verfügt, installiert werden.

Spezifikation	Voraussetzungen
Prozessor	Intel Core 2 Duo 2.0 GHz-Prozessor oder gleichwertiger Prozessor
RAM	512 MB
Festplattenspeicher	100 MB
Netzwerkverbindung	Verbindung mit PolicyServer
Betriebssystem	Jedes Microsoft Windows-Betriebssystem, das von PolicyServer oder den Endpoint Encryption Agents unterstützt wird
Andere	Microsoft .NET Framework 4.0

Full Disk Encryption Systemvoraussetzungen

Spezifikation	Voraussetzungen
Prozessor	Intel Core 2 Duo 2.0 GHz-Prozessor oder gleichwertiger Prozessor
RAM	1 GB
Festplattenspeicher	• 30 GB • 20% verfügbaren Festplattenspeicher • 256 MB zusammenhängender freier Speicher
Netzwerkverbindung	Kommunikation mit PolicyServer für verwaltete Agents erforderlich

Spezifikation	Voraussetzungen
Betriebssystem	• Windows™ Embedded POSReady 7 (32-Bit/64-Bit) • Windows™ 10 (32 Bit/64 Bit) **Hinweis** Auf älteren auf Endpunkten installierten Windows 10-Builds mit aktivierter UEFI treten möglicherweise Probleme auf, wenn "Sicherer Start" eingeschaltet ist. Installieren Sie zur Vermeidung dieses Problem alle Servicepacks, Hotfixes und Sicherheitspatches für Windows 10, bevor Sie mit der Installation fortfahren. • Windows™ 8.1 (32 Bit/64 Bit) • Windows™ 8 (32 Bit/64 Bit) • Windows™ 7 (32 Bit/64 Bit)
Firmware-Schnittstelle	• BIOS: alle unterstützten Betriebssysteme • UEFI: alle unterstützten Betriebssysteme
Andere Software	• Microsoft .NET Framework 3.5 SP1 oder höher (Windows 7 und neuere Betriebssysteme)

Spezifikation	Voraussetzungen
Festplatte	Full Disk Encryption verwendet die softwarebasierte Verschlüsselung für alle Standardlaufwerke (Laufwerke ohne Selbstverschlüsselung). Full Disk Encryption verwendet die hardwarebasierte Verschlüsselung für die folgenden selbstverschlüsselnden Laufwerke (SEDs): • Seagate OPAL- und OPAL 2-Laufwerke • Selbstverschlüsselnde SanDisk-Solid-State-Laufwerke (SSDs) Für Full Disk Encryption gelten folgende Einschränkungen: • Full Disk Encryption unterstützt keine RAID- und SCSI-Laufwerke. • Full Disk Encryption unterstützt keine eDrive-Laufwerke für Umgebungen mit Windows 8 oder höher.
Festplattencontroller	• Software-Verschlüsselung: ATA-, AHCI- oder IRRT-Festplattencontroller • Hardware-Verschlüsselung: AHCI-Festplattencontroller

Empfohlene Festplattenkombinationen

Endpoint Encryption unterstützt Endpunkte mit maximal 32 angeschlossenen Festplatten. Full Disk Encryption empfiehlt die folgenden Festplattenkombinationen:

Primäre Festplatte	Sekundäre Festplatte	Empfehlung
Normale Systemfestplatte	Normale Datenfestplatte	Ja Die Festplatte muss neu oder zuvor verschlüsselt und mit PolicyServer verbunden worden sein.

Primäre Festplatte	Sekundäre Festplatte	Empfehlung
Normale Systemfestplatte	Als Datenfestplatte angeschlossene normale Systemfestplatte	Ja Wenn die Richtlinie **Preboot-Umgehung** auf **Zulassen** gesetzt ist, werden Sie von Full Disk Encryption dazu aufgefordert, eine Systemfestplatte zu entfernen.
Normale Systemfestplatte	SED-Datenfestplatte	Ja Die Festplatte muss neu oder zuvor verschlüsselt und mit PolicyServer verbunden worden sein.
SED-Systemfestplatte	SED-Datenfestplatte	Ja Die Festplatte muss neu oder zuvor verschlüsselt und mit PolicyServer verbunden worden sein.
SED-Systemfestplatte	Als Datenfestplatte angeschlossene SED-Systemfestplatte	Nein Das Installationsprogramm von Full Disk Encryption schließt die Installation zwar ab, kann aber nicht beide Festplatten verwalten. Wenn die Richtlinie **Preboot-Umgehung** auf **Zulassen** gesetzt ist, werden Sie von Full Disk Encryption dazu aufgefordert, eine Systemfestplatte zu entfernen

Primäre Festplatte	Sekundäre Festplatte	Empfehlung
SED-Systemfestplatte	Normale Datenfestplatte	Nein Das Installationsprogramm von Full Disk Encryption schließt die Installation zwar ab, kann aber die Festplatten nicht verwalten.

Wenn eine nicht empfohlene Festplatte gefunden wird, schließt das Installationsprogramm von Full Disk Encryption die Installation zwar ab, kann die nicht empfohlene Festplatte aber nicht verwalten. Darüber hinaus meldet das Installationsprogramm den Status **Nicht verwaltet** für die nicht empfohlene Festplatte.

Systemvoraussetzungen für File Encryption

In der folgenden Tabelle werden die Systemvoraussetzungen für File Encryption beschrieben.

Spezifikation	Voraussetzungen
Prozessor	Intel Core 2 Duo 2.0 GHz-Prozessor oder gleichwertiger Prozessor
RAM	1 GB
Festplattenspeicher	• 30 GB • 20% verfügbaren Festplattenspeicher
Netzwerkverbindung	Kommunikation mit PolicyServer für verwaltete Agents erforderlich
Betriebssystem	• Windows™ 10 (32 Bit/64 Bit) • Windows™ 8.1 (32 Bit/64 Bit) • Windows™ 8 (32 Bit/64 Bit) • Windows™ 7 (32 Bit/64 Bit)

SPEZIFIKATION	VORAUSSETZUNGEN
Andere Software	• Microsoft .NET Framework 3.5 SP1 (Windows 7 und neuere Betriebssysteme) • Microsoft Windows Installer 3.1

Systemvoraussetzungen für die Encryption Management for Microsoft BitLocker

In der folgenden Tabelle werden die minimalen und empfohlenen Systemvoraussetzungen für die Encryption Management for Microsoft BitLocker beschrieben.

SPEZIFIKATION	VORAUSSETZUNGEN
Prozessor	Intel Core 2 Duo 2.0 GHz-Prozessor oder gleichwertiger Prozessor
RAM	Die Voraussetzungen basieren auf den Systemvoraussetzungen für Windows: • 64-Bit-Systeme: 2 GB • 32-Bit-Systeme: 1 GB
Festplattenspeicher	• 30 GB • 20% verfügbaren Festplattenspeicher
Festplatte	• Standardlaufwerke, die von Windows unterstützt werden
Netzwerkverbindung	Verbindung mit PolicyServer

Spezifikation	Voraussetzungen
Betriebssystem	• Windows™ Embedded POSReady 7 (32-Bit/64-Bit) • Windows™ 10 Enterprise- und Professional-Editionen (32-Bit/64-Bit) • Windows™ 8.1 Enterprise- und Professional-Editionen (32-Bit/64-Bit) • Windows™ 8 Enterprise- und Professional-Editionen (32-Bit/64-Bit) • Windows™ 7 Enterprise- und Professional-Editionen (32-Bit/64-Bit)
Andere Software	• Trusted Platform Module (TPM) 1.2 oder höher • Full Disk Encryption ist nicht installiert • Microsoft .NET Framework 3.5 • Windows BitLocker ist deaktiviert **Warnung!** Full Disk Encryption kann nicht auf SED-Festplatten installiert werden, die an Geräte mit UEFI angeschlossen sind, wenn diese Festplatten zuvor von Windows Bitlocker verwaltet wurden. Führen Sie zur Installation von Full Disk Encryption auf diesen Festplatten eine der folgenden Aufgaben durch: • Konfigurieren Sie Full Disk Encryption, um softwarebasierte Verschlüsselung zu verwenden, indem Sie den Parameter `FORCESOFTWARE` während der Installation hinzufügen. Weitere Informationen finden Sie im Abschnitt **Full Disk Encryption Agent installieren** im Endpoint Encryption Installationshandbuch. • Setzen Sie die SED-Festplatte auf die Werkseinstellungen zurück. Hierdurch werden alle vorhandenen Daten von der SED-Festplatte gelöscht. Führen Sie nach dem Zurücksetzen der Festplatte das Installationsprogramm erneut aus.

Systemvoraussetzungen für die Encryption Management for Apple FileVault

In der folgenden Tabelle werden die minimalen und empfohlenen Systemvoraussetzungen für die Encryption Management for Apple FileVault beschrieben.

SPEZIFIKATION	VORAUSSETZUNG
Prozessor	Intel Core 2 Duo 2.0 GHz-Prozessor oder gleichwertiger Prozessor
Arbeitsspeicher	• Mindestens 512 MB • 2 GB empfohlen
Festplattenspeicher	• Mindestens 400 MB
Netzwerkverbindung	• Verbindung mit PolicyServer
Betriebssystem	• OS X™„Sierra“ • OS X™„El Capitan“ • OS X™„Yosemite“ • OS X™„Mavericks“ • OS X™„Mountain Lion“
Andere Software	• Mono runtime environment (MRE) 2.1 • Apple FileVault ist deaktiviert.

SPEZIFIKATION	VORAUSSETZUNG
Überlegungen zur Hardware	• Lokale Konten oder mobile Konten von Mac OS können die Verschlüsselung auf Mac OS X Mountain Lion oder höher initiieren. Andere Mac OS-Benutzerkontentypen sind nicht in der Lage, die Verschlüsselung einzuleiten. Informationen darüber, wie Sie ein mobiles Konto für Active Directory auf dem Mac einrichten, finden Sie unter *Mobiles Konto für Active Directory unter Mac OS erstellen auf Seite 8-17*. • Encryption Management for Apple FileVault unterstützt Apple Fusion Drives unter Mac OS X Mountain Lion oder höher (ab Mac OS-Build 10.8.2).

Control Manager einrichten

Das folgende Verfahren bietet eine Übersicht über die Konfiguration von Control Manager für die Endpoint Encryption Verwaltung.

Hinweis

Informationen über die Konfiguration einzelner Richtlinien finden Sie unter *Richtlinien auf Seite 5-1*.

Prozedur

1. Installieren und Konfigurieren von PolicyServer.

   Weitere Informationen finden Sie im *Endpoint Encryption Installations- und Upgrade-Handbuch*.

2. Verbinden Sie PolicyServer mit Control Manager.

   a. *PolicyServer als verwaltetes Produkt zu Control Manager hinzufügen auf Seite 3-21*

   b. *Verzeichnisverwaltung für PolicyServer konfigurieren auf Seite 3-23*

3. Fügen Sie Richtlinienziele hinzu.

Weitere Informationen finden Sie unter *Eine Richtlinie erstellen auf Seite 5-11*.

4. Verifizieren Sie die Richtlinienkonfiguration auf PolicyServer MMC.

Zugehörige Informationen

- *Control Manager Architektur*
- *PolicyServer als verwaltetes Produkt zu Control Manager hinzufügen*
- *Verzeichnisverwaltung für PolicyServer konfigurieren*
- *Proxy-Einstellungen konfigurieren*

Control Manager Architektur

Trend Micro Control Manager bietet Funktionen, um Produkte und Dienste von Trend Micro von einer zentralen Stelle aus zu steuern. Diese Anwendung vereinfacht die Verwaltung der Viren/Malware- und Content-Sicherheitsrichtlinien im Unternehmen. Die folgende Tabelle enthält eine Liste der Komponenten, die von Control Manager verwendet werden.

TABELLE 3-1. Control Manager Komponenten

KOMPONENTE	BESCHREIBUNG
Control Manager server	Dient als ein Repository für alle Daten, die von den Agents erfasst werden. Dabei kann es sich um Server der Standard Edition oder der Advanced Edition handeln. Ein Control Manager unterstützt die folgenden Funktionen: • Eine SQL-Datenbank, in der die Konfigurationen und die Protokolle der verwalteten Produkte gespeichert werden. Control Manager arbeitet mit der Datenbank Microsoft SQL Server (`db_ControlManager.mdf`) zusammen, um Daten zu speichern, die in Protokollen, Communicator Zeitplänen, verwalteten Produkten und Informationen zu untergeordneten Servern, Benutzerkonten, Netzwerkumgebungen und Benachrichtigungseinstellungen enthalten sind. • Ein Webserver, der die Control Manager Webkonsole hostet • Ein Mail-Server, der die Benachrichtigungen bei Ereignissen in Form von E-Mail-Nachrichten versendet. Control Manager Manager kann Benachrichtigungen an Einzelpersonen oder Empfängergruppen über Ereignisse senden, die im Control Manager Netzwerk auftreten. In Event Center können Sie konfigurieren, ob Benachrichtigungen als E-Mail-Nachrichten, Windows Ereignisprotokoll, MSN Messenger, SNMP, Syslog, Pager oder an eine andere interne oder dem Branchenstandard entsprechende Anwendung gesendet werden, die von Ihrem Unternehmen zur Versendung von Benachrichtigungen eingesetzt wird. • Ein Berichtserver, der nur zum Umfang der Advanced Edition gehört, generiert Berichte zu Antiviren- und Content-Sicherheitsprodukten. Ein Control Manager Bericht ist eine Online-Sammlung von Zahlen über das Auftreten von Ereignissen zu Sicherheitsbedrohungen und Content-Sicherheit im Control Manager Netzwerk, die ein Sicherheitsrisiko darstellen.

Komponente	Beschreibung
Trend Micro Management Communication Protocol	MCP verarbeitet die Interaktion von Control Manager Server mit den verwalteten Produkten, die den Agent der nächsten Generation unterstützen. MCP ist das neue Rückgrat für das Control Manager System. MCP Agents werden mit den verwalteten Produkten installiert und nutzen eine Ein-Weg- oder Zwei-Wege-Kommunikation zur Kommunikation mit Control Manager. MCP Agents rufen Anweisungen und Updates vom Control Manager ab.
Trend Micro Management Infrastructure	Verarbeitet die Interaktion von Control Manager Server mit älteren verwalteten Produkten. Der Communicator bzw. das Message Routing Framework ist das Kommunikationsrückgrat für das ältere Control Manager System. Dabei handelt es sich um eine Komponente der Trend Micro Management Infrastructure (TMI). Communicators verarbeiten die gesamte Kommunikation zwischen dem Control Manager Server und den älteren verwalteten Produkten. Die Kommunikation mit den älteren verwalteten Produkten erfolgt durch Interaktion mit Control Manager 2.x Agents.
Control Manager 2.x Agents	Empfangen Befehle von Control Manager Server und senden Statusinformationen und Protokolle an den Control Manager Server Beim Control Manager Agent handelt es sich um eine Anwendung, die auf dem Server eines verwalteten Produkts installiert ist und die es möglich macht, dass Control Manager das Produkt verwaltet. Agents interagieren mit dem verwalteten Produkt und Communicator. Ein Agent dient als Brücke zwischen dem verwalteten Produkt und Communicator. Aus diesem Grund sollten Sie alle Agents auf demselben Computer wie die verwalteten Produkte installieren.

Komponente	Beschreibung
Webbasierte Management-Konsole	Dadurch kann ein Administrator Control Manager über einen Computer mit Internet-Verbindung und Microsoft Internet Explorer verwalten. Bei der Management-Konsole von Control Manager handelt es sich um eine webbasierte Konsole, die im Internet über den Microsoft Internet Information Server (IIS) veröffentlicht wurde und die vom Control Manager Server gehostet wird. Mit dieser Lösung können Sie das Control Manager Netzwerk von einem beliebigen Computer aus verwalten, auf dem ein kompatibler Webbrowser verwendet wird.
Widget-Framework	Ermöglicht Administratoren, ein angepasstes Dashboard zur Überwachung des Control Manager Netzwerks zu erstellen.

PolicyServer als verwaltetes Produkt zu Control Manager hinzufügen

Endpoint Encryption ermöglicht, dass Administratoren PolicyServer mit Hilfe von Trend Micro Control Manager steuern und Endpoint Encryption Agent-Richtlinien verwalten oder mit Trend Micro OfficeScan die Endpoint Encryption Agent-Software auf verwaltete Endpunkte verteilen.

Wenn Sie Control Manager zur Verwaltung von PolicyServer verwenden möchten, müssen Sie PolicyServer als verwaltetes Produkt hinzufügen.

Wichtig

Endpoint Encryption unterstützt jeweils nur eine PolicyServer Instanz in Control Manager. Es ist nicht möglich, mehrere PolicyServer Konfigurationen hinzuzufügen.

Prozedur

1. Melden Sie sich bei Control Manager an.
2. Wechseln Sie zu **Administration** > **Verwaltete Server**.

   Das Fenster **Verwaltete Server** wird angezeigt.

3. Wählen Sie im Listenfeld **Servertyp** die Option **Endpoint Encryption**.

4. Klicken Sie auf **Hinzufügen**.

   Das Fenster **Server hinzufügen** wird angezeigt.

5. Geben Sie die Optionen für die **Serverinformationen** an.

   - **Server**: Geben Sie den Host-Namen und die Portnummer für PolicyServer an. Verwenden Sie das folgende Format:

     `http://<Servername>:Portnummer`

     Hinweis

     Control Manager kommuniziert mit dem PolicyServer Endpoint Encryption Dienst. Die Standardportnummer lautet 8080.

   - **Anzeigename:** Geben Sie den Namen für PolicyServer an, der im Fenster **Verwaltete Server** angezeigt wird.

6. Geben Sie unter **Authentifizierung** den Benutzernamen und das Kennwort für das Endpoint Encryption Unternehmensadministratorkonto und das Unternehmen an, das während der PolicyServer-Installation festgelegt wurde.

7. Wählen Sie unter **Verbindung** den Eintrag **Einen Proxy-Server für die Verbindung verwenden** aus, wenn PolicyServer eine Proxy-Serververbindung benötigt.

8. Klicken Sie auf **Speichern**.

Hinweis

Die Synchronisierung zwischen Control Manager und PolicyServer dauert u. U. einige Minuten.

PolicyServer wird als neues verwaltetes Produkt zu Control Manager hinzugefügt.

Verzeichnisverwaltung für PolicyServer konfigurieren

Das folgende Verfahren erklärt die Konfiguration der Verzeichnisverwaltung für die Datenquelle des neuen PolicyServer. Im Fenster **Verzeichnisverwaltung** werden die verfügbaren Richtlinienziele in der Verzeichnisstruktur angezeigt.

Fügen Sie PolicyServer als verwalteten Server zu Control Manager hinzu, bevor Sie dieses Verfahren starten. Weitere Informationen finden Sie unter *PolicyServer als verwaltetes Produkt zu Control Manager hinzufügen auf Seite 3-21*.

Prozedur

1. Navigieren Sie zu **Richtlinien** > **Richtlinienressourcen** > **Verwaltete Server**.

   Das Fenster **Verwaltete Server** wird angezeigt.

2. Klicken Sie auf **Verzeichnisverwaltung**.

   Das Fenster **Verzeichnisverwaltung** wird angezeigt.

3. Wählen Sie den Server, und klicken Sie anschließend auf **Ordner hinzufügen**.

   Das Fenster **Verzeichnis hinzufügen** wird angezeigt.

4. Geben Sie den Verzeichnisnamen an, und klicken Sie anschließend auf **Speichern**.

5. Klicken Sie zur Bestätigung auf **OK**.

   Der neue Ordner wird erstellt.

6. Ziehen Sie die zuvor hinzugefügte PolicyServer Datenquelle in den neuen Ordner.

7. Klicken Sie zur Bestätigung auf **OK**.

8. Klicken Sie auf **< Zurück**, um zum Fenster **Richtlinienverwaltung** zurückzukehren.

Proxy-Einstellungen konfigurieren

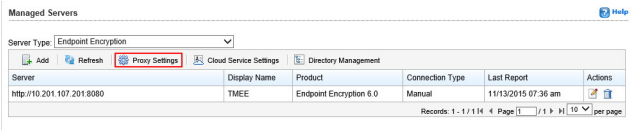
Verwenden Sie einen Proxy-Server, um eine Verbindung zu verwalteten Produkten herzustellen.

Prozedur

1. Wechseln Sie zu **Administration** > **Verwaltete Server**.

   Das Fenster **Verwaltete Server** wird angezeigt.

2. Klicken Sie auf **Proxy Settings**.

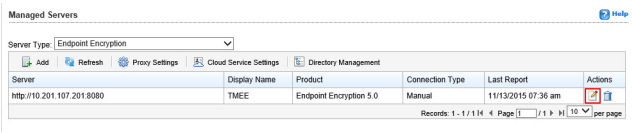


3. Geben Sie Ihre Proxy-Einstellungen an.

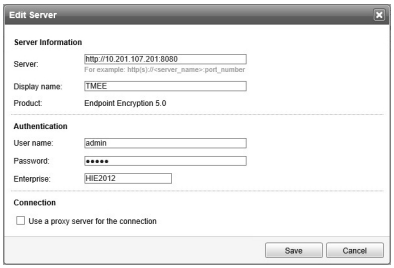
Option	Bezeichnung
Protokoll	Endpoint Encryption unterstützt eine Proxy-Verbindung über HTTP- oder SOCKS5-Protokolle.
Server	Geben Sie die IP-Adresse oder die URL des Proxy-Servers an.
Port	Geben Sie den Überwachungsport des Proxy-Servers an.
Benutzername	Geben Sie den Benutzernamen an, um auf den Server zuzugreifen, falls der Proxy eine Authentifizierung erfordert.
Kennwort	Geben Sie das Kennwort an, um auf den Server zuzugreifen, falls der Proxy eine Authentifizierung erfordert.

4. Klicken Sie auf **Save**.

5. Klicken Sie auf die Schaltfläche **Bearbeiten** neben Ihrem Endpoint Encryption-Server.



Das Fenster **Server bearbeiten** wird angezeigt.



6. Wählen Sie **Einen Proxy-Server für die Verbindung verwenden** aus.

7. Klicken Sie auf **Speichern**.

Active Directory-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.

Es werden folgende Themen behandelt:

- *Active Directory-Überblick auf Seite 3-26*
- *Active Directory konfigurieren auf Seite 3-27*

- *Active Directory-Benutzer importieren auf Seite 3-29*
- *Kennworteinstellungsobjekte aus Active Directory verwalten auf Seite 3-30*

Active Directory-Überblick

Für die PolicyServer AD-Synchronisierung sind drei Elemente erforderlich:

1. Eine konfigurierte AD-Domäne.
2. Eine PolicyServer Gruppe, die so konfiguriert ist, dass sie auf mindestens 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, sodass 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, sodass 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.

Um Nicht-Domänenbenutzer zu Gruppen hinzuzufügen, die mit der Domäne synchronisiert werden, können Sie eindeutige Endpoint Encryption Benutzer anlegen und diese zugeordneten PolicyServer Gruppen hinzufügen. Dabei ist es nicht erforderlich, diese Benutzer über das Synchronisierungssystem zu ändern.

Wenn Sie den Endpoint Encryption Benutzer aus einer zugeordneten Gruppe in PolicyServer entfernen, wird dieser Domänenbenutzer nicht automatisch vom Synchronisierungssystem wieder hinzugefügt. Dies verhindert das Überschreiben Ihrer Aktion für diesen Endpoint Encryption Benutzer. Wenn Sie einen synchronisierten Domänenbenutzer manuell wieder in eine zugeordnete Gruppe verschieben, 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 2012 eingerichtet wurde und Active Directory (AD) installiert ist.

Prozedur

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

   Das Fenster **Active Directory-Benutzer und -Computer** wird angezeigt.

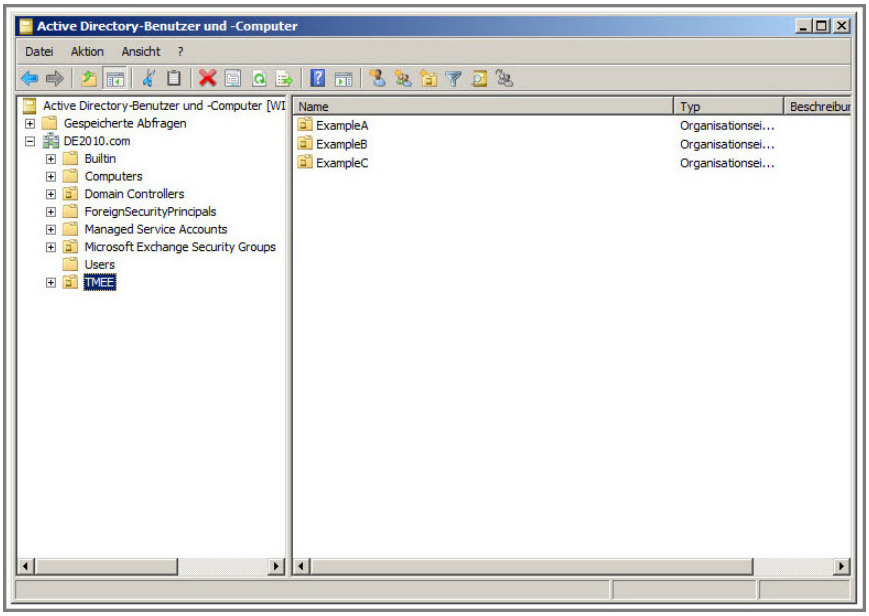


ABBILDUNG 3-1. Active Directory-Benutzer und -Computer

2. Erstellen Sie Ihre Organisationseinheiten.

   Führen Sie für jede Organisationseinheit, die Sie erstellen möchten, die folgenden Schritte aus:

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

   b. Wählen Sie **Organisationseinheit** aus.

   c. 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 dem Domänennamen angezeigt. Führen Sie diesen Schritt für alle Organisationseinheiten aus, die Sie mit PolicyServer verwenden möchten.

Wichtig

Endpoint Encryption unterstützt bis zu 12 Organisationseinheiten pro Richtlinie.

Die neuen Gruppen werden zur Synchronisierung mit einer PolicyServer Gruppe verwendet. Vor der Synchronisierung müssen die Benutzer zu den Gruppen hinzugefügt werden.

3. Fügen Sie neue Benutzer zu Ihren Organisationseinheiten hinzu.

   Führen Sie für jeden Benutzer, den Sie erstellen möchten, die folgenden Schritte aus:

   a. Klicken Sie mit der rechten Maustaste auf die gewünschte Organisationseinheit und navigieren Sie zu **Neu** > **Benutzer**.

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

   c. Geben Sie das Domänenkennwort des neuen Benutzers an und bestätigen Sie es. Klicken Sie dann auf **Weiter**.

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.

d. Wann 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.

Active Directory-Benutzer importieren

PolicyServer beinhaltet ein Benutzerverzeichnis getrennt von der Active Directory-Datenbank. Damit kann PolicyServer absolute Sicherheit für den Zugriff auf alle Endpoint Encryption Geräte, Benutzerrechte und Authentifizierungsmethoden gewährleisten.

Verwenden Sie das Widget **Endpoint Encryption Benutzer** in Control Manager, um Active Directory-Benutzer zu importieren. Weitere Informationen zur Verwaltung von Benutzern mit dem Widget **Endpoint Encryption Benutzer** finden Sie unter *Endpoint Encryption Benutzer auf Seite 4-7*.

Prozedur

1. Melden Sie sich bei Control Manager an.
2. Navigieren Sie zum Widget **Endpoint Encryption Benutzer**.
3. Klicken Sie auf das -Symbol.
4. Wählen Sie **Benutzer aus Active Directory importieren**.

   Das Fenster **Benutzer aus Active Directory importieren** wird angezeigt.
5. Geben Sie Ihre Anmeldedaten für den Active Directory LDAP-Server an.

Hinweis

Bei **Port** gibt der Wert „0“ den Standardport an. Der Standardport ist 389.

6. Klicken Sie auf **Weiter**.
7. Warten Sie darauf, dass die angegebe Active Directory-Domäne mit Daten gefüllt wird.

   Die Active Directory-Struktur für die angegebene Domäne wird im linken Fensterbereich angezeigt.
8. Wählen Sie in der Navigationsstruktur im linken Fensterbereich den Container, dem Benutzer hinzugefügt werden sollen.

   Die verfügbaren Benutzer werden im rechten Fensterbereich eingefügt.
9. Wählen Sie eine der folgenden Optionen:
   - Wählen Sie einzelne Benutzer, und klicken Sie anschließend auf **Ausgewählte Benutzer importieren**.
   - Klicken Sie auf **Alle Benutzer in diesem Container importieren**.
10. Klicken Sie auf **OK**, um die Benutzer zum angegebenen Speicherort hinzuzufügen.

    Eine Bestätigungsmeldung wird angezeigt.
11. Klicken Sie zur Bestätigung auf **OK**.

    Eine Importstatusmeldung wird angezeigt.
12. Klicken Sie auf **Schließen**, um den Schritt zu beenden, oder wiederholen Sie das Verfahren, um weitere Benutzer zum Importieren auszuwählen.

Kennworteinstellungsobjekte aus Active Directory verwalten

Endpoint Encryption unterstützt detaillierte Kennwortrichtlinien über Active Directory. Wenn sich PolicyServer in der Active Directory-Computerliste befindet, ersetzen die Kennwortrichtlinien in Active Directory die Richtlinieneinstellungen von PolicyServer sowohl aus Control Manager als auch aus PolicyServer MMC.

Das folgende Verfahren zeigt, wie PolicyServer zur Active Directory-Computerliste hinzugefügt wird.

Prozedur

1. Öffnen Sie die Sicherheitseinstellungen für Ihr Kennworteinstellungsobjekt (PSO).
   a. Navigieren Sie zu **Start** > **Verwaltung** > **Active Directory-Benutzer und -Computer**.
   b. Prüfen Sie im Menü **Ansicht**, ob **Erweiterte Funktionen** aktiviert sind.
   c. Suchen Sie in **Active Directory-Benutzer und -Computer** nach Ihrem Domänenknoten.
   d. Wechseln Sie zu **System** > **Kennworteinstellungscontainer**.
   e. Wählen Sie die PSO-Eigenschaft aus, die Sie für die Kennwortrichtlinienverwaltung verwenden möchten.
   f. Wechseln Sie zur Registerkarte **Sicherheit**.
2. Fügen Sie den PolicyServer-Endpunkt zur Liste **Gruppen- oder Benutzernamen** hinzu.
   a. Klicken Sie unter der Liste **Gruppen- oder Benutzernamen** auf **Hinzufügen...**.
   b. Wählen Sie im Fenster **Objekttypen** die Option **Computer** aus.
   c. Wählen Sie den PolicyServer-Endpunkt aus.
3. Überprüfen und bestätigen Sie Ihre Änderungen.

Kapitel 4

Dashboard

Das Control Manager Dashboard bietet Informationen für das Control Manager Netzwerk, die auf einen Blick abgelesen werden können. Das Dashboard besteht aus zwei Komponenten:

- **Registerkarten:** Ermöglicht Administratoren, ein Fenster zu erstellen, das mindestens ein Widget enthält.
- **Widgets:** Liefern bestimmte Informationen zu verschiedenen sicherheitsrelevanten Ereignissen und führen die Benutzer- und Geräteverwaltung durch

Für jedes Benutzerkonto wird ein eigenes Dashboard angezeigt. Wenn sich ein Benutzer zum ersten Mal bei Control Manager anmeldet, werden die Standardregisterkarten und -Widgets innerhalb der Registerkarten auf dem Dashboard angezeigt.

Das Dashboard, die Registerkarten und die Widgets können für jedes Benutzerkonto und die entsprechenden speziellen Anforderungen angepasst werden. Die Anpassung von Dashboard, Registerkarten oder Widgets für ein Benutzerkonto wirkt sich nicht auf das Dashboard, die Registerkarten oder die Widgets anderer Benutzerkonten aus. Jedes Benutzerkonto verfügt über ein Dashboard sowie Registerkarten und Widgets, die von jedem anderen Benutzerkonto komplett unabhängig sind.

Registerkarten

Sie können das Control Manager Dashboard anpassen, indem Sie zusätzliche Registerkarten hinzufügen, den neuen Registerkarten Namen nach Bedarf geben und die entsprechenden Widgets ergänzen. Sie können hinzugefügte Registerkarten ändern oder löschen.

Standardregisterkarten

Das Dashboard enthält die folgenden Registerkarten:

- Zusammenfassung
- Untersuchung von DLP-Vorfällen
- Prävention vor Datenverlust
- Einhaltung von Richtlinien
- Bedrohungserkennung
- Smart Protection Network

Hinweis

Wenn Sie die Standardregisterkarten endgültig löschen, werden die Registerkarten nicht mehr für das Benutzerkonto angezeigt, das die Registerkarten entfernt hat. Es gibt keine Möglichkeit, eine gelöschte Registerkarte wiederherzustellen. Das Löschen einer Standardregisterkarte hat für andere Benutzerkonten keine Auswirkung auf die Anzeige des Dashboards.

Neue Registerkarte hinzufügen

Prozedur

1. Navigieren Sie zum **Dashboard**.

2. Klicken Sie rechts neben der letzten benannten Registerkarte auf +.

   Das Fenster **Neue Registerkarte** wird angezeigt.

3. Geben Sie einen Namen für den **Titel** der neuen Registerkarte ein.

4. Aktivieren Sie das Optionsfeld für den entsprechenden Layout-Stil.

5. Wählen Sie **Automatisch anpassen Ein**, um die Höhe der Widgets entsprechend der Registerkarte festzulegen.

6. Klicken Sie auf **Speichern**.

Die neue Registerkarte wird rechts neben den vorhandenen Registerkarten hinzugefügt.

Registerkarteneinstellungen ändern

Prozedur

1. Navigieren Sie zu **Dashboard**, und öffnen Sie anschließend die entsprechende Registerkarte.

2. Klicken Sie auf **Registerkarteneinstellungen** in der oberen rechten Ecke der Registerkarte.

3. Nehmen Sie die erforderlichen Änderungen vor:

   - **Titel**
   - **Layout**
   - **Automatisch anpassen**

4. Klicken Sie auf **Speichern**.

Eine Registerkarte löschen

Hinweis

Wenn Sie die Standardregisterkarten endgültig löschen, werden die Registerkarten nicht mehr für das Benutzerkonto angezeigt, das die Registerkarten entfernt hat. Es gibt keine Möglichkeit, eine gelöschte Registerkarte wiederherzustellen. Das Löschen einer Standardregisterkarte hat für andere Benutzerkonten keine Auswirkung auf die Anzeige des Dashboards.

Prozedur

1. Navigieren Sie zum **Dashboard**.
2. Öffnen Sie die Registerkarte, die gelöscht werden soll.
3. Klicken Sie auf das **X** neben dem Namen der Registerkarte.
4. Klicken Sie zur Bestätigung auf **OK**.

Die Registerkarte wird gelöscht.

Widgets

Widgets sind die Hauptkomponenten des Dashboards. Registerkarten stellen das Layout und Widgets die tatsächlichen Daten für das Dashboard bereit.

Hinweis

Die Anpassung von Dashboard, Registerkarten oder Widgets für ein Benutzerkonto wirkt sich nicht auf das Dashboard, die Registerkarten oder die Widgets anderer Benutzerkonten aus. Jedes Benutzerkonto verfügt über ein Dashboard sowie Registerkarten und Widgets, die von jedem anderen Benutzerkonto komplett unabhängig sind.

Laden Sie den Control Manager Widget-Pool (unter **Product programs and widget pool** in den Fenstern **Manual Download** und **Scheduled Download**) regelmäßig herunter, um zu überprüfen, ob neue und aktualisierte Widgets vorliegen.

Die Daten, die auf einem Widget angezeigt werden, stammen aus den folgenden Quellen:

- Control Manager Datenbank
- Trend Micro Smart Protection Network
- Verwaltete Produkte, die der Dashboard-Liste **Server Visibility** hinzugefügt wurden

Hinweis

Smart Feedback muss aktiviert werden, um Daten für Widgets anzuzeigen, die Daten aus dem Smart Protection Network enthalten.

Die auf einem Widget angezeigten Daten werden auf zweierlei Art gesteuert:

TABELLE 4-1. Widget-Informationen

VORGANG	DETAILS
Benutzerkonto	Ein Benutzerkonto gewährt oder beschränkt den Zugang zu allen verwalteten Produkten, die in Control Manager registriert sind.
Bereich	Der Geltungsbereich der Daten auf vielen Widgets kann individuell konfiguriert werden. Das bedeutet, ein Benutzer kann ferner den Speicherort der Datenquelle für das Widget angegeben. **Beispiel:** Ein OfficeScan Administrator, der mehrere OfficeScan Server verwaltet, kann eine Registerkarte anlegen und Widgets hinzufügen, die nur Daten für einen OfficeScan Server anzeigen.

Widgets zu einer Registerkarte hinzufügen

Nachdem Sie Widgets einer Registerkarte hinzugefügt haben, können Sie das Widget an verschiedene Positionen innerhalb der Registerkarte ziehen.

Prozedur

1. Navigieren Sie zu **Dashboard**, und öffnen Sie anschließend die entsprechende Registerkarte.
2. Klicken Sie auf **Widgets hinzufügen** in der oberen rechten Ecke der Registerkarte.

   Das Fenster **Widgets hinzufügen** wird angezeigt.
3. Gehen Sie folgendermaßen vor:
   - Klicken Sie auf der linken Seite auf eine Kategorie, und aktivieren Sie anschließend das Kontrollkästchen neben dem Namen aller entsprechenden Widgets, die angezeigt werden.
   - Wählen Sie mit Hilfe der Suchleiste ein bestimmtes Widget.
4. Klicken Sie auf **Hinzufügen**.

Alle ausgewählten Widgets werden der Registerkarte hinzugefügt.

Widget-Optionen

Die folgende Darstellung und Tabelle vermitteln einen allgemeinen Überblick über die verfügbaren Widget-Optionen. Unterschiedliche Widgets können unterschiedliche Optionen haben.

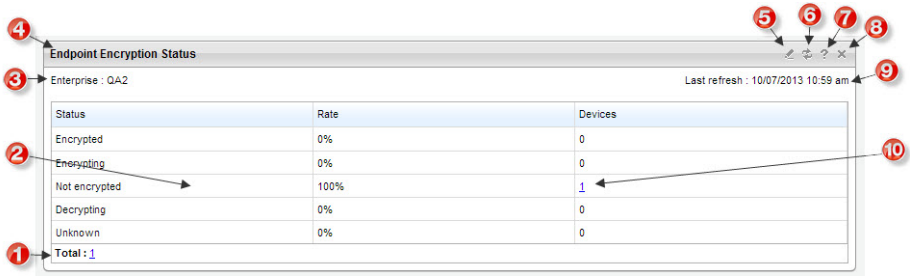


ABBILDUNG 4-1. Widget-Optionen

TABELLE 4-2. Beschreibungen der Widget-Optionen

VORGANG	BESCHREIBUNG
1	Die Gesamtzahl der Objekte (Beispiele: Ereignisse, Geräte, Protokolle), über die das Widget Daten sammelt. Klicken Sie auf die Zahl, um weitere Informationen anzuzeigen.
2	Die Informationen, die vom Widget angezeigt werden.
3	Das Unternehmen, das den Widget-Daten zugeordnet ist.
4	Der Name des Widgets. Ändern Sie den Namen im Fenster **Widget-Einstellungen**.
5	Klicken Sie auf das Symbol , um die Widget-Daten manuell zu aktualisieren. Die Standardaktualisierungsrate wird von den Control Manager Dashboard-Einstellungen bestimmt, die Sie unter **Administration** > **Einstellungen** > **Einstellungen der Webkonsole** festlegen.
6	Klicken Sie auf das Symbol , um die folgenden Widget-Optionen anzuzeigen: • **Widget-Einstellungen**: Konfigurieren Sie die anzeigbaren Optionen für dieses Widget. • **Hilfe**: Greifen Sie auf die Endpoint Encryption Online-Hilfe für dieses Widget zu. • **Widget schließen**: Entfernen Sie das Widget von der aktuellen Registerkarte.
7	Hier sehen Sie, wann das Widget zum letzten Mal eine Datenaktualisierung durchgeführt hat.
8	Klicken Sie auf die Zahl oder das Symbol, um auf bestimmte Widget-Daten zuzugreifen, z. B. Ereignisprotokolle oder Berichte.

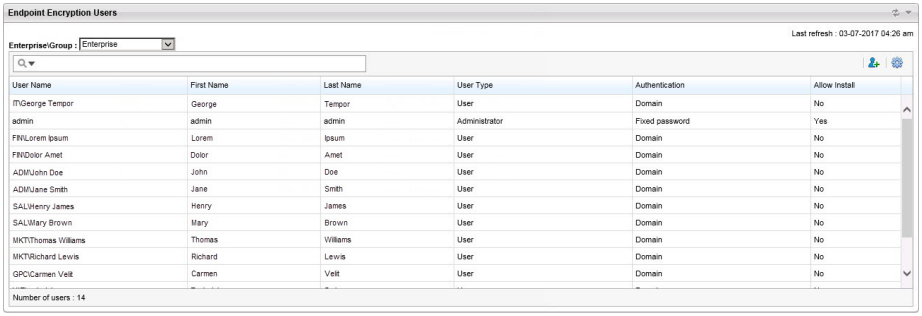
Endpoint Encryption Benutzer

Das Widget **Endpoint Encryption Benutzer** stellt Funktionen für die Benutzerverwaltung direkt vom Dashboard von Control Manager bereit. Mit dem

Widget **Endpoint Encryption Benutzer** fügen Sie Endpoint Encryption Benutzerkonten hinzu oder entfernen sie, setzen Kennwörter zurück, ändern Berechtigungen, konfigurieren die Priorität der Richtliniengruppen, importieren aus Active Directory und suchen nach bestimmten Benutzerkonten.

Hinweis

Informationen, wie Sie vorhandene Endpoint Encryption Benutzer zu einer Richtlinie hinzufügen, finden Sie unter *Endpoint Encryption Benutzerregeln konfigurieren auf Seite 5-14*.



Vorgang	Beschreibung
Anzeigen	Wählen Sie aus, welche Benutzer angezeigt werden sollen: alle Benutzer im Unternehmen oder Benutzer in einer bestimmten Richtlinie.
Suchen ( )	Klicken Sie auf das Symbol , um danach zu filtern, welche Endpoint Encryption Benutzer in der Tabelle angezeigt werden. Über das Suchfeld legen Sie Parameter für die Suche fest.
Einstellungen ( ) Anklicken eines Benutzers mit der rechten Maustaste	Klicken Sie auf das -Symbol, um die Benutzerattribute anzuzeigen oder Aktionen für einen beliebigen ausgewählten Benutzer auszuführen.
Benutzer hinzufügen ( )	Klicken Sie auf das -Symbol, um einzelne Benutzer hinzuzufügen oder um Benutzer aus einer CSV-Datei oder aus Active Directory LDAP zu importieren.

Vorgang	Beschreibung
Anzahl der Benutzer	Zeigt die Gesamtzahl der Benutzer im gesamten Unternehmen, in der ausgewählten Richtlinie oder in der angegebenen Suche an.

Benutzereinstellungen - Optionen

In der folgenden Tabelle werden die unter dem Einstellungssymbol verfügbaren Optionen erläutert.

Tabelle 4-3. Benutzereinstellungen - Optionen

Optionen	Beschreibung
Kennwort ändern	Geben Sie ein neues Kennwort für Benutzer an, die die feste Kennwortauthentifizierung verwenden. Das Widget bietet keine Unterstützung zum Ändern von Kennwörtern für den Domänenauthentifizierungstyp.
Benutzer löschen	Entfernt den ausgewählten Benutzer.
Benutzer ändern	Aktualisieren Sie die Eigenschaften des ausgewählten Benutzers. Die folgenden Eigenschaften können geändert werden: • Benutzername • Vorname • Nachname • Mitarbeiter-ID • E-Mail-Adresse • Einfrieren • Benutzertyp • Eine Richtlinie • Authentifizierungsmethode

Optionen	Beschreibung
Richtlinien auflisten	Zeigt die Richtlinien an, die dem ausgewählten Benutzer zugewiesen sind. Ist die Spalte **Installation zulassen** für den ausgewählten Benutzer auf **Ja** gesetzt, ist die Option zum Zulassen oder Verweigern der Installation ausgewählter Richtlinien sowie das Auswählen der Richtlinien mit höchster Priorität aktiviert.

Optionen zum Hinzufügen neuer Benutzer

In der folgenden Tabelle werden die verfügbaren Optionen beim Hinzufügen eines neuen Endpoint Encryption Benutzers beschrieben.

Tabelle 4-4. Optionen zum Hinzufügen neuer Benutzer

Optionen	Beschreibung
Benutzername	Geben Sie den Namen des Benutzerkontos ein, den der Benutzer bei der Authentifizierung verwendet.
Vorname	Geben Sie den Vornamen des Benutzers an.
Nachname	Geben Sie den Nachnamen des Benutzers an.
Mitarbeiter-ID	Geben Sie die Mitarbeiter-ID des Benutzers (optional) an.
E-Mail-Adresse	Geben Sie die E-Mail-Adresse des Benutzers (optional) an.
Einfrieren	Wählen Sie **Ja**, um das Konto vorübergehend zu sperren. Ein gesperrtes Konto kann sich nicht bei Endpoint Encryption Geräten anmelden.
Benutzertyp	Wählen Sie **Benutzer**, **Authentifizierer** oder **Administrator**. Weitere Informationen zu Benutzerrollen finden Sie unter *Benutzer auf Seite 5-3*.

Optionen	Beschreibung
Eine Gruppe	Wenn Sie **Ja** wählen, kann der Benutzer jeweils nur einer Richtlinie angehören. Der Benutzer kann zu keiner anderen Richtliniengruppe hinzugefügt werden. Wenn Sie diese Option auf **Ja** und den **Benutzertyp** auf **Authentifizierer** oder **Administrator** setzen, wird der Benutzer ein Gruppenauthentifizierer bzw. Gruppenadministrator.
Authentifizierungsmethode	Wählen Sie die Authentifizierungsmethode, die für den Benutzer verfügbar ist.

Richtlinienmitgliedschaft

Die folgende Tabelle dient zum Verständnis der Mitgliedschaft in einer Endpoint Encryption Benutzerrichtlinie.

Hinweis

Encryption Management for Apple FileVault und Encryption Management for Microsoft BitLocker erfordern keine Authentifizierung und werden nicht durch Authentifizierungsrichtlinien beeinflusst. Client, Anmeldung, Kennwort und Authentifizierungsrichtlinien oder die Berechtigung des Benutzers, die Endpoint Encryption Agent-Software zu deinstallieren, wirkt sich nur auf die Full Disk Encryption Agents und File Encryption Agents aus.

Header	Beispiel	Beschreibung
Priorität	1, 2. 3	Zeigt die Reihenfolge an, in der Endpoint Encryption Richtlinien anwendet. Wenn eine Richtlinie ausgelöst wird, die sich auf einen Benutzer auswirkt, führt Endpoint Encryption die Aktion aus. Für dieses Ereignis können sich dann keine anderen Richtlinien auf den Benutzer auswirken.
Name der Richtlinie	GP1	Zeigt den Namen aller Richtlinien an, denen der Benutzer gegenwärtig zugewiesen ist.

Header	Beispiel	Beschreibung
Beschreibung	Richtlinie zu temporären Mitarbeitern.	Zeigt die Beschreibung der Richtlinie an.
Installation zulassen	Ja, Nein	Zeigt an, ob der Benutzer neue Endpoint Encryption Geräte installieren kann.

Benutzer aus einer CSV-Datei importieren

Hinweis

Der Import von Benutzern aus einer CSV-Datei wird nur für Benutzer mit fester Kennwortauthentifizierung unterstützt.

Formatieren Sie jede Zeile in der CSV-Datei wie folgt:

```
<Benutzer-ID (erforderlich)>, <Vorname>, <Nachname>,
<Mitarbeiter-ID>, <E-Mail-Adresse>
```

In Feldern ohne Daten verwenden Sie ein Komma als Platzhalter. Im Folgenden ist ein Beispiel-CSV-Eintrag aufgeführt:

```
beispiel_id, name,,, name@beispiel.com
```

Prozedur

1. Klicken Sie im Widget **Endpoint Encryption Benutzer** auf **Benutzer hinzufügen**, und wählen Sie anschließend **Benutzer aus einer CSV-Datei importieren**.

   Das Fenster **Benutzer aus einer CSV-Datei importieren** wird angezeigt.

2. Klicken Sie auf **Datei wählen**, um die CSV-Datei auszuwählen.

   Das Fenster **CSV-Datei öffnen** wird angezeigt.

3. Wählen Sie die Datei, und klicken Sie anschließend auf **Öffnen**.

4. Klicken Sie auf **Hinzufügen**.

   Die Benutzer in der CSV-Datei werden importiert.

Active Directory-Benutzer importieren

PolicyServer beinhaltet ein Benutzerverzeichnis getrennt von der Active Directory-Datenbank. Damit kann PolicyServer absolute Sicherheit für den Zugriff auf alle Endpoint Encryption Geräte, Benutzerrechte und Authentifizierungsmethoden gewährleisten.

Verwenden Sie das Widget **Endpoint Encryption Benutzer** in Control Manager, um Active Directory-Benutzer zu importieren. Weitere Informationen zur Verwaltung von Benutzern mit dem Widget **Endpoint Encryption Benutzer** finden Sie unter *Endpoint Encryption Benutzer auf Seite 4-7*.

Prozedur

1. Melden Sie sich bei Control Manager an.
2. Navigieren Sie zum Widget **Endpoint Encryption Benutzer**.
3. Klicken Sie auf das -Symbol.
4. Wählen Sie **Benutzer aus Active Directory importieren**.

   Das Fenster **Benutzer aus Active Directory importieren** wird angezeigt.
5. Geben Sie Ihre Anmeldedaten für den Active Directory LDAP-Server an.

   Hinweis

   Bei **Port** gibt der Wert „0“ den Standardport an. Der Standardport ist 389.
6. Klicken Sie auf **Weiter**.
7. Warten Sie darauf, dass die angegebe Active Directory-Domäne mit Daten gefüllt wird.

Die Active Directory-Struktur für die angegebene Domäne wird im linken Fensterbereich angezeigt.

8. Wählen Sie in der Navigationsstruktur im linken Fensterbereich den Container, dem Benutzer hinzugefügt werden sollen.

   Die verfügbaren Benutzer werden im rechten Fensterbereich eingefügt.

9. Wählen Sie eine der folgenden Optionen:

   - Wählen Sie einzelne Benutzer, und klicken Sie anschließend auf **Ausgewählte Benutzer importieren**.
   - Klicken Sie auf **Alle Benutzer in diesem Container importieren**.

10. Klicken Sie auf **OK**, um die Benutzer zum angegebenen Speicherort hinzuzufügen.

    Eine Bestätigungsmeldung wird angezeigt.

11. Klicken Sie zur Bestätigung auf **OK**.

    Eine Importstatusmeldung wird angezeigt.

12. Klicken Sie auf **Schließen**, um den Schritt zu beenden, oder wiederholen Sie das Verfahren, um weitere Benutzer zum Importieren auszuwählen.

Endpoint Encryption - Geräte

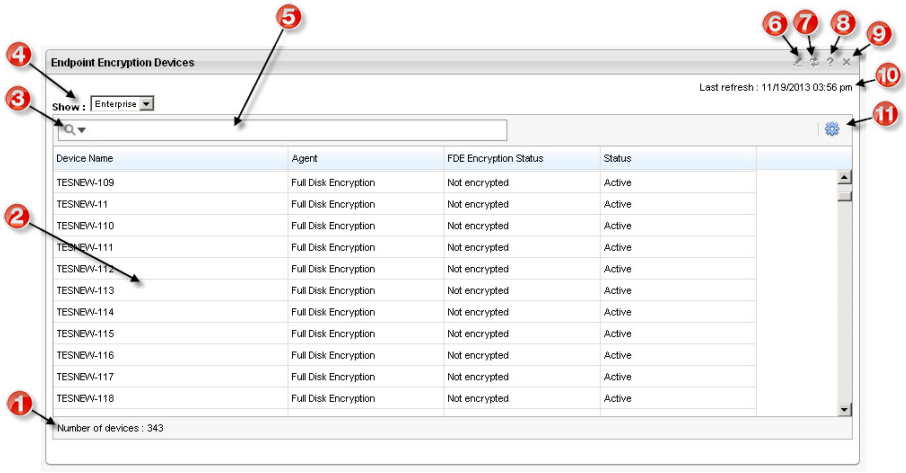
Endpoint Encryption Geräte sind Endpoint Encryption Agents, die mit PolicyServer registriert wurden. Bei der Installation eines Endpoint Encryption Agent wird der Endpunkt automatisch bei PolicyServer als ein Endpoint Encryption Gerät registriert. Da ein bestimmter Endpunkt von mehreren Endpoint Encryption Agents geschützt werden kann, erscheint ein einzelner Endpunkt möglicherweise als mehrere Endpoint Encryption Geräte auf PolicyServer.

Das Widget **Endpoint Encryption - Geräte** stellt Funktionen für die Endpoint Encryption Geräteverwaltung direkt vom Dashboard von Control Manager bereit. Verwenden Sie das Widget **Endpoint Encryption - Geräte**, um die Aktivität zu überwachen, nach Endpoint Encryption Geräten zu suchen oder Endpunktdaten zu

sichern, indem Sperr- oder Entfernungsbefehle zu senden, wenn ein Endpunkt verloren gegangen ist oder gestohlen wurde.

Hinweis

Informationen zum Hinzufügen von Endpoint Encryption Geräten zu einer Richtlinie finden Sie unter *Richtlinienziele angeben auf Seite 5-13*.



Optionen	Beschreibung
Anzeigen	Wählen Sie aus, welche Geräte angezeigt werden sollen: alle Geräte im Unternehmen oder Geräte in einer bestimmten Richtlinie.
Suchen ( )	Klicken Sie auf das Symbol , um den Endpoint Encryption Agent auszuwählen und die in der Tabelle angezeigten Geräte zu filtern. Über das Suchfeld legen Sie Parameter für die Suche fest. Sie können nach allen Attributen suchen, die in den Geräteattributen aufgeführt werden.

Optionen	Beschreibung
Einstellungen ( ) Anklicken eines Geräts mit der rechten Maustaste	Wählen Sie ein Gerät aus und klicken Sie auf das Symbol oder klicken Sie mit der rechten Maustaste auf ein Gerät, um Geräteattribute anzuzeigen oder Aktionen für das ausgewählte Gerät durchzuführen. Weitere Informationen finden Sie unter *Geräteaktionen auf Seite 4-16*.
Anzahl der Geräte	Zeigt die Gesamtzahl der Geräte im gesamten Unternehmen, in der ausgewählten Richtlinie oder in der angegebenen Suche an.

Geräteaktionen

Wählen Sie ein Gerät und klicken Sie auf das Symbol oder klicken Sie mit der rechten Maustaste auf ein Gerät, um die folgenden Aktionen durchzuführen:

Aktion	Beschreibung
Gerät löschen	Wenn Sie ein Endpoint Encryption Gerät aus dem Unternehmen löschen, wird das Gerät auch aus allen Richtliniengruppen entfernt. Das gelöschte Endpoint Encryption Gerät funktioniert, solange die Richtlinien für Konnektivität und Kennwort auf dem Gerät aktuell sind. Der Agent kann seine Richtlinien nicht mit PolicyServer synchronisieren. **Warnung!** Bevor Sie ein Full Disk Encryption Gerät löschen, entschlüsseln Sie Ihre Festplatte und deinstallieren Sie den Full Disk Encryption Agent. Falls Sie ein Full Disk Encryption Gerät löschen, ohne den Agent zu löschen, kann sich der Full Disk Encryption Preboot möglicherweise nicht bei PolicyServer authentifizieren, und die Daten können möglicherweise nicht abgerufen werden.

Aktion	Beschreibung
Soft-Token	Wenn Sie ein „Software-Token“ erstellen, wird eine eindeutige Zeichenfolge erstellt, mit deren Hilfe Endpoint Encryption Geräte entsperrt werden können. Auf diese Weise können Sie die Remote-Hilfe für Endpoint Encryption Benutzer ausführen, um vergessene Kennwörter zurückzusetzen. Das Software-Token ist nur in der Vollversion von Full Disk Encryption verfügbar, nicht in der Encryption Management for Apple FileVault oder Encryption Management for Microsoft BitLocker. Informationen über das Zurücksetzen von Kennwörtern oder Entsperren eines Benutzerkontos finden Sie unter *Unterstützung durch Remote-Hilfe auf Seite 9-36*.
Wiederherstellungsschlüssel	Wenn Sie einen „Wiederherstellungsschlüssel“ generieren, können Benutzer eine Festplatte entschlüsseln, wenn der Benutzer das ursprüngliche Kennwort oder den ursprünglichen Schlüssel vergessen hat. Der Wiederherstellungsschlüssel ist nur für die Encryption Management for Apple FileVault und die Encryption Management for Microsoft BitLocker Agents verfügbar, weil diese keine der anderen verfügbaren Wiederherstellungsmethoden in Full Disk Encryption verwenden. Informationen über das Zurücksetzen von Kennwörtern oder Entsperren eines Benutzerkontos finden Sie unter *Unterstützung durch Remote-Hilfe auf Seite 9-36*.
Geräteattribute	Zeigt einen aktuellen Snapshot des ausgewählten Geräts an. Weitere Informationen finden Sie unter *Geräteattribute auf Seite 4-18*.

Aktion	Beschreibung
Gerät auslöschen	Die Ausführung eines „Auslöschen“-Befehls löscht alle Endpoint Encryption Gerätedaten. Welche Daten gelöscht werden, ist abhängig vom Geltungsbereich der Daten, der vom verbundenen Endpoint Encryption Agent verwaltet wird. Wenn Sie beispielsweise einen „Auslöschen“-Befehl auf ein Full Disk Encryption Gerät ausführen, werden alle Daten vom Endpunkt gelöscht. Führen Sie dagegen einen „Auslöschen“-Befehl auf ein File Encryption Gerät aus, werden alle Dateien und Ordner auf dem lokalen Datenträger und auf den Wechselmedien gelöscht, die vom File Encryption Agent geschützt werden. Der „Auslöschen“-Befehl wird ausgegeben, wenn der Endpoint Encryption Agent mit PolicyServer kommuniziert. **Warnung!** Das Auslöschen eines Geräts kann nicht rückgängig gemacht werden. Führen Sie eine Datensicherung der gesamten Daten durch, bevor Sie einen Auslöschen-Befehl geben.
Gerät sperren	Wenn Sie den Befehl „Sperren“ auf das Endpoint Encryption Gerät anwenden, wird der Endpoint Encryption Benutzerzugriff verhindert, bis eine erfolgreiche Authentifizierung für die Remote-Hilfe durchgeführt wurde. Beim Sperren eines Gerät wird der Endpunkt neu gestartet und in einen Status gezwungen, der Remote-Hilfe erfordert. Der Sperren-Befehl wird ausgegeben, wenn der Endpoint Encryption Agent mit PolicyServer kommuniziert. Weitere Informationen finden Sie unter *Unterstützung durch Remote-Hilfe auf Seite 9-36*.
Warmstart	Wenn Sie einen „Warmstart“-Befehl geben, wird der Endpunkt neu gestartet. Der Befehl wird das nächste Mal ausgeführt, wenn der Agent mit PolicyServer kommuniziert.

Geräteattribute

In der folgenden Tabelle werden die Endpoint Encryption Geräteattribute beschrieben.

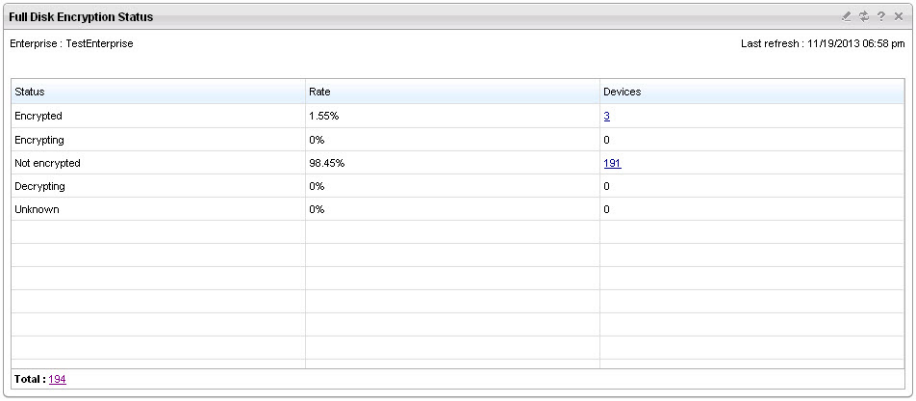
Attributname	Beispiel	Beschreibung
AD-NetBIOS-Name	Unternehmen	Der dem AD-NetBIOS zugewiesene Name.
AD-Objekt-GUID	6629bdeb-99a8-456b-b7c5-dbbc50ad13d0	Die dem AD-Objekt zugewiesene GUID.
Akkuanzahl	2	Die Anzahl der installierten Akkus.
.NET-Version	2.0.50727.3620	Die Versions- und Build-Nummer für das installierte .NET-Framework.
Build-Nummer des Common Framework	5.0.0.84	Der Endpoint Encryption Agent verwendet ein Common Framework zur Verschlüsselung. Die Build-Nummer wird dazu verwendet, um festzustellen, ob der Agent auf dem neuesten Stand ist.
Modell der Festplatte	VMware Virtual IDE	Das Festplattenmodell.
Festplattenname	`\\.\PHYSICALDRIVE0`	Der Name der Festplatte.
Seriennummer der Festplatte		Die Seriennummer der Festplatte.
Festplattenpartitionen	1	Die Anzahl der Partitionen auf der Festplatte, auf der der Agent installiert ist.
Größe der Festplatte	10733990400	Die Gesamtkapazität der Festplatte (in Byte).
Domänenname	WORKGROUP	Die Domäne, zu der der Endpunkt gehört.
Endpunkt-ID	85b1e3e2a3c25d882540ef6e4818c3e4	Die eindeutige ID des Endpunkts, die zur Control Manager Integration verwendet wird.
Version der File Encryption	6.0.0.1039	Die auf dem Endpunkt installierte Version von File Encryption.
Host-Name	TREND-4136D2DB3	Der Host-Name des Endpunkts.

Attributname	Beispiel	Beschreibung
IP-Adresse	`10.1.152.219`	Die IP-Adresse des Endpunkts.
Sprache	Deutsch (Deutschland)	Die vom Endpunkt verwendete Sprache.
Gebietsschema	de-DE	Das vom Endpunkt verwendete Gebietsschema.
MAC-Adresse	00-50-56-01-xx-xx	Die MAC-Adresse des Endpunkts.
Computername	TREND-4136D2DB 3	Der Computername, den der Endpunkt verwendet.
Hersteller	VMware, Inc.	Der Hersteller der Festplatte.
Modell	Virtuelle VMware-Plattform	Das Modell der Festplatte.
Betriebssystem	Microsoft Windows NT 5.1.2600 Service Pack 3	Das Betriebssystem, das auf derselben Festplatte wie der Agent installiert ist.
Name des Betriebssystems	Microsoft Windows XP Professional	Der allgemeine Name des Betriebssystems, das auf derselben Festplatte wie der Agent installiert ist.
Service Pack des Betriebssystems	Service Pack 3	Die Service Pack-Nummer des Betriebssystems, das auf derselben Festplatte wie der Agent installiert ist.
Version des Betriebssystems	5.1.2600.196608	Die Versionsnummer des Betriebssystems, das auf derselben Festplatte wie der Agent installiert ist.
Partitionsschema	Klassischer MBR	Das Partitionsschema für die Festplatte.
Prozessor	x86 Family 6 Modell 30 Stepping 5, Genuine Intel	Das Prozessorfabrikat und -modell des Endpunkts.
Prozessoranzahl	2	Die Anzahl der Prozessoren im Endpunkt.
Prozessorrevision	1e05	Die Prozessorrevisionsnummer.

Attributname	Beispiel	Beschreibung
Zeitzone	Taipei Standardzeit	Die Zeitzone, in der sich der Endpunkt befindet.
Gesamter physischer Arbeitsspeicher	2.047MB	Der im Endpunkt installierte oder dem Endpunkt zugewiesene Gesamtarbeitsspeicher.
Typ	X86-basierter PC	Der Prozessortyp des Endpunkts.
Windows Benutzername	TREND-4136D2DB 3\admin	Der Benutzername des Windows-Kontos, das sich zuletzt am Endpunkt angemeldet hat.
<Agent> Benutzer	john_smith	Der Benutzername des zuletzt angemeldeten Benutzers.
<Agent> Version	5.0.0.260	Die Versions- und die Build-Nummer für die Agent-Installation.

Full Disk Encryption Status

Im Widget **Full Disk Encryption Status** wird der aktuelle Verschlüsselungsstatus aller Endpoint Encryption Geräte im Unternehmen angezeigt.



Spalte	Beschreibung
Status	Der Status des Endpoint Encryption Geräts. Enthaltene Statusangaben: • **Verschlüsselt**: Das Endpoint Encryption ist zu 100% verschlüsselt. • **Verschlüsselung**: Die Festplatte des Endpoint Encryption Geräts wird momentan verschlüsselt. Der Status ändert sich in „Vollständig verschlüsselt“, sobald die Verschlüsselung abgeschlossen ist und der Endpunkt neu gestartet wird. • **Nicht verschlüsselt**: Das Endpoint Encryption ist zu 0% verschlüsselt. • **Entschlüsseln**: Die Festplatte des Endpoint Encryption Geräts wird momentan entschlüsselt. Der Status ändert sich in "Nicht verschlüsselt", sobald die Entschlüsselung abgeschlossen ist und der Endpunkt neu gestartet wird. • **Unbekannt**: Das Endpoint Encryption Gerät ist synchronisiert, jedoch kann PolicyServer den Verschlüsselungsstatus nicht ermitteln.
Rate	Der Prozentsatz der Verschlüsselung des Endpoint Encryption Geräts.
Geräte	Die Anzahl der Endpoint Encryption Geräte mit dem aktuellen Status. Klicken Sie auf die Zahl, um den Bericht zu den Endpoint Encryption Geräten anzuzeigen. Weitere Informationen finden Sie unter *Bericht "Full Disk Encryption Status" auf Seite 4-22*.

Hinweis

Klicken Sie unten im Widget auf die Zahl neben **Gesamt**, um den Endpoint Encryption Statusbericht anzuzeigen.

Bericht "Full Disk Encryption Status"

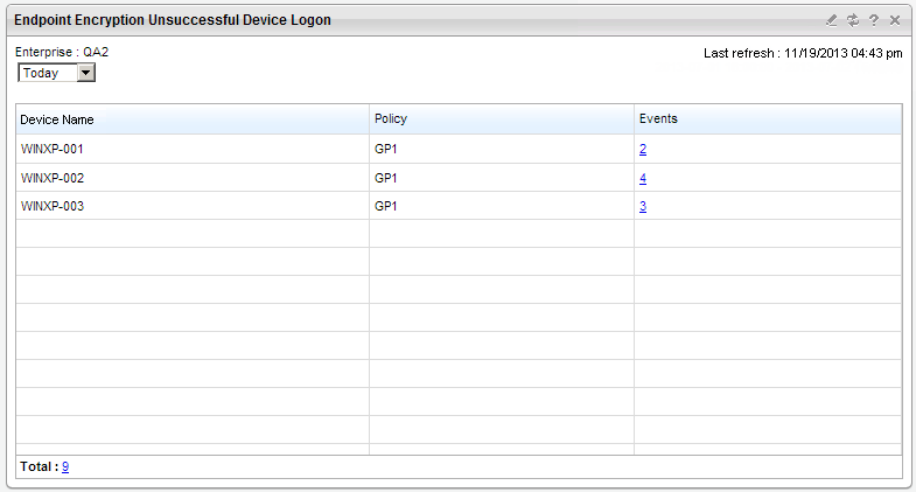
In der folgenden Tabelle wird der Bericht **Full Disk Encryption Status** beschrieben. Die Angaben sollen Ihnen helfen, die Details im Bericht zu verstehen.

TABELLE 4-5. Bericht "Full Disk Encryption Status" – Beispiel

HEADER	BEISPIEL	BESCHREIBUNG
Richtlinie	GP1	Der Titel der Richtlinie, die das Endpoint Encryption Gerät steuert.
Gerätename	TREND-4136D2DB3	Der vom Endpoint Encryption Gerät verwendete Computername.
Geräte-ID	1fabfbff-0001-06e5-000c-29 7085710000	Die eindeutige ID, die festgelegt wurde, nachdem der Endpoint Encryption Agent auf dem Endpunkt installiert und ein neues Endpoint Encryption Gerät bei PolicyServer registriert wurde.
Agent	Full Disk Encryption	Der derzeit installierte Endpoint Encryption Agent.
Status	Nicht verschlüsselt	Der aktuelle Zustand des Endpoint Encryption Geräts.
Datum der letzten Synchronisierung	07.10.2013 11:05	Der Zeitpunkt, als die Richtlinien zum letzten Mal auf dem Endpoint Encryption Gerät von PolicyServer aktualisiert wurden.
Letzte Richtliniendurchsetzung	07.10.2013 11:05	Der Zeitpunkt, als Control Manager zum letzten Mal Richtlinienänderungen auf PolicyServer durchgesetzt hat.

Erfolglose Anmeldeversuche am Endpoint Encryption Gerät

Auf dem Widget **Erfolglose Anmeldeversuche am Endpoint Encryption Gerät** werden alle Endpoint Encryption Geräte mit erfolglosen Anmeldeversuchen durch beliebige Benutzer (Endpoint Encryption Benutzer oder Nicht-Endpoint Encryption Benutzer) angezeigt. Erfolgloses Anmeldeversuche an einem Gerät stellen möglicherweise einen Sicherheitsverstoß dar oder der Endpoint Encryption Benutzer hat vielleicht seine Anmeldedaten vergessen.



Spalte	Beschreibung
Gerätename	Der Computername des Endpoint Encryption Geräts.
Richtlinie	Die Richtlinie, die das Endpoint Encryption Gerät verwaltet.
Ereignisse	Die Anzahl der Anmeldeversuche. Klicken Sie auf die Zahl, um den Bericht **Erfolglose Anmeldeversuche am Endpoint Encryption Gerät** anzuzeigen.

Bericht "Erfolglose Anmeldeversuche am Gerät"

In der folgenden Tabelle wird der Bericht **Erfolglose Anmeldeversuche am Endpoint Encryption Gerät** beschrieben. Die Angaben sollen Ihnen helfen, die Details im Bericht zu verstehen.

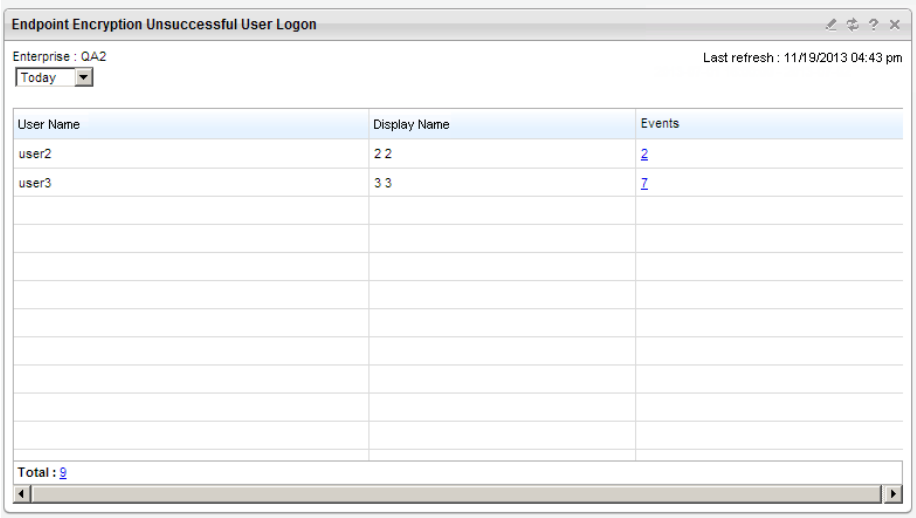
TABELLE 4-6. Bericht "Erfolglose Anmeldeversuche am Endpoint Encryption Gerät" – Beispiel

HEADER	BEISPIEL	BESCHREIBUNG
Ereigniszeitstempel	02.07.2012 13:56	Die Uhrzeit, als das Ereignis aufgetreten ist.
Richtlinie	GP1	Der Titel der Richtlinie, die das Endpoint Encryption Gerät steuert.
Gerätename	TREND-4136D2DB3	Der vom Endpoint Encryption Gerät verwendete Computername.
Geräte-ID	1fabfbff-0001-06e5-000c-297085710000	Die eindeutige ID, die festgelegt wurde, nachdem der Endpoint Encryption Agent auf dem Endpunkt installiert und ein neues Endpoint Encryption Gerät bei PolicyServer registriert wurde.
IP-Adresse	`10.1.152,219`	Die IP-Adresse des Endpoint Encryption Geräts.
Agent	Full Disk Encryption	Der derzeit installierte Endpoint Encryption Agent.
Benutzername	benutzer325	Der Name des Benutzers, der versuchte, sich an einem Endpoint Encryption Gerät anzumelden.
Anzeigename	Mary Jones	Der Vorname und der Nachname des Endpoint Encryption Benutzerkontos. Wenn es sich beim angegebenen Benutzernamen nicht um einen gültigen Endpoint Encryption Benutzernamen handelt, wird in der Spalte „Nicht aufgezeichnet“ angegeben.

Header	Beispiel	Beschreibung
Ereignis	Erfolglose Anmeldung per festem Kennwort	Das protokollierte Ereignis einschließlich der Authentifizierungsmethode.

Erfolglose Anmeldeversuche des Endpoint Encryption Benutzers

Auf dem Widget **Erfolglose Anmeldeversuche am Endpoint Encryption Gerät** werden alle Anmeldeversuche durch einen beliebigen Benutzer (Endpoint Encryption Benutzer oder Nicht-Endpoint Encryption Benutzer) an einem beliebigen Endpoint Encryption Gerät angezeigt.



Spalte	Beschreibung
Benutzername	Der Name des Benutzers, der versuchte, sich an einem Endpoint Encryption Gerät anzumelden.
Anzeigename	Der Anzeigename des Benutzerkontos, das versuchte, sich am Endpoint Encryption Gerät anzumelden.
Ereignisse	Die Anzahl der Authentifizierungsversuche. Klicken Sie auf die Zahl, um den Bericht "Erfolglose Anmeldeversuche des Endpoint Encryption Benutzers" anzuzeigen.

Bericht "Erfolglose Anmeldeversuche des Benutzers"

In der folgenden Tabelle wird der Bericht **Erfolglose Anmeldeversuche des Endpoint Encryption Benutzers** beschrieben. Die Angaben sollen Ihnen helfen, die Details im Bericht zu verstehen.

Tabelle 4-7. Bericht "Erfolglose Anmeldeversuche des Endpoint Encryption Benutzers" – Beispiel

Header	Beispiel	Beschreibung
Ereigniszeitstempel	02.07.2012 13:56	Die Uhrzeit, als das Ereignis aufgetreten ist.
Richtlinie	GP1	Der Titel der Richtlinie, die das Endpoint Encryption Gerät steuert.
Gerätename	TREND-4136D2DB3	Der vom Endpoint Encryption Gerät verwendete Computername.
Geräte-ID	1fabfbff-0001-06e5-000c-297085710000	Die eindeutige ID, die festgelegt wurde, nachdem der Endpoint Encryption Agent auf dem Endpunkt installiert und ein neues Endpoint Encryption Gerät bei PolicyServer registriert wurde.
IP-Adresse	`10.1.152,219`	Die IP-Adresse des Endpoint Encryption Geräts.
Agent	Full Disk Encryption	Der derzeit installierte Endpoint Encryption Agent.

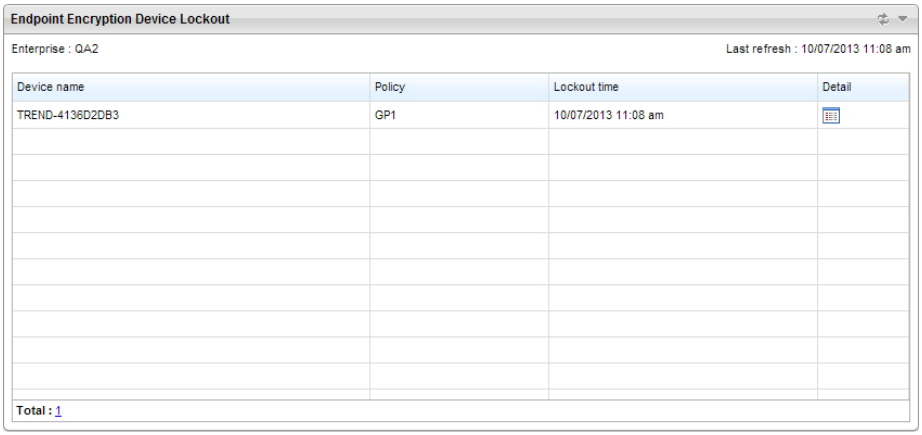
Header	Beispiel	Beschreibung
Benutzername	benutzer325	Der Name des Benutzers, der versuchte, sich an einem Endpoint Encryption Gerät anzumelden.
Anzeigename	Mary Jones	Der Vorname und der Nachname des Endpoint Encryption Benutzerkontos. Wenn es sich beim angegebenen Benutzernamen nicht um einen gültigen Endpoint Encryption Benutzernamen handelt, wird in der Spalte „Nicht aufgezeichnet“ angegeben.
Ereignis	Erfolglose Anmeldung per festem Kennwort	Das protokollierte Ereignis einschließlich der Authentifizierungsmethode.

Endpoint Encryption - Gerätesperrung

Das Widget **Endpoint Encryption - Gerätesperrung** zeigt Endpoint Encryption Geräte an, die aufgrund von Richtlinieneinschränkungen gesperrt wurden.

Hinweis

Informationen zu Regeln zur Gerätesperrung von Endpoint Encryption finden Sie unter *Sperraktionen auf Seite 5-27*.



HEADER	BESCHREIBUNG
Gerätename	Der vom Endpoint Encryption Gerät verwendete Computername.
Richtlinie	Der Titel der Richtlinie, die das Endpoint Encryption Gerät steuert.
Sperrung	Der Zeitpunkt, als PolicyServer den Befehl zum Sperren des Geräts gegeben hat. Das Endpoint Encryption Gerät wird faktisch erst gesperrt, nachdem der Endpoint Encryption Agent die Richtlinien mit PolicyServer synchronisiert hat.
Details	Klicken Sie auf das Detailsymbol, um den Bericht "Endpoint Encryption - Gerätesperrung" anzuzeigen.

Klicken Sie unten im Widget auf die Zahl neben **Gesamt**, um den Bericht anzuzeigen.

Bericht zur Gerätesperrung

In der folgenden Tabelle wird der Bericht **Endpoint Encryption Gerätesperrung** beschrieben. Die Angaben sollen Ihnen helfen, die Details im Bericht zu verstehen.

Hinweis

Informationen zu den Aktionen zum Sperren von Konten und Geräten finden Sie unter *Sperraktionen auf Seite 5-27*.

TABELLE 4-8. Bericht "Endpoint Encryption Gerätesperrung" – Beispiel

HEADER	BEISPIEL	BESCHREIBUNG
Ereigniszeitstempel	02.07.2012 13:56	Die Uhrzeit, als das Ereignis aufgetreten ist.
Richtlinie	GP1	Der Titel der Richtlinie, die das Endpoint Encryption Gerät steuert.
Gerätename	TREND-4136D2DB3	Der vom Endpoint Encryption Gerät verwendete Computername.
Geräte-ID	1fabfbff-0001-06e5-000c-29 7085710000	Die eindeutige ID, die festgelegt wurde, nachdem der Endpoint Encryption Agent auf dem Endpunkt installiert und ein neues Endpoint Encryption Gerät bei PolicyServer registriert wurde.
IP-Adresse	`10.1.152,219`	Die IP-Adresse des Endpoint Encryption Geräts.
Agent	Full Disk Encryption	Der derzeit installierte Endpoint Encryption Agent.
Benutzername	benutzer325	Der Name des Benutzers, der versuchte, sich an einem Endpoint Encryption Gerät anzumelden.

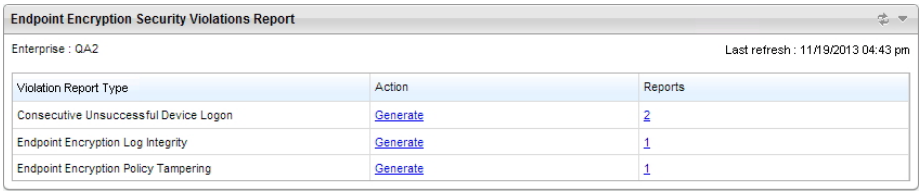
Header	Beispiel	Beschreibung
Anzeigename	Mary Jones	Der Vorname und der Nachname des Endpoint Encryption Benutzerkontos. Wenn es sich beim angegebenen Benutzernamen nicht um einen gültigen Endpoint Encryption Benutzernamen handelt, wird in der Spalte „Nicht aufgezeichnet“ angegeben.
Ereignis	Das Gerät wurde aufgrund einer Verletzung durch einen ungültigen Anmeldeversuch gesperrt.	Das protokollierte Ereignis einschließlich der Authentifizierungsmethode.

Endpoint Encryption Bericht zu Sicherheitsverstößen

Das Widget **Endpoint Encryption - Bericht zu Sicherheitsverstößen** zeigt die Sicherheitsverstöße aus folgenden Berichten an:

- **Endpoint Encryption - Aufeinanderfolgende erfolglose Anmeldeversuche am Gerät**
- **Endpoint Encryption - Richtlinienmanipulation**
- **Endpoint Encryption - Protokollintegrität**

Beim Generieren eines Berichts werden alle Sicherheitsverstöße erfasst, die momentan von PolicyServer protokolliert wurden. Klicken Sie nach der Generierung auf die Zahl in der Spalte **Berichte**, um die generierten Berichte für diesen Verstoß anzuzeigen.



Header	Beschreibung
Typ des Berichts zu Verstößen	Die verfügbaren Berichttypen für verschiedene Verstöße.
Aktion	Klicken Sie auf **Generieren**, um einen neuen Bericht zu erstellen.
Berichte	Die Gesamtzahl der generierten Berichte für diesen Verstoß. Klicken Sie auf die Zahl, um die verfügbaren Berichte anzuzeigen.

Hinweis

Zur Angabe der Anzahl erfolgloser Anmeldeversuche, die noch nicht als Sicherheitsverletzung betrachtet werden, klicken Sie auf ▼, um das Fenster **Widget-Einstellungen** zu öffnen, geben einen Wert im Textfeld **Aufeinanderfolgende erfolglose Anmeldungen** ein und klicken dann auf **Speichern**.

Bericht zu aufeinanderfolgenden erfolglosen Anmeldeversuchen am Gerät

In der folgenden Tabelle wird der Bericht **Endpoint Encryption - Aufeinanderfolgende erfolglose Anmeldeversuche am Gerät** beschrieben. Anhand der Informationen aus diesem Bericht sehen Sie, wann der Anmeldungsversuch durchgeführt wurde, welches Endpoint Encryption Gerät betroffen ist und wie oft der Benutzer versucht hat, sich am Endpoint Encryption Gerät anzumelden.

TABELLE 4-9. Bericht "Endpoint Encryption - Aufeinanderfolgende erfolglose Anmeldeversuche am Gerät" – Beispiel

EINTRAG	BEISPIEL	BESCHREIBUNG
Ereigniszeitstempel	02.07.2012 13:56	Die Uhrzeit, als das Ereignis aufgetreten ist.
Gerätename	TREND-4136D2DB3	Der vom Endpoint Encryption Gerät verwendete Computername.
Versuche	5	Die Häufigkeit, wie oft ein Benutzer versuchte, sich am Endpoint Encryption Gerät anzumelden.

Bericht zu Richtlinienmanipulationen

In der folgenden Tabelle wird der Bericht **Endpoint Encryption - Bericht zu Richtlinienmanipulationen** beschrieben. Die Angaben sollen Ihnen helfen, die Details im Bericht zu verstehen.

TABELLE 4-10. Bericht "Endpoint Encryption Richtlinienmanipulationen" – Beispiel

HEADER	BEISPIEL	BESCHREIBUNG
Ereigniszeitstempel	02.07.2012 13:56	Die Uhrzeit, als das Ereignis aufgetreten ist.
Ereignis	Integritätsprüfung des Richtlinienwerts fehlgeschlagen	Das protokollierte Ereignis einschließlich der Authentifizierungsmethode.

Bericht zur Protokollintegrität

In der folgenden Tabelle wird der Bericht **Endpoint Encryption - Bericht zur Protokollintegrität** beschrieben. Die Angaben sollen Ihnen helfen, die Details im Bericht zu verstehen.

TABELLE 4-11. Bericht "Endpoint Encryption Protokollintegrität" – Beispiel

HEADER	BEISPIEL	BESCHREIBUNG
Ereigniszeitstempel	02.07.2012 13:56	Die Uhrzeit, als das Ereignis aufgetreten ist.
Ereignis	Audit-Protokoll-Datensatz fehlt	Das protokollierte Ereignis einschließlich der Authentifizierungsmethode.

Kapitel 5

Richtlinien

In diesem Kapitel wird die Verwendung von Richtlinien erläutert. Weiterhin werden ausführliche Informationen zu einzelnen Richtlinienwerten bereitgestellt.

Authentifizierungsübersicht

Die primäre Form des Schutzes, den Endpoint Encryption bietet, besteht darin, nicht autorisierten Zugriff von Benutzern auf verschlüsselte Endpunkte und Geräte zu verhindern. Durch die ordnungsgemäße Konfiguration vonEndpoint Encryption-Geräten, -Benutzern und -Richtliniengruppen wird das Risiko eines Datenverlustes durch zufälliges Freigeben von Informationen oder absichtliche Sabotage vermieden.

Geräte auf Seite 5-2	Endpoint Encryption zählt die Anzahl der aufeinanderfolgenden Anmeldeversuche bei einem bestimmten Gerät und die Zeit, die seit der letzten Kommunikation mit PolicyServer in einer bestimmten Zeitspanne vergangen ist. Falls ein Gerät die Richtlinienkriterien verletzt, kann Endpoint Encryption die Festplatte zurücksetzen, sperren oder löschen.
Benutzer auf Seite 5-3	Neben der Prüfung der Authentifizierungsversuche bei einem Gerät zählt Endpoint Encryption auch die Anzahl der aufeinanderfolgenden Anmeldeversuche durch ein bestimmtes Benutzerkonto. Falls dieser Benutzer die Richtlinienkriterien verletzt, kann Endpoint Encryption die Festplatte zurücksetzen, sperren oder löschen.
Gruppen auf Seite 5-5	Gruppen fungieren als Behälter für Benutzer für die Richtlinienverwaltung. Administratoren und Authentifizierer innerhalb einer Gruppe haben jene besonderen Berechtigungen nur innerhalb dieser Gruppe, nicht zugewiesene Administratoren und Authentifizierer haben diese Rolle über das gesamte Unternehmen hinweg inne.

Eine komplette Liste mit den konfigurierbaren Methoden zur Authentifizierung von Benutzern und Geräten finden Sie unter *Authentifizierungsmethode auf Seite 2-11*.

Geräte

Endpoint Encryption Geräte sind Endpoint Encryption Agents, die mit PolicyServer registriert wurden. Bei der Installation eines Endpoint Encryption Agent wird der Endpunkt automatisch bei PolicyServer als ein Endpoint Encryption Gerät registriert. Da ein bestimmter Endpunkt von mehreren Endpoint Encryption Agents geschützt werden kann, erscheint ein einzelner Endpunkt möglicherweise als mehrere Endpoint Encryption Geräte auf PolicyServer.

Je nach Richtlinieneinstellungen führt Endpoint Encryption eine der folgende Aktionen durch, wenn Benutzer erfolglos versuchen, sich mehrmals hintereinander auf diesem Gerät anzumelden:

- Den nächsten Authentifizierungsversuch verzögern
- Das Gerät sperren
- Alle Daten auf dem Gerät löschen

Hinweis

Verwenden Sie zum Konfigurieren der Endpoint Encryption Geräte das Widget **Endpoint Encryption - Geräte**. Weitere Informationen finden Sie unter *Endpoint Encryption - Geräte auf Seite 4-14*.

Benutzer

Bei Endpoint Encryption Benutzern handelt es sich um alle Benutzerkonten, die manuell zum PolicyServer hinzugefügt oder die mit Active Directory synchronisiert wurden.

Endpoint Encryption verfügt über mehrere Typen von Kontorollen und Authentifizierungsmethoden, die eine umfassende, auf Identität basierende Authentifizierung und Verwaltung möglich machen. Mit Control Manager oder PolicyServer MMC können Sie Benutzerkonten hinzufügen oder importieren, die Authentifizierung steuern, mit Active Directory eine Synchronisierung durchführen und die Mitgliedschaft in Richtliniengruppen bei Bedarf verwalten.

In der folgenden Tabelle werden die Benutzerrollen von Endpoint Encryption beschrieben:

Rolle	Beschreibung
Administrator	Administratoren können auf die Management-Konsolen zugreifen und beliebige Konfigurationen innerhalb ihrer Domäne durchführen. Diese Rolle hat je nach Stufe, zu der der Administrator hinzugefügt wird, andere Rechte: • Unternehmensadministrator: Diese Administratoren haben Kontrolle über alle Richtlinien, Gruppen, Benutzer und Geräte im Unternehmen. • Gruppenadministrator: Diese Administratoren haben Kontrolle über Benutzer und Geräte, die sich innerhalb einer bestimmten Gruppe authentifizieren. Control Manager erstellt eine Gruppe für jede Richtlinie, sodass diese Administratoren auch als „Richtlinienadministratoren“ bekannt sein können.
Authentifizierer	Authentifizierer stehen für ortsferne Unterstützung zur Verfügung, wenn Benutzer ihre Kennwörter für Endpoint Encryption vergessen haben oder auf technische Probleme stoßen. Diese Rolle hat je nach Stufe, zu der die Authentifiziererrolle hinzugefügt wird, andere Rechte: • Unternehmensauthentifizierer: Diese Authentifizierer können beliebige Benutzer im Unternehmen unterstützen. • Gruppenauthentifizierer: Diese Authentifizierer können beliebige Benutzer innerhalb einer bestimmten Gruppen unterstützen. Control Manager erstellt eine Gruppe für jede Richtlinie, sodass diese Authentifizierer auch als „Richtlinienauthentifizierer“ bekannt sein können.
Benutzer	Einfache Endbenutzer haben keine besonderen Berechtigungen. Die Benutzerrolle kann sich möglicherweise nicht bei den Endpoint Encryption Management-Konsolen anmelden. Soweit nicht von PolicyServer zugelassen, kann die Benutzerrolle möglicherweise auch keine Wiederherstellungstools verwenden.

Hinweis

Verwenden Sie zum Konfigurieren der Endpoint Encryption Benutzer das Widget **Endpoint Encryption Benutzer**. Weitere Informationen finden Sie unter *Endpoint Encryption Benutzer auf Seite 4-7*.

Gruppen

Endpoint Encryption verwaltet Richtlinien nach Benutzergruppen. Die Gruppenverwaltung unterscheidet zwischen PolicyServer MMC und Control Manager. Nach der Änderung von Richtlinien und Gruppen synchronisiert PolicyServer Gruppen über beide Konsolen hinweg.

Wichtig

Control Manager hat für die Richtlinien- und Gruppenzuweisung immer Vorrang vor PolicyServer MMC. Alle mit PolicyServer MMC durchgeführten Änderungen an der Gruppenzuweisung werden beim nächsten Mal automatisch überschrieben, wenn Control Manager Richtlinien mit PolicyServer synchronisiert.

KONSOLE	GRUPPENVERWALTUNG
Control Manager	Endpoint Encryption erstellt eine Gruppe automatisch jedes Mal, wenn eine Richtlinie mit bestimmten Zielen bereitgestellt wird. Ändern Sie nach der Verteillung die Gruppen, in denen sich ein Benutzer befindet, über das Widget **Endpoint Encryption Benutzer** und ändern Sie die Benutzer in der Richtlinie über das Fenster **Richtlinienverwaltung**.

KONSOLE	GRUPPENVERWALTUNG
PolicyServer MMC	Fügen Sie Gruppen direkt aus dem linken Fensterbereich von PolicyServer MMC hinzu und ändern Sie diese. Gruppen in PolicyServer MMC können wie folgt zugewiesen werden: • **Top-Gruppe**: Top-Gruppen sind die höchste Stufe der Gruppen im Unternehmen. Jede Top-Gruppe hat einen eindeutigen Knoten unterhalb des Unternehmens. • **Untergruppe**: Untergruppen werden innerhalb von Top-Gruppen erstellt. Untergruppen erben bei der Erstellung die Richtlinien der Top-Gruppe, allerdings keine Änderungen, die an der Top-Gruppe vorgenommen werden. Untergruppen dürfen nicht weniger strenge Berechtigungen wie die Top-Gruppe aufweisen. **Hinweis** Sie müssen Geräte und Benutzer manuell zu jeder Untergruppe zuweisen. Beim Hinzufügen von Endpoint Encryption Benutzern zu einer Untergruppe werden die Benutzer nicht automatisch zur Top-Gruppe hinzugefügt. Sie können jedoch Benutzer sowohl zur Top-Gruppe als auch zur Untergruppe hinzufügen.

Hinweis

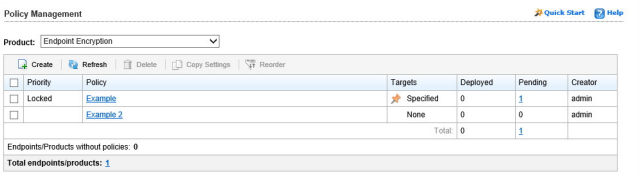
Um die Benutzer innerhalb einer Richtliniengruppe auf Control Manager zu konfigurieren, verwenden Sie das Widget **Endpoint Encryption Benutzer**. Weitere Informationen finden Sie unter *Endpoint Encryption Benutzer auf Seite 4-7*.

Informationen zur Konfiguration der Benutzer innerhalb einer Richtliniengruppe auf PolicyServer MMC finden Sie im *Endpoint Encryption PolicyServer MMC Handbuch*.

Richtlinien in Control Manager

In der Richtlinienliste werden die Informationen und der Status der Richtlinien angezeigt, die von allen Benutzern erstellt wurden. Wenn ein neuer Endpunkt in Control Manager registriert wird, wird die Liste der gefilterten Richtlinien in absteigender Reihenfolge abgearbeitet. Control Manager weist den neuen Endpunkt einer gefilterten Richtlinie zu, wenn die folgenden Bedingungen erfüllt sind:

- Der neue Endpunkt stimmt mit dem Zielkriterium der Richtlinie überein
- Der Verfasser der Richtlinie verfügt über die Berechtigung, den neuen Endpunkt zu verwalten



Die folgende Tabelle beschreibt die Elemente in der Richtlinienliste.

MENÜELEMENT	BESCHREIBUNG
Priorität	Diese Spalte wird in Endpoint Encryption nicht verwendet. Diese Spalte zeigt nur Folgendes an: • Gesperrt: Die Richtlinie wurde erstellt und wird derzeit verwendet. • Leer: Die Richtlinie ist ein Entwurf und wird derzeit nicht verwendet.
Richtlinie	Zeigt den Namen der Richtlinie an.
Ziele	Zeigt an, wie Administratoren Ziele für die Richtlinie auswählen. • Angabe: Wählt mit Hilfe der Funktionen zum Durchsuchen und Suchen bestimmte Ziele für die Richtlinie. Angegebene Richtlinien bleiben statisch ganz oben in der Richtlinienliste und haben eine höhere Priorität als jede gefilterte Richtlinie. • Gefiltert: Diese Option wird in Endpoint Encryption nicht verwendet. • Keine: Der Verfasser der Richtlinie speichert die Richtlinie als Entwurf, ohne Ziele auszuwählen.
Verteilt	Zeigt die Anzahl der Ziele an, die die Richtlinieneinstellungen angewendet haben.

MENÜELEMENT	BESCHREIBUNG
Ausstehend	Zeigt die Anzahl der Ziele an, die die Richtlinieneinstellungen nicht angewendet haben. Klicken Sie auf die Zahl für "Ausstehend", um den Status der Richtlinie zu überprüfen.
Verfasser	Zeigt den Benutzer an, der die Richtlinie erstellt hat.
Endpunkte/Produkte ohne Richtlinien	Zeigt die Anzahl der verwalteten Produkte oder Endpunkte an, denen Control Manager keine Richtlinie zugewiesen hat.
Gesamtzahl der Endpunkte/Produkte	Zeigt die Anzahl der verwalteten Produkte oder Endpunkte an, die für die Richtlinienverwaltung verfügbar sind.

Hinweis

In den Werten in "Verteilt", "Ausstehend", "Endpunkte/Produkte ohne Richtlinien" und "Gesamtzahl der Endpunkte/Produkte" werden nur die Endpunkte oder verwalteten Produkte erfasst, die ein Administrator laut seinen Berechtigungen verwalten darf.

Richtlinienoptionen

Über die Richtlinienverwaltung können Administratoren die Produkteinstellungen auf verwalteten Produkten von einer einzelnen Management-Konsole aus durchsetzen. Administratoren erstellen eine Richtlinie, indem sie die Ziele auswählen und eine Liste der Produkteinstellungen konfigurieren.

Control Manager Richtlinien weisen die folgenden Attribute auf:

TABELLE 5-1. Control Manager Richtlinienoptionen

ATTRIBUT	BESCHREIBUNG
Name der Richtlinie	Der Name der Richtlinienkonfiguration.

Attribut	Beschreibung
Ziele	Administratoren können Ziele auswählen, die ihren Richtlinien zugewiesen werden sollen. Die Methode zur Zielauswahl bestimmt den Richtlinientyp und wie die Richtlinie funktioniert. Administratoren können Ziele manuell auswählen oder Filter verwenden, um Zielen automatisch Richtlinien zuzuweisen. Die Methode zur Zielauswahl bestimmt den Richtlinientyp und wie die Richtlinie funktioniert. Weitere Informationen über Richtlinientypen finden Sie unter *Richtlinientypen auf Seite 5-10*. Wenn Sie ein verwaltetes Produkt oder einen Endpunkt als Ziel einbeziehen möchten, vergewissern Sie sich, dass die Produktversion des verwalteten Produkts oder Endpunkts die Richtlinienverwaltung in Control Manager unterstützt. Das Fenster **Policy Template Settings** enthält Informationen zu den unterstützten Produktversionen.
Einstellungen	Nachdem Control Manager eine Richtlinie auf die Ziele verteilt hat, überschreiben die in der Richtlinie definierten Einstellungen die bestehenden Einstellungen in den Zielen. Control Manager setzt die Richtlinieneinstellungen in den Zielen alle 24 Stunden durch. Obwohl lokale Administratoren Änderungen an den Einstellungen über die Konsole des verwalteten Produkts vornehmen können, werden die Änderungen jedes Mal überschrieben, wenn Control Manager die Richtlinieneinstellungen überschreibt. **Hinweis** Da Richtlinien nur alle 24 Stunden durchgesetzt werden, entsprechen die Produkteinstellungen in den Zielen möglicherweise nicht den Richtlinieneinstellungen, wenn lokale Administratoren Änderungen über die Konsole der verwalteten Produkte zwischen der Durchsetzungsperiode vornehmen.

Hinweis

Verwenden Sie das **Produktverzeichnis**, um die verwaltete PolicyServer Instanz aus dem Ordner "Neues Element" in den Endpoint Encryption Ordner im Produktverzeichnis zu verschieben.

Richtlinientypen

Control Manager unterstützt drei Richtlinientypen, die von Administratoren erstellt werden können. Jeder Richtlinientyp unterscheidet sich in der Auswahlmethode für Ziele, was sich auf die Arbeitsweise der Richtlinie auswirkt. Entsprechend der Beschreibung in der folgenden Tabelle werden die Richtlinientypen in der Richtlinienliste wie folgt sortiert.

TABELLE 5-2. Richtlinientypen

RICHTLINIENTYP	BESCHREIBUNG
Angebe	• Verwendet die Funktionen zum Durchsuchen und Suchen, um bestimmte Ziele zu finden und sie manuell einer Richtlinie zuzuweisen. • Nützlich, wenn Administratoren planen, bestimmte Einstellungen nur auf bestimmte Ziele zu verteilen. • Bleibt an statischer Position ganz oben in der Richtlinienliste und hat eine höhere Priorität als alle gefilterten Richtlinien.
Gefiltert	**Hinweis** Endpoint Encryption unterstützt keine gefilterten Richtlinien.
Entwurf	Ermöglicht, dass Administratoren die Richtlinieneinstellungen als Entwurf ohne Auswahl von Zielen speichern können. Control Manager speichert Entwurfsrichtlinien mit der untersten Priorität ganz unten in der Liste.

Eine Richtlinie erstellen

Das folgende Verfahren erklärt, wie Sie eine Control Manager Richtlinie konfigurieren, die sich auf Endpoint Encryption Benutzer und Geräte auswirkt.

Prozedur

1. Richten Sie Ihre Benutzer und Geräte für Endpoint Encryption ein.

   Die Benutzer- und Gerätekonfiguration von Endpoint Encryption verwendet die Widgets **Endpoint Encryption Benutzer** und **Endpoint Encryption - Geräte**. Informationen finden Sie unter *Endpoint Encryption Benutzer auf Seite 4-7* bzw. *Endpoint Encryption - Geräte auf Seite 4-14*.

   Falls Ihre Umgebung Active Directory enthält, stellen Sie sicher, dass Sie Active Directory konfiguriert und alle Benutzer synchronisiert haben. Weitere Informationen finden Sie unter *Active Directory-Synchronisierung auf Seite 3-25*.

   Eine allgemeine Beschreibung des Authentifizierungsvorgangs finden Sie unter *Authentifizierungsübersicht auf Seite 5-2*.

2. Wechseln Sie zum Fenster **Richtlinie erstellen**.

   a. Navigieren Sie zu **Richtlinien** > **Richtlinienverwaltung**.

   b. Wählen Sie im Listenfeld **Produkt** die Option **Endpoint Encryption**.

   c. Klicken Sie auf **Erstellen**.

   Das Fenster **Richtlinie erstellen** wird angezeigt.

3. Geben Sie einen Richtliniennamen an.

4. Aktivieren Sie eine der folgenden Optionen für das Richtlinienziel:

   - **Keines (nur Entwurf)**: Sie erstellen eine Richtlinie ohne Ziele (Endpunkte).

     Eine Richtlinie ohne Ziele kann nicht verteilt werden. Nach dem Erstellen eines Richtlinienentwurfs bearbeiten Sie die Richtlinie später, um Ziele anzugeben und sie in Ihrer Umgebung zu verteilen.

   - **Filter nach Kriterien**: Endpoint Encryption unterstützt keine Filterung nach Kriterien.

   - **Ziel(e) angeben**: Sie geben vorhandene Endpunkte an.

     Hinweis

     Weitere Informationen zu Richtlinienzielen finden Sie unter *Richtlinienziele angeben auf Seite 5-13*.

5. Geben Sie Endpoint Encryption Richtlinienoptionen an.

   Endpoint Encryption Einstellungen sind in die folgenden Regelsätze unterteilt:

REGELSATZ	REFERENZ
Benutzer	*Endpoint Encryption Benutzerregeln konfigurieren auf Seite 5-14*
Full Disk Encryption	*Full Disk Encryption Regeln konfigurieren auf Seite 5-17*
File Encryption	*File Encryption Regeln konfigurieren auf Seite 5-21*
Allgemein	*Allgemeine Regeln für Richtlinien konfigurieren auf Seite 5-24*

6. Klicken Sie auf **Speichern**.

Richtlinienziele angeben

Im Fenster **Ziel(e) angeben** weisen Sie die Endpoint Encryption Geräte der Richtlinie zu.

Hinweis

Das Fenster **Ziel(e) angeben** wird angezeigt, wenn Sie eine neue Richtlinie erstellen.

Informationen zum Erstellen einer Richtlinie finden Sie unter *Eine Richtlinie erstellen auf Seite 5-11*.

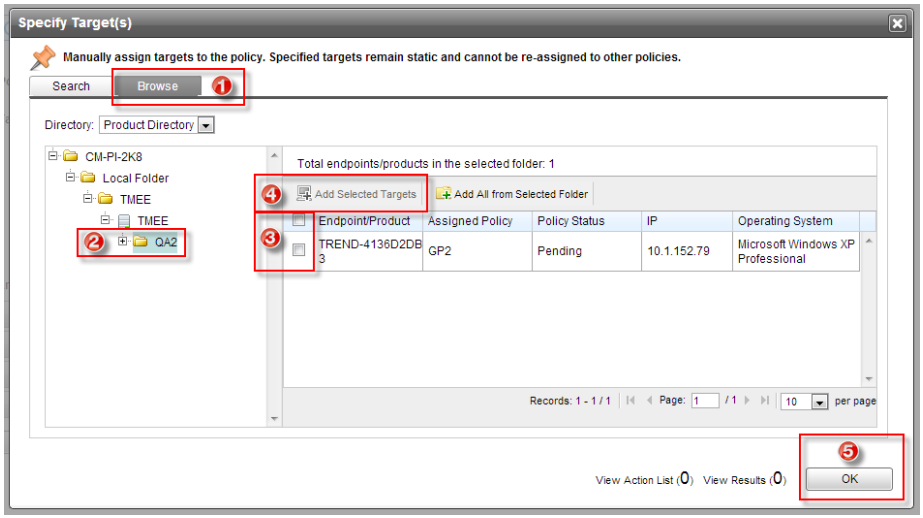


ABBILDUNG 5-1. Richtlinienziele angeben

Prozedur

1. Klicken Sie im Fenster **Ziel(e) angeben** auf die Registerkarte **Durchsuchen**.
2. Erweitern Sie die Struktur im linken Fensterbereich, um den verwalteten Ordner zu wählen.

   Beispiel: **CM-PI-2K8** > **Lokaler Ordner** > **TMEE** > **TMEE** > **QA2**

3. Wählen Sie die entsprechenden Endpoint Encryption Geräte aus oder aktivieren Sie das obere Kontrollkästchen, um alle Endpoint Encryption Geräte auszuwählen, die auf der aktuellen Seite aufgelistet werden.

4. Klicken Sie auf **Ausgewählte Ziele hinzufügen**.

Hinweis

Wenn Sie sofort alle Geräte im verwalteten Ordner auswählen möchten, klicken Sie auf **Alle aus ausgewähltem Ordner hinzufügen**.

„Aktionsliste anzeigen“ und „Ergebnisse anzeigen“ werden basierend auf der Auswahl aktualisiert.

5. Klicken Sie auf **OK**.

Endpoint Encryption Benutzerregeln konfigurieren

Das folgende Verfahren beschreibt die konfigurierbaren Optionen für Richtlinienregeln, die die Authentifizierung und Endpoint Encryption Benutzerkonten betreffen.

Prozedur

1. Erstellen Sie eine neue Endpoint Encryption Richtlinie.

   Weitere Informationen finden Sie unter *Eine Richtlinie erstellen auf Seite 5-11*.

2. Klicken Sie auf **Benutzer**.

Das Fenster zu den Richtlinienregeleinstellungen **Benutzer** wird angezeigt.

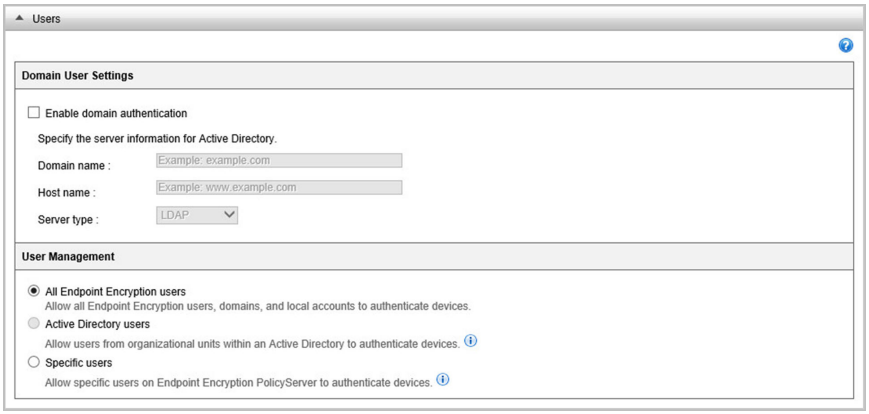


ABBILDUNG 5-2. Richtlinienregeln für Endpoint Encryption Benutzer

3. Wenn Benutzer Domänenauthentifizierung benötigen, wählen Sie die Option **Domänenauthentifizierung aktivieren** unter **Domänenbenutzereinstellungen** aus.

   Geben Sie bei Auswahl von **Domänenauthentifizierung aktivieren** die Serverinformationen für Ihr Active Directory (AD)-Konto an.

   a. Konfigurieren Sie den AD-Domänennamen.

   b. Konfigurieren Sie den Host-Namen des AD-Servers.

   c. Wählen Sie den Servertyp aus:

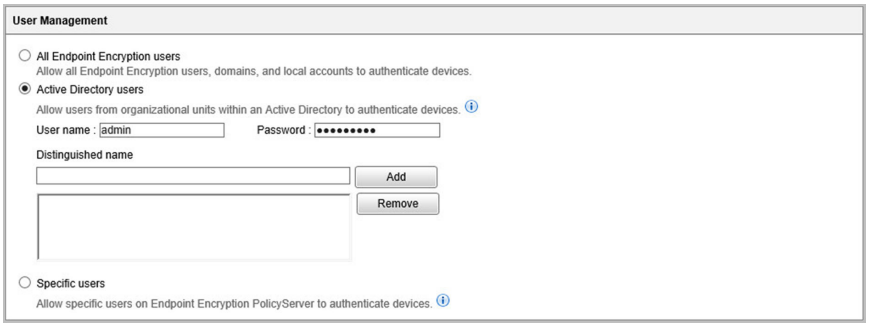
      - **LDAP**
      - **LDAP-Proxy**

4. Konfigurieren Sie unter **Benutzerverwaltung** den Benutzerzugriff.

OPTION	BEZEICHNUNG
Alle Endpoint Encryption Benutzer	Allen Benutzern, Domänen und lokalen Konten erlauben, Endpoint Encryption Geräte zu authentifizieren.
Active Directory-Benutzer	Benutzern aus Organisationseinheiten innerhalb eines AD erlauben, Endpoint Encryption Geräte zu authentifizieren. **Hinweis** Wählen Sie **Domänenauthentifizierung aktivieren** aus, um die Option **Active Directory-Benutzer** zu aktivieren. Weitere Informationen zum Konfigurieren der Domänenauthentifizierung finden Sie unter *Active Directory-Synchronisierung auf Seite 3-25*.
Bestimmte Benutzer auswählen	Legen Sie fest, welche bereits hinzugefügten Endpoint Encryption Benutzer sich an verwalteten Endpunkten authentifizieren können. **Hinweis** Um bestimmte Benutzer mit dieser Option auszuwählen, müssen Sie die Benutzerliste auffüllen. Fügen Sie Organisationseinheiten mit der Option **Active Directory-Benutzer** oder fügen Sie Benutzer mit dem Widget "Endpoint Encryption Benutzer" hinzu. Weitere Informationen zum Widget "Endpoint Encryption Benutzer" finden Sie unter *Endpoint Encryption Benutzer auf Seite 4-7*.

5. Wenn Sie **Active Directory-Benutzer** ausgewählt haben, fügen Sie der Richtlinie Organisationseinheiten nach ihrem eindeutigen Namen hinzu.

Nach Auswahl von **Active Directory-Benutzer** werden die folgenden zusätzlichen Optionen angezeigt:



Option	Bezeichnung
Benutzername	Geben Sie Ihren Active Directory-Benutzernamen ein.
Kennwort	Geben Sie Ihr Active Directory-Kennwort ein.
Eindeutiger Name	Legen Sie jede Organisationseinheit gemäß der Reihenfolge der relativen eindeutigen Namen getrennt durch Kommas fest. Beispiel: OU=TW, DC=mycompany, DC=com Wenn Sie den eindeutigen Namen für die Organisationseinheit festgelegt haben, klicken Sie auf **OK**. **Wichtig** Endpoint Encryption unterstützt bis zu 12 Organisationseinheiten pro Richtlinie.

Full Disk Encryption Regeln konfigurieren

Das folgende Verfahren beschreibt die konfigurierbaren Optionen für Richtlinienregeln, die sich auf Full Disk Encryption Geräte auswirken.

Hinweis

Encryption Management for Apple FileVault und Encryption Management for Microsoft BitLocker erfordern keine Authentifizierung und werden nicht durch Authentifizierungsrichtlinien beeinflusst. Client, Anmeldung, Kennwort und Authentifizierungsrichtlinien oder die Berechtigung des Benutzers, die Endpoint Encryption Agent-Software zu deinstallieren, wirkt sich nur auf die Full Disk Encryption Agents und File Encryption Agents aus.

Prozedur

1. Erstellen Sie eine neue Endpoint Encryption Richtlinie.

   Weitere Informationen finden Sie unter *Eine Richtlinie erstellen auf Seite 5-11*.

2. Klicken Sie auf **Full Disk Encryption**.

Das Fenster mit den Einstellungen für **Full Disk Encryption** Richtlinienregeln wird angezeigt.

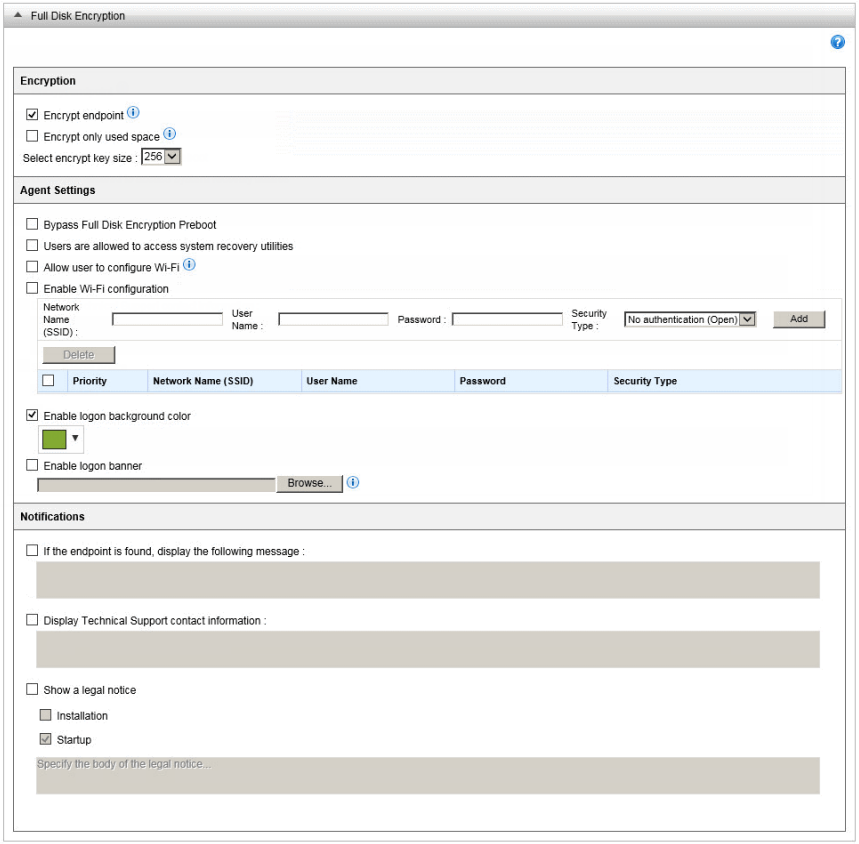


ABBILDUNG 5-3. Full Disk Encryption Richtlinienregeln

3. Wählen Sie unter **Verschlüsselung** die folgenden Optionen aus:

   - Wählen Sie **Gerät verschlüsseln** aus, um Festplattenverschlüsselung zu starten, wenn der Endpoint Encryption-Agent Richtlinien mit PolicyServer synchronisiert.

Warnung!

Sie sollten Full Disk Encryption Agents nicht verschlüsseln, ohne zuvor die Festplatte des Endpunkts vorzubereiten.

Informationen zur Vorbereitung der Festplatte finden Sie unter *Full Disk Encryption - Überblick über die Verteilung* im *Endpoint Encryption Installationshandbuch*.

- Wählen Sie **Nur verwendeten Speicherplatz verschlüsseln** aus, um nur den verwendeten Speicherplatz zu verschlüsseln.
- Wählen Sie **Größe des Verschlüsselungsschlüssels auswählen** aus, um die Größe des Verschlüsselungsschlüssels eines Geräts in Bit anzugeben.

4. Wählen Sie unter **Agent-Einstellungen** die folgenden Optionen:

   - Wählen Sie **Full Disk Encryption Preboot umgehen**, um dem Benutzer die Berechtigung zu geben, sich direkt bei Windows ohne den Schutz der Preboot-Authentifizierung zu authentifizieren.
   - Wählen Sie **Benutzer sind berechtigt, auf die Systemwiederherstellungstools des Geräts zuzugreifen**, um Benutzern zu erlauben, auf die Wiederherstellungskonsole zuzugreifen.

     Informationen zu den konfigurierbaren Optionen und verfügbaren Tools in Full Disk Encryption finden Sie unter *Wiederherstellungskonsole auf Seite 9-6*.
   - Wählen Sie **Konfiguration von WLAN durch Benutzer zulassen** aus, damit Benutzer während des Preboots WLAN-Richtlinien auf dem Gerät konfigurieren können.
   - Wählen Sie **WLAN-Konfiguration aktivieren** aus, um während des Preboots eine vordefinierte WLAN-Konfiguration zu verwenden. Geben Sie die folgenden Informationen an:
     - Netzwerkname (SSID)
     - Benutzername
     - Kennwort
     - Sicherheitstyp

- Wählen Sie **Hintergrundfarbe für Anmeldung aktivieren** aus, um die Hintergrundfarbe bei der Anmeldung anzugeben.
- Wählen Sie **Anmeldebanner aktivieren** aus, um ein Anmeldebannerbild anzugeben.

  Das Bild sollte 128 KB nicht überschreiten und 512 x 64 Pixel aufweisen. Akzeptierte Dateiformate sind PNG mit Transparenz (empfohlen), JPG und GIF

5. Konfigurieren Sie die folgenden Optionen unter **Benachrichtigungen**:
   - Wählen Sie **Falls der Endpunkt gefunden wird, folgende Meldung anzeigen**, um eine Meldung anzuzeigen, wenn die Richtlinie **Falls gefunden** aktiv ist.
   - Wählen Sie **Kontaktdaten für den Technischen Support anzeigen**, um eine Meldung anzuzeigen, wenn sich der Benutzer am Full Disk Encryption Agent anmeldet.
   - Wählen Sie **Rechtlichen Hinweis anzeigen**, um einen bestimmten rechtlichen Hinweis beim Start oder nur nach der Installation von Full Disk Encryption Agent anzuzeigen.

File Encryption Regeln konfigurieren

Das folgende Verfahren beschreibt die konfigurierbaren Optionen für Richtlinienregeln, die sich auf File Encryption Geräte auswirken.

Prozedur

1. Erstellen Sie eine neue Endpoint Encryption Richtlinie.

   Weitere Informationen finden Sie unter *Eine Richtlinie erstellen auf Seite 5-11*.

2. Klicken Sie auf "File Encryption".

Das Fenster mit den Einstellungen für **File Encryption** Richtlinienregeln wird angezeigt.

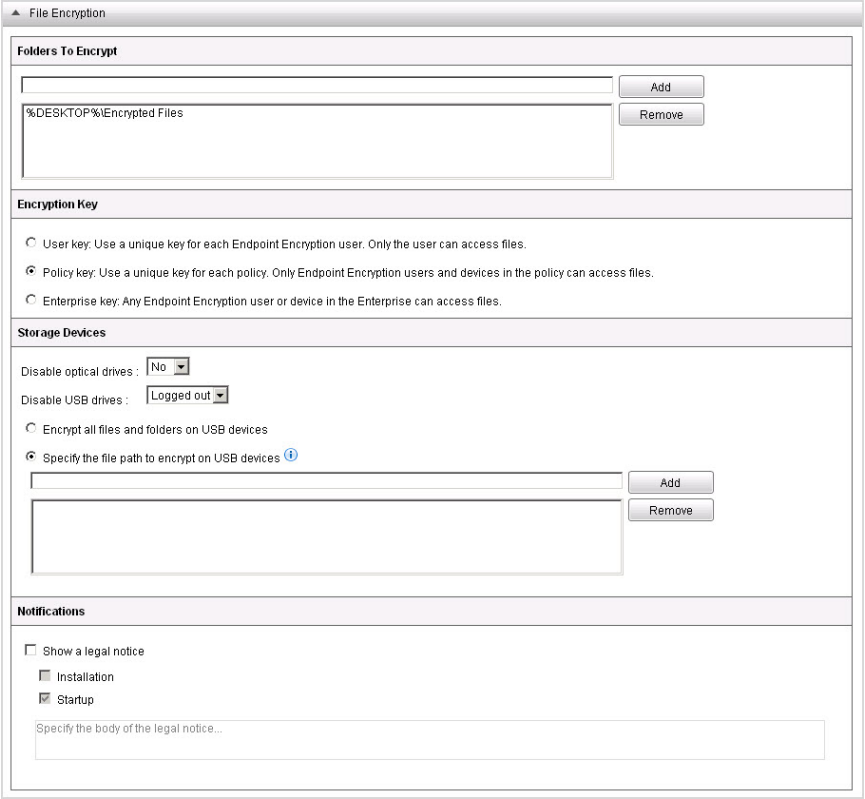


ABBILDUNG 5-4. File Encryption Richtlinienregeln

3. Legen Sie unter **Zu verschlüsselnde Ordner** die Ordner fest, die auf dem Endpunkt automatisch erstellt und verschlüsselt werden, wenn der File Encryption Agent Richtlinien synchronisiert.

4. Wählen Sie unter **Verschlüsselungsschlüssel** die Verschlüsselung für den verschlüsselten File Encryption Ordner.

- **Benutzerschlüssel**: Verwenden Sie einen eindeutigen Schlüssel für jeden Endpoint Encryption Benutzer. Nur der Endpoint Encryption Benutzer kann Dateien entschlüsseln, die von ihm oder von ihr verschlüsselt wurden.
- **Richtlinienschlüssel**: Verwenden Sie einen eindeutigen Schlüssel für jede Richtlinie. Nur Endpoint Encryption Benutzer und Geräte in der Richtlinie können Dateien entschlüsseln.
- **Unternehmensschlüssel**: Alle Endpoint Encryption Benutzer oder Geräte im Unternehmen können Dateien entschlüsseln.

Hinweis

Durch die Auswahl von **Richtlinienschlüssel** oder **Unternehmensschlüssel** steuern Sie den Austausch des gemeinsamen Schlüssels für File Encryption. Weitere Informationen finden Sie unter *File Encryption-Aktionen auf Seite 7-3*.

5. Konfigurieren Sie die folgenden Optionen unter **Speichergeräte**:
   - Wählen Sie **Optisches Laufwerk deaktivieren**, um festzulegen, ob der Zugriff auf Wechselmedien vom Endpunkt aus möglich ist.
   - Wählen Sie **USB-Laufwerk deaktivieren**, um festzulegen, ob USB-Ports deaktiviert sind. Folgende Optionen sind möglich:
     - **Immer**
     - **Abgemeldet**
     - **Nie**
   - Wählen Sie **Alle Dateien und Ordner auf USB-Geräten verschlüsseln**, um automatisch alle Dateien und Ordner auf Wechselmedien zu verschlüsseln, wenn diese mit dem Endpunkt verbunden sind.
   - Wählen Sie **Zu verschlüsselnden Dateipfad auf USB-Geräten angeben**, um verschlüsselte Ordner auf USB-Laufwerken hinzuzufügen oder zu entfernen. Nicht vorhandene Ordner werden erstellt. Wenn kein Laufwerksbuchstabe angegeben wird, gilt diese Regel für alle USB-Geräte.

6. Wählen Sie unter **Benachrichtigungen** die Option **Rechtlichen Hinweis anzeigen**, um einen bestimmten rechtlichen Hinweis beim Start oder nur nach der Installation von File Encryption Agent anzuzeigen.

Allgemeine Regeln für Richtlinien konfigurieren

In diesem Abschnitt werden die konfigurierbaren Optionen für Richtlinienregeln erläutert, die sich auf alle Endpoint Encryption Geräte auswirken.

Prozedur

1. Erstellen Sie eine neue Endpoint Encryption Richtlinie.

   Weitere Informationen finden Sie unter *Eine Richtlinie erstellen auf Seite 5-11*.

2. Klicken Sie auf **Allgemein**.

Das Fenster zu den Richtlinienregeleinstellungen **Allgemein** wird angezeigt.

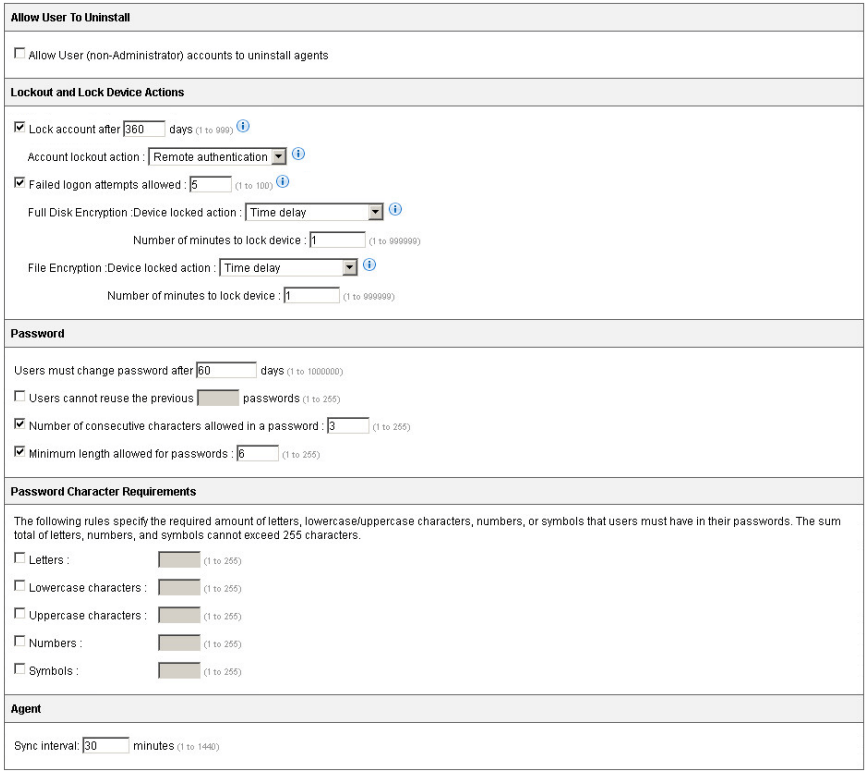


ABBILDUNG 5-5. Allgemeine Richtlinienregeln

3. Wählen Sie unter **Deinstallation durch Benutzer zulassen** die Option **Nicht-Administratorkonten können die Agent-Software deinstallieren**, um allen Endpoint Encryption Benutzern zu erlauben, den Agent zu deinstallieren.

Hinweis

Standardmäßig können nur Administratoren Endpoint Encryption Agents deinstallieren.

4. Konfigurieren Sie unter **Aktionen zum Sperren von Geräten** die folgenden Optionen:

   - Wählen Sie **Konto sperren nach <Anzahl> Tagen** aus, um die Anzahl der Tage anzugeben, nach denen das Endpoint Encryption Gerät gesperrt wird, wenn die Richtlinien nicht synchronisiert werden.

     - Geben Sie mit **Kontosperraktion** an, ob bei einer Sperrung die Remote-Authentifizierung oder Löschung aktiviert werden soll.

       Hinweis

       Weitere Informationen zu den Sperroptionen finden Sie unter *Sperraktionen auf Seite 5-27*.

   - Wählen Sie **Zulässige Anzahl fehlgeschlagener Anmeldeversuche**, um anzugeben, wie viele Authentifizierungsversuche möglich sind, bevor das Endpoint Encryption Gerät gesperrt wird.

   - Konfigurieren Sie für Full Disk Encryption oder File Encryption Geräte Folgendes separat:

     - Geben Sie mit **Aktion zur Gerätesperrung** an, ob bei einer Sperrung die „Remote-Authentifizierung“ oder die „Löschung“ aktiviert werden soll.

       Hinweis

       Weitere Informationen zu den Sperroptionen finden Sie unter *Sperraktionen auf Seite 5-27*.

     - Geben Sie unter **Anzahl der Minuten, die das Gerät gesperrt wird** die Dauer der Zeitverzögerung an, die das Endpoint Encryption Gerät gesperrt ist und nicht authentifiziert werden kann.

5. Konfigurieren Sie unter **Kennwort** die folgenden Optionen:

   - Wählen Sie **Benutzer muss das Kennwort nach <Anzahl> Tagen ändern**, um anzugeben, wenn ein Benutzer aufgefordert wird, das Kennwort zu aktualisieren.

- Wählen Sie **Benutzer darf die vorherigen <Anzahl> Kennwörter nicht wiederverwenden**, um anzugeben, wie viele vorherige Kennwörter der Benutzer nicht verwenden darf.
- Wählen Sie **Anzahl der zulässigen aufeinanderfolgenden Zeichen in einem Kennwort**, um anzugeben, wie viele gleiche Zeichen ein Kennwort enthalten darf.
- Wählen Sie **Zulässige Mindestlänge für Kennwörter**, um anzugeben, aus wie vielen Zeichen ein Kennwort mindestens bestehen muss.

6. Legen Sie unter **Kennwortvoraussetzungen** die Einschränkungen in Bezug auf Zeichen in Kennwörtern fest.
   - **Buchstaben**
   - **Kleinbuchstaben**
   - **Großbuchstaben**
   - **Zahlen**
   - **Symbole**

   Wichtig

   Die Gesamtzahl der Buchstaben, Ziffern und Symbole kann höchstens 255 betragen.

7. Geben Sie unter **Agent** das **Synchronisierungsintervall** in Minuten ein.

Sperraktionen

Einige Richtlinien verfügen über Einstellungen zum Sperren eines Benutzerkontos oder eines Geräts auf Grundlage bestimmter Kriterien. Aktionen zur Konto- oder Gerätesperrung wirken sich auf das Endpoint Encryption Gerät aus, unabhängig davon, ob der Agent die Richtlinien mit PolicyServer synchronisiert. Wenn der Endpoint Encryption Agent beispielsweise für eine bestimmte Zeitdauer nicht mit PolicyServer kommuniziert, sperrt der Endpoint Encryption Agent automatisch das Endpoint Encryption Gerät. Die nachfolgende Tabelle vermittelt Ihnen ein Verständnis der verfügbaren Aktionen zur Sperrung von Konten und Geräten.

In der folgenden Tabelle wird beschrieben, wann die Sperraktionen auftreten:

Typ	Beschreibung
Kontosperrung	Kontosperraktionen werden wirksam, wenn der Endpoint Encryption Agent innerhalb eines bestimmten Zeitraums, der durch die Richtlinie festgelegt wird, nicht mit PolicyServer kommuniziert.
Gerätesperrung bei Full Disk Encryption	Gerätesperraktionen bei Full Disk Encryption werden wirksam, wenn der Endpoint Encryption Benutzer wie durch die Richtlinie festgelegt die Anzahl von erfolglosen Anmeldeversuchen an diesem Full Disk Encryption Gerät überschreitet.
Gerätesperrung bei File Encryption	Gerätesperraktionen bei File Encryption werden wirksam, wenn der Endpoint Encryption Benutzer wie durch die Richtlinie festgelegt die Anzahl von erfolglosen Anmeldeversuchen an diesem File Encryption Gerät überschreitet.

Für Sperraktionen gibt es die folgenden Optionen:

Aktion	Beschreibung
Löschen	PolicyServer löscht alle Daten, die vom zugewiesenen Endpoint Encryption Agent gesteuert werden. **Warnung!** Der Endpoint Encryption Benutzer kann die gelöschten Daten nicht wiederherstellen.
Remote-Authentifizierung	PolicyServer sperrt das Endpoint Encryption Gerät, bis der Benutzer von Endpoint Encryption die Remote-Hilfe-Authentifizierung von einem Authentifizierer oder vom Support erhält. Weitere Informationen finden Sie unter *Remote-Hilfe auf Seite 2-14*.

Aktion	Beschreibung
Zeitverzögerung	PolicyServer sperrt das Endpoint Encryption Gerät vorübergehend und informiert den Benutzer von Endpoint Encryption darüber, dass das Gerät gesperrt ist. Während der Zeitverzögerung ist die Möglichkeit zur Authentifizierung oder Kennwortzurücksetzung deaktiviert. Die Dauer der Zeitverzögerung wird von der Richtlinie bestimmt. Nach Ablauf der Zeitverzögerung ist der Benutzer wieder berechtigt, sich zu authentifizieren.

Gruppen auf Control Manager migrieren

Gehen Sie wie folgt vor, um vorhandene Gruppen von PolicyServer MMC auf Control Manager zu migrieren.

Prozedur

1. Melden Sie sich bei PolicyServer MMC an.
2. Sammeln Sie folgenden Informationen:
   - Die Gesamtzahl der Gruppen, deren Namen und Untergruppen
   - Alle Benutzer, die den jeweiligen Gruppen zugeordnet sind
   - Die Richtlinienkonfiguration der jeweiligen Gruppen
3. Melden Sie sich bei Control Manager an.
4. Konfigurieren Sie für jede Gruppe in PolicyServer MMC eine neue Richtlinie, die der entsprechenden Gruppenrichtlinienkonfiguration entspricht.

Hinweis

Untergruppen werden in Control Manager nicht unterstützt. Erstellen Sie zum Replizieren der Richtlinieneinstellungen für Untergruppen eine separate Richtlinie für jede Untergruppe.

5. Fügen Sie jeder entsprechenden neuen Richtlinie Benutzer hinzu.
6. Verteilen Sie jede Richtlinie.

Kapitel 6

Full Disk Encryption

Mit Hilfe von obligatorischer starker Authentifizierung und Full Disk Encryption bietet Full Disk Encryption eine umfassende Endpunkt-Datensicherheit. 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.

Der Full Disk Encryption Agent verwendet FIPS-konforme XST-AES-Verschlüsselungsalgorithmen und die obligatorische Authentifizierung, damit auf Daten nicht ohne Authentifizierung zugegriffen werden kann. Full Disk Encryption verhindert Datenverluste durch die Verschlüsselung des gesamten Laufwerks, einschließlich Betriebssystem-, Programm-, temporären und Endbenutzerdateien. Administratoren können je nach benötigter Verschlüsselungsstärke oder Leistung in ihrer Umgebung eine Schlüsselgröße von 128 oder 256 Bit wählen.

Full Disk Encryption kann flexibel eingesetzt werden und unterstützt je nach Bedarf Festplattenverschlüsselung auf Software- oder Hardwarebasis. Selbstverschlüsselnde Solid-State-Laufwerke (SSDs) vom Typ Seagate DriveTrust™, OPAL, OPAL2 und SanDisk™ werden unterstützt. 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 steuert Richtlinien, die sich auf Full Disk Encryption auswirken. Auf diese Weise wird vollständige Endpunktsicherheit gewährleistet, die im

gesamten Unternehmen zentral verwaltet wird. Full Disk Encryption ist netzwerkorientiert und aktualisiert Richtlinien, bevor die Authentifizierung zugelassen wird. Sie können Daten auf dem Endpunkt auch von einem entfernten Standort aus sperren oder löschen, bevor auf das Betriebssystem oder auf andere vertrauliche Daten zugegriffen wird.

Full Disk Encryption Tools

In der folgenden Tabelle werden die verschiedenen Tools beschrieben, die für Endpoint Encryption verfügbar sind.

TOOL	BESCHREIBUNG
Kontextmenü	Greifen Sie über das Full Disk Encryption-Symbol ( ) in der Task-Leiste auf den Full Disk Encryption Agent zu. Über das Kontextmenü können Sie den Geräteverschlüsselungsstatus anzeigen und mit PolicyServer synchronisieren. Weitere Informationen finden Sie unter *Kontextmenü von Full Disk Encryption auf Seite 6-4*.
Preboot	Authentifizieren Sie sich mit PolicyServer über den Full Disk Encryption Preboot. Der Preboot wird geladen, wenn der Endpunkt startet, bevor Windows geladen wird. Verwenden Sie den Full Disk Encryption Preboot zur Konfiguration Ihres Netzwerks und der WLAN-Einstellungen und zur Behebung von Problemen mit Anmeldedaten.
Command Builder	Verwenden Sie Command Builder zur Generierung von Skripts für automatisierte Installationen und zur Erstellung von verschlüsselten Werten für Anmeldedaten bei der Erstellung von Skripts. Weitere Informationen finden Sie im *Endpoint Encryption Installationshandbuch*.
Command Line Helper	Mit Command Line Helper erstellen Sie verschlüsselte Werte, um beim Erstellen von Installationsskripts die Anmeldedaten zu schützen. Weitere Informationen finden Sie unter *Command Line Helper verwenden auf Seite 6-26*.
DAAutoLogin	Mit DAAutoLogin führen Sie Windows-Patches durch. Mit DAAutoLogin kann Endpoint Encryption Preboot einmalig umgangen werden. Weitere Informationen finden Sie unter *Patching-Verfahren für Full Disk Encryption auf Seite 6-27*.

TOOL	BESCHREIBUNG
Wiederherstellungskonsole	Mit der Wiederherstellungskonsole führen Sie eine Datenwiederherstellung nach einem kritischen Betriebssystemfehler durch, analysieren und lösen Netzwerkprobleme und verwalten Benutzer und Protokolle. Weitere Informationen finden Sie unter *Wiederherstellungskonsole auf Seite 9-6*.
Recovery-Tool	Mit der bootfähigen Reparatur-CD entschlüsseln Sie die Festplatte, bevor Sie Full Disk Encryption in Fällen entfernen, in denen der Datenträger beschädigt wurde. Die Reparatur-CD sollte nur dann verwendet werden, wenn die Standardmethoden zum Entfernen nicht durchführbar sind. Ein typisches Symptom einer beschädigten Festplatte ist ein schwarzer Bildschirm. Weitere Informationen finden Sie unter *Recovery-Tool auf Seite 9-26*.

Kontextmenü von Full Disk Encryption

Verwenden Sie das Full Disk Encryption-Symbol ( ) in der Task-Leiste, um auf den Full Disk Encryption Agent zuzugreifen. Klicken Sie mit der rechten Maustaste auf das Agent-Symbol, um die Menüelemente anzuzeigen. In der folgenden Tabelle werden die verfügbaren Menüoptionen beschrieben.

TABELLE 6-1. Menüoptionen des Full Disk Encryption Agents

MENÜELEMENT	FUNKTION
Richtlinien synchronisieren	Laden Sie Richtlinien-Updates manuell vom PolicyServer herunter. **Hinweis** Full Disk Encryption Agents können Richtlinien ohne Benutzerauthentifizierung synchronisieren. Full Disk Encryption Agents aktualisieren Richtlinieneinstellungen automatisch auf Basis Ihrer PolicyServer-Konfigurationen. Weitere Informationen finden Sie unter *Synchronisierung von Richtlinien auf Seite 7-18*.
Symbol ausblenden	Entfernt das Full Disk Encryption Task-Leistensymbol vorübergehend. Um das Task-Leistensymbol für Full Disk Encryption erneut anzuzeigen, führen Sie Full Disk Encryption über Ihren Desktop oder über das Startmenü aus.
Info über Full Disk Encryption	Zeigt Informationen zu Full Disk Encryption an, einschließlich der Version, der letzten Synchronisierungszeit und des authentifizierten Benutzers. Die Registerkarte **Verschlüsselungsstatus** zeigt den Status jeder einzelnen Festplatte an, die von diesem Agent verwaltet wird.
Online-Hilfe	Zeigt die Dokumentation zu Full Disk Encryption online an.

Full Disk Encryption Preboot

Nach der Installation von Full Disk Encryption wird jetzt Full Disk Encryption Preboot vor dem Laden von Windows angezeigt. Full Disk Encryption Preboot sorgt dafür, dass nur autorisierte Benutzer auf Endpunkte zugreifen können, und aktualisiert bei einer Verbindung mit PolicyServer die lokalen Sicherheitsrichtlinien.

Hinweis

Verwenden Sie PolicyServer MMC, um den Preboot-Bildschirm zu konfigurieren und anzupassen.

Menüoptionen

Im oberen linken Menü von Full Disk Encryption Preboot stehen mehrere Optionen zur Verfügung.

TABELLE 6-2. Full Disk Encryption Preboot Menüoptionen

MENÜELEMENT	BESCHREIBUNG
Authentifizierung	Sie können die Authentifizierungsmethode wechseln, die zur Anmeldung bei Endpoint Encryption Geräten verwendet wird.
Kommunikation	Manuelle Synchronisierung mit PolicyServer.
Computer	Anzeige von Informationen über Full Disk Encryption, Anzeige von Informationen über Ihr Netzwerk, Änderung der Tastaturbelegung, Zugang zur Bildschirmtastatur oder Neustart bzw. Herunterfahren des Endpunkts.

Netzwerkverbindung

Das Symbol für die Netzwerkverbindung ( ) wird in der oberen rechten Ecke angezeigt, wenn Full Disk Encryption als verwalteter Endpunkt installiert ist. Dieses Symbol wird nur hervorgehoben, wenn das Gerät mit dem Netzwerk verbunden ist und eine Kommunikation mit dem PolicyServer stattfindet.

Verbindung mit einem Wireless-Netzwerk aufbauen

Das Symbol für eine Wireless-Verbindung ( ) wird in der oberen rechten Ecke im Anmeldefenster von Full Disk Encryption Preboot angezeigt, wenn im Endpunkt eine WLAN-Netzwerkkarte installiert ist. Wenn keine WLAN-Netzwerkkarte erkannt wird, wird kein Wireless-Netzwerksymbol angezeigt.

Hinweis

Full Disk Encryption Preboot kann nicht automatisch die Authentifizierung für WEP-Sicherheit erkennen. Wenn es sich beim Authentifizierungstyp um WEP-OPEN oder WEP-PSK handelt, geben Sie den Sicherheitstyp manuell an.

Falls Ihre Unternehmensrichtlinie keine WLAN-Konfiguration zulässt, sind die Schaltflächen **Alle Zugangspunkte** und **Verbindung trennen** deaktiviert.

Weitere Informationen finden Sie im *Administratorhandbuch für PolicyServer MMC*.

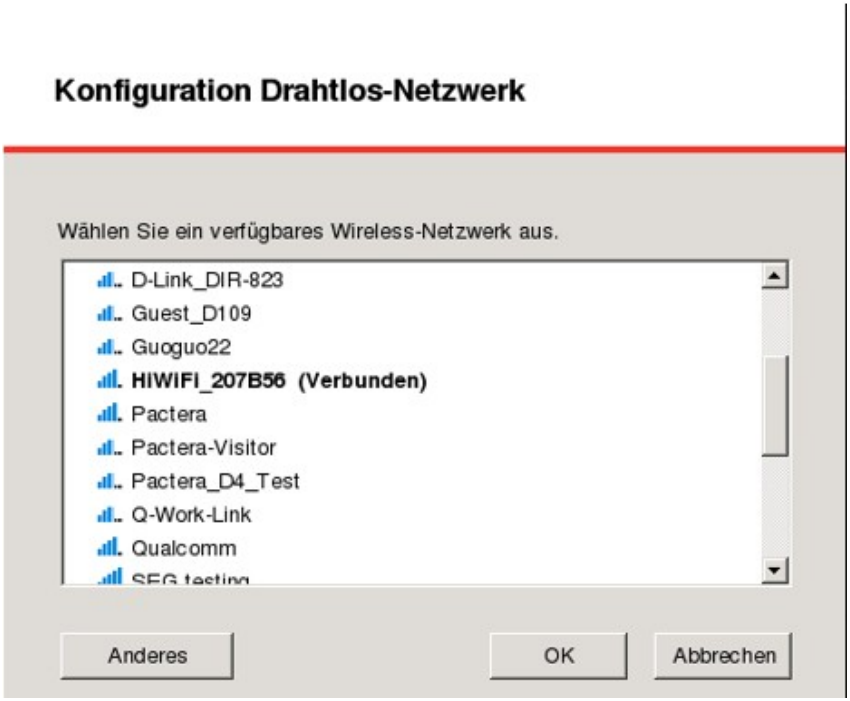
Prozedur

1. Klicken Sie auf das Symbol für die WLAN-Verbindung in der oberen rechten Ecke des Anmeldefensters von Full Disk Encryption Preboot.

   Das Fenster **Wireless-Zugang** wird angezeigt.

2. Klicken Sie auf **Alle Zugangspunkte**.

   Das Fenster **Konfiguration des drahtlosen Netzwerks** wird angezeigt.



3. Wählen Sie Ihr Netzwerk aus.

   - Um das aufgeführte Netzwerk zu verwenden, wählen Sie die SSID, und klicken Sie anschließend auf **OK**.
   - Um ein nicht aufgeführtes Netzwerk zu konfigurieren, klicken Sie auf **Anderes Netzwerk**, geben Sie die SSID-Einstellungen ein, und klicken Sie anschließend auf **Verbinden**.

Wichtig

Schließen Sie weder das Fenster noch starten Sie Ihren Endpunkt während der Konfiguration neu.

4. Klicken Sie auf **Schließen**, um die Einrichtung des Wireless-Netzwerks abzuschließen.

Netzwerkinformationen

Zeigen Sie Netzwerk- und Verbindungsinformationen über Full Disk Encryption Preboot an, indem Sie zu **Menü** > **Computer** > **Netzwerkinformationen** navigieren.

Das Fenster **Netzwerkinformationen** umfasst Folgendes:

Abschnitt	Beschreibung
Angaben zur Hardware	In diesem Abschnitt werden die gefundenen Ethernet-Controller und WLAN-Karten angezeigt.
Netzwerkinformationen	In diesem Abschnitt werden für jeden Ethernet-Port die Informationen zur Netzwerkidentifikation angezeigt, einschließlich der folgenden: • MAC-Adresse • IPv4- und IPv6-Adressen • Subnetzmaske • Standard-Gateway • Status der Netzwerkverbindung, der unabhängig davon, ob der Ethernet-Port verbunden ist, angezeigt wird
DNS-Auflösung	In diesem Abschnitt werden die Ergebnisse der DNS-Auflösung angezeigt, einschließlich der während der Ermittlung des PolicyServer kontaktierten Server und Adressen.
PolicyServer-Informationen	In diesem Abschnitt wird die PolicyServer-URL angezeigt. Wenn die URL den Hostnamen des Servers enthält, muss PolicyServer auch die Hostnamenauflösung durchführen, um die entsprechende IP-Adresse zu ermitteln. Wenn die URL stattdessen die IP-Adresse von PolicyServer enthält, überspringt Full Disk Encryption Preboot die Hostnamenauflösung.

Abschnitt	Beschreibung
PolicyServer-Verbindungsstatus	In diesem Abschnitt wird angezeigt, ob Full Disk Encryption Preboot erfolgreich eine Verbindung zu PolicyServer hergestellt hat.

Klicken Sie auf **Verbindung wiederherstellen**, um erneut zu versuchen, eine Verbindung zu PolicyServer herzustellen, oder um die aktuellen Informationen zu aktualisieren.

Bildschirmtastatur

Sie können von Full Disk Encryption Preboot auf die Bildschirmtastatur zugreifen. Navigieren Sie dazu zu **Menü** > **Computer** > **Bildschirmtastatur**.

Um den Cursor in das gewünschte Feld zu setzen, wenn die Tastatur angezeigt wird, klicken Sie in der unteren rechten Ecke der Tastatur auf **Fokus**.

Tastaturbelegung ändern

Wird die Tastaturbelegung geändert, so wirkt sich dies sowohl auf Tastatureingaben als auch auf die Bildschirmtastatur aus. Nach dem Starten von Windows wird die Tastaturbelegung vom Windows-Betriebssystem festgelegt. Ein Neustart ist erforderlich, um die Änderung der Tastaturbelegung zu übernehmen.

Prozedur

1. Navigieren Sie zu **Menü** > **Computer** > **Tastaturbelegung ändern**.

   Das Fenster **Wählen Sie die Sprache für das Tastaturlayout aus** wird angezeigt.

2. Wählen Sie ein Tastaturlayout aus.

3. Klicken Sie auf **OK**.

4. Klicken Sie auf **OK**, um den Endpunkt neu zu starten.

Authentifizierungsmethode ändern

Hinweis

Weitere Informationen zu Authentifizierungsmethoden finden Sie unter *Authentifizierungsmethode auf Seite 2-11*.

Prozedur

1. Wählen Sie in Full Disk Encryption Preboot die Option **Kennwort nach der Anmeldung ändern**.
2. Geben Sie den Benutzernamen und das Kennwort ein.
3. Klicken Sie auf **Anmelden**.

Das Fenster **Kennwort ändern** wird angezeigt. Die Benutzeroberfläche unterscheidet sich je nach Authentifizierungsmethode.

ABBILDUNG 6-1. Beispiel zum Ändern eines festen Kennworts

4. Wählen Sie aus dem Menü oben links **Authentifizierung**, und wählen Sie dann die gewünschte Authentifizierungsmethode.

   Das Fenster **Neues Kennwort** der ausgewählten Authentifizierungsmethode wird angezeigt.

5. Geben Sie das neue Kennwort an, bestätigen Sie es, und klicken Sie anschließend auf **Weiter**.

   Das Gerät startet Windows.

Kennwörter ändern

Das folgende Verfahren erklärt, wie Sie das Kennwort für ein Endpoint Encryption Benutzerkonto mit Full Disk Encryption Preboot ändern.

Prozedur

1. Geben Sie den Endpoint Encryption Benutzernamen und das Kennwort ein.
2. Wählen Sie **Kennwort nach der Anmeldung ändern**.
3. Klicken Sie auf **Anmelden**.

   Das Fenster **Kennwort ändern** wird angezeigt. Die Benutzeroberfläche unterscheidet sich je nach Authentifizierungsmethode.

ABBILDUNG 6-2. Fenster zum Ändern eines festen Kennworts

4. Geben Sie das neue Kennwort an, bestätigen Sie es, und klicken Sie anschließend auf **Weiter**.

   Das Gerät startet Windows.

ColorCode

ColorCode™ ist eine einzigartige Authentifizierungsmethode, bei deren Entwicklung eine schnelle Eingabe und eine leichte Merkfähigkeit im Vordergrund standen. Die ColorCode-Authentifizierung besteht nicht aus alphanumerischen Zeichen oder Symbolen, sondern aus einer vom Benutzer erstellten Farbfolge (Beispiel: rot, rot, blau, gelb, blau, grün).

ABBILDUNG 6-3. Das Fenster "ColorCode-Authentifizierung"

ColorCode-Kennwort erstellen

Die Gesamtanzahl von Schritten in ColorCode (Anzahl) wird von PolicyServer definiert. Die Standardanzahl ist 6.

Prozedur

1. Starten Sie den Endpunkt, und warten Sie, bis Full Disk Encryption Preboot angezeigt wird.
2. Folgen Sie den Anweisungen zum Ändern von Kennwörtern.

   Weitere Informationen finden Sie unter *Kennwörter ändern auf Seite 6-13*.
3. Ändern Sie die Authentifizierungsmethode in ColorCode.

   Hinweis

   Weitere Informationen über das Ändern von Authentifizierungsmethoden finden Sie unter *Authentifizierungsmethode ändern auf Seite 6-11*.

   Das Fenster **ColorCode Kennwort ändern** wird angezeigt.

ABBILDUNG 6-4. Fenster "ColorCode Kennwort ändern"

4. Wählen Sie die erste Farbe, indem Sie im linken Quadrat darauf klicken.

   Die Anzahl erhöht sich um 1.
5. Klicken Sie auf die weiteren Farben in der Folge.

Tipp

Klicken Sie auf **Zurück**, um die zuletzt angeklickte Farbe zu ändern, oder klicken Sie auf **Löschen**, um von vorn zu beginnen.

6. Wenn der Vorgang abgeschlossen ist, bestätigen Sie das ColorCode-Kennwort im rechten Quadrat.
7. Klicken Sie zum Abschluss auf **Weiter**.

Remote-Hilfe

Mit der Remote-Hilfe können Gruppen- oder Unternehmensauthentifizierer ausgesperrte Endpoint Encryption Benutzer unterstützen, die sich nach zu vielen erfolglosen Versuchen oder, wenn zu viel Zeit seit der letzten PolicyServer Synchronisierung vergangen ist, nicht bei Endpoint Encryption Geräten anmelden können.

Hinweis

Die Remote-Hilfe-Authentifizierung wird durch die Richtlinienregeln des Endpoint Encryption Geräts ausgelöst. Die Richtlinienregeln für die Remote-Hilfe können sowohl mit PolicyServer MMC als auch mit Control Manager konfiguriert werden.

Remote-Hilfe zum Entsperren von Full Disk Encryption Geräten verwenden

Wichtig

- Durch einen Neustart des Endpoint Encryption Geräts wird der Herausforderungscode zurückgesetzt.
- Durch eine manuelle Synchronisierung der Richtlinien mit PolicyServer wird der Herausforderungscode ebenfalls geändert.
- Bei Herausforderungscodes und Antwortcodes muss die Groß-/Kleinschreibung nicht berücksichtigt werden.

Prozedur

1. Navigieren Sie in Full Disk Encryption Preboot zu **Menü** > **Authentifizierung** > **Remote-Hilfe**.
2. Übermitteln Sie den **Herausforderungscode** an den Richtlinien-/Gruppenadministrator.
3. Geben Sie den **Antwortcode** ein, den Sie vom Richtlinien-/Gruppenadministrator erhalten haben.
4. Klicken Sie auf **Anmelden**.

   Das Fenster **Kennwort ändern** wird angezeigt.

   Hinweis

   Wenn für das Konto die Domänenauthentifizierung verwendet wird, startet der Endpunkt direkt in Windows.

5. Geben Sie das neue Kennwort an, bestätigen Sie es und klicken Sie anschließend auf **Weiter**.

   Das Gerät startet Windows.

Smartcard

Die Smartcard-Authentifizierung erfordert sowohl eine PIN als auch ein physisches Token zur Bestätigung der Identität des Benutzers. Smartcard-Zertifikate sind mit dem Benutzerkonto und der zugewiesenen Gruppe des Benutzer verbunden. Nach der Registrierung kann der Benutzer die Smartcard-Authentifizierung von jedem Endpoint Encryption Gerät in der betreffenden Gruppe verwenden. Benutzer können nach Belieben jedes Endpoint Encryption Gerät in ihrer Gruppe verwenden und müssen kein Einmalkennwort anfordern.

Stellen Sie zur Verwendung der Smartcard-Authentifizierung sicher, dass die folgenden Anforderungen erfüllt werden:

- Das Smartcard-Lesegerät ist mit dem Endpunkt verbunden, wobei sich die Smartcard im Lesegerät befindet.

- ActivClient 6.1 ist mit allen Service Packs und Updates installiert.
- Geben Sie die Smartcard-PIN in das Kennwortfeld ein.

Warnung!

Wenn kein gültiges Kennwort eingegeben wird, wird ein Kennwortfehler gesendet und die Smartcard kann gesperrt werden.

Hinweis

Smartcard-Authentifizierung kann nur mit PolicyServer MMC konfiguriert werden.

Smartcard-Registrierung

Smartcard-Zertifikate sind mit dem Benutzerkonto und der zugewiesenen Gruppe des Benutzer verbunden. Nach der Registrierung kann der Benutzer die Smartcard-Authentifizierung von jedem Endpoint Encryption Gerät in der betreffenden Gruppe verwenden. Benutzer können nach Belieben jedes Endpoint Encryption Gerät in ihrer Gruppe verwenden und müssen kein Einmalkennwort anfordern.

Eine Smartcard in Full Disk Encryption Preboot registrieren

Prozedur

1. Folgen Sie den Anweisungen, um Kennwörter zu ändern, und wählen Sie anschließend **Smartcard**.

   Weitere Informationen finden Sie im *Administratorhandbuch für PolicyServer MMC*.

2. Führen Sie die Smartcard in das Lesegerät ein.
3. Verbinden Sie das Lesegerät mit dem Endpunkt.
4. Geben Sie den Benutzernamen und das feste Kennwort ein.
5. Klicken Sie auf **Fortfahren**.
6. Wenn die Bestätigungsmeldung angezeigt wird, klicken Sie auf **Fortfahren**.

7. Führen Sie im Fenster **Token registrieren** Folgendes aus:

   a. Geben Sie die neue PIN ein, die Sie vom Gruppen- oder Unternehmensadministrator erhalten haben.

   b. Bestätigen Sie die neue PIN.

   c. Wählen Sie den Typ der Smartcard aus dem Listenfeld **Token** aus.

   d. Klicken Sie auf **Fortfahren**, um die Registrierung des Smartcard-Tokens abzuschließen.

Selbsthilfe

Mit der Selbsthilfe-Authentifizierung können Endpoint Encryption Benutzer, die ihre Anmeldedaten vergessen haben, ohne die Hilfe durch den technischen Support Sicherheitsfragen beantworten und sich bei Endpoint Encryption Geräten anmelden. Die Endpoint Encryption Benutzer werden aufgefordert, die vordefinierten persönlichen Herausforderungsfragen der Selbsthilfe zu beantworten. Mit der Selbsthilfe kann ein festes Kennwort oder eine andere Authentifizierungsmethode ersetzt werden.

Beachten Sie bei der Auswahl Ihrer Authentifizierungsmethode oder bei der Konfiguration von der Selbsthilfe Folgendes:

- Die Selbsthilfe ist nicht für Administrator- und Authentifiziererkonten verfügbar.
- Die Selbsthilfe ist nicht für Konten verfügbar, die die Domänenauthentifizierung verwenden. PolicyServer kann vorherige Domänenkennwörter nicht ändern oder wiederherstellen.
- Die Selbsthilfe verfügt über maximal sechs Fragen für jedes Benutzerkonto. Benutzer können sich möglicherweise über die Selbsthilfe nicht anmelden, wenn mehr als sechs Fragen konfiguriert sind.
- Die Selbsthilfe kann nur mit PolicyServer MMC konfiguriert werden.

Selbsthilfe einrichten

Wenn die Selbsthilfe-Richtlinie aktiviert ist, wird der Benutzer nach der ersten Anmeldung aufgefordert, Antworten auf diese Selbsthilfe-Fragen festzulegen. Wenn Benutzer ihr Kennwort ändern, müssen sie die Selbsthilfe-Fragen erneut festlegen.

Hinweis

Die Antworten zur Selbsthilfe werden auf dem Gerät gespeichert. Wenn ein Benutzer sich bei einem anderen Full Disk Encryption Gerät anmeldet, muss er Antworten für die Selbsthilfe für dieses Gerät festlegen.

Prozedur

1. Geben Sie den Benutzernamen und das Kennwort ein.
2. Klicken Sie auf **Anmelden**.

   Das Fenster **Selbsthilfe** wird angezeigt.
3. Legen Sie Antworten auf alle Selbsthilfe-Fragen fest.
4. Klicken Sie auf **Weiter**.

   Das Gerät startet Windows.

Selbsthilfe verwenden

Prozedur

1. Wechseln Sie im oberen linken Menü von Full Disk Encryption Preboot zu **Menü** > **Authentifizierung** > **Selbsthilfe**.

   Das Fenster **Selbsthilfe** wird angezeigt.
2. Beantworten Sie alle Fragen zur Selbsthilfe.
3. Klicken Sie auf **Anmelden**.

4. Legen Sie ein neues Kennwort fest und klicken Sie anschließend auf **Weiter**.

   Das Gerät startet Windows.

Antworten für die Selbsthilfe ändern

Prozedur

1. Geben Sie in Full Disk Encryption Preboot Ihre Anmeldedaten ein, wählen Sie **Kennwort nach der Anmeldung ändern**, und klicken Sie anschließend auf **Anmelden**.

   Das Fenster **Kennwort ändern** wird angezeigt.

2. Geben Sie das neue Kennwort an, bestätigen Sie es, und klicken Sie anschließend auf **Weiter**.

   Das Fenster **Selbsthilfe** wird angezeigt.

3. Legen Sie neue Antworten auf alle Selbsthilfe-Fragen fest, und klicken Sie anschließend auf **Weiter**.

   Das Endpoint Encryption startet Windows.

Synchronisierung der Full Disk Encryption Richtlinien

In der folgenden Liste werden die Ereignisse beschrieben, die die Richtliniensynchronisierung zwischen allen Agents und PolicyServer einleiten:

- Nachdem das Betriebssystem geladen und der Agent-Dienst gestartet wurde

  Informationen zu Endpoint Encryption Diensten finden Sie unter *Endpoint Encryption Dienste auf Seite C-1*.

- Wenn der Full Disk Encryption Preboot startet

- In regelmäßigen Intervallen auf Basis der PolicyServer-Synchronisierungsrichtlinie
- Manuell, über das Kontextmenü des Agents oder den Full Disk Encryption Preboot

  Weitere Informationen finden Sie unter *Full Disk Encryption Agents manuell aktualisieren auf Seite 6-23*.

Hinweis

Aktionen für Geräte werden eingeleitet, nachdem der Agent Richtlinien-Updates erhält.

Full Disk Encryption Konnektivitätsanforderungen

Endpoint Encryption verwendet einen zugelassenen FIPS 140-2-Verschlüsselungsprozess für Daten, die zwischen Full Disk Encryption Preboot und PolicyServer übertragen werden. Full Disk Encryption Agents haben eine Netzwerkverbindung zum PolicyServer und können Richtlinien-Updates empfangen und Audit-Daten vom Agent hochladen. Die gesamte Client-Server-Kommunikation wird intern verschlüsselt und kann über ungesicherte Verbindungen wie das Internet gesendet werden.

Sie können PolicyServer innerhalb eines Umkreisnetzwerks platzieren, sodass sowohl der Zugriff auf interne Netzwerke als auch auf das Internet sichergestellt ist. Weitere Informationen zu unterschiedlichen Konfigurationen der Netzwerktopologie finden Sie im *Endpoint Encryption Installationshandbuch*.

TABELLE 6-3. Full Disk Encryption Konnektivitätsanforderungen

RESSOURCE	FUNKTION
PolicyServer	Aktualisierte Sicherheitsrichtlinien vom PolicyServer können an Full Disk Encryption Preboot oder mit Hilfe von Verbindungen innerhalb von Windows, LAN oder VPN gesendet werden.

Ressource	Funktion
TCP/IP-Zugriff	Netzwerkverbindungen erfordern vollen TCP/IP-Netzwerkzugriff. DFÜ- oder Telefonzugriff kann nicht zur Bereitstellung der Verbindung mit dem PolicyServer während der Preboot-Authentifizierung verwendet werden.
Port	Endpoint Encryption Agents verwenden für die Kommunikation standardmäßig Port 8080. Um die Standardportnummer zu ändern, navigieren Sie zur Wiederherstellungskonsole und aktualisieren Sie den PolicyServer. Weitere Informationen finden Sie unter *Full Disk Encryption PolicyServer wechseln auf Seite 9-22*.

Full Disk Encryption Agents manuell aktualisieren

Full Disk Encryption Agents erhalten automatisch Sicherheitsrichtlinien-Updates vom PolicyServer in Intervallen, die von der Richtlinie vorgegeben werden.

Führen Sie eine der folgenden Aktionen aus, um Richtlinien manuell zu aktualisieren.

Prozedur

- Verwenden Sie Full Disk Encryption Preboot.
  a. Navigieren Sie zu **Kommunikation** > **Richtlinien synchronisieren**.
  b. Navigieren Sie zu **Computer** > **Info über Full Disk Encryption**.

     Der Zeitstempel der aktuellsten PolicyServer Richtliniensynchronisierung wird angezeigt.
- Verwenden Sie den Full Disk Encryption Agent.
  a. Doppelklicken Sie in der Windows-Task-Leiste auf das Full Disk Encryption-Symbol ( ).

     Der Full Disk Encryption Agent wird geöffnet.
  b. Klicken Sie auf **Mit PolicyServer synchronisieren**.

Nach kurzer Zeit setzt PolicyServer alle neue Richtlinienänderungen durch.

Full Disk Encryption Festplatten verschieben

Wenn eine Full Disk Encryption Festplatte auf einen anderen bei PolicyServer registrierten Endpunkt verschoben wird, erkennt Full Disk Encryption die Änderung automatisch und sendet ein Update an die PolicyServer-Datenbank. Ein Administratorkonto ist für diesen Vorgang nicht erforderlich.

Hinweis

Stellen Sie vor dem Verschieben der Festplatte sicher, dass die folgenden Anforderungen erfüllt sind:

- Der Quellendpunkt und der Zielendpunkt gehören zur selben Gruppe und verwenden denselben PolicyServer.
- Bei der zu verschiebenden Festplatte handelt es sich um eine Festplatte, die aktuell von Full Disk Encryption verwaltet wird.

Prozedur

1. Schalten Sie den Quellendpunkt ab und bauen Sie die vorhandene Festplatte aus.
2. Schalten Sie den Zielendpunkt ab und bauen Sie die Festplatte ein, die aus dem Quellendpunkt ausgebaut wurde.
3. Starten Sie die Endpunkte neu.
4. Full Disk Encryption erkennt die entfernten oder hinzugefügten Festplatten und sendet beim Start ein Update an die PolicyServer-Datenbank.
5. Klicken Sie in der Task-Leiste auf das Full Disk Encryption-Symbol ( ) und zeigen Sie die Registerkarte **Verschlüsselungsstatus** an, um zu überprüfen, ob der Vorgang erfolgreich ausgeführt wurde.

   Hinweis

   Während dieses Vorgangs kann auf die neue Festplatte auf dem Zielendpunkt nicht zugegriffen werden.

6. Starten Sie den Endpunkt neu, an den die neue Festplatte angeschlossen wurde, und initiieren Sie die Neuauthentifizierung bei PolicyServer.

7. Klicken Sie nach dem Neustart in der Task-Leiste auf das Full Disk Encryption-Symbol ( ) und zeigen Sie die Registerkarte **Verschlüsselungsstatus** an, um zu überprüfen, ob der Vorgang erfolgreich ausgeführt wurde.

   Die neue Festplatte ist jetzt verfügbar und kann verwendet werden.

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

- Vergewissern Sie sich, dass beide Tools auf einem Gerät ausgeführt werden, 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. Hilfe erhalten Sie beim Support von Trend Micro.

Command Line Helper verwenden

Command Line Helper ermöglicht, dass verschlüsselte Werte über das Installationsskript an Full Disk Encryption Preboot und das Full Disk Encryption-Installationsprogramm übergeben werden. Sie können Command Line Helper manuell verwenden, um verschlüsselte Werte von Zeichenfolgen für Installationsskripts oder die Patch-Verwaltung zu generieren.

Prozedur

1. Laden Sie Command Line Helper herunter und suchen Sie das Tool anschließend im Download-Ordner von Endpoint Encryption.

   Command Line Helper ist im PolicyServer-Installationspaket enthalten. Wechseln Sie zum Trend Micro Download Center, wählen Sie Endpoint Encryption und laden Sie das PolicyServer-Paket herunter.

   http://downloadcenter.trendmicro.com/?regs=DE/

   Command Line Helper befindet sich im folgenden Verzeichnis:

   ```
   <download_directory>\TMEE_PolicyServer\Tools\Command Line
   Helper
   ```

2. Öffnen Sie eine Eingabeaufforderung.

3. Ändern Sie das Verzeichnis in das Verzeichnis von Command Line Helper.

   Beispiel:

   ```
   cd C:\TMEE_PolicyServer\Tools\Command Line Helper
   ```

4. Geben Sie `CommandLineHelper.exe` gefolgt von der zu verschlüsselnden Zeichenfolge ein und drücken Sie die EINGABETASTE.

   Beispiel:

   ```
   CommandLineHelper.exe beispielkennwort
   ```

Tipp

Es ist möglicherweise einfacher, den generierten Wert direkt aus einer Textdatei zu kopieren.

In diesem Fall ändern Sie das oben erwähnte Beispiel wie folgt:

```
CommandLineHelper.exe beispielkennwort > datei.txt
```

Command Line Helper erzeugt eine verschlüsselte Zeichenfolge.

Patching-Verfahren für Full Disk Encryption

Prozedur

1. Sie können Patch-Dateien auf bestimmte Full Disk Encryption Geräte übertragen.
2. Senden Sie ein Skript, das `DAAutoLogin` ausführt.
3. Senden Sie einen Befehl zum Neustarten, so dass das Full Disk Encryption Gerät Windows GINA lädt und die erfolgreiche Durchführung des Patching bestätigt oder um weitere Patches per Push-Verfahren zu senden.

Kapitel 7

File Encryption

Der Trend Micro File Encryption Agent setzt AES-Verschlüsselung zum Schutz von Daten ein, die zwischen den Endpoint Encryption Benutzern ausgetauscht wurden bzw. die auf Wechseldatenträgern oder auf Netzwerkressourcen gespeichert sind. File Encryption kann ferner verschiedene Dateien mit unterschiedlichen Schlüsseln schützen, Sie können Zugriffsrichtlinien für den File Encryption Agent festlegen und anschließend separate Richtlinien zum Zugriff auf bestimmte Dateien anlegen. Diese Funktion ist in Umgebungen nützlich, in denen mehrere Benutzer auf denselben Endpunkt zugreifen. Verschlüsselung wird durchgeführt, nachdem die Authentifizierung stattgefunden hat.

Endbenutzer sind ebenfalls in der Lage, File Encryption flexibel lokal zu verwalten, indem individuelle Dateien, Ordner oder Wechseldatenträger umgehend verschlüsselt werden. Benutzer sind so in der Lage, auch auf Geschäftsreisen Daten sicher zu schützen.

File Encryption kann auch verschiedene Dateien mit unterschiedlichen Schlüsseln schützen, wodurch Sie in der Lage sind, Zugriffsrichtlinien für ein File Encryption Gerät und separate Richtlinien für den Zugriff auf bestimmte Dateien festzulegen. Dies ist in Umgebungen nützlich, in denen mehrere Benutzer auf einen Endpunkt zugreifen.

File Encryption registrieren

Nach der Installation von File Encryption ist eine erste Registrierung zum Identifizieren von PolicyServer erforderlich. Die Authentifizierungsmethode "Festes Kennwort" ist die Standardmethode und für die erste Registrierung erforderlich. Je nach den Richtlinieneinstellungen sind möglicherweise weitere Optionen verfügbar.

Wichtig

Ohne Authentifizierung bei File Encryption wird der Zugriff auf Dateien und Wechselmedien verweigert.

Prozedur

1. Nach der File Encryption-Installation wird beim nächsten Starten Ihres Endpunkts das Fenster **Anmelden** angezeigt. Wenn Sie zu einem späteren Zeitpunkt auf das Fenster **Anmelden** zugreifen müssen, klicken Sie mit der rechten Maustaste auf das File Encryption Symbol in der Task-Leiste und wählen Sie dann **Registrieren** aus.
2. Geben Sie den Endpoint Encryption Benutzernamen und das Kennwort ein.
3. Geben Sie die IP-Adresse (oder den Host-Namen) sowie das Unternehmen ein.
4. Klicken Sie auf **OK**.

   Das Fenster **Kennwort ändern** wird angezeigt.
5. Wählen Sie eine verfügbare Authentifizierungsmethode.

   Weitere Informationen zu Authentifizierungsmethoden finden Sie unter *File Encryption Authentifizierung auf Seite 7-15*.
6. Geben Sie das neue Kennwort an, und bestätigen Sie es.
7. Klicken Sie auf **OK**.

   Das Kennwort wird aktualisiert und eine Bestätigungsmeldung wird angezeigt.

File Encryption-Aktionen

Nach der Registrierung des File Encryption Agents stehen File Encryption Optionen für Dateien und Ordner zur Verfügung. Klicken Sie mit der rechten Maustaste auf eine Datei oder einen Ordner, um die verfügbaren Optionen anzuzeigen.

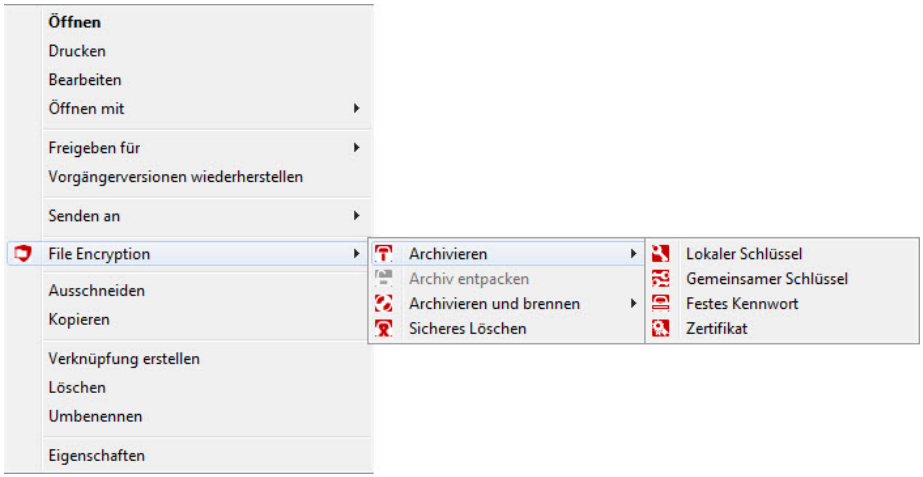


ABBILDUNG 7-1. File Encryption-Aktionen

Die folgende Tabelle soll Ihnen helfen, die verfügbaren Menüoptionen zu verstehen.

TABELLE 7-1. File Encryption Optionen im Kontextmenü

MENÜOPTION	BESCHREIBUNG
Archivieren	Erstellen Sie eine verschlüsselte Kopie der angegebenen Datei. Weitere Informationen finden Sie unter *Datei oder Ordner verschlüsseln auf Seite 7-4*.
Archiv entpacken	Öffnet ein zuvor erstelltes Archiv.

MENÜOPTION	BESCHREIBUNG
Archivieren und brennen	Erstellt eine verschlüsselte Kopie der angegebenen Datei und schreibt sie auf eine CD oder DVD. Weitere Informationen finden Sie unter *Datei oder Ordner verschlüsseln auf Seite 7-4*.
Sicheres Löschen	Sie können die ausgewählten Dateien und die Dateihistorie auf dem File Encryption Gerät sicher löschen. Weitere Informationen finden Sie unter *Funktion "Sicheres Löschen" von File Encryption verwenden auf Seite 7-10*.

Datei oder Ordner verschlüsseln

Prozedur

1. Klicken Sie mit der rechten Maustaste auf die Datei oder den Ordner, die bzw. der verschlüsselt werden soll.
2. Wählen Sie den Speicherort, um die verschlüsselte Datei zu erstellen.

OPTIONEN	BESCHREIBUNG	DETAILS
Archiv	Erstellen Sie die verschlüsselte Datei lokal.	Die verschlüsselte Datei wird im selben Ordner wie die Originaldatei angezeigt.
Archivieren und brennen	Schreiben Sie die verschlüsselte Datei auf eine CD oder DVD.	Im Authentifizierungsfenster werden Sie aufgefordert, Ihr beschreibbares Laufwerk auszuwählen.

3. Wählen Sie die Authentifizierungsmethode, um auf die verschlüsselte Datei zuzugreifen.

Optionen	Beschreibung	Hinweise
Lokaler Schlüssel	Erstellt eine verschlüsselte Datei, die nur vom Benutzer aufgerufen werden kann, der sie erstellt hat.	Diese Option ist nur verfügbar, wenn Sie **Archivieren** auswählen. Nach der Auswahl dieser Option wird kein Fenster angezeigt. Die verschlüsselte Datei wird sofort erstellt. Je nach Windows Betriebssystem kann ein Benutzer den Inhalt von Ordnern bei einem Benutzerwechsel ohne einen Neustart von Windows anzeigen. Während Dateinamen und Ordnerinhalte angezeigt werden können, ist der Dateiinhalt nicht verfügbar. Dies liegt daran, dass das Windows Betriebssystem die Dateistruktur für die Schnellsuche zwischenspeichert.
Gemeinsamer Schlüssel	Erstellt eine verschlüsselte Datei, die nur von Mitgliedern der Richtliniengruppe des aktuellen Benutzers aufgerufen werden kann.	Diese Option ist nur verfügbar, wenn Sie **Archivieren** auswählen. Nach der Auswahl dieser Option wird kein Fenster angezeigt. Die verschlüsselte Datei wird sofort erstellt. Je nach Windows Betriebssystem kann ein Benutzer den Inhalt von Ordnern bei einem Benutzerwechsel ohne einen Neustart von Windows anzeigen. Während Dateinamen und Ordnerinhalte angezeigt werden können, ist der Dateiinhalt nicht verfügbar. Dies liegt daran, dass das Windows Betriebssystem die Dateistruktur für die Schnellsuche zwischenspeichert.

OPTIONEN	BESCHREIBUNG	HINWEISE
Festes Kennwort	Erstellt eine verschlüsselte Datei, für deren Zugriff ein Kennwort benötigt wird.	Für die Kennwortwiederherstellung bei selbstextrahierenden Dateien steht keine Funktion zur Verfügung. Wenn ein Kennwort vergessen wird, kann die verschlüsselte Datei nicht wiederhergestellt werden. Auf Grund einer Einschränkung von Windows dürfen ausführbare (selbstextrahierende) Dateien nicht größer als 2 GB sein.
Zertifikat	Erstellt eine verschlüsselte Datei, für deren Zugriff spezielle digitale Zertifikate benötigt werden.	Die digitalen Zertifikate können je nach Umgebung und Richtlinieneinstellungen auf Smartcards gespeichert werden.

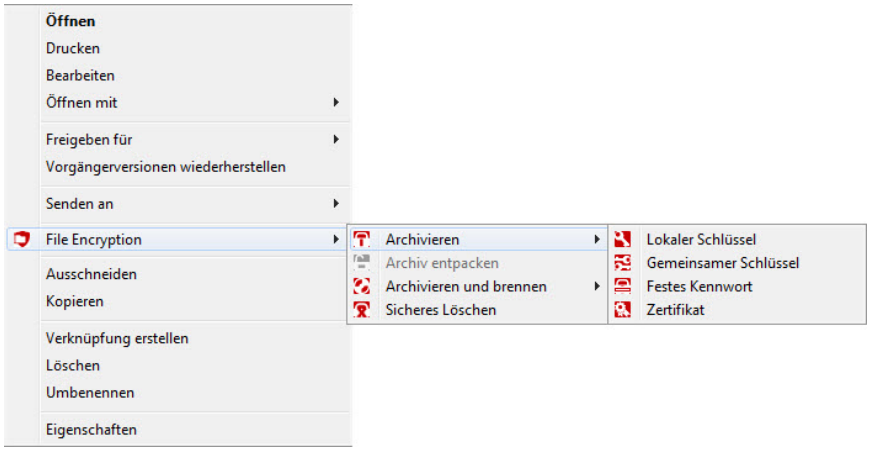


ABBILDUNG 7-2. File Encryption-Aktionen

4. Wenn ein Fenster angezeigt wird, arbeiten Sie alle Anweisungen auf dem Bildschirm ab.

File Encryption erstellt die verschlüsselte Datei am vorgesehenen Speicherort. Die Originaldateien bzw. -ordner werden nicht geändert und können aufbewahrt oder gelöscht werden.

File Encryption Entschlüsselung mit festem Kennwort

Wenn Sie versuchen, eine Datei oder einen Ordner mit einem festen Kennwort zu verschlüsseln, wird folgender Bildschirm angezeigt:

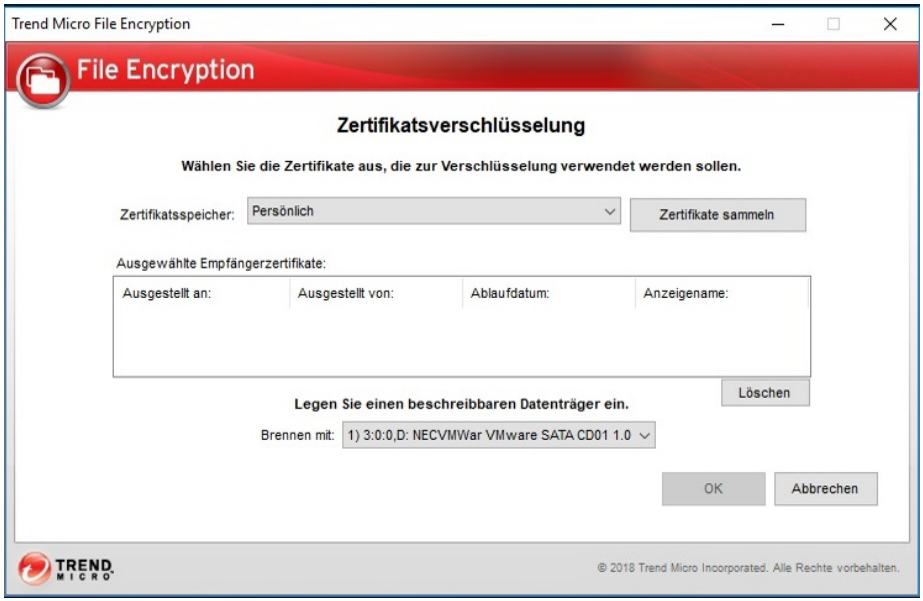
In diesem Fenster gibt es die folgenden Optionen:

TABELLE 7-2. Optionen für feste Kennwörter

OPTIONEN	DETAILS
Kennwort **Bestätigen**	Geben Sie ein Kennwort, das zum Öffnen der verschlüsselten Datei benötigt wird, ein und bestätigen Sie es.
Brennen mit	Wählen Sie das Laufwerk mit der CD oder DVD, auf die die verschlüsselte Datei geschrieben werden soll. Falls noch nicht geschehen, legen Sie eine beschreibbare CD oder DVD mit ausreichend freiem Speicherplatz ein. Diese Option ist nur verfügbar, wenn Sie **Archivieren und brennen** auswählen.
Verschlüsselte Daten als selbstextrahierendes Archiv ausgeben	Wählen Sie diese Option, um die verschlüsselte Datei als selbstextrahierendes Archiv zu erstellen. selbstextrahierende Archive können auf Geräten geöffnet werden, die über keine File Encryption Agents verfügen. Auf Grund einer Einschränkung von Windows dürfen ausführbare (selbstextrahierende) Dateien nicht größer als 2 GB sein. **Hinweis** Für die Kennwortwiederherstellung bei selbstextrahierenden Dateien steht keine Funktion zur Verfügung. Wenn ein Kennwort vergessen wird, kann die verschlüsselte Datei nicht wiederhergestellt werden.

File Encryption Verschlüsselung mit digitalem Zertifikat

Wenn Sie versuchen, eine Datei oder einen Ordner mit einem digitalen Zertifikat zu verschlüsseln, wird folgender Bildschirm angezeigt:



In diesem Fenster gibt es die folgenden Optionen:

TABELLE 7-3. Zertifikatoptionen

OPTIONEN	DETAILS
Zertifikatspeicher	Wählen Sie eine Gruppe aus der Dropdownliste und klicken Sie auf **Zertifikate sammeln**, um ein Fenster mit einer Liste der Zertifikate anzuzeigen, die mit dieser Gruppe verknüpft sind. Wählen Sie aus dem Fenster **Zertifikatsauswahl** ein Zertifikat aus und klicken Sie auf **OK**, um dieses Zertifikat in **Ausgewählte Empfängerzertifikate** zu verschieben.

OPTIONEN	DETAILS
Ausgewählte Empfängerzertifikate	Zeigt die Liste der derzeit ausgewählten Zertifikate an. Diese Zertifikate werden benötigt, um die verschlüsselte Datei zu öffnen. Klicken Sie auf **Löschen**, um alle Zertifikate zu entfernen. **Wichtig** Um einzelne Zertifikate zu entfernen, steht keine Methode zur Verfügung. Wenn Sie nur ein oder mehrere Zertifikate entfernen müssen, entfernen Sie alle Zertifikate und fügen Sie die benötigten Zertifikate erneut hinzu.
Brennen mit	Wählen Sie das Laufwerk mit der CD oder DVD, auf die die verschlüsselte Datei geschrieben werden soll. Falls noch nicht geschehen, legen Sie eine beschreibbare CD oder DVD mit ausreichend freiem Speicherplatz ein. Diese Option ist nur verfügbar, wenn Sie **Archivieren und brennen** auswählen.

Funktion "Sicheres Löschen" von File Encryption verwenden

Mit der Funktion "Sicheres Löschen" können Sie die ausgewählten Dateien und die Dateihistorie auf dem File Encryption Gerät sicher löschen.

Prozedur

1. Klicken Sie mit der rechten Maustaste auf die Datei, und navigieren Sie zu **File Encryption** > **Sicheres Löschen**.
2. Klicken Sie auf **Ja**, um die Datei dauerhaft zu löschen.

File Encryption - Kontextmenü

Klicken Sie in der Task-Leiste auf das File Encryption-Symbol (), um auf den File Encryption Agent zuzugreifen. Klicken Sie mit der rechten Maustaste auf das Agent-Symbol, um die Menüelemente anzuzeigen. In der folgenden Tabelle werden die verfügbaren Menüoptionen beschrieben.

TABELLE 7-4. Menüoptionen für File Encryption Agent

MENÜELEMENT	FUNKTION
Registrieren	Dient der erstmaligen Benutzerregistrierung von File Encryption beim PolicyServer. Weitere Informationen finden Sie unter *File Encryption registrieren auf Seite 7-2*. Diese Option wird nur angezeigt, wenn Sie die Registrierung von File Encryption noch nicht abgeschlossen haben.
Anmelden/Abmelden	Dient der Authentifizierung mit PolicyServer.
Kennwort ändern	Damit können Benutzer ihr Kennwort und ihre Authentifizierungsmethode ändern. Weitere Informationen finden Sie unter *Kennwort in File Encryption ändern auf Seite 7-13*.
Remote-Hilfe	Sie können File Encryption mit der Remote-Hilfe zur Authentifizierung entsperren, wenn der Benutzer das Endpoint Encryption Kennwort vergessen hat, es zu viele erfolglose Authentifizierungsversuche gab oder das Endpoint Encryption Gerät während eines bestimmten Zeitraums nicht mit dem PolicyServer kommuniziert hat. Weitere Informationen finden Sie unter *Mit Remote-Hilfe ein File Encryption Gerät entsperren auf Seite 7-13*. Diese Option steht nur zur Verfügung, wenn der File Encryption Agent gesperrt ist. Weitere Informationen zu gesperrten Konten finden Sie unter *Erzwungene Kennwortzurücksetzung auf Seite 7-16*.

MENÜELEMENT	FUNKTION
Richtlinien synchronisieren	Laden Sie Richtlinien-Updates manuell vom PolicyServer herunter. **Hinweis** File Encryption Agents können Richtlinien ohne Benutzerauthentifizierung synchronisieren. File Encryption Agents aktualisieren Richtlinieneinstellungen automatisch basierend auf Ihren PolicyServer-Konfigurationen. Weitere Informationen finden Sie unter *Synchronisierung von Richtlinien auf Seite 7-18*.
Offline-Dateien synchronisieren	Über die Synchronisierung mit PolicyServer Offline-Dateien mit Hilfe einer Importdatei anstelle der direkten Kommunikation mit PolicyServer können neue Sicherheitsrichtlinien durchgesetzt werden.
Benachrichtigungen anzeigen/verbergen	Schaltet alle File Encryption Benachrichtigungen aus.
Symbol ausblenden	Entfernt das File Encryption Task-Leistensymbol vorübergehend. Um das Task-Leistensymbol für File Encryption erneut anzuzeigen, führen Sie File Encryption über Ihren Desktop oder über das Startmenü aus.
Info über die File Encryption	Zeigt Informationen zu File Encryption an, einschließlich der Version, der letzten Synchronisierungszeit und des authentifizierten Benutzers. Sie können den PolicyServer ändern, der Richtlinien mit Ihrem File Encryption Agent über das Fenster **Info über die File Encryption** synchronisiert. Um Ihren PolicyServer zu ändern, klicken Sie auf **PolicyServer bearbeiten**.
Online-Hilfe	Zeigt die Dokumentation zu File Encryption online an.

Kennwort in File Encryption ändern

Um das Kennwort zu ändern, muss der Benutzer sich mit der Kontorolle "Benutzer" bei File Encryption authentifizieren. Der Benutzer kann anschließend das Kennwort mit einer der Authentifizierungsmethoden ändern, die von der Richtlinie zugelassen werden.

Sie können mit PolicyServer MMC die Richtlinie verwalten:

Gruppenname > **Richtlinien** > **File Encryption** > **Anmelden** > **Zulässige Authentifizierungsmethoden**

Prozedur

1. Klicken Sie mit der rechten Maustaste auf das File Encryption Symbol in der Task-Leiste, und wählen Sie **Kennwort ändern**.
2. Geben Sie das Kennwort ein.
3. Klicken Sie auf **Weiter**.
4. Wählen Sie eine verfügbare Authentifizierungsmethode.

   Weitere Informationen zu Authentifizierungsmethoden finden Sie unter *File Encryption Authentifizierung auf Seite 7-15*.
5. Geben Sie das neue Kennwort an, und bestätigen Sie es.
6. Klicken Sie auf **OK**.

   Das Kennwort wird aktualisiert und eine Bestätigungsmeldung wird angezeigt.

Mit Remote-Hilfe ein File Encryption Gerät entsperren

Wenn ein Benutzer die Anzahl an Authentifizierungsversuchen überschritten hat und die Remote-Authentifizierung auf Grund von Richtlinien aktiviert ist, sperrt File Encryption die Endpoint Encryption Ordner und benachrichtigt den Benutzer, dass Remote-Hilfe erforderlich ist. Wenn Sie File Encryption über die Remote-Hilfe entsperren möchten, benötigen Sie die Hilfe vom Unternehmensauthentifizierer oder Gruppenauthentifizierer.

Hinweis

Informationen über die Verwendung der Remote-Hilfe finden Sie unter *Remote-Hilfe auf Seite 2-14*.

Prozedur

1. Klicken Sie mit der rechten Maustaste auf das File Encryption Symbol in der Task-Leiste, und wählen Sie **Remote-Hilfe**.

   Das Fenster **Remote-Hilfe** wird angezeigt.

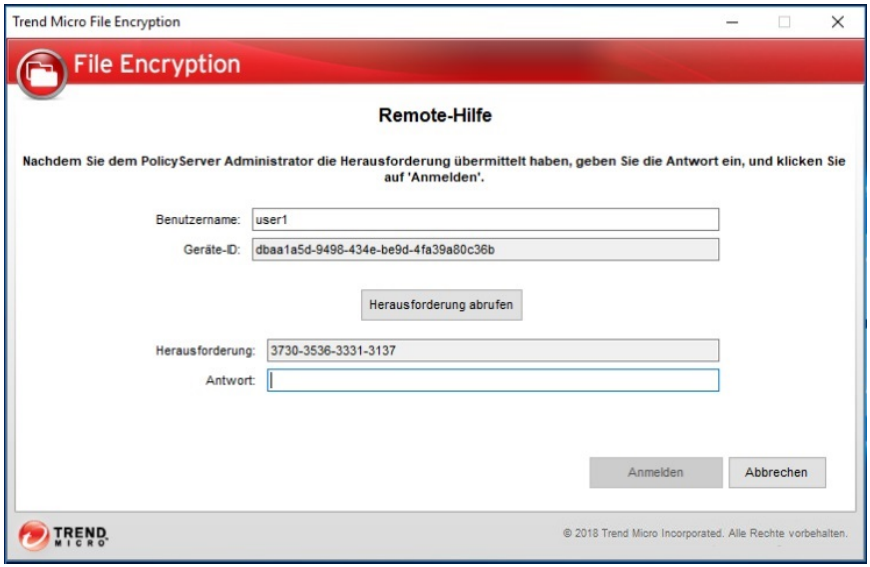


ABBILDUNG 7-3. File Encryption Remote-Hilfe

2. Geben Sie den Benutzernamen an.

3. Klicken Sie auf **Herausforderung abrufen**.

4. Geben Sie die **Antwort** ein, die vom Unternehmens- oder Gruppenauthentifizierer bereitgestellt wurde.

5. Klicken Sie auf **Anmeldung**.

   Der Benutzer wird bei File Encryption authentifiziert und eine Benachrichtigung wird angezeigt.

File Encryption Authentifizierung

In diesem Abschnitt wird erklärt, wie Sie sich bei File Encryption authentifizieren und das Produkt verwenden. Alle Authentifizierungsmethoden für Endpoint Encryption sind in File Encryption verfügbar.

Hinweis

Weitere Informationen zu Authentifizierungsmethoden finden Sie unter *Authentifizierungsmethode auf Seite 2-11*.

Für Endpoint Encryption Administratoren und Benutzer stehen mehrere Authentifizierungsmethoden zur Anmeldung bei File Encription zur Verfügung. Die verfügbaren Methoden werden vom PolicyServer Richtlinienkonfiguration bestimmt.

TABELLE 7-5. Unterstützte Authentifizierungsmethoden

AUTHENTIFIZIERUNGSMETHODE	BESCHREIBUNG
ColorCode™	Eine eindeutige Farbfolge. Weitere Informationen finden Sie unter *ColorCode auf Seite 2-12*.
Domänenauthentifizierung	Active Directory LDAP-Synchronisierung für Single Sign-On (SSO). Weitere Informationen finden Sie unter *Domänenauthentifizierung auf Seite 2-12*.
Festes Kennwort	Eine Zeichenfolge aus Zeichen, Ziffern und Symbolen. Weitere Informationen finden Sie unter *Festes Kennwort auf Seite 2-13*.

AUTHENTIFIZIERUNGSMETHODE	BESCHREIBUNG
Smartcard	Eine physische Karte wird in Verbindung mit einer PIN oder einem festen Kennwort verwendet. Weitere Informationen finden Sie unter *SmartCard auf Seite 2-15*.
PIN	Eine herkömmliche PIN. Weitere Informationen finden Sie unter *PIN auf Seite 2-13*.

Voraussetzungen für die Domänenauthentifizierung

Stellen Sie für die Domänenauthentifizierung mit SSO (Single Sign-On) sicher, dass die folgenden Voraussetzungen erfüllt werden:

- Der Benutzer gehört zu einer Richtliniengruppe mit aktivierter Domänenauthentifizierung.
- Vergewissern Sie sich, dass der Host-Name und der Domänenname ordnungsgemäß konfiguriert wurden.
- PolicyServer und alle Endpoint Encryption Geräte, die die Domänenauthentifizierung verwenden, befinden sich in derselben Domäne.
- Das Benutzerkonto wird in Active Directory und PolicyServer konfiguriert. Der Benutzername muss genau übereinstimmen, auch hinsichtlich der Groß- und Kleinschreibung.

Außerdem gelten für die Domänenauthentifizierung folgende Einschränkungen:

- Die Domänenauthentifizierung kann nicht mit einer Smartcard-PIN verwendet werden.
- Die Remote-Hilfe ist für Domänenbenutzer verfügbar. Das Domänenkennwort muss allerdings in Active Directory zurückgesetzt werden, wenn es vergessen wird.

Erzwungene Kennwortzurücksetzung

File Encryption verhindert den unberechtigten Zugriff auf verschlüsselte Dateien und Ordner, indem geschützte Dateien gesperrt werden, wenn zu viele erfolglose

Authentifizierungsversuche durchgeführt werden oder wenn für eine bestimmte Dauer keine Kommunikation zwischen Endpunkt und dem PolicyServer erfolgte. Auf Grund der Richtlinien-Konfiguration sperrt File Encryption den Benutzer für den Zugriff oder aktiviert eine Zeitverzögerung, bevor Authentifizierungsversuche durchgeführt werden können.

Richtlinienregeln für Endpoint Encryption Geräte

In der folgenden Tabelle werden die Regeln der Sicherheitsrichtlinie für verlorene oder gestohlene Endpoint Encryption Geräte beschrieben. Abhängig von den Richtlinieneinstellungen wird nach zu vielen aufeinanderfolgenden erfolglosen Authentifizierungsversuchen an den Endpoint Encryption Geräten der nächste Authentifizierungsversuch verzögert, das Endpoint Encryption Gerät wird gesperrt oder alle Daten, die vom jeweiligen Endpoint Encryption Agent kontrolliert werden, werden gelöscht.

TABELLE 7-6. Optionen zur Gerätesicherheit

SICHERHEITSOPTION	BESCHREIBUNG
Zeitverzögerung	PolicyServer sperrt das Endpoint Encryption Gerät vorübergehend und informiert den Benutzer von Endpoint Encryption darüber, dass das Gerät gesperrt ist. Während der Zeitverzögerung ist die Möglichkeit zur Authentifizierung oder Kennwortzurücksetzung deaktiviert. Die Dauer der Zeitverzögerung wird von der Richtlinie bestimmt. Nach Ablauf der Zeitverzögerung ist der Benutzer wieder berechtigt, sich zu authentifizieren. **Hinweis** Der Endpoint Encryption Benutzer kann die Selbsthilfe- oder Remote-Hilfe-Authentifizierung verwenden, wenn er nicht bis zum Ablauf der Zeitverzögerung warten will.

SICHERHEITSOPTION	BESCHREIBUNG
Remote-Authentifizierung erforderlich	PolicyServer sperrt das Endpoint Encryption Gerät, bis der Benutzer von Endpoint Encryption die Remote-Hilfe-Authentifizierung von einem Authentifizierer oder vom Support erhält. **Hinweis** Weitere Informationen finden Sie unter *Remote-Hilfe auf Seite 2-14*.
Gerät wird gelöscht	PolicyServer löscht alle Daten, die vom zugewiesenen Endpoint Encryption Agent gesteuert werden. **Warnung!** Der Endpoint Encryption Benutzer kann die gelöschten Daten nicht wiederherstellen.

Synchronisierung von Richtlinien

In der folgenden Liste werden die Ereignisse beschrieben, die die Richtliniensynchronisierung zwischen allen Agents und PolicyServer einleiten:

- Nachdem das Betriebssystem geladen und der Agent-Dienst gestartet wurde

  Hinweis
  Informationen zu Endpoint Encryption Diensten finden Sie unter *Endpoint Encryption Dienste auf Seite C-1*.

- In regelmäßigen Intervallen auf Basis der PolicyServer-Synchronisierungsrichtlinie
- Manuell durch Klicken auf die Schaltfläche **Richtlinien synchronisieren** im Kontextmenü des Agents

Hinweis

Aktionen für Geräte werden eingeleitet, nachdem der Agent Richtlinien-Updates erhält.

Kapitel 8

Encryption Management für Fremdprodukte

Eine Hauptfunktion von Full Disk Encryption ist die Fähigkeit, Verschlüsselungsprodukte von Fremdherstellern zu verwalten. Die Endpoint Encryption Agents können vollständig in die Verschlüsselungslösungen integriert werden, die Teil des Host-Betriebssystems sind.

Info über Agents zur Encryption Management

In der folgenden Tabelle werden die beiden Full Disk Encryption Agents für die Verschlüsselungsverwaltung von Produkten von Fremdherstellern erläutert.

Hinweis

Informationen zu allen verfügbaren Endpoint Encryption Agents finden Sie unter *Endpoint Encryption Agents auf Seite 2-9*.

TABELLE 8-1. Agents zur Encryption Management

AGENT	BESCHREIBUNG
Encryption Management for Microsoft BitLocker	Der Endpoint Encryption Full Disk Encryption Agent für Microsoft Windows-Umgebungen, auf denen lediglich Microsoft BitLocker auf dem Hosting-Endpunkt aktiviert werden muss.
Encryption Management for Apple FileVault	Der Endpoint Encryption Full Disk Encryption Agent für Mac OS-Umgebungen, auf denen lediglich Apple FileVault auf dem Hosting-Endpunkt aktiviert werden muss.

Einschränkungen der Agent-Richtlinie der Encryption Management

In der folgenden Tabelle werden die Richtlinieneinschränkungen für die Encryption Management for Apple FileVault und die Encryption Management for Microsoft BitLocker beschrieben. Um alle Richtlinien zu verwalten, installieren Sie stattdessen den Full Disk Encryption Agent.

Hinweis

- Encryption Management for Microsoft BitLocker erfordert keine Authentifizierung und ist von Authentifizierungsrichtlinien nicht betroffen. Client, Anmeldung, Kennwort und Authentifizierungsrichtlinien oder die Berechtigung des Benutzers, die Endpoint Encryption Agent-Software zu deinstallieren, wirkt sich nur auf die Full Disk Encryption Agents und File Encryption Agents aus.
- Encryption Management for Apple FileVault erfordert keine Authentifizierung für Endpunkte mit Festplatten, die APFS (Apple File System) nicht verwenden. Bei Endpunkten unter Mac OS High Sierra (10.13) mit SSDs, die APFS verwenden, fordert Encryption Management for Apple FileVault jedoch zur Eingabe des Benutzerkennworts auf, wenn die Richtlinie **Gerät verschlüsseln** zu einem späteren Zeitpunkt in **Keine** geändert wird.

In der folgenden Tabelle werden die Richtlinien beschrieben, die sich auf jeden Agent auswirken. Anhand der Tabelle können Sie die Richtlinieneinschränkungen bei Agents von Fremdherstellern verstehen.

TABELLE 8-2. Richtlinien, die sich auf Full Disk Encryption Agents auswirken

RICHTLINIE	FULL DISK ENCRYPTION	ENCRYPTION MANAGEMENT FOR APPLE FILEVAULT	ENCRYPTION MANAGEMENT FOR MICROSOFT BITLOCKER
Wiederherstellung durch Benutzer zulassen	●		
Deinstallation durch Benutzer zulassen	●		
Gerät verschlüsseln	●	●	●
Kontosperraktion	●		
Zeitraum bis Kontosperrung	●		
Kennwort zur Auslöschung	●		

Richtlinie	Full Disk Encryption	Encryption Management for Apple FileVault	Encryption Management for Microsoft BitLocker
Aktion zur Gerätesperrung	●		
Aktion zur Auslöschung des Geräts	●	●	●
Zulässige Anzahl fehlgeschlagener Anmeldeversuche	●		
Falls gefunden	●		
Rechtlicher Hinweis	●	●	●
Zeitverzögerung bei Gerätesperre	●		
Preboot-Umgehung	●		
Support-Informationen	●		
Token-Authentifizierung	●		
Zulässige Authentifizierungsmethoden	●		
Synchronisierungsintervall	●	●	●
Konfiguration von WLAN durch Benutzer zulassen	●		

Richtlinie	Full Disk Encryption	Encryption Management for Apple FileVault	Encryption Management for Microsoft BitLocker
WLAN-Einstellungen WLAN-Einstellungen anwenden (in Control Manager)	●		
Nur verwendeten Speicherplatz verschlüsseln	●		
Größe des Verschlüsselungsschlüssels auswählen	●		
Hintergrundfarbe für Anmeldung Hintergrundfarbe anpassen (in Control Manager)	●		
Anmeldebanner Banner anpassen (in Control Manager)	●		

Encryption Management for Microsoft BitLocker

Encryption Management for Microsoft BitLocker verwaltet BitLocker Drive Encryption™ für Endpunkte mit Microsoft Windows als Betriebssystem. Die Encryption Management for Microsoft BitLocker schützt Daten durch die

Verschlüsselung ganzer Volumes. Standardmäßig verwendet BitLocker den AES-Verschlüsselungsalgorithmus im CBC-Modus mit einem 128-Bit- oder 256-Bit-Schlüssel.

Status der Verschlüsselung anzeigen

Prozedur

1. Klicken Sie auf das Full Disk Encryption Symbol ( ).
   - Unter Windows wechseln Sie in die Task-Leiste.
   - Unter Mac OS wechseln Sie zur Menüleiste.
2. Öffnen Sie die Registerkarte **Verschlüsselungsstatus**.
3. Weitere Informationen finden Sie unter *Grundlegendes zum Verschlüsselungsstatus auf Seite 8-6*.

Grundlegendes zum Verschlüsselungsstatus

Auf der Registerkarte **Verschlüsselungsstatus** finden Sie Details zu den verschlüsselten Laufwerken, den Verschlüsselungstypen und dem Verhältnis zwischen verschlüsselten

und nicht verschlüsselten Anteilen auf dem Laufwerk. Weitere Informationen finden Sie im nachfolgenden Diagramm und in der Beschreibung.

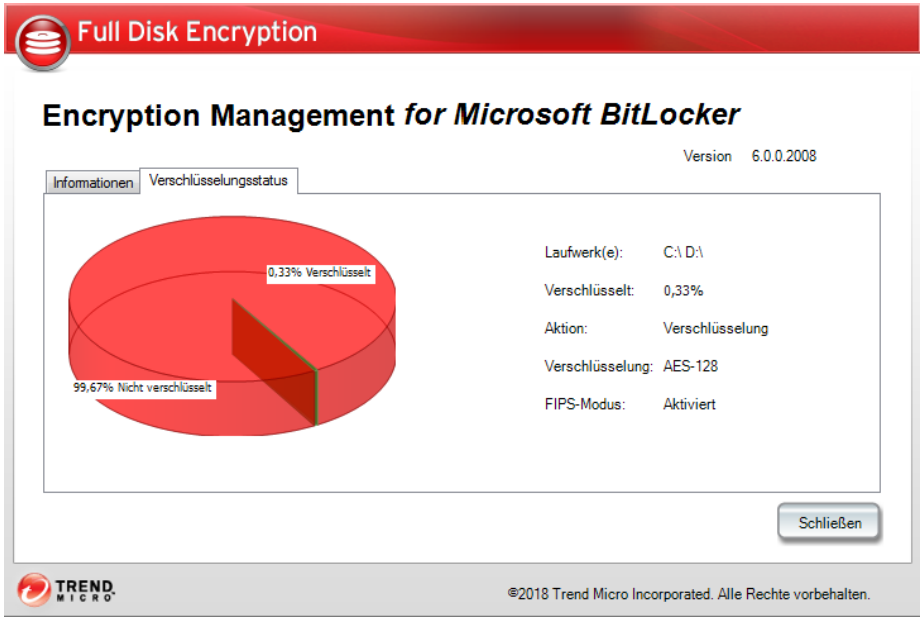


TABELLE 8-3. Geräteverschlüsselungsstatus

VORGANG	BESCHREIBUNG
Kreisdiagramm	Das Kreisdiagramm stellt das Verhältnis dar, in dem die Festplatte verschlüsselt und nicht verschlüsselt ist.
Laufwerk	Die Festplatte mit installiertem Agent.
Verschlüsselt	Der Prozentsatz der Verschlüsselung des Laufwerks.
Aktion	Der aktuelle Verschlüsselungsstatus.

VORGANG	BESCHREIBUNG
Verschlüsselung	Die Art der Verschlüsselung auf dem Endpunkt. **Hinweis** Die Encryption Management for Apple FileVault und die Encryption Management for Microsoft BitLocker verwenden immer die Software-basierte Verschlüsselung.
FIPS-Modus	Gibt an, ob FIPS aktiviert ist.

Grundlegendes zu Agent-Informationen

Auf der Registerkarte **Informationen** finden Sie ausführliche Informationen zum Benutzerkonto, zum Endpoint Encryption Gerät und zur Richtliniensynchronisierung. Weitere Informationen finden Sie im nachfolgenden Diagramm und in der Beschreibung.

TABELLE 8-4. Agent-Informationen

BEZEICHNUNG	BESCHREIBUNG
TMEE Benutzername	Das Endpoint Encryption Konto, das zur Anmeldung am Endpoint Encryption Gerät verwendet wird. Dabei handelt es sich um ein anderes Konto als für die Windows-Anmeldung.
Geräte-ID	Die eindeutige ID, die den Agent und den Endpunkt für PolicyServer identifiziert.
Betriebssystem	Das momentan auf dem Endpunkt installierte Betriebssystem, einschließlich der Version.
Computername	Der Name, mit dem der Endpunkt-Computer im Netzwerk identifiziert wird.
Letzte Synchronisierung	Der Zeitstempel für die letzte Richtliniensynchronisierung mit PolicyServer.
Mit PolicyServer synchronisieren	Erzwingt eine unverzügliche Aktualisierung der Richtlinien.

Richtlinien mit PolicyServer synchronisieren

Es gibt zwei Methoden, um Richtlinien mit PolicyServer zu synchronisieren. Informationen zu Richtlinien, die sich auf Geräte mit der Encryption Management for Microsoft BitLocker auswirken, finden Sie unter *Einschränkungen der Agent-Richtlinie der Encryption Management auf Seite 8-2*.

- *Richtlinien über die Menüleiste synchronisieren auf Seite 8-16*
- *Richtlinien über das Fenster "Info" synchronisieren auf Seite 8-10*

Synchronisierung von Richtlinien

In der folgenden Liste werden die Ereignisse beschrieben, die die Richtliniensynchronisierung zwischen allen Agents und PolicyServer einleiten:

- Nachdem das Betriebssystem geladen und der Agent-Dienst gestartet wurde

Hinweis

Informationen zu Endpoint Encryption Diensten finden Sie unter *Endpoint Encryption Dienste auf Seite C-1*.

- In regelmäßigen Intervallen auf Basis der PolicyServer-Synchronisierungsrichtlinie
- Manuell durch Klicken auf die Schaltfläche **Richtlinien synchronisieren** im Kontextmenü des Agents

Hinweis

Aktionen für Geräte werden eingeleitet, nachdem der Agent Richtlinien-Updates erhält.

Richtlinien über das Fenster "Info" synchronisieren

Informationen zu Richtlinieneinschränkungen, die sich auf die Encryption Management for Microsoft BitLocker Agent auswirken, finden Sie unter *Einschränkungen der Agent-Richtlinie der Encryption Management auf Seite 8-2*.

Prozedur

1. Vergewissern Sie sich, dass das Endpoint Encryption Gerät Netzwerkzugriff hat.
2. Klicken Sie auf das Agent-Symbol ( ).
3. Wählen Sie **Info über Full Disk Encryption**, um das Menü des Agent zu öffnen.
4. Öffnen Sie die Registerkarte **Informationen**.
5. Klicken Sie auf **Mit PolicyServer synchronisieren**.

Bei Erfolg sind alle Endpoint Encryption Richtlinien aktuell.

Richtlinien über die Task-Leiste synchronisieren

Prozedur

1. Vergewissern Sie sich, dass das Endpoint Encryption Gerät Netzwerkzugriff hat.
2. Klicken Sie auf das Agent-Symbol ( ).
3. Wählen Sie **Mit PolicyServer synchronisieren**.

Bei Erfolg sind alle Endpoint Encryption Richtlinien aktuell.

Encryption Management for Apple FileVault

Encryption Management for Apple FileVault verwaltet Apple FileVault™ zur Verschlüsselung des gesamten OS X-Startlaufwerks, welche normalerweise das Startverzeichnis einschließt. Dabei wird der Festplattenimage-Ansatz außer Acht gelassen. Die Encryption Management for Apple FileVault verwaltet die Verschlüsselung mit Apple FileVault, wobei das Kennwort des Benutzers als Passphrase für die Verschlüsselung verwendet wird. Die Encryption Management for Apple FileVault verwendet den AES-XTS-Modus von AES mit 128-Bit-Blöcken und einem 256-Bit-Schlüssel zur Verschlüsselung des Datenträgers entsprechend der NIST-Empfehlung. Nur Benutzer mit der Berechtigung, Laufwerke zu entsperren, können das Laufwerk starten und entsperren. Einmal entsperrt, können Benutzer den Computer auch nutzen, bis dieser heruntergefahren wird.

Hinweis

Lokale Konten oder mobile Konten von Mac OS können die Verschlüsselung auf Mac OS X Mountain Lion oder höher initiieren. Andere Mac OS-Benutzerkontentypen sind nicht in der Lage, die Verschlüsselung einzuleiten.

Informationen darüber, wie Sie ein mobiles Konto für Active Directory auf dem Mac einrichten, finden Sie unter *Mobiles Konto für Active Directory unter Mac OS erstellen auf Seite 8-17*.

Status der Verschlüsselung anzeigen

Prozedur

1. Klicken Sie auf das Full Disk Encryption Symbol ( ).
   - Unter Windows wechseln Sie in die Task-Leiste.
   - Unter Mac OS wechseln Sie zur Menüleiste.
2. Öffnen Sie die Registerkarte **Verschlüsselungsstatus**.
3. Weitere Informationen finden Sie unter *Grundlegendes zum Verschlüsselungsstatus auf Seite 8-6*.

Grundlegendes zum Verschlüsselungsstatus

Auf der Registerkarte **Verschlüsselungsstatus** finden Sie Details zu den verschlüsselten Laufwerken, den Verschlüsselungstypen und dem Verhältnis zwischen verschlüsselten

und nicht verschlüsselten Anteilen auf dem Laufwerk. Weitere Informationen finden Sie im nachfolgenden Diagramm und in der Beschreibung.

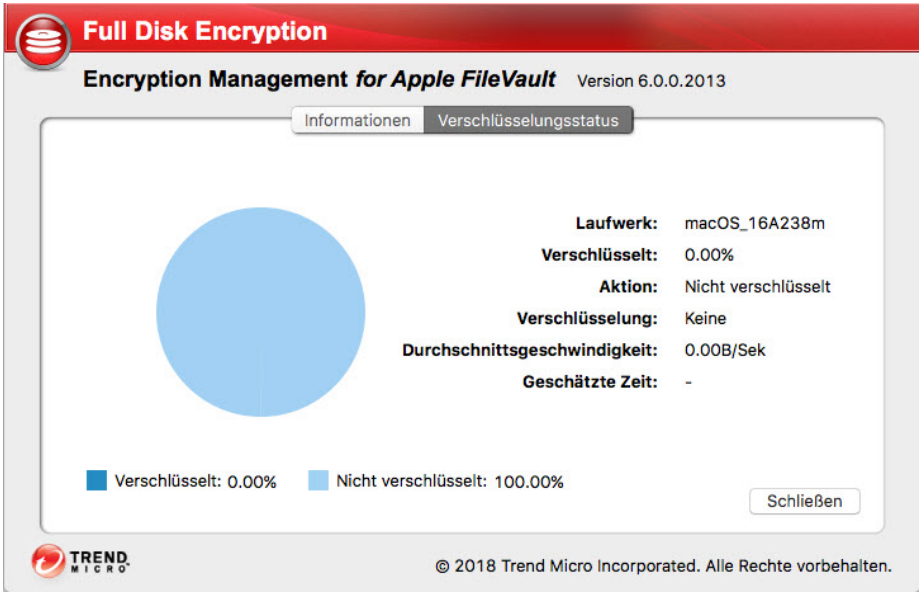


TABELLE 8-5. Geräteverschlüsselungsstatus

VORGANG	BESCHREIBUNG
Kreisdiagramm	Das Kreisdiagramm stellt das Verhältnis dar, in dem die Festplatte verschlüsselt und nicht verschlüsselt ist.
Laufwerk	Die Festplatte mit installiertem Agent.
Verschlüsselt	Der Prozentsatz der Verschlüsselung des Laufwerks.
Aktion	Der aktuelle Verschlüsselungsstatus.
Durchschnittsgeschwindigkeit	Die Rate (MB/Sekunden), mit der das Laufwerk verschlüsselt oder entschlüsselt wird.
Geschätzte Zeit	Die Zeitdauer, bis das Laufwerk vollständig verschlüsselt oder entschlüsselt wurde.

Grundlegendes zu Agent-Informationen

Auf der Registerkarte **Informationen** finden Sie ausführliche Informationen zum Benutzerkonto, zum Endpoint Encryption Gerät und zur Richtliniensynchronisierung. Weitere Informationen finden Sie im nachfolgenden Diagramm und in der Beschreibung.

TABELLE 8-6. Agent-Informationen

BEZEICHNUNG	BESCHREIBUNG
TMEE Benutzername	Das Endpoint Encryption Konto, das zur Anmeldung am Endpoint Encryption Gerät verwendet wird. Dabei handelt es sich um ein anderes Konto als für die Mac OS-Anmeldung.
Geräte-ID	Die eindeutige ID, die den Agent und den Endpunkt für PolicyServer identifiziert.

BEZEICHNUNG	BESCHREIBUNG
Betriebssystem	Das momentan auf dem Endpunkt installierte Betriebssystem, einschließlich der Version.
Computername	Der Name, mit dem der Endpunkt-Computer im Netzwerk identifiziert wird.
Unternehmen	Der Unternehmensname des PolicyServer, der die Agent-Richtlinien verwaltet.
Letzte Synchronisierung	Der Zeitstempel für die letzte Richtliniensynchronisierung mit PolicyServer. Weitere Informationen zur Synchronisierung von Richtlinien finden Sie unter *Richtlinien über die Menüleiste synchronisieren auf Seite 8-16*.
Jetzt synchronisieren	Erzwingt eine unverzügliche Aktualisierung der Richtlinien.

Richtlinien mit PolicyServer synchronisieren

Es gibt zwei Methoden, um Richtlinien mit PolicyServer zu synchronisieren. Informationen zu Richtlinien, die sich auf Geräte mit der Encryption Management for Apple FileVault auswirken, finden Sie unter *Einschränkungen der Agent-Richtlinie der Encryption Management auf Seite 8-2*.

- *Richtlinien über das Fenster "Info" synchronisieren auf Seite 8-16*
- *Richtlinien über die Menüleiste synchronisieren auf Seite 8-16*

Synchronisierung von Richtlinien

In der folgenden Liste werden die Ereignisse beschrieben, die die Richtliniensynchronisierung zwischen allen Agents und PolicyServer einleiten:

- Nachdem das Betriebssystem geladen und der Agent-Dienst gestartet wurde

Hinweis

Informationen zu Endpoint Encryption Diensten finden Sie unter *Endpoint Encryption Dienste auf Seite C-1*.

- In regelmäßigen Intervallen auf Basis der PolicyServer-Synchronisierungsrichtlinie
- Manuell durch Klicken auf die Schaltfläche **Richtlinien synchronisieren** im Kontextmenü des Agents

Hinweis

Aktionen für Geräte werden eingeleitet, nachdem der Agent Richtlinien-Updates erhält.

Richtlinien über das Fenster "Info" synchronisieren

Informationen zu Richtlinieneinschränkungen, die sich auf die Encryption Management for Apple FileVault Agents auswirken, finden Sie unter *Einschränkungen der Agent-Richtlinie der Encryption Management auf Seite 8-2*.

Prozedur

1. Vergewissern Sie sich, dass das Endpoint Encryption Gerät Netzwerkzugriff hat.
2. Klicken Sie auf das Agent-Symbol ( ).
3. Wählen Sie **Info über Full Disk Encryption**, um das Menü des Agent zu öffnen.
4. Öffnen Sie die Registerkarte **Informationen**.
5. Klicken Sie auf **Jetzt synchronisieren**.

Bei Erfolg sind alle Endpoint Encryption Richtlinien aktuell.

Richtlinien über die Menüleiste synchronisieren

Prozedur

1. Vergewissern Sie sich, dass das Endpoint Encryption Gerät Netzwerkzugriff hat.
2. Klicken Sie auf das Agent-Symbol ( ).
3. Wählen Sie **Richtlinien synchronisieren**.

Bei Erfolg sind alle Endpoint Encryption Richtlinien aktuell.

Mobiles Konto für Active Directory unter Mac OS erstellen

Lokale Konten oder mobile Konten von Mac OS können die Verschlüsselung auf Mac OS X Mountain Lion oder höher initiieren. Andere Mac OS-Benutzerkontentypen sind nicht in der Lage, die Verschlüsselung einzuleiten.

Falls ein anderes Mac OS-Konto als das lokale Konto oder das mobile Konto versucht, die Verschlüsselung zu starten, wird folgende Benachrichtigung angezeigt:

Die folgende Aufgabe zeigt, wie Sie ein mobiles Konto für Ihr Mac OS-Konto erstellen, um dieses Problem zu umgehen.

Prozedur

1. Navigieren Sie im Apple-Menü zu **Systemeinstellungen...**.

   Das Fenster **Systemeinstellungen** wird angezeigt.

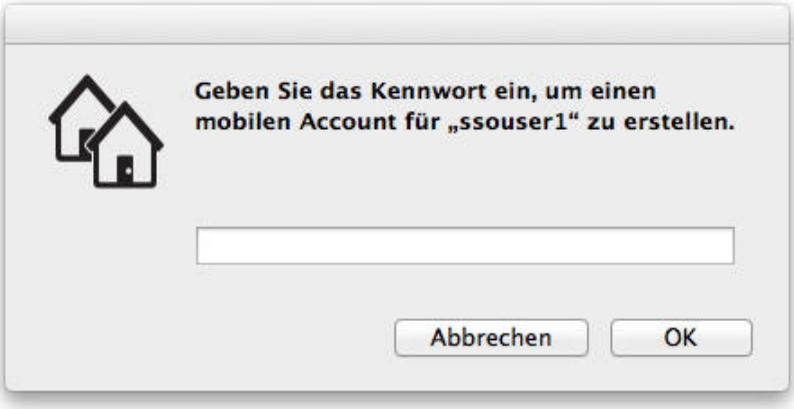
2. Wählen Sie **Benutzergruppen** im Abschnitt **System**.

3. Klicken Sie in der unteren linken Ecke auf das Sperrsymbol.

4. Klicken Sie auf **Erstellen...** neben **Mobiles Konto**.

5. Wählen Sie in den folgenden Fenster die persönlichen Einstellungen, und klicken Sie auf **Erstellen**, um zum jeweils nächsten Fenster zu gelangen.

6. Wenn Sie dazu aufgefordert werden, geben Sie Ihr Active Directory-Kennwort ein, und klicken Sie auf **OK**.



Ihr mobiles Konto wurde erstellt. Sie können nun mit diesem mobilen Konto die Verschlüsselung einleiten.

Fehlerbehebung bei Kennwort- und Verschlüsselungsproblemen

Nach dem Installieren von Encryption Management for Apple FileVault und dem Neustarten des Endpunkts versucht Apple FileVault, die Festplatte zu verschlüsseln.

Wenn das während der Installation angegebene Kennwort nicht mit dem angegebenen Benutzerkonto übereinstimmt, wird das folgende Fenster angezeigt:

- Starten Sie für Endpunkte mit Festplatten, die APFS (Apple File System) nicht verwenden, den Endpunkt nach Angabe des korrekten Kennworts neu. Wenn das Kennwort die Ursache des Problems war, entschlüsselt Apple FileVault den Endpunkt nach dem Neustart.
- Für Endpunkte unter Mac OS High Sierra (10.13) mit SSDs, die APFS verwenden, ist ein Neustart nicht erforderlich. Apple FileVault verschlüsselt den Endpunkt nach Angabe des korrekten Kennworts.

Besteht das Problem weiterhin oder wird im Verschlüsselungsstatus angezeigt, dass der Endpunkt nicht verschlüsselt wird, wird das ordnungsgemäße Funktionieren von Apple FileVault aufgrund eines anderen Problems eingeschränkt. Führen Sie das folgende Verfahren durch, um zu ermitteln, wo das Problem auftritt und ob es an den Support von Trend Micro gesendet werden sollte.

Prozedur

1. Navigieren Sie im Apple-Menü zu **Sicherheit & Datenschutz** > **FileVault**.
2. Wenn das Schlosssymbol geschlossen dargestellt wird, klicken Sie darauf, um Änderungen vorzunehmen.

3. Klicken Sie auf **FileVault aktivieren...**.

   Ein Fenster mit der Aufforderung, Ihr Kennwort einzugeben, wird angezeigt.

4. Geben Sie Ihr Kennwort ein und klicken Sie auf **Verschlüsselung starten**.

   Wenn Ihr Benutzerkonto zum Aktivieren von FileVault berechtigt ist, Ihre Anmeldedaten korrekt sind und FileVault ordnungsgemäß funktioniert, beginnt FileVault mit dem Verschlüsseln der Festplatte.

5. Wenn danach während der Verschlüsselung Probleme bei FileVault auftreten, erstellen Sie aussagekräftige Screenshots dieser Probleme und wenden Sie sich an den Support von Trend Micro.

Kapitel 9

Recovery

In diesem Kapitel werden Methoden zur Wiederherstellung von mittels Full Disk Encryption verschlüsselten Laufwerken, auf die nicht zugegriffen werden kann, erläutert.

Preboot-Fehler nach der Installation

Wenn bei der ersten Ausführung von Preboot direkt nach der Installation das Laden nicht möglich ist, führt Full Disk Encryption die folgenden Schritte aus:

- Der reguläre Boot-Prozess wird wiederhergestellt und Windows wird gestartet
- Das Starten der Verschlüsselung wird verhindert
- Die folgende Meldung wird angezeigt:

Dies kann auf folgende Probleme zurückzuführen sein:

Problem	Description	Lösung
Unvollständige Installation	Die Installation konnte vom Installationsprogramm nicht abgeschlossen werden.	Deinstallieren Sie Full Disk Encryption, führen Sie einen Neustart durch, und versuchen Sie, das Installationsprogramm erneut auszuführen.
Unerwartetes Herunterfahren	Verursacht in der Regel kein Problem. Möglicherweise kann jedoch die Installation vom Installationsprogramm nicht abgeschlossen werden.	Starten Sie zunächst den Endpunkt neu. Sollte das Problem weiterhin bestehen, deinstallieren Sie Full Disk Encryption, führen Sie einen Neustart durch, und versuchen Sie, das Installationsprogramm erneut auszuführen.
Inkompatible Hardware	Das Preboot-Laden kann aufgrund von inkompatibler Hardware oder Firmware nicht abgeschlossen werden.	Deinstallieren Sie Full Disk Encryption, und führen Sie dann einen der folgenden Schritte aus: • Entfernen Sie sämtliche inkompatible Hardware • Aktualisieren Sie sämtliche inkompatible Firmware **Hinweis** Um festzustellen, ob eine bestimmte Hardware oder Firmware mit der Full Disk Encryption-Installation inkompatibel ist, wenden Sie sich wegen weiterer Informationen an den Trend Micro Support. • Installieren Sie Full Disk Encryption erneut.

Sollte das Problem weiterhin bestehen, wenden Sie sich an den Trend Micro Support.

Full Disk Encryption Wiederherstellungsmethoden

Wenn ein Gerät mit Full Disk Encryption vollständig verschlüsselt ist, können Probleme mit dem System oder Programm auftreten, die einen Zugriff auf Windows oder zugehörige Dienste erschweren oder verhindern. In diesen Fällen verwenden Sie die folgenden Methoden und Tools zur Wiederherstellung Ihres Systems. Die Reihenfolge reicht dabei von der am wenigsten schwerwiegenden bis zur am schwerwiegendsten Situation.

Situation	Wiederherstellungsmethode	Beschreibung
Windows funktioniert normal, Full Disk Encryption beeinträchtigt jedoch einige Anwendungen, beeinträchtigt die Leistung von Windows oder zeigt Fehlermeldungen an.	Full Disk Encryption deinstallieren	Durch die Deinstallation von Full Disk Encryption wird Full Disk Encryption vom Gerät entfernt. Nachdem die Deinstallation abgeschlossen wurde, müssen Sie möglicherweise andere Wiederherstellungsaktionen in Windows durchführen. Danach können Sie versuchen, Full Disk Encryption neu zu installieren. Die Schritte zur Deinstallation finden Sie im *Endpoint Encryption Installationshandbuch*.

Situation	Wiederherstellungsmethode	Beschreibung
Full Disk Encryption Preboot wird geladen, Windows jedoch nicht.	*Wiederherstellungskonsole auf Seite 9-6*	Die Wiederherstellungskonsole von Full Disk Encryption kann über den Full Disk Encryption Preboot angezeigt werden. Öffnen Sie zum Entschlüsseln der Festplatte die Full Disk Encryption Option **Wiederherstellungskonsole** > **Festplatte verwalten** > **Diese Festplatte entschlüsseln**, mit der die ausgewählte Festplatte direkt entschlüsselt oder ein Image der entschlüsselten Festplatte auf einem Wechselmedium gespeichert wird. **Hinweis** Diese Methode sollte nicht ausgeführt werden, wenn Windows normal funktioniert.
Beim Start fährt weder Windows noch der Full Disk Encryption Preboot hoch. Der Endpunkt zeigt einen schwarzen Bildschirm mit einem fest stehenden Eingabesymbol an.	*Recovery-Tool auf Seite 9-26*	Dieses Problem tritt normalerweise auf, wenn der MBR beschädigt ist. Das Recover-Tool von Full Disk Encryption versucht, den MBR zu reparieren. Verläuft dies erfolgreich, wird der Full Disk Encryption Preboot das nächste Mal, wenn der Endpunkt gestartet wird, ordnungsgemäß geladen.
Beim Start zeigt der Endpunkt den Hintergrund von Full Disk Encryption Preboot, aber das Anmeldefenster wird nicht geladen.	*Recovery-Tool auf Seite 9-26*	Dieses Problem tritt normalerweise auf, wenn die Datenbank von Full Disk Encryption beschädigt ist. Das Recovery-Tool versucht, Informationen von PolicyServer zu erhalten und die beschädigte Datenbank von Full Disk Encryption zu ersetzen. Verläuft dies erfolgreich, wird der Full Disk Encryption Preboot das nächste Mal, wenn der Endpunkt gestartet wird, ordnungsgemäß geladen.

Situation	Wiederherstellungsmethode	Beschreibung
Der Endpunkt kann Windows nicht starten oder nicht auf den Full Disk Encryption Preboot zugreifen. Das Recovery-Tool kann die Festplatte nicht reparieren.	Technischen Support kontaktieren	Versuchen Sie zunächst andere Wiederherstellungsmethoden. Wenn die vorherigen Wiederherstellungsmethoden nicht verfügbar sind oder nicht funktionieren, wenden Sie sich an den Support von Trend Micro. Das Support-Team von Trend Micro gibt sein Bestes, um Ihr Problem zu beheben. Weitere Informationen finden Sie unter *Technischer Support auf Seite 11-1*.

Wiederherstellungskonsole

Die Wiederherstellungskonsole von Full Disk Encryption ermöglicht Administratoren, Authentifizierern und Benutzern mit entsprechenden Rechten Folgendes:

- Wiederherstellen von Full Disk Encryption Geräten bei Ausfall des primären Betriebssystems
- Fehlerbehebung bei Problemen mit der Netzwerkverbindung
- Entschlüsseln von Festplatten zum Abrufen von Daten, auf die nicht zugegriffen werden kann
- Verwalten von Richtlinien, wenn keine Verbindung mit PolicyServer besteht

Warnung!

Wenn die Festplatte verschlüsselt ist, verwenden Sie keine Reparaturdienstprogramme von Windows oder Drittanbietern zum Wiederherstellen von Daten. Verwenden Sie die Wiederherstellungskonsole und entschlüsseln Sie zuerst die Festplatte. Andernfalls können Daten verloren gehen, beschädigt werden, oder auf die Daten kann möglicherweise nicht mehr zugegriffen werden.

Alle Änderungen an Richtlinien werden überschrieben, wenn der Full Disk Encryption Agent Richtlinien mit PolicyServer synchronisiert.

Optionen der Wiederherstellungskonsole

Konsolenmenü	Beschreibung
Festplatten verwalten	Zeigt Optionen für die Verwaltung von Festplatten auf dem Endpunkt an. Weitere Informationen finden Sie unter *Festplattenoptionen verwalten auf Seite 9-10*
Partit. bereitst.	Bereitstellung von Zugriff auf die verschlüsselten Partitionen zur Dateiverwaltung. Zeigen Sie verschlüsselte Dateien an oder kopieren Sie Dateien auf ein externes Gerät. **Hinweis** Diese Option ist nur für Festplatten mit Softwareverschlüsselung verfügbar. Diese Option steht nicht zur Verfügung, wenn es sich bei der Festplatte um eine SED-Festplatte handelt.
Benutzer verwalten	Hinzufügen oder Entfernen von Benutzern von einem Gerät, wenn es nicht mit dem PolicyServer verbunden ist.

KONSOLENMENÜ	BESCHREIBUNG
Richtlinien verwalten	Ändern Sie die Richtlinien für Geräte, die entweder nicht von PolicyServer verwaltet werden oder die verwaltet werden, aber die vorübergehend nicht mit PolicyServer verbunden sind. Wenn das Gerät verwaltet ist, werden Richtlinienänderungen bei der nächsten Kommunikation des Geräts mit PolicyServer überschrieben.
Protokolle anzeigen	Anzeigen und Durchsuchen verschiedener Full Disk Encryption Protokolle. **Hinweis** Protokolle sind nur verfügbar, wenn von Windows aus auf die Wiederherstellungskonsole zugegriffen wird.
Netzwerk	Wenn Sie auf **Netzwerk** klicken, werden zwei Fensteroptionen geöffnet: • **Setup**: Hier können Sie die Einstellungen für Ihre Internetverbindung, einschließlich der Verwendung einer statischen oder dynamischen IP-Adresse, Ihre PolicyServer Adresse und Ihre WLAN-Einstellungen konfigurieren. • **Fehlerbehebung**: Hier können Sie DHCP-Protokolle anzeigen und Traceroute-Befehle ausführen.
Zurück zur Anmeldung	Beendet die Wiederherstellungskonsole und kehrt zum Anmeldefenster zurück.
Beenden	Beenden der Wiederherstellungskonsole.

Von Full Disk Encryption Preboot auf die Wiederherstellungskonsole zugreifen

Standardmäßig können nur Administrator- und Authentifiziererkonten auf die Wiederherstellungskonsole zugreifen. Um anderen Benutzern Zugriff auf die Wiederherstellungskonsole zu erlauben, aktivieren Sie die Wiederherstellung durch

Benutzer über Ihre Management-Konsole. Weitere Informationen zu Control Manager finden Sie unter *Full Disk Encryption Regeln konfigurieren auf Seite 5-17*.

Prozedur

1. Starten Sie den Endpunkt oder starten Sie ihn neu.

   Full Disk Encryption Preboot wird angezeigt.

2. Aktivieren Sie das Kontrollkästchen **Wiederherstellungskonsole**.

3. Geben Sie die Anmeldedaten für das Endpoint Encryption Benutzerkonto ein.

4. Klicken Sie auf **Anmelden**.

   Die Wiederherstellungskonsole wird geöffnet.

Auf die Wiederherstellungskonsole von Windows aus zugreifen

Prozedur

1. Wechseln Sie unter Windows zum Installationsverzeichnis von Full Disk Encryption.

   Der Standardordner ist `C:\Program Files\Trend Micro\Full Disk Encryption\`.

2. Öffnen Sie `RecoveryConsole.exe`.

   Das Fenster **Wiederherstellungskonsole** wird angezeigt.

3. Geben Sie den Endpoint Encryption Benutzernamen und das Kennwort ein und klicken Sie anschließend auf **Anmelden**.

   Die Wiederherstellungskonsole wird mit der Seite **Festplatten verwalten** geöffnet.

Festplattenoptionen verwalten

Die im Fenster **Festplatten verwalten** angezeigten Optionen variieren je nach dem Status der Festplatten, die an das Gerät angeschlossen sind.

OPTIONEN	BESCHREIBUNG
Verschlüsseln	Verschlüsseln neuer unverschlüsselter Festplatten Dies ist die einzige verfügbare Option, wenn über Windows auf die Wiederherstellungskonsole zugegriffen wird. Die Systemfestplatte ist standardmäßig ausgewählt. Weitere Informationen finden Sie unter *Verschlüsseln von Festplatten auf Seite 9-11*.
Alle entschlüsseln	Entschlüsseln der Systemfestplatte und aller Datenfestplatten, die an den Endpunkt angeschlossen sind
Diese Festplatte entschlüsseln	Entschlüsseln der ausgewählte Festplatte Weitere Informationen finden Sie unter *"Festplatte entschlüsseln" in Preboot verwenden auf Seite 9-13*.
Beenden	Beenden des Entschlüsselungsvorgangs
Festplatte trennen	Ausschließen der Festplatte aus der Verwaltung durch Full Disk Encryption Diese Option steht nur für Datenfestplatten mit abgeschlossener Entschlüsselung zur Verfügung. Nach dem Trennen der Festplatte vom System erkennt Full Disk Encryption die Festplatte als neue Festplatte und schließt sie aus allen Richtlinien aus. Um die Festplatte wieder zu verwalten, verwenden Sie Full Disk Encryption zum erneuten Verschlüsseln der Festplatte.
Boot-Partition wiederherstellen	Rollback des MBR in einen Zustand vor der Installation von Full Disk Encryption Diese Option steht nur für Systemfestplatten mit abgeschlossener Entschlüsselung zur Verfügung. Trennen Sie zum Aktivieren dieser Option alle Datenfestplatten vom Endpunkt. Weitere Informationen finden Sie unter *Boot wiederherst. auf Seite 9-15*.

OPTIONEN	BESCHREIBUNG
SED entsperren	Entfernen des Preboots aus einer SED-Systemfestplatte Diese Option steht nur für SED-Systemfestplatten mit abgeschlossener Entschlüsselung zur Verfügung. Trennen Sie zum Aktivieren dieser Option alle Datenfestplatten vom Endpunkt.

Verschlüsseln von Festplatten

Verwenden Sie die Wiederherstellungskonsole, um die Verschlüsselung neuer unverschlüsselter Festplatten zu initialisieren.

Hinweis

Dieser Vorgang erfordert eine funktionsfähige Verbindung zu PolicyServer.

Prozedur

1. Schalten Sie den Endpunkt aus und schließen Sie die neue Festplatte an.
2. Starten Sie Windows.

   Windows erkennt und installiert Treiber für die neue Festplatte.
3. Starten Sie die Wiederherstellungskonsole in Windows.

   Weitere Informationen finden Sie unter *Auf die Wiederherstellungskonsole von Windows aus zugreifen auf Seite 9-9*.
4. Melden Sie sich an der Wiederherstellungskonsole an.
5. Klicken Sie im Fenster **Festplatten verwalten** auf **Zusammenfassung**, um festzustellen, welche Festplatten verschlüsselt werden müssen.

   Hinweis

   In Full Disk Encryption werden unverschlüsselte Festplatten als **nicht verwaltete Festplatten** angezeigt.

6. Wählen Sie das Laufwerk aus, das bereitgestellt werden soll, und klicken Sie auf **Festplatte verschlüsseln**.

   Der Benutzer wird in einer Benachrichtigung darüber informiert, dass die Festplatte erfolgreich zur Verschlüsselung bereitgestellt wurde.

7. (Optional) Wiederholen Sie für Geräte mit mehreren Festplatten den vorherigen Schritt, um weitere Festplatten für die Verschlüsselung bereitzustellen.

8. Starten Sie den Endpunkt neu, um mit der Verschlüsselung zu beginnen.

9. Klicken Sie nach dem Neustart auf das Full Disk Encryption-Symbol in der Taskleiste und verwenden Sie die Registerkarte **Verschlüsselungsstatus**, um den Fortschritt der Verschlüsselung zu überwachen.

Festplatten entschlüsseln

Full Disk Encryption bietet die folgenden Optionen zum Entschlüsseln von Festplatten:

- Verwenden Sie PolicyServer, um eine Richtlinie zu verteilen, die alle Festplatten für eine bestimmte Gruppe entschlüsselt. Setzen Sie den Wert **Gerät verschlüsseln** auf **Nein**.

  Weitere Informationen finden Sie im Endpoint Encryption 6.0 PolicyServer MMC Handbuch.

- Bei der Deinstallation von Full Disk Encryption werden automatisch alle an ein Gerät angeschlossenen Festplatten entschlüsselt.

  Weitere Informationen zu Deinstallationsschritten finden Sie im Endpoint Encryption Installationshandbuch.

- Starten Sie die Festplattenentschlüsselung über die Wiederherstellungskonsole in Preboot.

  Weitere Informationen finden Sie unter *"Festplatte entschlüsseln" in Preboot verwenden auf Seite 9-13*.

Wichtig

Verwenden Sie die Preboot-Funktion "Festplatte entschlüsseln" nur, wenn beim Starten von Windows Probleme auftreten. Treten beim Zugriff auf Full Disk Encryption über Windows keine Probleme auf, empfiehlt Trend Micro, PolicyServer oder das Full Disk Encryption-Deinstallationsprogramm zum Entschlüsseln von Festplatten zu verwenden.

"Festplatte entschlüsseln" in Preboot verwenden

Durch Auswählen von **Festplatte entschlüsseln** in Preboot wird eine verschlüsselte Full Disk Encryption Festplatte entschlüsselt, die Verschlüsselungstreiber werden jedoch nicht entfernt.

Warnung!

- Lesen Sie zuerst die Anweisungen, bevor Sie **Festplatte entschlüsseln** verwenden. Bei falscher Vorgehensweise kann der Verlust von Daten nicht ausgeschlossen werden.
- Verwenden Sie die Preboot-Funktion **Festplatte entschlüsseln** nur dann, wenn beim Starten von Windows Probleme auftreten. Entfernen Sie Full Disk Encryption nicht mit Hilfe von **Festplatte entschlüsseln**, wenn das Endpoint Encryption Gerät normal funktioniert. Verwenden Sie stattdessen `TMFDEUninstall.exe`.

Zum Entschlüsseln des Full Disk Encryption Geräts benötigt der Benutzer ausreichende Rechte für den Zugriff auf die Wiederherstellungskonsole. Damit alle Benutzer in einer Gruppe/Richtlinie Zugriff auf die Wiederherstellungskonsole haben, aktivieren Sie die folgende Richtlinie:

Management-Konsole	Menüpfad
PolicyServer MMC	Navigieren Sie zu **Full Disk Encryption** > **Agent** > **Wiederherstellung durch Benutzer zulassen**.

MANAGEMENT-KONSOLE	MENÜPFAD
Control Manager	Erstellen oder bearbeiten Sie eine Richtlinie, navigieren Sie anschließend zu **Full Disk Encryption** > **Benutzer sind berechtigt, auf die Systemwiederherstellungstools zuzugreifen**.

Führen Sie in der Rolle eines Administrators, Authentifizierers oder berechtigten Benutzers die folgenden Schritte durch, um eine Festplatte zu entschlüsseln.

Prozedur

1. Melden Sie sich an der Wiederherstellungskonsole an.

   Weitere Informationen finden Sie unter *Von Full Disk Encryption Preboot auf die Wiederherstellungskonsole zugreifen auf Seite 9-8*.

   Die Wiederherstellungskonsole wird mit der Seite **Festplatte verwalten** geöffnet.

2. Wählen Sie eine der folgenden Optionen:

   - Klicken Sie auf **Alle entschlüsseln**, um alle entschlüsselten Festplatten im Gerät zu verschlüsseln.
   - Klicken Sie auf **Zusammenfassung**, wählen Sie eine Festplatte aus und klicken Sie auf **Entschlüsseln**, um nur die ausgewählte Festplatte zu entschlüsseln.

   Mit der Entschlüsselung wird direkt begonnen und die Seite **Festplatte verwalten** mit dem Entschlüsselungsfortschritt wird geöffnet.

3. Nach Abschluss der Verschlüsselung zeigt Full Disk Encryption die folgenden Optionen an:

   - Bei Systemfestplatten zeigt Full Disk Encryption je nach Festplattentyp die Option **Boot-Partition wiederherstellen** oder **SED entsperren** an.

     Weitere Informationen finden Sie unter *Boot wiederherst. auf Seite 9-15*.

   - Bei Datenfestplatten zeigt Full Disk Encryption die Option **Festplatte trennen** an. Klicken Sie auf diese Option, um zu verhindern, dass die Festplatte von Full Disk Encryption verwaltet wird.

4. Klicken Sie auf **Beenden**, um das Endpoint Encryption Gerät neu zu starten.
5. Melden Sie sich bei Full Disk Encryption Preboot an.
6. Melden Sie sich bei Windows an.

   Stellen Sie sicher, dass alle zur Entschlüsselung ausgewählten Festplatten nicht mehr verschlüsselt sind.

Partit. bereitst.

Kopieren Sie mit Hilfe von **Partitionen bereitstellen** Dateien zwischen der verschlüsselten externen Festplatte und einem Speichergerät, bevor Sie ein Image der Festplatte erstellen oder diese neu formatieren. Der verschlüsselte Inhalt auf dem Laufwerk wird im linken Fensterbereich angezeigt, und das unverschlüsselte Gerät kann im rechten Fensterbereich gemountet werden. Verschieben Sie Dateien mit Kopieren und Einfügen zwischen den Fensterbereichen. Dateien, die auf das verschlüsselte Laufwerk kopiert werden, werden verschlüsselt. Bei Dateien, die vom verschlüsselten Laufwerk kopiert werden, wird die Verschlüsselung aufgehoben.

Boot wiederherst.

Mithilfe der Option **Boot wiederherstellen** wird der ursprüngliche Boot-Sektor auf der Systemfestplatte eines Endpoint Encryption Geräts wiederhergestellt, wenn das Gerät vollständig entschlüsselt ist. **Bootsektor wiederherstellen** ist nur über Full Disk Encryption Preboot verfügbar.

Entschlüsseln Sie die Festplatte, bevor Sie den Master Boot Record (MBR) wiederherstellen.

Warnung!

Lesen Sie zuerst die Anweisungen, bevor Sie **Festplatte entschlüsseln** verwenden. Bei falscher Vorgehensweise kann der Verlust von Daten nicht ausgeschlossen werden.

Prozedur

1. Melden Sie sich an der Wiederherstellungskonsole an.

   Weitere Informationen finden Sie unter *Von Full Disk Encryption Preboot auf die Wiederherstellungskonsole zugreifen auf Seite 9-8*.

   Die Wiederherstellungskonsole wird mit der Seite **Festplatten verwalten** geöffnet.

2. Klicken Sie auf **Zusammenfassung** und dann auf **Alle entschlüsseln**.

3. Warten Sie, bis die Entschlüsselung der Festplatte abgeschlossen ist.

4. Wählen Sie nach der Entschlüsselung eine Datenfestplatte aus und klicken Sie auf **Trennen**.

   Wiederholen Sie diesen Vorgang für alle Datenfestplatten auf dem Endpunkt. Nur die Systemfestplatte sollte zurückbleiben.

   Boot-Partition wiederherstellen steht zur Verfügung, nachdem alle Datenfestplatten vom Endpunkt getrennt wurden.

   Hinweis

   Handelt es sich bei der Systemfestplatte um eine SED-Festplatte, wird in der Wiederherstellungskonsole stattdessen **SED entsperren** angezeigt.

5. Klicken Sie auf **Boot-Partition wiederherstellen**.

   Das Bestätigungsfenster **Möchten Sie den MBR wirklich ersetzen?** wird angezeigt.

6. Klicken Sie auf **Ja**, um den MBR zu ersetzen.

   Eine Nachricht mit der Bestätigung, dass der MBR ersetzt wurde, wird angezeigt.

7. Klicken Sie auf **Beenden**.

   Das Endpoint Encryption startet Windows.

Full Disk Encryption Benutzer verwalten

Bei der Verwaltung von Benutzern mit **Benutzer verwalten** werden Benutzer dem Full Disk Encryption Preboot-Cache hinzugefügt bzw. daraus entfernt, oder das im Cache gespeicherte Kennwort des Benutzers wird geändert. Die Option **Benutzer verwalten** ist nützlich, wenn der Full Disk Encryption Agent keine Verbindung zum PolicyServer aufbauen kann. Diese Option kann sowohl von Full Disk Encryption Preboot als auch von der Windows Wiederherstellungskonsole verwendet werden.

Hinweis

- **Benutzer verwalten** ist nur verfügbar, wenn keine Verbindung mit PolicyServer besteht.
- Änderungen, die an Benutzern vorgenommen wurden, werden überschrieben, wenn Full Disk Encryption eine Verbindung zu PolicyServer aufbaut.

Einige Überlegungen zu Kennwörtern:

- Bei zugewiesenen Kennwörtern handelt es sich immer um feste Kennwörter.
- Legen Sie das Ablaufdatum für das Benutzerkennwort mit Hilfe des Kalenders **Kennwort läuft ab** fest.
- Wenn Sie als Datum das aktuelle Datum oder ein älteres Datum festlegen, wird eine sofortige Kennwortänderung durchgesetzt. Wenn Sie als Datum ein zukünftiges Datum festlegen, wird die Änderung an dem angegebenen Datum umgesetzt.

Benutzer bearbeiten

Die Bearbeitung von Benutzern in der Wiederherstellungskonsole folgt denselben Regeln, die auch für das Unternehmen gelten. Weitere Informationen zu Rollen und Authentifizierung finden Sie unter *Authentifizierungsübersicht auf Seite 5-2*.

Prozedur

1. Wählen Sie den Benutzer aus der Benutzerliste aus.

2. Aktualisieren Sie die gewünschten Informationen.
3. Wählen Sie den Benutzertyp.

   Eine Erklärung der Kontorollen finden Sie unter *Authentifizierungsübersicht auf Seite 5-2*.
4. Legen Sie das Ablaufdatum für das Kennwort fest.
5. Klicken Sie auf **Speichern**.

   Das Benutzerkonto wird aktualisiert.

Benutzer hinzufügen

Prozedur

1. Klicken Sie auf **Benutzer hinzufügen**.
2. Geben Sie Ihren Benutzernamen und das Kennwort ein, und bestätigen Sie dann das Kennwort.
3. Wählen Sie die Authentifizierungsmethode aus der Dropdown-Liste **Authentifizierungstyp**.
4. Legen Sie das Ablaufdatum für das Kennwort fest.
5. Klicken Sie auf **Speichern**.

   Der neue Benutzer wird in der Benutzerliste angezeigt, und ein Bestätigungsfenster erscheint.
6. Klicken Sie auf **OK**, um das Bestätigungsfenster zu schließen.

   Das neue Benutzerkonto wird hinzugefügt.

Benutzer löschen

Prozedur

1. Wählen Sie einen Benutzer aus der Benutzerliste aus.
2. Klicken Sie auf **Benutzer löschen**.

   Ein Bestätigungsfenster zum Löschen des Benutzers wird angezeigt.
3. Klicken Sie auf **Ja**.

   Der Benutzer wird aus der Benutzerliste gelöscht.

Richtlinien verwalten

Verwenden Sie **Richtlinien verwalten**, um die verschiedenen Richtlinien für die Full Disk Encryption Wiederherstellungskonsole festzulegen.

Weitere Informationen zu diesen Richtlinien finden Sie im *Administratorhandbuch für PolicyServer MMC*.

Hinweis

Die Option **Richtlinien verwalten** ist nur verfügbar, wenn keine Verbindung mit PolicyServer besteht. Die vorgenommenen Änderungen werden überschrieben, wenn Full Disk Encryption das nächste Mal eine Verbindung zu PolicyServer aufbaut.

Protokolle anzeigen

Wählen Sie **Protokolle anzeigen**, um auf Grundlage bestimmter Kriterien nach Protokollen zu suchen und diese anzuzeigen. **Protokolle anzeigen** ist nur in der Wiederherstellungskonsole unter Windows verfügbar. Der Befehl ist über Full Disk Encryption Preboot nicht verfügbar.

Informationen über das Anzeigen von Full Disk Encryption Protokollen finden Sie unter *Auf die Wiederherstellungskonsole von Windows aus zugreifen auf Seite 9-9*.

Netzwerk

Navigieren Sie zu **Netzwerk** > **Setup**, um die von Full Disk Encryption Preboot verwendeten Netzwerkeinstellungen zu überprüfen, zu testen und/oder zu ändern.

Navigieren Sie zu **Netzwerk** > **Fehlerbehebung**, um DHCP-Protokolle anzuzeigen und Traceroute-Befehle auszuführen.

Netzwerkkonfiguration verwalten

Standardmäßig ist **Einstellungen von Windows abrufen** für IPv4 und IPv6 ausgewählt. Deaktivieren Sie diese Option, um die Netzwerkeinstellungen manuell zu konfigurieren.

- Die Auswahl von **DHCP** (IPv4) oder **Adresse automatisch abrufen** (IPv6) verwendet die dynamisch zugewiesene IP-Adresse.
- Bei Auswahl von **Statische IP-Adresse** werden alle Felder in diesem Abschnitt aktiviert.
- Wenn Sie auf der Registerkarte **IPv6** die Option **Statische IP-Adresse** auswählen und das Feld "IP-Adresse" leer ist, wird eine eindeutige IP-Adresse auf Grundlage der Hardware-Adresse des Computers erzeugt.

Full Disk Encryption in ein anderes Unternehmen migrieren

Eine PolicyServer Instanz kann mehrere Unternehmenskonfigurationen haben, die einen Geschäftsbereich oder eine Abteilung repräsentieren. Wenn Sie ein Gerät in ein neues Unternehmen verschieben, wird das Endpoint Encryption Gerät aus dem alten Unternehmen entfernt und das Endpoint Encryption Gerät wird dem neuen Unternehmen innerhalb derselben PolicyServer Instanz hinzugefügt. Möglicherweise muss der Full Disk Encryption Agent in ein neues Unternehmen verschoben werden, wenn der Mitarbeiter in eine andere Abteilung oder an einen anderen Standort versetzt wird.

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. Klicken Sie auf **Netzwerk-Setup**.
2. Wählen Sie die Registerkarte **PolicyServer**.
3. Klicken Sie auf **Unternehmen wechseln**.

   Das Fenster **Unternehmen wechseln** wird angezeigt.

ABBILDUNG 9-1. Wiederherstellungskonsole – Unternehmen wechseln

4. Konfigurieren Sie die folgenden Optionen:

OPTION	BEZEICHNUNG
Neuer Serverbenutzer	Geben Sie den Benutzernamen eines Gruppenadministratorkontos oder den Benutzernamen eines Kontos an, das berechtigt ist, Installationen für die Gruppe auf dem neuen PolicyServer durchzuführen.
Neues Benutzerkennwort	Geben Sie das Kennwort für den Unternehmensadministrator an.
Neue Serveradresse	Geben Sie die neue IP-Adresse oder den neuen Host-Namen für den PolicyServer ein.
Neues Unternehmen	Geben Sie das neue Unternehmen für den PolicyServer an.

5. Klicken Sie auf **Speichern**.

   Full Disk Encryption validiert die neuen Informationen für den PolicyServer.

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

Hinweis

Starten Sie den Full Disk Encryption Agent neu, um den in PolicyServer MMC und Control Manager angezeigten Verschlüsselungsstatus zu aktualisieren.

Full Disk Encryption PolicyServer wechseln

Hinweis

Ein Wechsel des PolicyServer erfordert Zugriff auf die Full Disk Encryption Wiederherstellungskonsole.

Prozedur

1. Starten Sie den Endpunkt oder starten Sie ihn neu.

   Full Disk Encryption Preboot wird angezeigt.

2. Aktivieren Sie das Kontrollkästchen **Wiederherstellungskonsole**.
3. Geben Sie die Anmeldedaten für das Endpoint Encryption Benutzerkonto ein.

Hinweis

Standardmäßig können nur Administrator- und Authentifiziererkonten auf die Wiederherstellungskonsole zugreifen. Um anderen Benutzern Zugriff auf die Wiederherstellungskonsole zu erlauben, aktivieren Sie die Wiederherstellung durch Benutzer über Ihre Management-Konsole.

4. Klicken Sie auf **Anmelden**.

   Die Wiederherstellungskonsole wird geöffnet.
5. Wechseln Sie zu **Netzwerk** > **Setup**.
6. Wählen Sie die Registerkarte **PolicyServer**.
7. Klicken Sie auf **Server wechseln**.
8. Klicken Sie auf **Ja**, wenn die Warnmeldung angezeigt wird.
9. Geben Sie die neue Serveradresse ein.
10. Klicken Sie auf **Speichern**.

WLAN-Einstellungen konfigurieren

WLAN-Einstellungen stehen über die Wiederherstellungskonsole zur Verfügung, auf die über den Full Disk Encryption Preboot zugegriffen werden kann.

Hinweis

Full Disk Encryption Preboot kann nicht automatisch die Authentifizierung für WEP-Sicherheit erkennen. Wenn es sich beim Authentifizierungstyp um WEP-OPEN oder WEP-PSK handelt, geben Sie den Sicherheitstyp manuell an.

Prozedur

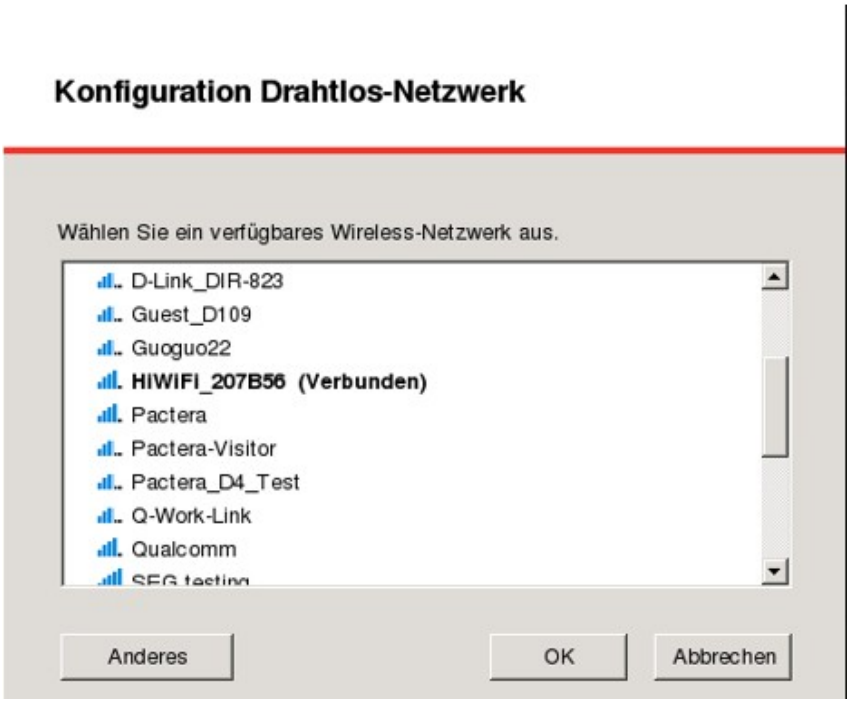
1. Wechseln Sie auf dem Bildschirm **Netzwerk-Setup** zur Registerkarte **WLAN**.

   Der Bildschirm mit den WLAN-Einstellungen wird angezeigt.

   Sie können über den Bildschirm mit den WLAN-Einstellungen die WLAN-Verbindung trennen, indem Sie auf **Verbindung trennen** klicken.

2. Klicken Sie auf **Konfigurieren**, um Ihr WLAN-Netzwerk zu ändern.

Das Fenster **Konfiguration des drahtlosen Netzwerks** wird angezeigt.



3. Wählen Sie Ihr Netzwerk aus.

- Um das aufgeführte Netzwerk zu verwenden, wählen Sie die SSID, und klicken Sie anschließend auf **OK**.
- Um ein nicht aufgeführtes Netzwerk zu konfigurieren, klicken Sie auf **Anderes Netzwerk**, geben Sie die SSID-Einstellungen ein, und klicken Sie anschließend auf **Verbinden**.

Wichtig

Schließen Sie weder das Fenster noch starten Sie Ihren Endpunkt während der Konfiguration neu.

Fehlerbehebung bei Netzwerkproblemen

Die Registerkarten im Fenster **Fehlerbehebung** ermöglichen Ihnen eine eingehendere Untersuchung von Netzwerkproblemen. Die folgenden Registerkarten sind verfügbar:

- **DHCP-Client**: Auf dieser Registerkarte werden die neuesten DHCP-Clientprotokolle angezeigt. Wenn keine DHCP-Anforderung gestellt wurde oder ein Fehler aufgetreten ist, klicken Sie auf **Schnittstelle einrichten**, um Ihre Netzwerkkarte automatisch zu konfigurieren und eine erneute DHCP-Anforderung auszuführen.
- **Traceroute**: Verwenden Sie diese Registerkarte zum Testen Ihrer Netzwerkleistung, indem Sie eine Traceroute zum PolicyServer ausführen. Klicken Sie auf **Traceroute**, um eine neue Traceroute-Anforderung auszuführen.

Recovery-Tool

Das Full Disk Encryption-Recovery-Tool ist ein bootfähiger Datenträger, der zum Reparieren eines Geräts verwendet wird, wenn das Gerät nicht mehr gestartet werden kann. Die aktuelle Version des Recovery-Tools steht im Trend Micro Download Center zum Herunterladen bereit:

http://downloadcenter.trendmicro.com/?regs=DE/

Mit dem Recovery-Tool können Benutzer Folgendes durchführen:

- Überprüfen und Reparieren von Full Disk Encryption-Problemen, aufgrund derer Benutzer sich nicht mehr bei Windows anmelden können
- Öffnen von Full Disk Encryption Preboot, wenn der Agent nicht normal auf Preboot zugreifen kann
- Wiederherstellen von Dateien von einer verschlüsselten Festplatte

Hinweis

In früheren Versionen von Endpoint Encryption war im Lieferumfang des Produkts eine Reparatur-CD enthalten. In Endpoint Encryption 5.0 Patch 4 wurde die Reparatur-CD durch das Recovery-Tool ersetzt.

Recovery-Tool vorbereiten

Das Full Disk Encryption-Recovery-Tool ist eine vorkonfigurierte Linux-Umgebung innerhalb einer ISO-Datei. Um das Recovery-Tool verwenden zu können, installieren Sie es als bootfähige Festplatte auf einer DVD, einem USB-Stick oder einem anderen Wechselmedium.

Das folgende Verfahren enthält ein Beispiel dazu, wie das Recovery-Tool unter Verwendung des kostenlosen Fremdprogramms Rufus auf einem USB-Speichergerät installiert wird.

Prozedur

1. Laden Sie das Full Disk Encryption Installationspaket herunter.

   Die Endpoint Encryption-Installationspakete stehen im Trend Micro Download Center zur Verfügung:

   http://downloadcenter.trendmicro.com/?regs=DE/

2. Laden Sie das Dienstprogramm Rufus herunter und führen Sie es aus.

   Das Dienstprogramm Rufus steht auf der Rufus-Website zur Verfügung:

   http://rufus.akeo.ie/?locale=en_US

3. Schließen Sie ein USB-Speichergerät an den Endpunkt an.

   Warnung!

   Bei diesem Verfahren wird das USB-Gerät neu formatiert und alle Daten werden entfernt. Trend Micro empfiehlt, alle Dateien auf dem USB-Gerät zu sichern, bevor Sie fortfahren.

4. Wählen Sie im Feld **Gerät** das USB-Gerät aus.

5. Wählen Sie unter **Partitionsschema und Typ des Zielsystems** die Option **MBR-Partitionsschema für BIOS oder UEFI-CSM** aus.

6. Wählen Sie die Option **Bootfähigen Datenträger erstellen mithilfe von** und dann die Option **ISO-Image** aus.

7. Klicken Sie auf das Image-Symbol ( ) und wählen Sie das Image `RecoveryTool_x.x.x.xxxx.iso` aus.

   Das Recovery-Tool befindet sich im Full Disk Encryption-Installationspaket.

   Wenn Sie beispielsweise das Paket der TMEE Suite verwenden, befindet sich das Recovery-Tool im folgenden Verzeichnis:

   ```
   <Basispfad>\TMEE Suite\TMEE_Full Disk Encryption-Windows
   \Tools\RecoveryTool\RecoveryTool_x.x.x.xxxx.iso
   ```

8. Klicken Sie auf **Starten**.

9. Wählen Sie im Fenster **ISOHybrid-Image erkannt** eine Option für den Endpunkt aus, auf dem das Tool verwendet wird:

   - Wählen Sie für Endpunkte mit BIOS die Option **Im ISO-Image-Modus schreiben (Empfohlen)** aus und klicken Sie auf **OK**.
   - Wählen Sie für Endpunkte mit UEFI die Option **Im DD-Image-Modus schreiben** aus und klicken Sie auf **OK**.

   Rufus beginnt mit der Neuformatierung des USB-Geräts und installiert das Recovery-Tool darauf.

10. Wenn Rufus mit der Erstellung des bootfähigen Datenträgers fertig ist, schließen Sie das Programm und entfernen Sie das USB-Gerät vom Endpunkt.

Eine Festplatte überprüfen und reparieren

Wenn Sie Windows oder Full Disk Encryption Preboot auf einem Gerät nicht öffnen können, verwenden Sie das Full Disk Encryption Recovery-Tool zur Erkennung und gegebenenfalls zur Reparatur von Problemen auf diesem Gerät. Die folgende Aufgabe setzt voraus, dass das Recovery-Tool bereits auf einer bootfähigen Festplatte installiert wurde.

Prozedur

1. Legen Sie auf dem zu reparierenden Endpunkt die Startreihenfolge so fest, dass von dem Gerät gestartet wird, auf dem das Recovery-Tool installiert wurde.

Wenn Ihr System beispielsweise BIOS verwendet, öffnen Sie das BIOS-Fenster und wählen Sie die Registerkarte **Starten** aus. Wenn Sie ein USB-Speichergerät für das Recovery-Tool verwendet haben, legen Sie **Wechselmedien** als erstes Element in der Startreihenfolge fest.

2. Fahren Sie den Endpunkt herunter.

3. Schließen Sie das Recovery-Tool-Gerät an den Endpunkt an oder legen Sie die Recovery-Tool-CD oder -DVD in das entsprechende Laufwerk ein.

4. Starten Sie den Endpunkt.

   Das Gerät verwendet das Recovery-Tool beim Start. Beim Systemstart öffnet das Recovery-Tool automatisch das Dienstprogramm für die Wiederherstellung und beginnt mit der Überprüfung der Systemfestplatte.

   Wenn ein Problem mit der Systemfestplatte erkannt wird, versucht das Recovery-Tool, dieses Problem zu beheben.

5. Das Recovery-Tool zeigt eine der folgenden Statusangaben an:

   - **FDE-Systemfestplatte erfolgreich repariert**: Die Reparatur wurde erfolgreich durchgeführt und es ist keine weitere Aktion erforderlich.

     Klicken Sie auf **Anzeigen**, um weitere Informationen zu erhalten.

   - **Gerät kann nicht repariert werden**: Das Recovery-Tool benötigt ein Administratorkonto zur Durchführung der Reparatur und zeigt die Option **Umfangreiche Reparatur** an.

     Klicken Sie auf **Umfangreiche Reparatur**, um sich als Administrator anzumelden und eine umfangreiche Reparatur durchzuführen.

     Weitere Informationen finden Sie unter *Verwenden von Umfangreiche Reparatur auf Seite 9-30*.

6. Klicken Sie auf **Herunterfahren**, um den Endpunkt herunterzufahren.

7. Entfernen Sie das Recovery-Tool vom Endpunkt.

8. Starten Sie den Endpunkt.

Bei erfolgreich durchgeführten Reparaturen lädt der Endpunkt das Full Disk Encryption Preboot-Fenster während des Starts.

Verwenden von Umfangreiche Reparatur

Im Recovery-Tool wird der Status **Gerät kann nicht repariert werden** angezeigt, wenn ein Administratorkonto zum Durchführen der Reparatur benötigt wird. Darüber hinaus wird die Option **Umfangreiche Reparatur** zum Fenster hinzugefügt. Beim Klicken auf **Anzeigen** werden Sie auch darüber informiert, dass Sie sich zur Durchführung von Reparaturen authentifizieren müssen.

Prozedur

1. Klicken Sie auf **Umfangreiche Reparatur**.
2. Melden Sie sich mit den folgenden Anmeldedaten bei PolicyServer an:

FELD	BESCHREIBUNG
Benutzername	Geben Sie ein Administratorkonto an. Der Authentifizierer und normale Benutzerkonten dürfen unabhängig von der Richtlinienkonfiguration nicht auf das Recovery-Tool zugreifen.
Kennwort	Geben Sie das Kennwort für diesen Benutzernamen an.
PolicyServer	Geben Sie die PolicyServer-IP-Adresse oder den PolicyServer-Hostnamen an.

FELD	BESCHREIBUNG
Geräte-ID	Geben Sie die Geräte-ID an. Bei Geräten mit Full Disk Encryption 5.0 Patch 4 oder höher versucht das Recovery-Tool, dieses Feld automatisch zu generieren. Wenn die MBR- oder Full Disk Encryption-Datenbank beschädigt ist, kann das Recovery-Tool diese Informationen möglicherweise nicht abrufen. Wenn das Recovery-Tool diese Informationen nicht abrufen kann oder auf dem Gerät Full Disk Encryption 5.0 Patch 3 oder eine frühere Version installiert ist, müssen Sie die Geräte-ID in PolicyServer MMC oder Control Manager suchen und kopieren. In Control Manager können Sie auf die Geräte-ID über das Widget "Bericht 'Full Disk Encryption Status'" zugreifen. Weitere Informationen finden Sie unter *Full Disk Encryption Status auf Seite 4-21*.

Hinweis

Wenn das Recovery-Tool keine Verbindung zu PolicyServer herstellen kann, wird eine Meldung mit einer Aufforderung, Ihr Netzwerk zu konfigurieren, angezeigt. Klicken Sie in diesem Fall auf **Netzwerkstatus und -konfiguration**, um den aktuellen Netzwerkstatus anzuzeigen. Klicken Sie auf **Konfigurieren**, um die Einstellungen für die IP-Adresse des Endpunkts anzugeben. Klicken Sie auf **Verbindung wiederherstellen**, um erneut zu versuchen, eine Verbindung mit PolicyServer herzustellen und Ihre Netzwerkinformationen zu aktualisieren.

3. Das Recovery-Tool führt automatisch weitere Überprüfungen und Reparaturen durch.

   Nach diesem Vorgang wird im Recovery-Tool Folgendes angezeigt: **FDE-Systemfestplatte erfolgreich repariert**.

4. (Optional) Um sicherzustellen, dass sich alle Benutzer nach der Reparatur anmelden können, klicken Sie auf **Erweiterte Funktionen** und dann auf **Alle Benutzer zwischenspeichern**.

   Der Benutzer wird in einer Benachrichtigung darüber informiert, dass alle Benutzerkonten erfolgreich zwischengespeichert wurden.

   Weitere Informationen zur Verfügbarkeit erweiterter Funktionen finden Sie unter *Erweiterte Funktionen auf Seite 9-33*.

5. (Optional) Wenn Sie Protokolle zur weiteren Fehlerbehebung sammeln müssen, klicken Sie auf **Start** > **CDT-Sammlung**, um das Case Diagnostic Tool auszuführen.

   Das Recovery-Tool speichert die gesammelten Protokolle auf dem USB-Laufwerk und zeigt nach Abschluss der Sammlung eine Benachrichtigung an.

6. Klicken Sie auf **Herunterfahren**, um den Endpunkt herunterzufahren.

7. Entfernen Sie das Recovery-Tool vom Endpunkt.

8. Starten Sie den Endpunkt.

   Bei erfolgreich durchgeführten Reparaturen lädt der Endpunkt das Full Disk Encryption Preboot-Fenster während des Starts.

Optionen des Recovery-Tools

Das Full Disk Encryption-Recovery-Tool öffnet ein Linux-Betriebssystem, in dem folgende Optionen verfügbar sind:

Optionen	Beschreibung
Recovery	Wählen Sie diese Option aus, um das Hauptdienstprogramm des Recovery-Tools zu öffnen. Dieses Dienstprogramm überprüft das Gerät und versucht, es zu reparieren. Nach der Überprüfung werden zusätzliche Funktionen für den Zugriff auf Full Disk Encryption Preboot und die Anzeige von verschlüsselten Dateien auf der Festplatte verfügbar. **Hinweis** Das Recovery-Tool erfordert möglicherweise zusätzliche Informationen von PolicyServer, um das Gerät vollständig zu reparieren. Nach einer ersten Überprüfung verlangt das Recovery-Tool möglicherweise, dass Sie sich bei PolicyServer authentifizieren. Vergewissern Sie sich vor dem Verwenden des Recovery-Tools, dass das Netzwerk verfügbar ist. Das Recovery-Tool unterstützt Ethernet-Kabelverbindungen.

OPTIONEN	BESCHREIBUNG
Zoom	Wählen Sie diese Option aus, um den Videokonferenzdienst Zoom zu öffnen. Der Support von Trend Micro fordert Sie möglicherweise dazu auf, diesen Dienst zum Teilen Ihres Bildschirms zu verwenden, sodass der Support-Mitarbeiter Sie besser bei der Durchführung notwendiger Aufgaben unterstützen kann. **Hinweis** Die Verwendung von Zoom erfordert Zugriff auf das Internet.
Spracheingabe	Das Recovery-Tool unterstützt die Eingabe in mehreren Sprachen. Navigieren Sie zu **Start** > **Spracheingabe** und wählen Sie die Sprache für Ihre Tastatur aus.
Herunterfahren/Neu starten	Navigieren Sie zum Herunterfahren oder Neustarten des Endpunkts zu **Start** > **Herunterfahren** und wählen Sie entweder **Herunterfahren** oder **Neu starten** aus.

Erweiterte Funktionen

Nachdem das Recovery-Tool das Durchsuchen und den Versuch der Reparatur des Geräts abgeschlossen hat, enthält der Abschlussbildschirm die Optionen **Erweiterte Funktionen** und **Herunterfahren**. Klicken Sie auf **Erweiterte Funktionen**, um abhängig von den auf dem Gerät installierten Festplattentypen ein Fenster mit einer oder mehreren Optionen anzuzeigen.

Hinweis

Für den Zugriff auf den Bildschirm **Erweiterte Funktionen** ist eine Authentifizierung erforderlich. Weitere Informationen zum Durchsuchen, Reparieren und Authentifizieren finden Sie unter *Eine Festplatte überprüfen und reparieren auf Seite 9-28*.

Für Standardfestplatten (keine selbstverschlüsselnde Festplatte) stehen folgende Optionen zur Verfügung:

- **Dateiexplorer starten**: Klicken Sie auf diese Option, um ein Fenster mit dem Dateiverzeichnis zu öffnen. Sie können Dateien von Ihrer Festplatte auf externe Speichergerät kopieren. Das Recovery-Tool entschlüsselt diese Dateien, bevor sie zum externen Gerät hinzugefügt werden.

  Hinweis

  Trend Micro empfiehlt, die wichtigsten Dateien auf diese Weise zu sichern. Die Entschlüsselung mit dieser Funktion dauert möglicherweise lange. Wenn Sie also alle Dateien auf dem Laufwerk entschlüsseln und kopieren möchten, entschlüsseln Sie stattdessen das gesamte Laufwerk mit der Wiederherstellungskonsole.

- **Preboot aktivieren**: Klicken Sie auf diese Option, um den Endpunkt zum Öffnen von Full Disk Encryption Preboot beim nächsten Neustart mit dem Recovery-Tool festzulegen. Das Recovery-Tool enthält eine interne Kopie von Full Disk Encryption Preboot, mit der Sie auf die Wiederherstellungskonsole zugreifen und Netzwerkeinstellungen konfigurieren oder das Gerät entschlüsseln können.
- **Alle Benutzer zwischenspeichern**: Klicken Sie auf diese Option, um Authentifizierung ohne Verbindung zum PolicyServer zuzulassen. Wenn nach einer Reparaturaufgabe am Endpunkt Netzwerkverbindungsprobleme auftreten, können Benutzer weiterhin das korrekte Kennwort eingeben, um sich ohne Herstellung einer Verbindung zum PolicyServer zu authentifizieren.

Für selbstverschlüsselnde Festplatten (SED) steht folgende Option zur Verfügung:

- **SED entsperren**: In der Wiederherstellungskonsole wird je nach Festplattenkonfiguration eine der folgenden Aktionen durchgeführt:
  - Handelt es sich bei der SED-Festplatte um eine Systemfestplatte, entfernt die Wiederherstellungskonsole den Full Disk Encryption Preboot von der Festplatte, sodass das Gerät nicht mehr bei PolicyServer authentifiziert werden muss.
  - Handelt es sich bei der SED-Festplatte um eine Datenfestplatte, schließt die Wiederherstellungskonsole die Festplatte von der Verwaltung durch Full Disk Encryption aus.

Hinweis

Wenn das Gerät eine selbstverschlüsselnde Festplatte als Systemfestplatte verwendet und die Option **Erweiterte Funktionen** nicht verfügbar ist, fahren Sie das Gerät herunter und verwenden Sie das Recovery-Tool zum erneuten Starten des Geräts.

Dateiexplorer verwenden

Im folgenden Beispiel wird dargestellt, wie der im Recovery-Tool enthaltene Dateiexplorer zum Kopieren lokaler Dateien auf ein externes Speichergerät verwendet wird.

Prozedur

1. Nachdem das Recovery-Tool die Überprüfung und den Versuch, das Gerät zu reparieren, abgeschlossen hat, klicken Sie im Fenster **Erweiterte Funktionen** auf **Dateiexplorer starten**.

   Das Dateiexplorer-Fenster wird angezeigt.

2. Wählen Sie die zu kopierenden Dateien oder Ordner aus.

3. Klicken Sie mit der rechten Maustaste auf die zu kopierenden Dateien oder Ordner und wählen Sie im Kontextmenü die Option **Kopieren** aus.

   Alternativ können Sie zum Kopieren der ausgewählten Dateien **STRG+C** drücken.

4. Schließen Sie ein externes Speichergerät an den Endpunkt an.

   Der Dateiexplorer zeigt eine neue untergeordnete Struktur für das zuletzt angeschlossene Speichergerät an.

5. Navigieren Sie zum externen Speichergerät und suchen Sie einen Zielordner.

6. Klicken Sie mit der rechten Maustaste in einen leeren Bereich im Fenster für den Zielordner und wählen Sie im Kontextmenü die Option **Einfügen** aus.

   Alternativ können Sie zum Einfügen der ausgewählten Dateien **STRG+V** drücken.

   Der Dateiexplorer fügt die zuvor kopierten Dateien in den Zielordner ein.

Hinweis

Das Recovery-Tool entschlüsselt Dateien, bevor sie auf dem externen Gerät hinzugefügt werden. Die Entschlüsselung mit dieser Funktion nimmt möglicherweise viel Zeit in Anspruch. Wenn Sie alle Dateien auf dem Laufwerk entschlüsseln und kopieren möchten, besteht eine mögliche Alternative darin, mithilfe der Wiederherstellungskonsole das gesamte Laufwerk zu entschlüsseln.

Unterstützung durch Remote-Hilfe

Mit Hilfe von Remote-Hilfe können Benutzer ein vergessenes Kennwort oder ein gesperrtes Konto zurücksetzen. Jeder Endpoint Encryption Benutzer mit einem gesperrten Konto oder vergessenen Kennwort muss das Kennwort zurücksetzen, bevor er sich wieder bei einem Endpoint Encryption Gerät anmelden kann. Remote-Hilfe setzt voraus, dass der Benutzer beim Helpdesk eine Herausforderungsantwort anfordert. Für die Remote-Hilfe ist keine Netzwerkverbindung zu PolicyServer erforderlich.

Prozedur

1. Melden Sie sich bei PolicyServer MMC mit einem beliebigen Konto mit Gruppenadministrator-Berechtigungen aus derselben Richtliniengruppe wie der Benutzer an.
2. Fordern Sie den Benutzer auf, vom Endpoint Encryption Agent aus zu **Hilfe** > **Remote-Hilfe** zu navigieren.
3. Fragen Sie den Benutzer nach der **Geräte-ID**.

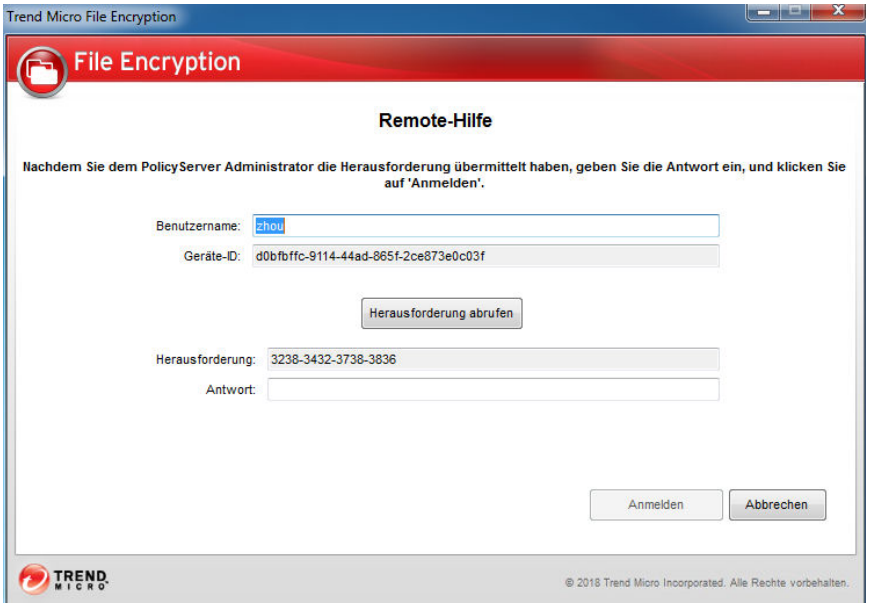


ABBILDUNG 9-2. Unterstützung durch Remote-Hilfe

4. Öffnen Sie in PolicyServer MMC die Option **Unternehmen - Geräte**, oder erweitern Sie die Gruppe des Benutzers, und öffnen Sie **Geräte**.

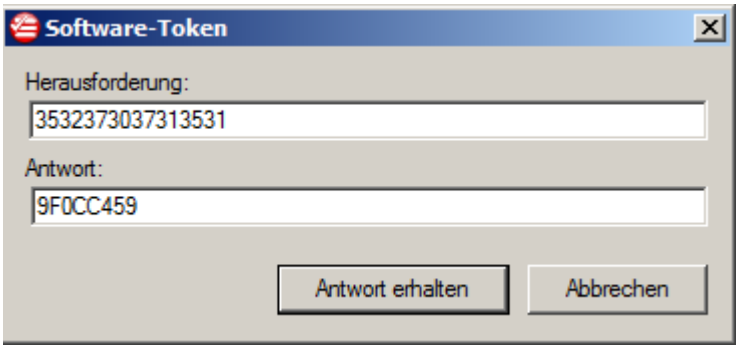
5. Klicken Sie im rechten Fenster mit der rechten Maustaste auf das Benutzergerät, und wählen Sie **Software-Token** aus.

   Das Fenster **Soft-Token** wird angezeigt.

6. Fragen Sie den Benutzer nach dem aus 16 Ziffern bestehenden Herausforderungscode, und geben Sie ihn in das Feld **Herausforderung** im Fenster **Software-Token** ein.

7. Klicken Sie auf **Antwort erhalten**.

Das Feld **Antwort** wird mit einer aus 8 Zeichen bestehenden Zeichenfolge geladen.



8. Teilen Sie dem Benutzer die aus 8 Zeichen bestehende Zeichenfolge über das Feld **Antwort** mit.
9. Der Benutzer gibt die Zeichenfolge im Feld **Antwort** am Endpunkt ein und klickt auf **Anmelden**.
10. Der Benutzer muss ein neues Kennwort eingeben.

Kapitel 10

Behobene und bekannte Probleme

In diesem Abschnitt werden behobene Endpoint Encryption-Probleme und die verbleibenden Probleme und Einschränkungen beschrieben.

Behobene Probleme

In diesem Abschnitt werden die früheren Endpoint Encryption-Probleme beschrieben, die bereits behoben wurden.

Behobene Probleme in Endpoint Encryption 6.0

	Problem	Lösung
1	Die Ladezeit vom Boot- zum Preboot-Fenster kann bei bestimmten Endpunkten über 5 Minuten in Anspruch nehmen.	In dieser Version wurden Verbesserungen vorgenommen, damit das Full Disk Encryption Preboot-Fenster schneller geladen wird.
2	Probleme beim Skalieren von Fenstern auf HD- und UltraHD-Displays führen möglicherweise dazu, dass die Seiten und Zeichenfolgen des Anmeldefensters für Full Disk Encryption Preboot zu klein angezeigt werden.	In dieser Version wurde das Problem behoben, indem das Fenster "Full Disk Encryption Preboot" mit einer festen Auflösung versehen wurde.
3	Die Preboot-Authentifizierung ist langsam, wenn auf PolicyServer nicht zugegriffen werden kann.	In dieser Version wurden Verbesserungen an der Netzwerkverbindungsstruktur von Full Disk Encryption Preboot vorgenommen.
4	Das PolicyServer-Fenster "Geräteverwaltung" zeigt für selbstverschlüsselnde Laufwerke den Status "Nicht verschlüsselt" an.	In dieser Version wurde das Problem mit dem Status "Nicht verschlüsselt", der im PolicyServer-Fenster "Geräteverwaltung" für selbstverschlüsselnde Laufwerke angezeigt wurde, behoben.
5	Die WLAN-Verbindung kann für manche Endpunkte bei Full Disk Encryption Preboot keine Verbindung zu PolicyServer herstellen.	In dieser Version wurde durch Verbesserungen an Full Disk Encryption Preboot sichergestellt, dass die WLAN-Verbindung erfolgreich eine Verbindung zu PolicyServer herstellt.

	Problem	Lösung
6	Beim Kennwortsynchronisierungs-Tool von Full Disk Encryption treten Probleme auf, wenn mit Full Disk Encryption Agents der Version 6.0 gearbeitet wird.	Das Kennwortsynchronisierungs-Tool von Full Disk Encryption unterstützt Endpoint Encryption 5.0 und 6.0 Agents.
7	Beim Support-Tool von Full Disk Encryption treten Probleme auf, wenn mit Full Disk Encryption Agents der Version 6.0 gearbeitet wird.	Das Support-Tool von Full Disk Encryption unterstützt Endpoint Encryption 5.0 und 6.0 Agents.

Behobene Probleme in Endpoint Encryption 6.0 Update 1

	Problem	Lösung
1	PolicyServer kann das Upgrade auf Version 6.0 nicht abschließen, wenn bei der Verbindung zur Datenbank Zeitüberschreitungsfehler auftreten.	Das Problem wurde in dieser Version behoben, indem die Zeitüberschreitungseinstellung auf 600 Sekunden festgelegt wurde.
2	Das an Control Manager gesendete Protokoll mit dem PolicyServer-Aktualisierungsstatus enthält möglicherweise Zeichenfolgen, die nicht als gültige Datums-/Uhrzeitformate erkannt werden, wodurch Control Manager falsche Richtlinien- und Gerätestatusinformationen anzeigt.	Diese Version enthält Verbesserungen für die Analyse von Datums-/Uhrzeitwerten.
3	Domänenanmeldung schlägt fehl, wenn die Standardkennwortrichtlinie nicht abgerufen werden kann.	In dieser Version wurde die Verarbeitung von Nullausnahmen verbessert.
4	Wenn der Anwendungspool für die Aktivierung von 32-Bit-Anwendungen eingerichtet ist, funktioniert die automatische Porterkennung nicht.	Diese Version bietet Unterstützung für Anwendungspools, die 32-Bit-Anwendungen in X64-Systemen ausführen.

	PROBLEM	LÖSUNG
5	Bei Verwendung einer Encryption Management for Apple FileVault (Build 6.0.0.1033)-PKG-Datei mit abgelaufenem Zertifikat können während der Installation Probleme auftreten.	In dieser Version wird das Zertifikat für die PKG-Installationsdatei aktualisiert.
6	Das Trend Micro Endpoint Encryption Verteilungstool (Build 6.0.0.1087) konnte auf OfficeScan XG nicht erfolgreich installiert oder aktualisiert werden.	In dieser Version (6.0.0.2005) wurde das AU-Modul aktualisiert, um Probleme in Zusammenhang mit der Verifizierung von SSL-Zertifikaten zu beheben.

Bekannte Probleme

In diesem Abschnitt werden die Probleme und Einschränkungen von Endpoint Encryption, gruppiert nach Agent oder Konsole, beschrieben.

Probleme in Verbindung mit PolicyServer MMC

Im Folgenden werden Probleme und Einschränkungen in Verbindung mit PolicyServer MMC aufgeführt:

1. Wenn ein Domänenbenutzer die Rolle Unternehmensadministrator oder Unternehmensauthentifizierer innehat, wird kein Eintrag im Ereignisprotokoll erstellt, falls die Synchronisierung mit Active Directory fehlschlägt.

2. PolicyServer MMC kann nicht Informationen für mehrere Unternehmen anzeigen. PolicyServer kann nur das erste in PolicyServer MMC eingegebene Unternehmen anzeigen.

3. Berechtigungsprobleme verhindern möglicherweise die direkte Aktualisierung von PolicyServer 5.0.0.3506 auf 6.0. Zur Vermeidung dieses Problems erteilen Sie dem Datenbankbenutzerkonto von PolicyServer vor der Aktualisierung auf 6.0 die Berechtigung "db_ddladmin" oder aktualisieren Sie PolicyServer zuerst auf 5.0.0.3793 und dann auf 6.0.

4. Während des Preboots erzeugt Full Disk Encryption die Meldungs-ID "10029" (Erfolgreiche Anmeldung mit festem Kennwort), wenn ein Benutzer über ein Domänenkennwort authentifiziert ist. Zur Unterscheidung zwischen fester Kennwortauthentifizierung und Domänenauthentifizierung weist Full Disk Encryption die Meldungs-ID "100057" für Domänenauthentifizierung zu.

5. Die Endpoint Encryption 5.0 MMC-Konsole kann neue in Endpoint Encryption 6.0 hinzugefügte Richtlinien nicht ordnungsgemäß anzeigen. Aktualisieren Sie zur Vermeidung dieses Problems die Endpoint Encryption MMC von 5.0 auf 6.0, nachdem PolicyServer aktualisiert wurde.

6. Die Zeitfilterfunktion in Protokollereignissen zeigt falsche Ergebnisse an, wenn die Endpoint Encryption 6.0 MMC eine Verbindung zu einer 6.0-Betaversion von PolicyServer herstellt. Aktualisieren Sie zur Behebung dieses Problems sowohl den PolicyServer als auch die Endpoint Encryption MMC auf die Version 6.0.

7. Control Manager und die Endpoint Encryption MMC zeigen vor dem Neustart des Geräts einen falschen Verschlüsselungsstatus für das Gerät an, nachdem es in ein neues Unternehmen migriert wurde. Control Manager und die Endpoint Encryption MMC sollten nach dem Neustart des Geräts den richtigen Verschlüsselungsstatus anzeigen.

8. Im Bericht **Warnung zur Protokollintegrität** werden Protokollereignisse aus der PolicyServer 6.0-Betaversion möglicherweise als Ereignisse mit „gefährdeter Integrität“ angezeigt. Protokollereignisse aus der Version 5.0 oder 6.0 von PolicyServer sollten ordnungsgemäß gemeldet werden.

Probleme bei der Integration von Control Manager

Im Folgenden werden Probleme und Einschränkungen in Verbindung mit Control Manager aufgeführt:

1. Nach der Verteilung einer neuen Richtlinie von Control Manager auf PolicyServer wird eine neue Richtliniengruppe nicht sofort in PolicyServer MMC angezeigt. Um die neue Richtliniengruppe zu sehen, melden Sie sich von PolicyServer MMC ab und wieder an.

2. Benutzer können nicht zur Richtlinie hinzugefügt werden, wenn der Benutzerbereich in der Richtlinienverwaltung von Control Manager deaktiviert ist.

3. Beim Löschen einer Richtlinie, die in Control Manager erstellt wurde, wird die Richtlinie nicht von PolicyServer entfernt. Die Richtlinie kann nach wie vor in PolicyServer MMC angezeigt werden.

Probleme mit dem Plug-in des Endpoint Encryption Verteilungstools

Im Folgenden werden Probleme und Einschränkungen in Verbindung mit dem Plug-in des Endpoint Encryption Verteilungstools aufgeführt:

1. Wenn der OfficeScan Administrator versucht, Servereinstellungen über ein Benutzerkonto von Endpoint Encryption auf PolicyServer zu verteilen, wird eine Fehlermeldung angezeigt, dass die Verbindung nicht erfolgreich war.
2. Der Plug-in Manager zeigt keine Fehlermeldung an, wenn das Plug-in für das Endpoint Encryption Verteilungstool auf einem Server installiert wird, der die Mindestsystemanforderung von 1 GB freiem Festplattenspeicher nicht erfüllt.
3. Das Endpoint Encryption Gerät erscheint möglicherweise weiterhin in Plug-in Manager, auch wenn der Endpoint Encryption Agent deinstalliert wurde. Agents werden das nächste Mal, wenn PolicyServer mit OfficeScan synchronisiert wird und der Bildschirm des Plug-In Managers aktualisiert wird, nicht mehr angezeigt.
4. Benutzer von Endpoint Encryption mit einem Einmalkennwort können Agents mit dem Plug-in des Endpoint Encryption-Verteilungstools nur einmal verteilen. Alle weiteren Verteilungen schlagen fehl. Nach der ersten Verteilung muss der Benutzer vor der erneuten Verteilung ein festes Kennwort festlegen.
5. Wenn der Deinstallationsbefehl von OfficeScan auf Full Disk Encryption Geräte verteilt wird, wird die Meldung „Anforderung zu Deinstallation des Agents erfolgreich“ angezeigt, bevor die Deinstallation abgeschlossen wurde. Endpoint Encryption entschlüsselt den Endpunkt, bevor die Deinstallation abgeschlossen wurde.

Probleme von Full Disk Encryption

Im Folgenden werden Probleme und Einschränkungen in Verbindung mit Full Disk Encryption aufgeführt.

1. Die Anmeldung beim Full Disk Encryption Preboot kann möglicherweise Leistungseinbußen erleiden, wenn der WLAN-Adapter mit einem Zugangspunkt ohne Netzwerkzugriff auf PolicyServer verbunden ist.

   Dieses Problem tritt auf, wenn die IP-Adresse von PolicyServer bei der Installation von Full Disk Encryption verwendet wurde. Verwenden Sie während der Installation den FQDN von PolicyServer, um das Problem zu beheben.

2. Die WLAN-Funktion von Full Disk Encryption kann Zugangspunkte, die WEP-Verschlüsselung mit gemeinsamem Schlüssel verwenden, nicht automatisch erkennen.

   Geben Sie manuell den Sicherheitstyp WEP-OPEN oder WEP-PSK an.

3. Der Full Disk Encryption Preboot kann sich nicht bei Windows 8, 8.1 oder 10 anmelden, wenn es auf einer virtuellen Maschine über VMWare Workstation mit aktiviertem e1000e Ethernettreiber installiert ist.

   Der e1000e Ethernettreiber ist der Standardtreiber für Windows 8 und 8.1. Full Disk Encryption unterstützt den e1000e Ethernettreiber nicht.

   Um dieses Problem zu beheben, ändern Sie den Treiber in e1000:

   a. Fahren Sie VMWare Workstation herunter.

   b. Öffnen Sie in einem Texteditor die Datei `vmware.vmx`.

   c. Suchen Sie nach folgender Treiberzeile:

      ```
      ethernet0.virtualDev = "e1000e"
      ```

   d. Ändern Sie `"e1000e"` in `"e1000"`.

   e. Speichern Sie die Datei und starten Sie die virtuelle Maschine neu.

4. Full Disk Encryption zeigt eine Fehlermeldung an und kann das System nicht sperren, wenn die Richtlinie „LockDeviceTimeDelay“ auf 999999 Minuten eingestellt ist.

5. Full Disk Encryption kann sich nicht per Single Sign-On anmelden, wenn der Endpunkt aus dem Ruhezustand zurückgeholt wird.

6. Wenn sich ein Benutzer bei Full Disk Encryption anmeldet, zeigt das Task-Leistensymbol den korrekten Benutzernamen. Wenn sich jedoch der Benutzer

abmeldet, nachdem der Endpunkt im Ruhezustand war, und sich ein anderer Benutzer anmeldet, wird weiterhin der vorherige Benutzername angezeigt. Die Benutzerdaten sind nicht gefährdet.

7. Toshiba Tecra-Computer mit selbstverschlüsselnden Laufwerken können Windows nach der Installation von Full Disk Encryption nicht ausführen.

8. Full Disk Encryption Preboot unterstützt bei Verwendung des spanischen Tastaturlayouts keine Kombinationen aus Zeichen mit der „Alt Gr“-Taste.

9. Full Disk Encryption Preboot kann die Num-Tastenanzeige bei einigen HP-Laptops nicht steuern. In diesen Fällen kann die Num-Tastenanzeige in den BIOS-Einstellungen konfiguriert werden.

10. Die Installation zusammen mit Drittanbieter-Produkten zur Verschlüsselung kompletter Festplatten wird von Full Disk Encryption nicht unterstützt. Wenn mehrere Verschlüsselungsprodukte auf demselben Endpunkt installiert werden, kann der Endpunkt möglicherweise Windows nicht starten und verursacht einen blauen Fehlerbildschirm.

11. Das Full Disk Encryption-Recovery-Tool stößt bei der Anmeldung bei Zoom über Single Sign-On oder bei Verwendung von Google- oder Facebook-Konten möglicherweise auf Fehler.

    Um dieses Problem zu vermeiden, verwenden Sie nur Zoom, um sich mit Besprechungen zu verbinden, die durch den Support von Trend Micro gehostet werden. Versuchen Sie nicht, Besprechungen über das Recovery-Tool zu hosten.

12. Full Disk Encryption ist nicht mit Dell Latitude E5420 kompatibel, wenn die Startkonfiguration auf UEFI gesetzt ist. Um Full Disk Encryption auf diesem Endpunkt zu verwenden, setzen Sie die Startkonfiguration auf BIOS.

13. Full Disk Encryption kann auf dem HP Probook 6570b und HP EliteBook Folio 9470m nicht installiert werden, wenn die Startkonfiguration für diese Endpunkte auf UEFI gesetzt ist. Um eine erfolgreiche Installation sicherzustellen, setzen Sie die Startkonfiguration vor der Installation auf BIOS.

14. Das Installationsprogramm von Full Disk Encryption kann kein Upgrade von älteren Full Disk Encryption Versionen auf Geräten durchführen, auf denen die Systemfestplatte mehr als 8 erweiterte Partitionen enthält. Um ein Upgrade dieser Geräte auf die Version 6.0 durchzuführen, deinstallieren Sie zunächst die alte Version und führen dann stattdessen eine Neuinstallation durch.

15. Full Disk Encryption zeigt möglicherweise eine falsche Prozentzahl der Fertigstellung an, wenn sich der Wert der Einstellung **Verschlüsselungsrichtlinie** während der Verschlüsselung ändert. Um dieses Problem zu beheben, entschlüsseln Sie die gesamte Festplatte und verschlüsseln Sie sie erneut.

16. Eine Festplattenkonvertierung von MBR in GPT kann nicht bei einer Festplatte durchgeführt werden, die von Full Disk Encryption verwaltet wird. Um eine verwaltete Festplatte von MBR in GPT zu konvertieren, entschlüsseln Sie zunächst die gesamte Festplatte und trennen Sie dann die Festplatte von Full Disk Encryption. Führen Sie danach die Festplattenkonvertierung wie gewohnt durch.

17. Während des Preboots wird im Fenster **Konfiguration des Kabelnetzwerks** die verborgene SSID **\x00\x00\x00\x00\x00\x00\x00\x00** angezeigt.

18. In seltenen Fällen werden Sektoren beschädigt, wenn die Stromversorgung beim Verschlüsseln unterbrochen wird. Stellen Sie zur Vermeidung dieses Problems sicher, dass das Stromkabel während der erstmaligen Verschlüsselung von Full Disk Encryption angeschlossen ist.

19. Mehrere vom selben Gerät ausgegebene Meldungen mit dem Inhalt **Geräteverschlüsselung abgeschlossen** werden im Audit-Protokoll für einen bestimmten Zeitraum angezeigt. Der Grund hierfür besteht darin, dass Full Disk Encryption für PolicyServer jedes Mal dann eine Meldung mit dem Inhalt "Verschlüsselung abgeschlossen" für verschlüsselte Festplatten erstellt, wenn der Full Disk Encryption Dienst neu gestartet wird, um sicherzustellen, dass der Verschlüsselungsstatus auf dem Server auf dem neuesten Stand ist.

20. Full Disk Encryption ist nicht kompatibel mit PLEXTOR PX-128M5 Pro (alte Firmware). Der Verschlüsselungsstatus der Festplatte wird als (**NaN%**) angezeigt, wenn die Verschlüsselung beginnt.

21. Full Disk Encryption fragt in der Regel DNS-Suffixe aus Windows ab und wendet sie in Preboot an. Full Disk Encryption verwendet jedoch nur das erste gefundene DNS-Suffix. Zur Reduzierung von Problemen stellen Sie sicher, dass das bevorzugte DNS-Suffix als erstes DNS-Suffix in Windows festgelegt ist.

22. Full Disk Encryption kennzeichnet die Netzwerkinformationsanzeige von Windows XP-VMware-Images unter Umständen fälschlicherweise mit einem (X). Hierbei handelt es sich jedoch nur um ein Anzeigeproblem. Die Netzwerkverbindung ist nicht betroffen.

23. Während des Preboots reagiert das Touchpad eines Acer V3-372 ASUS BU400A-Computers möglicherweise nicht mehr. Ändern Sie zur Behebung dieses Problems die Touchpad-Einstellung in der Firmware von **Erweitert** in **Grundlegend** oder verwenden Sie eine externe USB-Maus.

24. Bei der Verteilung von Full Disk Encryption mithilfe des Endpoint Encryption Verteilungstool-Plug-ins werden in diesem Plug-in keine Ergebnisse der Sicherheitsüberprüfung (eine neue Funktion von Full Disk Encryption in 6.0) angezeigt. Zur Umgehung dieses Problems können Administratoren die Ergebnisse der Sicherheitsüberprüfung manuell über Control Manager oder die Endpoint Encryption MMC-Konsole prüfen.

25. In Full Disk Encryption treten bei Installation auf einem ASUS BU400A-Computer, der eine UEFI SED-Konfiguration verwendet, möglicherweise Probleme auf. Dies führt dazu, dass die Firmware den Starteintrag löscht, nachdem das Gerät in Windows gestartet wurde, wodurch das Entsperren des selbstverschlüsselnden Laufwerks nach dem erneuten Einschalten des Geräts erschwert wird. Wechseln Sie zur Reduzierung von Problemen zu BIOS mit SED-Konfiguration oder zu UEFI mit normaler Festplattenkonfiguration. Wenn das selbstverschlüsselnde Laufwerk nicht entsperrt werden kann, können Administratoren das Recovery-Tool zum Entsperren des Laufwerks nach der Authentifizierung verwenden.

26. Aus Control Manager verteilte WLAN SSID-Einstellungen bieten keine Unterstützung für spitze Klammern (< >). Entfernen Sie spitze Klammern aus den WLAN SSID-Einstellungen.

27. Das Fenster für die Preboot-Authentifizierung benötigt 50 Sekunden zum Laden von HP Elite X2 1012 G1, Acer Aspire V 13 V3-372-55KU und Microsoft Surface Pro 4. Innerhalb dieses Zeitraums ist es auch möglich, dass der Cursor 30 Sekunden lange nicht blinkt. Dieses Problem wird in einer zukünftigen Version behoben.

28. Full Disk Encryption Preboot bietet keine Unterstützung für den Netzwerkport des Microsoft Surface Dock. Full Disk Encryption Preboot bietet jedoch Unterstützung für das auf Surface Pro 3 und Surface Pro 4 gefundene integrierte WLAN. Um eine Verbindung zu PolicyServer herzustellen, konfigurieren Sie Full Disk Encryption Preboot zur Verwendung des integrierten WLAN.

29. Die Installation von Full Disk Encryption kann möglicherweise dazu führen, dass der Endpunkt zur Rückkehr aus dem Ruhezustand mehr Zeit benötigt. Die Rückkehr aus dem Ruhezustands dauert durchschnittlich höchstens 80 Sekunden für BIOS-konfigurierte Endpunkte und 30 Sekunden für UEFI-konfigurierte Endpunkte.

30. Nach der Ausführung eines Warmstarts auf Microsoft Surface Pro 4 Type Cover reagieren Tastatur und Touchpad beim Preboot nicht mehr. Tastatur und Touchpad auf Microsoft Surface Pro 4 Typ Cover funktionieren in Preboot ordnungsgemäß, wenn der Endpunkt mithilfe eines Kaltstarts gestartet wird.

31. Wenn die Full Disk Encryption Datenbank einer Datenfestplatte beschädigt ist, kann in Windows nicht mehr auf die Datenfestplatte zugegriffen werden. Verwenden Sie zur Behebung dieses Problems das Full Disk Encryption Recovery-Tool. Das Full Disk Encryption Recovery-Tool meldet die Festplatte als "Keine FDE-Festplatte", repariert aber weiterhin die Datenbank auf der Datenfestplatte. Sollte das Problem weiterhin bestehen, wenden Sie sich zur Wiederherstellung der Daten an den Support von Trend Micro.

Probleme mit File Encryption

Im Folgenden werden Probleme und Einschränkungen in Verbindung mit Full Disk Encryption aufgeführt.

1. Wenn Sie versuchen, Dateien oder Ordner in einem verschlüsselten Ordner zu löschen, gibt Windows folgende Fehlermeldung aus: „Die Quelldatei oder vom Quelldatenträger kann nicht gelesen werden.“

   Dieser Fehler tritt auf, da File Encryption nicht in der Lage ist, gelöschte Dateien und Ordner in einem verschlüsselten Ordner in den Papierkorb zu verschieben. Um Dateien und Ordner in einem verschlüsselten Ordner zu löschen, verwenden Sie den permanenten Löschbefehl Umschalt+Entf.

2. File Encryption unterstützt keine Fragen und Antworten zu "Selbsthilfe". Bei der Registrierung sollten Selbsthilfe-Fragen angezeigt werden, wenn der Endpoint Encryption Benutzer zum Fenster "Kennwort ändern" navigiert.

3. Nach dem Upgrade von PolicyServer und File Encryption von 3.1.3 SP1 auf 5.0 können Richtlinien nicht synchronisiert werden, wenn der File Encryption 3.1.3 Agent Port 8080 (TMEE-Dienst) während der Registrierung verwendet.

4. Nach dem Upgrade von PolicyServer und File Encryption von 3.1.3 SP1 auf 5.0 ist die Authentifizierung auf dem Bildschirm "Kennwort ändern" gesperrt, wenn der File Encryption 3.1.3 Agent Port 8080 (TMEE-Dienst) während der Registrierung verwendet.
5. Nach der Deinstallation von File Encryption ohne Neustart des Endpunkts wird das Programm nicht automatisch aus der Liste in "Programme hinzufügen/ entfernen" entfernt.
6. Der rechtliche Hinweis wird beim Start des Endpunkts nicht angezeigt.
7. Die Desktop-Verknüpfung des File Encryption Agent und das Agent-Symbol blinken, wenn der File Encryption Agent eine Synchronisierung mit PolicyServer durchführt.

Probleme bei Encryption Management for Microsoft BitLocker

Es sind keine Probleme bei Encryption Management for Microsoft BitLocker in dieser Version bekannt.

Probleme bei Encryption Management for Apple FileVault

Es sind keine Probleme bei Encryption Management for Microsoft BitLocker in dieser Version bekannt.

Kapitel 11

Technischer Support

Erfahren Sie mehr über die folgenden Themen:

Ressourcen zur Fehlerbehebung

Vor der Kontaktaufnahme mit dem technischen Support sollten Sie die folgenden Online-Ressourcen zu Trend Micro heranziehen.

Support-Portal verwenden

Über das Trend Micro Support-Portal können Sie rund um die Uhr online auf die aktuellsten Informationen über allgemeine und ungewöhnliche Probleme zugreifen.

Prozedur

1. Gehen Sie zu http://esupport.trendmicro.com.
2. Wählen Sie unter den verfügbaren Produkten aus oder klicken Sie auf die entsprechende Schaltfläche, um nach Lösungen zu suchen.
3. Mit dem Feld **Support durchsuchen** können Sie nach verfügbaren Lösungen suchen.
4. Falls Sie keine Lösung finden, klicken Sie auf **Support kontaktieren** und wählen Sie den gewünschten Support aus.

   Tipp

   Um online eine Supportanfrage zu senden, besuchen Sie die folgende URL:

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

   Das Problem wird von einem Support-Mitarbeiter von Trend Micro untersucht, der innerhalb von 24 Stunden oder weniger auf Ihre Anfrage reagiert.

Bedrohungsenzyklopädie

Die meiste Malware besteht heutzutage aus komplexen Bedrohungen, bei denen zwei oder mehr Technologien miteinander kombiniert werden, um Computer-

Sicherheitsprotokolle zu umgehen. Trend Micro bekämpft diese komplexe Malware mit Produkten, die eine benutzerdefinierte Verteidigungsstrategie verfolgen. Die Bedrohungsenzyklopädie enthält eine ausführliche Liste mit Namen und Symptomen von verschiedenen kombinierten Bedrohungen, wie etwa bekannte Malware, Spam, bösartige URLs und bekannte Schwachstellen.

Auf http://about-threats.trendmicro.com/de/threatencyclopedia#malware finden Sie weitere Informationen zu folgenden Themen:

- Malware und bösartige mobile Codes, die zum jeweiligen Zeitpunkt aktiv und im Umlauf sind
- Seiten mit Bedrohungsinformationen, die eine umfassende Ressource für Internet-Angriffe darstellen
- Beratung zu Internet-Bedrohungen bezüglich gezielten Angriffen und Sicherheitsbedrohungen
- Informationen zu Internet-Angriffen und Online-Trends
- Wöchentliche Malware-Berichte

Kontaktaufnahme mit Trend Micro

Sie erreichen unsere Trend Micro Vetriebspartner telefonisch oder per E-Mail:

Adresse	Trend Micro Deutschland GmbH Zeppelinstraße 1 85399 Hallbergmoos Deutschland
Telefon	+49 (0) 811 88990-700
Website	http://www.trendmicro.de
E-Mail-Adresse	sales_info@trendmicro.de

- Weltweite Support-Büros:

  http://www.trendmicro.com/us/about-us/contact/index.html

- Kontaktaufnahme mit Trend Micro:

  http://www.trendmicro.de/ueber-uns/kontakt/index.html

- Trend Micro Produktdokumentation:

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

Problemlösung beschleunigen

Sie sollten die folgenden Informationen zur Hand haben, um die Problemlösung zu beschleunigen:

- Schritte, um das Problem nachvollziehen zu können
- Informationen zur Appliance und zum Netzwerk
- Marke und Modell des Computers sowie zusätzlich angeschlossene Hardware oder Geräte
- Größe des Arbeitsspeichers und des freien Festplattenspeichers
- Betriebssystem- und Service Pack-Version
- Version des installierten Agents
- Seriennummer oder Aktivierungscode
- Ausführliche Beschreibung der Installationsumgebung
- Genauer Wortlaut eventueller Fehlermeldungen

Verdächtige Inhalte an Trend Micro senden

Es gibt mehrere Optionen, um verdächtige Inhalte an Trend Micro zur weiteren Analyse zu senden.

E-Mail-Reputation-Dienste

Fragen Sie die Reputation einer bestimmten IP-Adresse ab, und geben Sie einen Message Transfer Agent zum Hinzufügen zur Liste der allgemein zulässigen Adressen an:

https://ers.trendmicro.com/

Informationen zum Senden von Nachrichten an Trend Micro finden Sie im folgenden Knowledge Base-Artikel:

http://esupport.trendmicro.com/solution/en-US/1112106.aspx

File-Reputation-Dienste

Sammeln Sie Systeminformationen, und senden Sie verdächtige Dateiinhalte an Trend Micro:

http://esupport.trendmicro.com/solution/en-us/1059565.aspx

Notieren Sie sich die Anfragenummer für die weitere Bearbeitung Ihrer Anfrage.

Web-Reputation-Dienste

Sie können die Sicherheitsbewertung und den Inhaltstyp einer URL abfragen, hinter der Sie eine Phishing-Website oder einen Infektionsüberträger vermuten, d. h. eine Quelle von Internet-Bedrohungen, wie z. B. Spyware und Viren:

http://global.sitesafety.trendmicro.com/

Falls die zugewiesene Bewertung nicht zutrifft, senden Sie eine Neuklassifizierungsanforderung an Trend Micro.

Sonstige Ressourcen

Neben Lösungen und Support sind online viele zusätzliche hilfreiche Ressourcen verfügbar, damit Sie immer auf dem neuesten Stand sind, Innovationen kennenlernen und mit den neuesten Sicherheitstrends vertraut sind.

Download Center

Trend Micro veröffentlicht in bestimmten Abständen Patches für gemeldete bekannte Probleme oder Upgrades zu bestimmten Produkten oder Diensten. Auf folgender Seite können Sie feststellen, ob Patches verfügbar sind:

http://downloadcenter.trendmicro.com/index.php?regs=de

Falls ein Patch nicht angewendet wurde (Patches sind datiert), öffnen Sie die Readme-Datei, um festzustellen, ob er für Ihre Umgebung relevant ist. In der Readme-Datei finden Sie außerdem Installationsanweisungen.

Anregungen und Kritik

Das Trend Micro Team ist stets bemüht, die Dokumentationen zu verbessern. Bei Fragen, Anmerkungen oder Anregungen zu diesem oder einem anderen Dokument von Trend Micro besuchen Sie diese Website:

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

Anhänge

Anhänge

Anhang A

Wartungstools

In diesem Abschnitt werden zusätzliche Dienstprogramme beschrieben, die im Lieferumfang von Endpoint Encryption enthalten sind und zur Durchführung von Produktwartungsaufgaben verwendet werden. Endpoint Encryption enthält die folgenden Tools:

TOOL	BESCHREIBUNG
Diagnostics Monitor	Zeigt Ereignisprotokolle von Endpoint Encryption in Echtzeit an. Weitere Informationen finden Sie unter *Diagnostics Monitor verwenden auf Seite A-2*.
Protokollserver-Tool	Erzeugt ein Protokollpaket für alle Ereignisse, die beim Replizieren bestimmter Probleme auftreten. Weitere Informationen finden Sie unter *Das Protokollserver-Tool verwenden auf Seite A-5*.
Tool zum Ändern von Einstellungen für PolicyServer	Ändert die Benutzeranmeldedaten Ihres SQL-Servers und Windows-Dienstes, ohne PolicyServer neu zu installieren. Weitere Informationen finden Sie unter *Das Tool zum Ändern von Einstellungen für PolicyServer verwenden auf Seite A-6*.

Diagnostics Monitor verwenden

Der Diagnostics Monitor ermöglicht Administratoren, Ereignisse im Zusammenhang mit Endpoint Encryption in Echtzeit anzuzeigen.

Prozedur

1. Kopieren Sie ein PolicyServer-Installationspaket, laden Sie es herunter oder suchen Sie es auf dem Endpunkt, auf dem PolicyServer installiert ist.

   Gehen Sie zum Herunterladen des PolicyServer-Installationspakets oder der Endpoint Encryption Suite zum Trend Micro Download Center:

   http://downloadcenter.trendmicro.com/?regs=DE/

2. Navigieren Sie zu `<PolicyServer-Verzeichnis>\TMEE_PolicyServer\Tools\Diagnostics Monitor`.

3. Führen Sie die Datei `DiagnosticMonitor.exe` als Administrator aus.

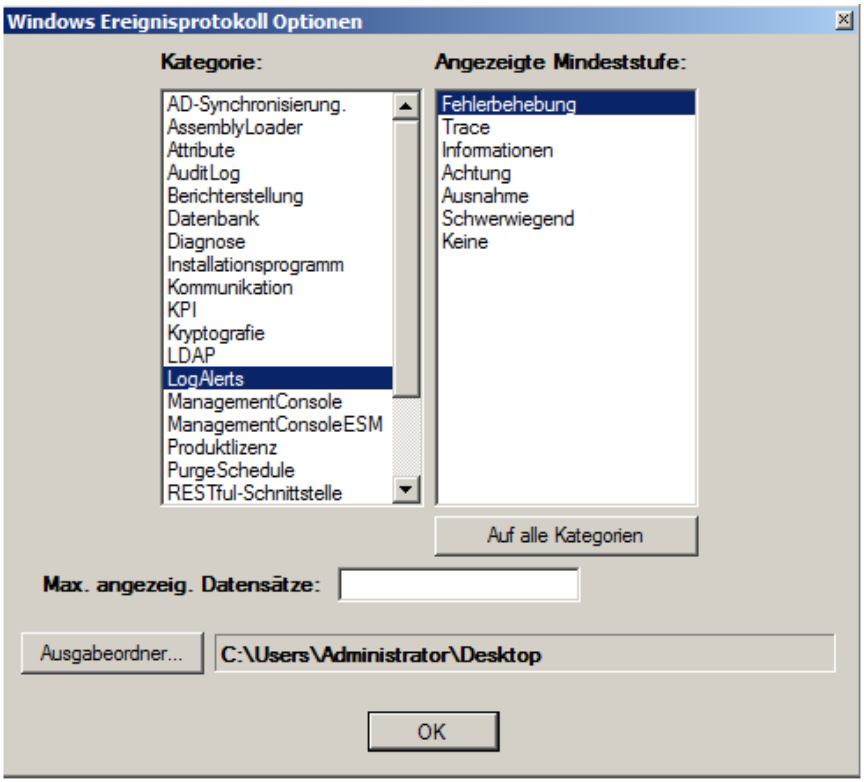
   Das Fenster **Tool zur Lizenzverlängerung** wird geöffnet.

   Wichtig

   Windows stellt möglicherweise zu diesem Zeitpunkt einen Fehler mit dem Titel **Xenocode Postbuild 2010** fest. Im Meldungstext steht, dass die Anwendung eine erforderliche Komponente einer virtuellen Maschine nicht laden kann. Wenn dieser Fehler auftritt, öffnen Sie Windows Update, entfernen Sie das Update „KB3045999“ und führen Sie Diagnostics Monitor erneut aus.

4. Navigieren Sie zu **Datei** > **Optionen...**.

Das Fenster **Live-Monitor-Optionen** wird angezeigt.



5. Gehen Sie zu **LogAlerts** und legen Sie **Angezeigte Mindeststufe** auf **Fehlerbehebung** fest.

6. Legen Sie für das Feld **Maximale Anzahl angezeigter Datensätze** einen Wert zwischen „3000“ und „50000“ fest.

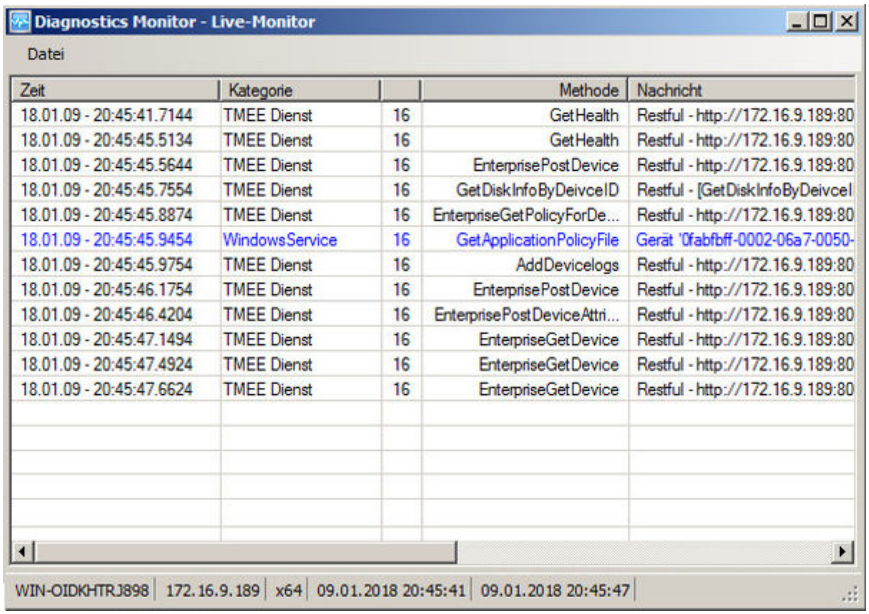
   Nach dem Festlegen des Werts für **Maximale Anzahl angezeigter Datensätze** wird möglicherweise im Diagnostics Monitor ein Ereignis mit einer Meldung, dass das System nicht über genügend Arbeitsspeicher verfügt, angezeigt. Wenn dieses Ereignis angezeigt wird, kehren Sie zu diesem Fenster zurück und legen Sie für **Maximale Anzahl angezeigter Datensätze** einen niedrigeren Wert fest.

7. Klicken Sie auf **Auf alle Kategorien anwenden** oder wählen Sie einzelne Kategorien aus und wenden Sie auf jede davon spezifische Einstellungen an.

8. Starten Sie den Dienst PolicyServerWindowsService über den Windows Task-Manager.

   Wenn der PolicyServer-Dienst neu gestartet wird, wird Active Directory mit PolicyServer synchronisiert. Der Diagnostics Monitor zeigt Ereignisse im Zusammenhang mit der Active Directory-Synchronisierung an.

9. Zeigen Sie die Protokolle im Diagnostics Monitor-Fenster an.



Zeit	Kategorie		Methode	Nachricht
18.01.09 - 20:45:41.7144	TMEE Dienst	16	GetHealth	Restful - http://172.16.9.189:80
18.01.09 - 20:45:45.5134	TMEE Dienst	16	GetHealth	Restful - http://172.16.9.189:80
18.01.09 - 20:45:45.5644	TMEE Dienst	16	EnterprisePostDevice	Restful - http://172.16.9.189:80
18.01.09 - 20:45:45.7554	TMEE Dienst	16	GetDiskInfoByDeivceID	Restful - [GetDiskInfoByDeivceI
18.01.09 - 20:45:45.8874	TMEE Dienst	16	EnterpriseGetPolicyForDe...	Restful - http://172.16.9.189:80
18.01.09 - 20:45:45.9454	WindowsService	16	GetApplicationPolicyFile	Gerät '0fabfbff-0002-06a7-0050-
18.01.09 - 20:45:45.9754	TMEE Dienst	16	AddDevicelogs	Restful - http://172.16.9.189:80
18.01.09 - 20:45:46.1754	TMEE Dienst	16	EnterprisePostDevice	Restful - http://172.16.9.189:80
18.01.09 - 20:45:46.4204	TMEE Dienst	16	EnterprisePostDeviceAttri...	Restful - http://172.16.9.189:80
18.01.09 - 20:45:47.1494	TMEE Dienst	16	EnterpriseGetDevice	Restful - http://172.16.9.189:80
18.01.09 - 20:45:47.4924	TMEE Dienst	16	EnterpriseGetDevice	Restful - http://172.16.9.189:80
18.01.09 - 20:45:47.6624	TMEE Dienst	16	EnterpriseGetDevice	Restful - http://172.16.9.189:80

10. Wenn Sie den Diagnostics Monitor zum Beheben eines bestimmten Problems verwenden, führen Sie alle zum Replizieren dieses Problems erforderlichen Aufgaben bei geöffnetem Diagnostics Monitor durch.

11. Navigieren Sie zum Generieren einer Datei aus den Diagnoseprotokollen zu **Datei** > **In Datei speichern**.

Unter Ihrem ausgewählten Ausgabeordner befindet sich nun eine Protokolldatei. Der Standardausgabeordner ist der Desktop. Navigieren Sie zum Ändern des ausgewählten Ausgabeordners zu **Datei** > **Option** > **Ausgabeordner**.

Der Name der Datei ist ein Zeitstempel des Zeitpunkts, zu dem Sie die Datei generiert haben, und das Format ist PSDM.

Hinweis

Wenn Sie sich bezüglich eines Problems an den Support von Trend Micro wenden, fordert Sie der Support-Mitarbeiter möglicherweise dazu auf, eine Kopie der Diagnoseprotokolle zu senden, damit er den Fehler überprüfen kann.

Das Protokollserver-Tool verwenden

Mit dem Protokollserver-Tool können Administratoren alle Ereignisse im Zusammenhang mit Endpoint Encryption über einen bestimmten Zeitraum aufzeichnen, um Probleme zu beheben. Die aufgezeichneten Protokolle sind für die Verwendung durch den Trend Micro Support vorgesehen. Trend Micro rät daher davon ab, das Protokollserver-Tool in eigener Regie zu verwenden. Wenn ein Problem bei Ihnen auftritt, wenden Sie sich an den Support von Trend Micro. Der Support-Mitarbeiter fordert Sie dann möglicherweise dazu auf, Ihr Problem zu replizieren, während Sie das Protokollserver-Tool verwenden.

Prozedur

1. Öffnen Sie den Programmordner von PolicyServer.

   Der standardmäßige Installationspfad lautet `C:\Programme\Trend Micro\PolicyServer`.

2. Führen Sie die Datei `LogServer.exe` als Administrator aus.

   Eine Eingabeaufforderung mit dem Titel **LogServer.exe** wird angezeigt. Das Protokollserver-Tool wird zu diesem Zeitpunkt ausgeführt.

Das Protokollserver-Tool generiert die PolicyServer-Diagnoseprotokolle. Die Protokolle befinden sich ein einer Datei mit dem Namen `psdedebug.log` in einem Ordner mit dem Namen `log` im Programmordner von PolicyServer.

3. Führen Sie alle erforderlichen Aufgaben zum Replizieren des Problems durch, wegen dem Sie sich an den Support von Trend Micro gewendet haben.
4. Schließen Sie die Eingabeaufforderung mit dem Titel **LogServer.exe**.
5. Senden Sie die Datei `psdedebug.log` an den Support-Mitarbeiter, der Sie dazu aufgefordert hat, dieses Tool zu verwenden.

Das Tool zum Ändern von Einstellungen für PolicyServer verwenden

Der Hauptzweck des Tools zum Ändern von Einstellungen für PolicyServer besteht darin, dass Administratoren ihre Anmeldedaten für die SQL Server-Datenbank ändern können, ohne dass der Benutzer PolicyServer erneut installieren muss. Darüber hinaus umfasst dieses Tool mehrere damit im Zusammenhang stehende Funktionen, wie etwa das Testen der Datenbankverbindung und das Ändern der Anmeldedaten für den PolicyServer Windows-Dienst.

Prozedur

1. Kopieren Sie ein PolicyServer-Installationspaket, laden Sie es herunter oder suchen Sie es auf dem Endpunkt, auf dem PolicyServer installiert ist.

   Gehen Sie zum Herunterladen des PolicyServer-Installationspakets oder der Endpoint Encryption Suite zum Trend Micro Download Center:

   http://downloadcenter.trendmicro.com/?regs=DE/

2. Navigieren Sie zu `<PolicyServer-Verzeichnis>\TMEE_PolicyServer\Tools\PolicyServer Change Settings`.
3. Führen Sie die Datei `PolicyServerChangeSettings.exe` als Administrator aus.

4. Stimmen Sie der Endbenutzer-Lizenzvereinbarung (EULA) zu, um fortzufahren.

   Die Endbenutzer-Lizenzvereinbarung wird nur beim ersten Ausführen dieses Tools angezeigt.

5. Ändern Sie Ihre Einstellungen nach Bedarf und verwenden Sie hierzu eine der folgenden Optionen:

OPTION	BEZEICHNUNG
Primäre Datenbank	Geben Sie in diesem Abschnitt die SQL Server-Anmeldedaten für Ihre primäre Datenbank an. Wenn Sie nur über eine Datenbank verfügen, die sowohl als primäre als auch als Protokolldatenbank dient, wählen Sie **Einstellungen für primäre Datenbank für Protokolldatenbank verwenden** aus.
Protokolldatenbank	Wenn Sie separate Datenbanken für die primäre und die Protokolldatenbank haben, geben Sie in diesem Abschnitt die SQL Server-Anmeldedaten für Ihre Protokolldatenbank an. Dieser Abschnitt ist deaktiviert, wenn die Option **Einstellungen für primäre Datenbank für Protokolldatenbank verwenden** ausgewählt ist.
Von Festplatte laden	Setzen Sie die Anmeldedaten für die Abschnitte **Primäre Datenbank** und die **Protokolldatenbank** auf die zuletzt gespeicherte Konfiguration zurück.
Verbindung testen	Vergewissern Sie sich, dass PolicyServer mit den in den Abschnitten **Primäre Datenbank** und **Protokolldatenbank** angezeigten Datenbanken kommunizieren kann.
Auf Festplatte schreiben	Überschreiben Sie die zuletzt gespeicherte Konfiguration mit den Anmeldedaten in den Abschnitten **Primäre Datenbank** und **Protokolldatenbank**.
PS neu starten	Starten Sie PolicyServer neu. Wenn Sie die Anmeldedaten geändert und auf **Auf Festplatte schreiben** geklickt haben, versucht

Option	Bezeichnung
	PolicyServer, mithilfe der neuen SQL Server-Anmeldedaten eine Verbindung herzustellen.
Anmeldedaten für den Dienst ändern...	Ändern Sie die Anmeldedaten für den PolicyServer Windows-Dienst. Das Fenster **PS-Anmeldedaten ändern** wird angezeigt, wenn Sie diese Option auswählen. Sie können entweder das lokale Windows-Systemkonto verwenden oder die Anmeldedaten für ein anderes Konto angeben.

Anhang B

PolicyServer Nachrichten-IDs

In den folgenden Tabellen werden die PolicyServer-Fehlermeldungen erläutert. Die Tabellen sind nach Kategorie gruppiert.

- *Administratorwarnungen auf Seite B-2*
- *Audit-Protokoll-Warnungen auf Seite B-6*
- *Zertifikatswarnungen auf Seite B-8*
- *Gerätewarnungen auf Seite B-8*
- *Fehlerwarnungen auf Seite B-10*
- *Warnungen bei Full Disk Encryption auf Seite B-11*
- *Installationswarnungen auf Seite B-14*
- *Anmelde-/Abmeldewarnungen auf Seite B-14*
- *Mobilgerätewarnungen auf Seite B-18*
- *OCSP-Warnungen auf Seite B-19*
- *OTA-Warnungen auf Seite B-19*
- *Kennwortwarnungen auf Seite B-20*
- *PIN-Änderungswarnungen auf Seite B-23*
- *Smartcard-Warnungen auf Seite B-24*

Administratorwarnungen

Nachrichten-ID	Beschreibung	Anwendungen
100002	Gerät wird identifiziert	Full Disk Encryption, File Encryption, PolicyServer
100003	Sicherheitsverstoß	Full Disk Encryption, File Encryption, PolicyServer
100007	Kritischer Schweregrad	Full Disk Encryption, File Encryption, PolicyServer
100019	Ändern der Richtlinie fehlgeschlagen	Full Disk Encryption, File Encryption, PolicyServer
100045	Nicht unterstützte Konfiguration	Full Disk Encryption, File Encryption, PolicyServer
100046	Unternehmenspool erstellt	Full Disk Encryption, File Encryption, PolicyServer
100047	Unternehmenspool gelöscht	Full Disk Encryption, File Encryption, PolicyServer
100048	Unternehmenspool geändert	Full Disk Encryption, File Encryption, PolicyServer

Nachrichten-ID	Beschreibung	Anwendungen
100049	Admin-Benutzer auf Grund zu vieler fehlgeschlagener Anmeldungen gesperrt.	Full Disk Encryption, File Encryption, PolicyServer
100052	Integritätsprüfung des Richtlinienwerts fehlgeschlagen	Full Disk Encryption, File Encryption, PolicyServer
100053	Richtlinienanforderung auf Grund fehlgeschlagener Richtlinienintegritätsprüfung abgebrochen.	Full Disk Encryption, File Encryption, PolicyServer
100054	Dateianforderung auf Grund fehlgeschlagener Richtlinienintegritätsprüfung abgebrochen.	Full Disk Encryption, File Encryption, PolicyServer
100055	Admin-Authentifizierung erfolgreich	Full Disk Encryption, File Encryption, PolicyServer
100056	Admin-Authentifizierung fehlgeschlagen	Full Disk Encryption, File Encryption, PolicyServer
100062	Admin-Kennwort zurückgesetzt	Full Disk Encryption, File Encryption, PolicyServer
100463	Benutzer kann nicht entfernt werden. Versuchen Sie es erneut.	Full Disk Encryption, File Encryption, PolicyServer

Nachrichten-ID	Beschreibung	Anwendungen
100464	Benutzer kann nicht deaktiviert werden. Versuchen Sie es erneut.	Full Disk Encryption, File Encryption, PolicyServer
100470	Selbsthilfe-Kennwort kann nicht geändert werden. Eine Antwort auf eine der persönlichen Herausforderungsfragen war falsch.	Full Disk Encryption, File Encryption, PolicyServer
102000	Unternehmen hinzugefügt	Full Disk Encryption, File Encryption, PolicyServer
102001	Unternehmen gelöscht	Full Disk Encryption, File Encryption, PolicyServer
102002	Unternehmen geändert	Full Disk Encryption, File Encryption, PolicyServer
102003	Die Anzahl der Benutzer hat das unter dieser Lizenz zulässige Maximum überschritten. Verringern Sie die Anzahl der vorhandenen Benutzer, um dieses Benutzerkonto wiederherzustellen.	PolicyServer
200000	Administrator hat Richtlinie aktualisiert	PolicyServer
200001	Administrator hat Richtlinie hinzugefügt	PolicyServer
200002	Administrator hat Richtlinie gelöscht	PolicyServer
200003	Administrator hat Richtlinie aktiviert	PolicyServer
200004	Administrator hat Richtlinie deaktiviert	PolicyServer
200100	Administrator hat Benutzer hinzugefügt	PolicyServer

Nachrichten-ID	Beschreibung	Anwendungen
200101	Administrator hat Benutzer gelöscht	PolicyServer
200102	Administrator hat Benutzer aktualisiert	PolicyServer
200103	Administrator hat Benutzer zu Gruppe hinzugefügt	PolicyServer
200104	Administrator hat Benutzer von Gruppe entfernt	PolicyServer
200200	Benutzer hinzugefügt	PolicyServer
200201	Benutzer gelöscht	PolicyServer
200202	Benutzer zu Gruppe hinzugefügt	PolicyServer
200203	Benutzer von Gruppe entfernt	PolicyServer
200204	Benutzer aktualisiert	PolicyServer
200300	Administrator hat Gerät gelöscht	PolicyServer
200301	Administrator hat Gerät zu Gruppe hinzugefügt	PolicyServer
200302	Administrator hat Gerät von Gruppe entfernt	PolicyServer
200500	Administrator hat Gruppe hinzugefügt	PolicyServer
200501	Administrator hat Gruppe gelöscht	PolicyServer
200502	Administrator hat Gruppe aktualisiert	PolicyServer
200503	Administrator hat Gruppe kopiert/eingefügt	PolicyServer
200600	Update des PolicyServer angewendet.	PolicyServer
200602	Benutzer zu Gerät hinzugefügt	PolicyServer
200603	Benutzer von Gerät entfernt	PolicyServer
200700	Ereignis erfolgreich ausgeführt	PolicyServer
200701	Ereignisausführung fehlgeschlagen	PolicyServer

Nachrichten-ID	Beschreibung	Anwendungen
200800	Ereignis installiert	PolicyServer
200801	Installation des Ereignisses fehlgeschlagen	PolicyServer

Audit-Protokoll-Warnungen

Nachrichten-ID	Beschreibung	Anwendungen
100015	Protokollmeldung	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer
103000	Audit-Protokoll-Verbindung geöffnet	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer
103001	Audit-Protokoll-Verbindung geschlossen	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer
103100	Audit-Protokoll-Datensatz fehlt	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer

Nachrichten-ID	Beschreibung	Anwendungen
103101	Keine Integrität bei Audit-Protokoll-Datensatz	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer
103102	Integrität von Audit-Protokoll-Datensatz gefährdet	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer
103103	Validierung der Integrität des Audit-Protokoll-Datensatzes gestartet	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer
104003	Authentifizierungsmethode auf Smartcard festgelegt.	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer
904008	Protokollwarnung kann nicht gesendet werden	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer

Zertifikatswarnungen

Nachrichten-ID	Beschreibung	Anwendungen
104008	Zertifikat abgelaufen.	Full Disk Encryption, File Encryption, PolicyServer

Gerätewarnungen

Nachrichten-ID	Beschreibung	Anwendungen
100001	Authentifizierung für die Synchronisierung zwischen PDA und Desktop war nicht erfolgreich. Es wurde für diesen PDA keine Geräte-ID gefunden.	Full Disk Encryption, File Encryption, PolicyServer
100012	Gerät befindet sich nicht in seiner eigenen Kennwortauthentifizierungsdatei. PAF beschädigt?	Full Disk Encryption, File Encryption, PolicyServer
100044	Aktion zum Sperren von Geräten empfangen	Full Disk Encryption, File Encryption, PolicyServer
100100	Installation gestartet	Full Disk Encryption, File Encryption
100101	Installation abgeschlossen	Full Disk Encryption, File Encryption
100462	Verbindung mit PolicyServer nicht möglich.	Full Disk Encryption, File Encryption, PolicyServer

Nachrichten-ID	Beschreibung	Anwendungen
101001	Die Netzwerkverbindung funktioniert nicht. Die Richtliniendateien können nicht vom PolicyServer abgerufen werden.	Full Disk Encryption, File Encryption, PolicyServer
101002	Beschädigte PAF-Datei (DAFolder.xml)	Full Disk Encryption, File Encryption, PolicyServer
105000	Richtlinien können nicht mit Client synchronisiert werden. Überprüfen Sie, ob eine Netzwerkverbindung vorhanden ist, und versuchen Sie es erneut.	Full Disk Encryption, File Encryption, PolicyServer
200400	Gerät hinzugefügt	PolicyServer
200401	Gerät gelöscht	PolicyServer
200402	Gerät zu Gruppe hinzugefügt	PolicyServer
200403	Gerät von Gruppe entfernt	PolicyServer
200404	Gerät geändert	PolicyServer
200405	Gerätestatus aktualisiert	PolicyServer
200406	Gerätestatus zurückgesetzt	PolicyServer
200407	Auslöschen des Geräts ausgelöst	Full Disk Encryption, File Encryption, PolicyServer
200408	Gerätesperre ausgestellt	Full Disk Encryption, File Encryption, PolicyServer
200409	Gerät synchronisiert	PolicyServer
904012	Der Benutzer darf kein neues Gerät registrieren.	PolicyServer
1000052	Deinstallation des Produkts	Full Disk Encryption, File Encryption

Nachrichten-ID	Beschreibung	Anwendungen
1000053	Deinstallation des Produkts von Richtlinie verweigert	Full Disk Encryption, File Encryption
907001	Datenbankbeschädigung	Full Disk Encryption
907002	Datenbank wurde erfolgreich repariert	Full Disk Encryption
907003	Datenbank konnte nicht repariert werden	Full Disk Encryption
907004	Datenbank der Datenfestplatte ist beschädigt	Full Disk Encryption
907005	Datenbank der Datenfestplatte wurde erfolgreich repariert	Full Disk Encryption
907006	Datenbank der Datenfestplatte konnte nicht repariert werden	Full Disk Encryption

Fehlerwarnungen

Nachrichten-ID	Beschreibung	Anwendungen
100005	Allgemeiner Fehler	Full Disk Encryption, File Encryption, PolicyServer
100006	Anwendungsfehler	Full Disk Encryption, File Encryption, PolicyServer

Warnungen bei Full Disk Encryption

Nachrichten-ID	Beschreibung	Anwendungen
300700	Maximale Größe des Geräteprotokolls erreicht, Ereignisprotokoll wird abgeschnitten.	Full Disk Encryption
400001	Benutzer hat sich angemeldet.	Full Disk Encryption
400002	Benutzeranmeldung fehlgeschlagen.	Full Disk Encryption
400003	Geräteentschlüsselung gestartet.	Full Disk Encryption
400004	Geräteverschlüsselung gestartet.	Full Disk Encryption
400005	Verschlüsselte Partition gemountet.	Full Disk Encryption
400006	Nativer OS-MBR wiederhergestellt.	Full Disk Encryption
400007	Anwendungs-MBR wiederhergestellt.	Full Disk Encryption
400008	Geräteverschlüsselung abgeschlossen	Full Disk Encryption
400009	Geräteentschlüsselung abgeschlossen	Full Disk Encryption
400010	Geräteverschlüsselung wird durchgeführt	Full Disk Encryption
400011	System-MBR beschädigt	Full Disk Encryption
400012	Preboot-Kernel des Systems gelöscht	Full Disk Encryption
401000	Zugriff auf Wiederherstellungskonsole	Full Disk Encryption
401009	Fehler bei Wiederherstellungskonsole	Full Disk Encryption
401010	In-Place-Entschlüsselung gestartet	Full Disk Encryption
401011	In-Place-Entschlüsselung gestoppt	Full Disk Encryption
401012	In-Place-Entschlüsselung abgeschlossen	Full Disk Encryption
401013	Entschlüsselung des Wechseldatenträgers gestartet	Full Disk Encryption

Nachrichten-ID	Beschreibung	Anwendungen
401014	Entschlüsselung des Wechseldatenträgers gestoppt	Full Disk Encryption
401015	Entschlüsselung des Wechseldatenträgers abgeschlossen	Full Disk Encryption
401018	Fehler bei In-Place-Entschlüsselung	Full Disk Encryption
401019	Fehler bei Entschlüsselung des Wechseldatenträgers	Full Disk Encryption
401020	Zugriff auf verschlüsselte Dateien	Full Disk Encryption
401021	Verschlüsselte Dateien geändert	Full Disk Encryption
401022	Verschlüsselte Dateien auf Wechseldatenträger kopiert	Full Disk Encryption
401029	Fehler beim Zugriff auf verschlüsselte Dateien	Full Disk Encryption
401030	Zugriff auf Netzwerkadministration	Full Disk Encryption
401031	PolicyServer Adresse geändert	Full Disk Encryption
401032	PolicyServer Portnummer geändert	Full Disk Encryption
401033	Zu IPv6 gewechselt	Full Disk Encryption
401034	Zu IPv4 gewechselt	Full Disk Encryption
401035	Zur dynamischen IP-Konfiguration gewechselt	Full Disk Encryption
401036	Zur statischen IP-Konfiguration gewechselt	Full Disk Encryption
401037	DHCP-Portnummer geändert	Full Disk Encryption
401038	IP-Adresse geändert	Full Disk Encryption
401039	Subnetzmaske geändert	Full Disk Encryption
401040	Broadcast-Adresse geändert	Full Disk Encryption

Nachrichten-ID	Beschreibung	Anwendungen
401041	Gateway geändert	Full Disk Encryption
401042	Domänenname geändert	Full Disk Encryption
401043	Domain Name Server geändert	Full Disk Encryption
401049	Fehler bei Netzwerkadministration	Full Disk Encryption
401050	Zugriff auf Benutzeradministration	Full Disk Encryption
401051	Benutzer hinzugefügt	Full Disk Encryption
401052	Benutzer entfernt	Full Disk Encryption
401053	Benutzer geändert	Full Disk Encryption
401069	Fehler bei Benutzeradministration	Full Disk Encryption
401070	Zugriff auf lokal gespeicherte Protokolle	Full Disk Encryption
401079	Fehler bei Zugriff auf lokal gespeicherte Protokolle	Full Disk Encryption
401080	Ursprünglicher MBR wiederhergestellt	Full Disk Encryption
401089	Fehler beim Wiederherstellen des ursprünglichen MBR	Full Disk Encryption
401090	Standarddesign wiederhergestellt	Full Disk Encryption
401099	Fehler bei Wiederherstellung des Standarddesigns	Full Disk Encryption
402000	Start der Anwendung	Full Disk Encryption
402001	Herunterfahren der Anwendung	Full Disk Encryption
600001	Preboot-Update war erfolgreich.	Full Disk Encryption
600002	Preboot-Update fehlgeschlagen	Full Disk Encryption
905003	Verschieben der Festplatte erfolgreich FDE	Full Disk Encryption
905004	Verschieben der Festplatte fehlgeschlagen	Full Disk Encryption

Installationswarnungen

Nachrichten-ID	Beschreibung	Anwendungen
100004	Installationsfehler	Full Disk Encryption, File Encryption, PolicyServer
100020	Erfolgreiche Installation	Full Disk Encryption, File Encryption, PolicyServer
905002	Installation von Festplatten fehlgeschlagen	Full Disk Encryption
905003	Verschieben der Festplatte erfolgreich	Full Disk Encryption

Anmelde-/Abmeldewarnungen

Nachrichten-ID	Beschreibung	Anwendungen
100013	Fehlgeschlagener Anmeldeversuch	Full Disk Encryption, File Encryption, PolicyServer
100014	Erfolgreiche Anmeldung	Full Disk Encryption, File Encryption, PolicyServer
100016	Anmeldung nicht möglich. Verwenden Sie die Remote-Authentifizierung, um den PolicyServer Administrator mit einem Herausforderungscode zu versehen.	Full Disk Encryption, File Encryption, PolicyServer

Nachrichten-ID	Beschreibung	Anwendungen
100021	Erfolglose ColorCode-Anmeldung	Full Disk Encryption, File Encryption, PolicyServer
100022	Erfolglose Anmeldung per festem Kennwort	Full Disk Encryption, File Encryption, PolicyServer
100023	Erfolglose PIN-Anmeldung	Full Disk Encryption, File Encryption, PolicyServer
100024	Erfolglose X99-Anmeldung	Full Disk Encryption, File Encryption, PolicyServer
100028	Erfolgreiche ColorCode-Anmeldung	Full Disk Encryption, File Encryption, PolicyServer
100031	Erfolgreiche X9.9-Anmeldung	Full Disk Encryption, File Encryption, PolicyServer
100032	Erfolgreiche Remote-Anmeldung	Full Disk Encryption, File Encryption, PolicyServer
100035	Erfolgreiche WebToken-Anmeldung	Full Disk Encryption, File Encryption, PolicyServer

Nachrichten-ID	Beschreibung	Anwendungen
100036	Erfolglose WebToken-Anmeldung	Full Disk Encryption, File Encryption, PolicyServer
100050	Anmeldung mit festem Kennwort durch Sperre blockiert.	Full Disk Encryption, File Encryption, PolicyServer
100051	Benutzeranmeldung entsperrt	Full Disk Encryption, File Encryption, PolicyServer
100057	LDAP-Benutzerauthentifizierung erfolgreich	Full Disk Encryption, File Encryption, PolicyServer
100058	LDAP-Benutzerauthentifizierung fehlgeschlagen	Full Disk Encryption, File Encryption, PolicyServer
100059	Änderung des LDAP-Benutzerkennworts erfolgreich	Full Disk Encryption, File Encryption, PolicyServer
100060	Änderung des LDAP-Benutzerkennworts fehlgeschlagen	Full Disk Encryption, File Encryption, PolicyServer
100061	Zugriffsanforderung auf Grund fehlgeschlagener Richtlinienintegritätsprüfung abgebrochen.	Full Disk Encryption, File Encryption, PolicyServer

Nachrichten-ID	Beschreibung	Anwendungen
100070	Erfolgreiche Abmeldung	Full Disk Encryption, File Encryption, PolicyServer
100433	Die eingegebenen ColorCode-Kennwörter stimmen nicht überein.	Full Disk Encryption, File Encryption, PolicyServer
100434	ColorCode kann nicht geändert werden. Der neue ColorCode muss sich vom aktuellen unterscheiden.	Full Disk Encryption, File Encryption, PolicyServer
100435	ColorCode kann nicht geändert werden. Der neue ColorCode muss die von PolicyServer definierten Mindestanforderungen für die Länge erfüllen.	Full Disk Encryption, File Encryption, PolicyServer
100436	ColorCode kann nicht geändert werden. Der neue ColorCode muss sich von allen zuvor verwendeten ColorCodes unterscheiden.	Full Disk Encryption, File Encryption, PolicyServer
100437	Ändern des ColorCode fehlgeschlagen - Interner Fehler	Full Disk Encryption, File Encryption, PolicyServer
100459	X9.9 - Fehler bei Kennwortänderung - Verbindung zu PolicyServer-Host nicht möglich	Full Disk Encryption, File Encryption, PolicyServer
100460	X9.9 - Fehler bei Kennwortänderung - Leere Seriennummer	Full Disk Encryption, File Encryption, PolicyServer

Nachrichten-ID	Beschreibung	Anwendungen
100461	X9.9 - Fehler bei Kennwortänderung - Interner Fehler	Full Disk Encryption, File Encryption, PolicyServer
101004	Gesperrtes Gerät kann nicht zurückgesetzt werden.	Full Disk Encryption, File Encryption, PolicyServer
104000	Smartcard-Anmeldung erfolgreich.	Full Disk Encryption, File Encryption, PolicyServer
104001	Smartcard-Anmeldung nicht erfolgreich. Prüfen Sie, ob die Karte ordnungsgemäß eingelegt wurde und die Smartcard-PIN gültig ist.	Full Disk Encryption, File Encryption, PolicyServer

Mobilgerätewarnungen

Nachrichten-ID	Beschreibung	Anwendungen
100037	Palm-Richtliniendatenbank fehlt	Full Disk Encryption, File Encryption oder PolicyServer
100038	Fehler bei Palm-Verschlüsselung	Full Disk Encryption, File Encryption oder PolicyServer
100039	PPC - Geräteverschlüsselung geändert	Full Disk Encryption, File Encryption oder PolicyServer

Nachrichten-ID	Beschreibung	Anwendungen
100040	PPC - Fehler bei Verschlüsselung	Full Disk Encryption, File Encryption oder PolicyServer

OCSP-Warnungen

Nachrichten-ID	Beschreibung	Anwendungen
104005	OCSP-Zertifikatsstatus gut.	Full Disk Encryption, File Encryption, PolicyServer
104006	OCSP-Zertifikatsstatus widerrufen.	Full Disk Encryption, File Encryption, PolicyServer
104007	OCSP-Zertifikatsstatus unbekannt.	Full Disk Encryption, File Encryption, PolicyServer

OTA-Warnungen

Nachrichten-ID	Beschreibung	Anwendungen
100041	OTA-Objekt fehlt oder ist beschädigt.	Full Disk Encryption, File Encryption, PolicyServer

Nachrichten-ID	Beschreibung	Anwendungen
100042	OTA-Synchronisierung erfolgreich	Full Disk Encryption, File Encryption, PolicyServer
100043	OTA-Gerät ausgelöscht	Full Disk Encryption, File Encryption, PolicyServer

Kennwortwarnungen

Nachrichten-ID	Beschreibung	Anwendungen
100017	Fehler beim Ändern des Kennworts	Full Disk Encryption, File Encryption, PolicyServer
100018	Anzahl der Versuche zur Kennworteingabe überschritten	Full Disk Encryption, File Encryption, PolicyServer
100025	Kennwort zurückgesetzt auf 'ColorCode'	Full Disk Encryption, File Encryption, PolicyServer
100026	Kennwort zurückgesetzt auf 'Fest'	Full Disk Encryption, File Encryption, PolicyServer
100027	Kennwort zurückgesetzt auf PIN	Full Disk Encryption, File Encryption, PolicyServer

Nachrichten-ID	Beschreibung	Anwendungen
100029	Erfolgreiche Anmeldung per festem Kennwort	Full Disk Encryption, File Encryption, PolicyServer
100030	Erfolgreiche Anmeldung per PIN-Kennwort	Full Disk Encryption, File Encryption, PolicyServer
100033	Kennwort kann nicht zurückgesetzt werden	Full Disk Encryption, File Encryption, PolicyServer
100432	Das Kennwort kann nicht geändert werden. Das neue Kennwort muss sich vom aktuellen Kennwort unterscheiden.	Full Disk Encryption, File Encryption, PolicyServer
100439	Das Kennwort kann nicht geändert werden. Die Kennwörter stimmen nicht überein.	Full Disk Encryption, File Encryption, PolicyServer
100441	Das Kennwort kann nicht geändert werden. Das Kennwortfeld muss ausgefüllt werden.	Full Disk Encryption, File Encryption, PolicyServer
100442	Das Kennwort kann nicht geändert werden. Das Kennwort erfüllt nicht die von PolicyServer definierten Mindestanforderungen für die Länge.	Full Disk Encryption, File Encryption, PolicyServer
100443	Das Kennwort kann nicht geändert werden. Ziffern sind nicht zulässig.	Full Disk Encryption, File Encryption, PolicyServer

Nachrichten-ID	Beschreibung	Anwendungen
100444	Das Kennwort kann nicht geändert werden. Buchstaben sind nicht zulässig.	Full Disk Encryption, File Encryption, PolicyServer
100445	Das Kennwort kann nicht geändert werden. Sonderzeichen sind nicht zulässig.	Full Disk Encryption, File Encryption, PolicyServer
100446	Das Kennwort kann nicht geändert werden. Das Kennwort darf den Benutzernamen nicht enthalten.	Full Disk Encryption, File Encryption, PolicyServer
100447	Das Kennwort kann nicht geändert werden. Das Kennwort enthält nicht genügend Sonderzeichen.	Full Disk Encryption, File Encryption, PolicyServer
100448	Das Kennwort kann nicht geändert werden. Das Kennwort enthält nicht genügend Ziffern.	Full Disk Encryption, File Encryption, PolicyServer
100449	Das Kennwort kann nicht geändert werden. Das Kennwort enthält nicht genügend Zeichen.	Full Disk Encryption, File Encryption, PolicyServer
100450	Das Kennwort kann nicht geändert werden. Das Kennwort enthält zu viele aufeinanderfolgende Zeichen.	Full Disk Encryption, File Encryption, PolicyServer
100451	Das Kennwort kann nicht geändert werden. Das neue Kennwort muss sich von allen zuvor verwendeten Kennwörtern unterscheiden.	Full Disk Encryption, File Encryption, PolicyServer

Nachrichten-ID	Beschreibung	Anwendungen
100452	Ändern des Kennworts fehlgeschlagen - Interner Fehler	Full Disk Encryption, File Encryption, PolicyServer
101003	Festes Kennwort wurde geändert.	Full Disk Encryption, File Encryption, PolicyServer

PIN-Änderungswarnungen

Nachrichten-ID	Beschreibung	Anwendungen
100438	PIN kann nicht geändert werden. Die PINs stimmen nicht überein.	Full Disk Encryption, File Encryption, PolicyServer
100440	PIN kann nicht geändert werden. Eines der Felder ist leer.	Full Disk Encryption, File Encryption, PolicyServer
100453	PIN kann nicht geändert werden. Die PINs stimmen nicht überein.	Full Disk Encryption, File Encryption, PolicyServer
100454	Änderung der PIN möglich. Die neue PIN muss sich von der alten PIN unterscheiden.	Full Disk Encryption, File Encryption, PolicyServer
100455	PIN kann nicht geändert werden. Die neue PIN erfüllt nicht die von PolicyServer definierten Mindestanforderungen für die Länge.	Full Disk Encryption, File Encryption, PolicyServer

Nachrichten-ID	Beschreibung	Anwendungen
100456	PIN kann nicht geändert werden. Die PIN darf den Benutzernamen nicht enthalten.	Full Disk Encryption, File Encryption, PolicyServer
100457	PIN kann nicht geändert werden. Die neue PIN muss sich von allen zuvor verwendeten PINs unterscheiden.	Full Disk Encryption, File Encryption, PolicyServer
100458	Ändern der PIN fehlgeschlagen - Interner Fehler	Full Disk Encryption, File Encryption, PolicyServer

Smartcard-Warnungen

Nachrichten-ID	Beschreibung	Anwendungen
104002	Registrierte Smartcard.	Full Disk Encryption, File Encryption, PolicyServer
104004	Smartcard kann nicht registriert werden. Prüfen Sie, ob die Karte ordnungsgemäß eingelegt wurde und die Smartcard-PIN gültig ist.	Full Disk Encryption, File Encryption, PolicyServer

Anhang C

Endpoint Encryption Dienste

In der folgenden Tabelle werden alle Endpoint Encryption Dienste beschrieben. Die Informationen vermitteln ein Verständnis darüber, welche Dienste welche Endpoint Encryption Agents bzw. Funktion steuern und wie Sie ein Problem lösen.

TABELLE C-1. Endpoint Encryption Dienste

BETRIEBSSYSTEM	DIENST- ODER DAEMON-NAMEN	ANZEIGENAME	BESCHREIBUNG	DATEINAME
PolicyServer	PolicyServer Windows-Diensts	PolicyServer Windows-Diensts	Verwaltet die Kommunikation zwischen Endpoint Encryption Diensten und Datenbanken.	`PolicyServerWindowService.exe`
	TMEE Dienst	Endpoint Encryption Dienst	Verwaltet die Kommunikation zwischen Endpoint Encryption Agent 5.0 (und höher) über einen verschlüsselten Kanal (RESTful).	`TMEEService.exe`
	IIS/ MAWebService 2	Legacy Web-Service	Verwaltet die Kommunikation zwischen Endpoint Encryption Agent 3.1.3 (und älter) über einen verschlüsselten Kanal (SOAP).	n. v.
	TMEEForward	TMEEForward	Leitet den Datenverkehr von Endpoint Encryption 6.0 Agents zu PolicyServer weiter.	TMEEForward.exe
	TMEEProxyWindowsService	PolicyServer LDAProxy-Windows-Dienst	Bietet sichere Kommunikation zwischen Trend Micro PolicyServer und den Remote-LDAP-Servern.	`LDAProxyWindowsServices.exe`

Betriebssystem	Dienst- oder Daemon-Namen	Anzeigename	Beschreibung	Dateiname
Full Disk Encryption	DrAService	Trend Micro Full Disk Encryption	Bietet Sicherheit für Trend Micro Endpunkte und die Verschlüsselung ganzer Festplatten.	`DrAService.exe`
Encryption Management for Microsoft BitLocker	FDE_MB	Trend Micro Full Disk Encryption, Encryption Management for Microsoft BitLocker	Gewährleistet Datensicherheit für Endpunkte mit Microsoft BitLocker	`FDEforBitLocker.exe`
Encryption Management for Apple FileVault	Daemon: TMFDEMM Agent: Trend Micro Full Disk Encryption	Trend Micro Full Disk Encryption, Encryption Management for Apple FileVault	Gewährleistet Datensicherheit für Endpunkte mit Apple FileVault.	
File Encryption	FileEncryption Service	Trend Micro File Encryption	Bietet Sicherheit für Trend Micro Endpunkte und Datenschutz für Dateien, Ordner und Wechselmedien.	`FEService.exe`

Anhang D

Richtlinienzuordnung zwischen Management-Konsolen

Administratoren können Endpoint Encryption Endpoint Encryption nur mit PolicyServer MMC verwalten oder sie verwalten Endpoint Encryption mit Control Manager zur Verwaltung von Richtlinien, Benutzern und Geräten und setzen PolicyServer MMC für die erweiterte Protokollverwaltung und Berichterstellung ein.

In den folgenden Tabellen wird beschrieben, wie Richtlinien zwischen PolicyServer MMC und Control Manager zugeordnet werden. In Umgebungen, in denen Control Manager zur Verwaltung von PolicyServer eingesetzt wird, sollten Sie alle Richtlinien, die nicht in der Tabelle aufgeführt werden, mit PolicyServer MMC verwalten.

TABELLE D-1. Richtlinienzuordnung für Full Disk Encryption

CONTROL MANAGER KENNZEICHNUNG	POLICYSERVER MMC PFAD
Verschlüsselung	
Endpunkt verschlüsseln	**Full Disk Encryption** > **Verschlüsselung** > **Gerät verschlüsseln**
Client-Einstellungen	
Full Disk Encryption Preboot umgehen	**Full Disk Encryption** > **Anmelden** > **Preboot-Umgehung**

Control Manager Kennzeichnung	PolicyServer MMC Pfad
Benutzer sind berechtigt, auf die Systemwiederherstellungstools des Geräts zuzugreifen	**Full Disk Encryption** > **Agent** > **Wiederherstellung durch Benutzer zulassen**
Benachrichtigungen	
Die folgende Meldung wird angezeigt, wenn der Endpunkt gefunden wird	**Full Disk Encryption** > **Anmelden** > **Falls gefunden**
Die Kontaktinformationen für den technischen Support werden angezeigt	**Full Disk Encryption** > **Anmelden** > **Support-Informationen**
Rechtlichen Hinweis anzeigen	**Full Disk Encryption** > **Anmelden** > **Rechtlicher Hinweis**
• **Rechtlichen Hinweis anzeigen** > **Installation** • **Rechtlichen Hinweis anzeigen** > **Start**	**Full Disk Encryption** > **Anmelden** > **Rechtlicher Hinweis** > **Rechtlicher Hinweis** > **Anzeigezeit für den rechtlichen Hinweis**
Rechtlichen Hinweis anzeigen	**Full Disk Encryption** > **Anmelden** > **Rechtlicher Hinweis** > **Rechtlicher Hinweis** > **Text des rechtlichen Hinweises**

Tabelle D-2. Richtlinienzuordnung für File Encryption

Control Manager Kennzeichnung	PolicyServer MMC Pfad
Zu verschlüsselnde Ordner	
Zu verschlüsselnde Ordner Textfeld	**File Encryption** > **Verschlüsselung** > **Ordner zum Verschlüsseln angeben**
Verwendeter Verschlüsselungsschlüssel	
Verwendeter Verschlüsselungsschlüssel	**File Encryption** > **Verschlüsselung** > **Verwendeter Verschlüsselungsschlüssel**

Control Manager Kennzeichnung	PolicyServer MMC Pfad
Speichereinheiten	
Optisches Laufwerk deaktivieren	**File Encryption** > **Verschlüsselung** > **Optisches Laufwerk deaktivieren**
USB-Laufwerk deaktivieren	**File Encryption** > **Verschlüsselung** > **Wechselmedien** > **USB-Laufwerk deaktivieren**
Alle Dateien und Ordner auf USB-Laufwerken verschlüsseln	**File Encryption** > **Verschlüsselung** > **Wechselmedien** > **Gerät vollständig verschlüsseln**
Zu verschlüsselnden Dateipfad auf USB-Geräten angeben	**File Encryption** > **Verschlüsselung** > **Wechselmedien** > **Zu verschlüsselnde Ordner auf Wechselmedien**
Benachrichtigungen	
Rechtlichen Hinweis anzeigen	**File Encryption** > **Anmelden** > **Rechtlicher Hinweis**
• **Rechtlichen Hinweis anzeigen** > **Installation** • **Rechtlichen Hinweis anzeigen** > **Start**	**File Encryption** > **Anmelden** > **Rechtlicher Hinweis** > **Anzeigezeit für den rechtlichen Hinweis**
Rechtlichen Hinweis anzeigen Textfeld	**File Encryption** > **Anmelden** > **Rechtlicher Hinweis** > **Text des rechtlichen Hinweises**

Tabelle D-3. Allgemeine Richtlinienzuordnung

Control Manager Kennzeichnung	PolicyServer MMC Pfad
Deinstallation durch Benutzer zulassen	

Control Manager Kennzeichnung	PolicyServer MMC Pfad
Nicht-Administratorkonten können die Agent-Software deinstallieren	• **Full Disk Encryption** > **Agent** > **Deinstallation durch Benutzer zulassen** • **File Encryption** > **Agent** > **Deinstallation durch Benutzer zulassen**
Aktionen zum Sperren von Geräten	
Konto sperren nach *<number>* **Tagen**	**Full Disk Encryption** > **Anmelden** > **Zeitraum bis Kontosperrung**
Kontosperraktion	**Full Disk Encryption** > **Anmelden** > **Kontosperraktion**
Zulässige Anzahl fehlgeschlagener Anmeldeversuche	**Full Disk Encryption** > **Anmelden** > **Zulässige Anzahl fehlgeschlagener Anmeldeversuche**
Full Disk Encryption: **Aktion zur Gerätesperrung**	**Full Disk Encryption** > **Anmelden** > **Aktion zur Gerätesperrung**
Full Disk Encryption: **Anzahl der Minuten, die das Gerät gesperrt wird**	**Full Disk Encryption** > **Anmelden** > **Zeitverzögerung bei Gerätesperre**
File Encryption: **Aktion zur Gerätesperrung**	**File Encryption** > **Anmelden** > **Aktion zur Gerätesperrung**
File Encryption: **Anzahl der Minuten, die das Gerät gesperrt wird**	**File Encryption** > **Anmelden** > **Zeitverzögerung bei Gerätesperre**
Kennwort	
Benutzer muss das Kennwort nach *<number>* **Tagen ändern**	**Allgemein** > **Authentifizierung** > **Lokale Anmeldung** > **Benutzerkennwort** > **Kennwort ändern alle**

CONTROL MANAGER KENNZEICHNUNG	POLICYSERVER MMC PFAD
Benutzer darf die vorherigen *<number>* Kennwörter nicht wiederverwenden	**Allgemein** > **Authentifizierung** > **Lokale Anmeldung** > **Benutzerkennwort** > **Aufbewahrung des Kennwortverlaufs**
Anzahl der zulässigen aufeinanderfolgenden Zeichen in einem Kennwort	**Allgemein** > **Authentifizierung** > **Lokale Anmeldung** > **Benutzerkennwort** > **Zulässige aufeinanderfolgende Zeichen**
Zulässige Mindestlänge für Kennwörter	**Allgemein** > **Authentifizierung** > **Lokale Anmeldung** > **Benutzerkennwort** > **Mindestlänge**
Anforderungen an die Zeichen für Kennwörter	
Buchstaben	**Allgemein** > **Authentifizierung** > **Lokale Anmeldung** > **Benutzerkennwort** > **Erforderliche Anzahl an Zeichen**
Kleinbuchstaben	**Allgemein** > **Authentifizierung** > **Lokale Anmeldung** > **Benutzerkennwort** > **Erforderliche Anzahl an Kleinbuchstaben**
Großbuchstaben	**Allgemein** > **Authentifizierung** > **Lokale Anmeldung** > **Benutzerkennwort** > **Erforderliche Anzahl an Großbuchstaben**
Zahlen	**Allgemein** > **Authentifizierung** > **Lokale Anmeldung** > **Benutzerkennwort** > **Erforderliche Anzahl an Ziffern**
Symbole	**Allgemein** > **Authentifizierung** > **Lokale Anmeldung** > **Benutzerkennwort** > **Erforderliche Anzahl an Sonderzeichen**

TABELLE D-4. Richtlinienspeicherorte für die Remote-Hilfe

NAME DER RICHTLINIE	MENÜPFAD FÜR POLICYSERVER MMC	CONTROL MANAGER MENÜPFAD
Kontosperraktion	**Anmelden** > **Kontosperraktion**	**Allgemein** > **Aktionen zum Sperren von Geräten** > **Kontosperraktion**
Zeitraum bis Kontosperrung	**Anmelden** > **Zeitraum bis Kontosperrung**	**Allgemein** > **Aktionen zum Sperren von Geräten** > **Konto sperren nach [ ] Tagen**
Aktion zur Gerätesperrung	Für jeden Agent: **Anmelden** > **Aktion zur Gerätesperrung**	Für jeden Agent: **Allgemein** > **Aktionen zum Sperren von Geräten** > **Aktion zur Gerätesperrung**
Zulässige Anzahl fehlgeschlagener Anmeldeversuche	Für jeden Agent: **Anmelden** > **Zulässige Anzahl fehlgeschlagener Anmeldeversuche**	Für jeden Agent: **Allgemein** > **Aktionen zum Sperren von Geräten** > **Zulässige Anzahl fehlgeschlagener Anmeldeversuche**

Anhang E

Glossar

In der folgenden Tabelle wird die Terminologie beschrieben, die in der gesamten Endpoint Encryption Dokumentation verwendet wird.

TABELLE E-1. Endpoint Encryption Begriffe

BEGRIFF	BESCHREIBUNG
Agent	Software, die auf einem Endpunkt installiert ist und die mit einem Verwaltungsserver kommuniziert.
Authentifizierung	Der Prozess des Identifizierens eines Benutzers.
ColorCode™	Die Authentifizierungsmethode, bei der eine Farbfolge als Kennwort eingegeben werden muss.
Command Builder	Ein Trend Micro Tool zur Generierung von Skripts für die Installation von PolicyServer und Endpoint Encryption Agents für automatische und Massenverteilungen.
Command Line Helper	Ein Trend Micro Tool zum Erstellen von verschlüsselten Werten zur Sicherung von Anmeldedaten, die von Endpoint Encryption Agent-Installationsskripts verwendet werden.
Control Manager	Trend Micro Control Manager ist eine zentrale Management-Konsole zur Verwaltung von Produkten und Diensten von Trend Micro auf Gateway-, Mailserver-, Dateiserver- und Corporate-Desktop-Ebene.

Begriff	Beschreibung
Gerät	Ein beliebiger Computer, ein Laptop oder ein Wechselmedium (externes Laufwerk, USB-Laufwerk), das von Endpoint Encryption verwaltet wird.
Domänenauthentifizierung	Die Authentifizierungsmethode, die Single Sign-On (SSO) mit Hilfe von Active Directory unterstützt.
DriveTrust™	Hardware-basierte Verschlüsselungstechnologie von Seagate™.
Encryption Management for Microsoft BitLocker	Der Endpoint Encryption Full Disk Encryption Agent für Microsoft Windows-Umgebungen, auf denen lediglich Microsoft BitLocker auf dem Hosting-Endpunkt aktiviert werden muss. Mit dem Encryption Management for Microsoft BitLocker Agent können Sie Endpunkte mit Trend Micro Full Disk Encryption in einer bestehenden Windows-Infrastruktur sichern.
Encryption Management for Apple FileVault	Der Endpoint Encryption Full Disk Encryption Agent für Mac OS-Umgebungen, auf denen lediglich Apple FileVault auf dem Hosting-Endpunkt aktiviert werden muss. Mit der Encryption Management for Apple FileVault Agent können Sie Endpunkte mit Trend Micro Full Disk Encryption in einer bestehenden Mac OS-Infrastruktur sichern.
Endpoint Encryption Dienst	Der PolicyServer Dienst, der die gesamte Kommunikation mit Agents für Endpoint Encryption 6.0 sicher verwaltet. Angaben zur Kommunikation von Endpoint Encryption 3.1.3 Agents und niedriger finden Sie unter "Legacy Web Service".
Unternehmen	Das Endpoint Encryption-Unternehmen ist der eindeutige Bezeichner für das Unternehmen in der PolicyServer Datenbank, der bei der Installation von PolicyServer konfiguriert wurde. Eine PolicyServer Datenbank darf mehrere Unternehmenskonfigurationen haben. Endpoint Encryption Konfigurationen unter Verwendung von Control Manager haben jedoch möglicherweise nur ein Unternehmen.

Begriff	Beschreibung
File Encryption	Der Endpoint Encryption Agent für die Verschlüsselung von Dateien und Ordnern auf lokalen Laufwerken und Wechselmedien. Mit File Encryption können Sie die Dateien und Ordner auf nahezu jedem Gerät, das als Laufwerk im Host-Betriebssystem angezeigt wird, schützen.
Festes Kennwort	Die Authentifizierungsmethode zur Verwendung herkömmlicher Benutzerkennwörter, die aus Buchstaben und/oder Ziffern und/oder Sonderzeichen bestehen.
Full Disk Encryption	Der Endpoint Encryption Agent für die Verschlüsselung von Hardware und Software mit Preboot-Authentifizierung. Full Disk Encryption sichert Datendateien, Anwendungen, Registrierungseinstellungen, temporäre Dateien, Auslagerungsdateien, Druck-Spooler und gelöschte Dateien auf allen Windows-Endpunkten. Eine starke Preboot-Authentifizierung beschränkt den Zugriff auf das anfällige System, bis der Benutzer validiert wird.
Legacy Web-Service	Der PolicyServer Dienst, der die gesamte Kommunikation mit Agents für Endpoint Encryption 3.1.3 und niedriger sicher verwaltet. Weitere Informationen finden Sie unter *Info über PolicyServer auf Seite 2-6*. Informationen zur Kommunikation mit Endpoint Encryption 6.0 finden Sie unter "Endpoint Encryption Dienst".
OfficeScan	OfficeScan schützt Unternehmensnetzwerke vor Malware, Netzwerkviren, webbasierten Bedrohungen, Spyware und kombinierten Bedrohungen. OfficeScan ist eine integrierte Lösung und besteht aus einem Agent am Endpunkt sowie einem Serverprogramm, das alle Agents verwaltet.
OPAL	Die Subsystemklasse für Sicherheit der Trusted Computing Group für Client-Geräte.
Kennwort	Alle Arten von Authentifizierungsdaten, die in Kombination mit einem Benutzernamen verwendet werden, wie feste Kennwörter, PINs und ColorCode.

Begriff	Beschreibung
PIN	Die Authentifizierungsmethode zur Verwendung einer PIN, die von Geldautomaten her bekannt ist.
PolicyServer	Der zentrale Verwaltungsserver, der die Richtlinien zur Verschlüsselung und Authentifizierung auf die Endpoint Encryption Agents verteilt.
Remote-Hilfe	Die Authentifizierungsmethode für Endpoint Encryption-Benutzer, die ihre Anmeldedaten vergessen haben, oder für Endpoint Encryption Geräte, deren Richtlinien nicht innerhalb eines bestimmten Zeitraums synchronisiert wurden.
Wiederherstellungskonsole	Die Benutzeroberfläche von Full Disk Encryption zur Wiederherstellung von Endpoint Encryption Geräten, wenn es zu einem Ausfall des primären Betriebssystems gekommen ist, Netzwerkprobleme untersucht werden und Benutzer, Richtlinien und Protokolle verwaltet werden.
Recovery-Tool	Ein startfähige Festplatte, die zum Reparieren eines Geräts verwendet wird, wenn das Gerät nicht mehr gestartet werden kann. Das Recovery-Tool wird als ISO-Datei im Installationspaket von Full Disk Encryption verteilt.
SED	Ein selbstverschlüsselndes Laufwerk. SEDs bieten „hardwarebasierte Verschlüsselung“, im Gegensatz zum Verschlüsselungstyp von Full Disk Encryption, welcher als „softwarebasierte Verschlüsselung“ bekannt ist.
Selbsthilfe	Die Authentifizierungsmethode, um Endpoint Encryption Benutzer dabei zu unterstützen, Antworten auf Sicherheitsfragen zu geben, bevor der technische Support bei einem vergessenen Kennwort kontaktiert wird.
Smartcard	Die Authentifizierungsmethode, bei der eine physische Karte zusammen mit einer PIN oder einem festen Kennwort erforderlich ist.

Stichwortverzeichnis

A

Active Directory, 2-12, 2-13, 3-25
    Benutzer importieren, 3-29, 4-13
    Konfiguration, 3-27
    Übersicht, 3-26
Agents, 2-9
ändern
    Registerkarten, 4-3
Angegebene Richtlinien, 5-10
    Priorität, 5-10
Anhänge, 1
Anregungen und Kritik, 11-6
Ausstehende Ziele, 5-8
Authentifizierung, 2-3, 2-11
    ColorCode, 2-11, 2-12, 6-14
    Domäne, 2-12
    Domänenauthentifizierung, 2-11
    Festes Kennwort, 2-11, 2-13
    File Encryption, 7-2, 7-15
    Full Disk Encryption, 6-5
    Info über, 5-2
    Kennwort ändern, 7-13
    LDAP, 2-13
    Methode ändern, 6-11
    PIN, 2-13
    Remote-Hilfe, 2-11, 2-14, 6-16
    Selbsthilfe, 2-11, 2-14, 6-19, 6-20
        Antworten, 6-21
    Setup-Voraussetzungen, 2-13
    Sicherheitsoptionen, 7-17
    Single Sign-On, 7-16
    Smartcard, 2-15, 6-17
    Voraussetzungen, 2-13
Authentifizierungsmethode, 2-11

B

Begriffe, E-1
Benutzer, 5-3
    Sperrung, 5-27
    Von AD importieren, 3-29, 4-13
Berichte, 2-1, 2-3
Bildschirmtastatur, 6-10
Boot wiederherst, 9-15

C

ColorCode, 2-12, 6-14
Command Line Helper, 6-3, 6-25, 6-26
Command Line Helper
Installationsprogramm, 6-3
Computer
    Netzwerkinformationen, 6-9
Control Manager, 3-19
    Agent, 3-20
    Berichtserver, 3-19
    Mail-Server, 3-19
    MCP, 3-20
    Richtlinien, 5-1
    SQL-Datenbank, 3-19
    Trend Micro Management Infrastructure, 3-20
    Webbasierte Management-Konsole, 3-21
    Webserver, 3-19
    Widget-Framework, 3-21

D

DAAutoLogin, 6-3, 6-25
dashboard, 4-1
Datenschutz, 2-1
Datenwiederherstellung, 9-28

Demilitarisierte Zone, 6-22
Diagnostics Monitor, A-2
Domänenauthentifizierung, 2-12
File Encryption, 7-16

E

Encryption Management for Apple FileVault
Info über, 8-11
Systemvoraussetzungen, 3-16
Unterstützte Betriebssysteme, 3-16
Encryption Management for Microsoft BitLocker
Info über, 8-5
Systemvoraussetzungen, 3-14
Unterstützte Betriebssysteme, 3-14
Endpoint Encryption, 2-1
Tools, 6-3
Entschlüsselung
Wiederherstellungskonsole, 9-13
Entwurfsrichtlinien, 5-10

F

Fehlermeldungen
Authentifizierung, 7-17
Festes Kennwort, 2-13
Festpl. entschlüss, 9-13
File Encryption, 7-1
Authentifizierung, 7-15
Domäne, 7-16
Erstmals, 7-2
Erste Verwendung, 7-2
Gerät entsperren, 7-13
Kennwort ändern, 7-13
Kennwort zurücksetzen, 7-11, 7-16
PolicyServer Synchronisierung, 6-4, 7-11
Remote-Hilfe, 7-13
Sicheres Löschen, 7-10
Single Sign-On, 7-16
system requirements, 3-13
Task-Leistensymbol
Info über, 7-11
Full Disk Encryption, 6-1
Authentifizierung, 2-14, 6-19
Kennwort ändern, 6-13
Deinstallieren, 9-4
Fehlerbehebung bei Netzwerkproblemen, 9-26
Festpl. entschlüss., 9-13
Konnektivität, 6-22
Kontextmenü, 6-4
Menüoptionen, 6-6
Netzwerk, 9-20
Netzwerkkonfiguration, 9-20
patching, 6-27
PolicyServer Einstellungen, 6-22
Porteinstellungen, 6-22
Recovery-Tool, 9-26
Remote-Hilfe, 6-16
Selbsthilfe, 6-20
Synchronisierung von Richtlinien, 6-23
Systemvoraussetzungen, 3-9–3-11
Task-Leistensymbol
Info über, 6-4
TCP/IP-Zugriff, 6-22
Tools, 6-3
Unternehmen wechseln, 9-20
wechseln, 9-22
Wiederherstellungskonsole, 9-8
Benutzer verwalten, 9-17
Richtlinien verwalten, 9-19
Windows, 9-9
Wiederherstellungsmethoden, 9-4

Windows patches, 6-25
Full Disk Encryption Preboot, 6-5
Authentifizierung, 6-11
Bildschirmtastatur, 6-10
Menüoptionen, 6-6
Netzwerkinformationen, 6-9
Netzwerkverbindung, 6-6
Tastaturbelegung, 6-10
Wireless-Verbindung, 6-6

G

Gefilterte Richtlinien, 5-10
Gerät, 2-3
Geräte
Sperren, 5-27
Widget "Endpoint Encryption - Geräte", 4-14

H

Hardware-basierte Verschlüsselung, 3-9–3-11, 3-14, 3-16

I

Info über
Authentifizierung, 5-2
Encryption Management for Microsoft BitLocker, 8-5
Endpoint Encryption Dienst, 2-6
Legacy Web-Service, 2-6
PolicyServer, 2-6, 3-1
Widgets, 4-4
Integration des Control Managers, 2-7

K

Kennwörter, 2-3
Remote-Hilfe, 9-36
Kennwörter ändern, 6-13

L

LDAP, 2-13
Liste der verwalteten Server
Proxy-Einstellungen konfigurieren, 3-24
löschen
Registerkarten, 4-4

M

Management-Konsolen, 2-7
MBR
Ersetzen, 9-15
MCP, 3-20

N

Netzwerk
Fehlerbehebung, 9-26
Netzwerkinformationen, 6-9
Netzwerk-Setup, 9-20
Neues, 2-4

O

OPAL, 3-9–3-11, 3-14

P

Persönliche Identifikationsnummer (PIN), 2-13
PIN, 2-11
PolicyServer
AD-Synchronisierung, 3-25
Erste Schritte, 3-1
Remote-Hilfe, 9-36
Software-Voraussetzungen, 3-6, 3-7
SQL-Konten, 3-8
Systemvoraussetzungen
hardware, 3-2
von der internen Website herunterzuladen., 3-7, 3-8
Voraussetzungen

Dateien durchsuchen, 3-7, 3-8
Konten, 3-8
SQL, 3-2
Voraussetzungen für SQL, 3-2
PolicyServer MMC, 2-9
Produktdefinitionen, E-1
Protokolle, 9-19
Proxy-Einstellungen
Liste der verwalteten Server, 3-24
Proxy-Einstellungen konfigurieren
Liste der verwalteten Server, 3-24

R

Recovery-Tool, 9-26
reparieren, 9-28
überprüfen, 9-28
Registerkarten
ändern, 4-3
Info über, 4-2
löschen, 4-4
Übersichtsdashboard, 4-2
Remote-Hilfe, 2-14, 6-16, 7-17, 9-36
Reparatur-CD, 6-3, 9-4, 9-26
Richtlinien, 2-3, 5-1
Allgemein, 5-24
Benutzer, 5-14
File Encryption, 5-21
Full Disk Encryption, 5-17, 6-23
Richtlinienzuordnung, D-1
Synchronisieren, 6-23
Synchronisierung, 6-1
Wiederherstellung durch Benutzer zulassen, 9-8
Richtlinienliste, 5-6
Richtlinienpriorität, 5-7
Richtlinientypen
Angebe, 5-10
Entwurf, 5-10
Gefiltert, 5-10
Richtlinienpriorität, 5-7
Richtlinienverwaltung, 5-8
Angegebene Richtlinien, 5-10
Ausstehende Ziele, 5-8
Entwurfsrichtlinien, 5-10
Gefilterte Richtlinien, 5-10
Richtlinienliste, 5-6
Richtlinienpriorität, 5-7, 5-10
verstehen, 5-8
Ziele, 5-7
Richtlinienziele, 5-7
Richtlinienzuordnung
Control Manager, D-1
PolicyServer, D-1

S

Seagate DriveTrust-Laufwerke, 3-9–3-11, 3-14
Selbsthilfe, 2-14, 6-19
Antworten, 6-21
Antworten festlegen, 6-20
Sicherheit
Gerätesperre, 2-14, 6-16
Gerät löschen, 7-17
Kontosperraktion, 2-14, 6-16
Kontosperre, 2-14, 6-16
Remote-Authentifizierung erforderlich, 7-17
Zeitraum bis Kontosperrung, 2-14, 6-16
Zeitverzögerung, 7-17
Zulässige Anzahl fehlgeschlagener Anmeldeversuche, 2-14, 6-16
Smartcard, 2-15, 6-17
Smartcards, 2-15, 6-17
SSO, 2-12
support

Probleme schneller beheben, 11-4
system requirements
File Encryption, 3-13
Systemvoraussetzungen
Encryption Management for Apple FileVault, 3-16
Encryption Management for Microsoft BitLocker, 3-14
Full Disk Encryption, 3-9–3-11
PolicyServer, 3-2, 3-6, 3-7
PolicyServer MMC, 3-9

T

Token, 6-19
Tools
Command Line Helper, 6-25
DAAutoLogin, 6-25
Recovery, 9-26
Wiederherstellungskonsole, 9-20
Tool zum Ändern von Einstellungen für PolicyServer, A-6

U

Übersichtsdashboard
Hinzufügen von Registerkarten, 4-2
Registerkarten, 4-2
Registerkarten ändern, 4-3
Registerkarten löschen, 4-4

V

Verbesserungen, 2-4
Verschlüsselung
Datei und Ordner, 7-1
File Encryption, 7-1
Funktionen, 2-3
Hardware-basiert, 6-1
Software-basiert, 6-1
Vollständige Festplatte, 6-1
VMware Virtual Infrastructure, 3-2

W

Wichtigste Funktionen, 2-3
Widgets
Endpoint Encryption - Bericht zu Sicherheitsverstößen, 4-31
Endpoint Encryption - Gerätesperrung, 4-28
Endpoint Encryption Status, 4-21
Erfolglose Anmeldeversuche am Endpoint Encryption Gerät, 4-24
Erfolglose Anmeldeversuche des Endpoint Encryption Benutzers, 4-26
hinzufügen, 4-5
Hinzufügen von Registerkarten, 4-2
Konfigurieren, 4-6
Optionen, 4-6
verstehen, 4-4
Wiederherstellungskonsole, 9-6
Anmelden, 9-8
Anmeldung, 9-9
Benutzer
Bearbeiten, 9-17
Hinzufügen, 9-18
Löschen, 9-19
Benutzer verwalten, 9-17
Boot wiederherst, 9-15
Fehlerbehebung bei Netzwerkproblemen, 9-26
Festpl. entschlüss, 9-13
Funktionen, 9-6
Netzwerk, 9-20
Netzwerkkonfiguration, 9-20
Partit. bereitst., 9-15
PolicyServer wechseln, 9-22

Protokolle anzeigen, 9-19
Richtlinien verwalten, 9-19
Unternehmen wechseln, 9-20
Wiederherstellungsmethoden, 9-4
WLAN, 9-23
Zugreifen, 9-8
Windows, 9-9
Wiederherstellungsmethoden, 9-4
Windows Patch-Verwaltung, 6-25
WLAN, 6-6, 9-23

Z

Zentrale Verwaltung, 2-3
Ziele, 5-7
Ausstehend, 5-8
Zugänglichkeit
Bildschirmtastatur, 6-10

TREND MICRO INCORPORATED

Trend Micro Deutschland GmbH Zeppelinstraße 1 Hallbergmoos, Bayern 85399 Deutschland

Tel.: +49 (0) 811 88990-700 Fax: +4981188990799

sales@trendmicro.de marketing@trendmicro.de

www.trendmicro.com

Item Code: APGM68099/171128