F-Secure Policy Manager

Administratorhandbuch

Inhalt

Kapitel 1: Einführung.....7

Systemanforderungen.....8
Policy Manager Server.....8
Policy Manager Console.....8
Hauptkomponenten.....9
Funktionen.....10
Produktregistrierung.....11
Verwaltung auf Richtlinienbasis.....12
Management Information Base.....12

Kapitel 2: Installieren von das Produkt.....15

Sicherheitsprobleme.....16
Installieren von Policy Manager in hochsicheren Umgebungen.....16
Installationsreihenfolge.....16
Installieren von Policy Manager Server.....17
Herunterladen und Ausführen des Installationspakets.....17
Auswählen der zu installierenden Komponenten.....17
Abschließen des Migrationsassistenten.....18
Abschließen der Produktinstallation.....19
Überprüfen, dass die Installation erfolgreich war.....19
Ändern des Pfads für den Webbrowser.....19
das Produkt deinstallieren.....19

Kapitel 3: Verwenden von Policy Manager Console.....21

Übersicht.....22
Grundlegende Informationen und Aufgaben.....22
Anmelden.....22
Client SecurityVerwaltung von.....23
Benutzeroberfläche des erweiterten Modus.....24
Richtliniendomänen-Baum.....24
Inhalte der Benutzeroberfläche "Erweiterter Modus".....24
Fensterbereich "Meldung".....26
Die Symbolleiste.....26
Menübefehle.....27
Verwalten von Domänen und Hosts.....29
Hinzufügen von Richtliniendomänen.....29
Hinzufügen von Hosts.....30
Software-Verteilung.....33

Push-Installationen....34
Installation auf Richtlinienbasis....37
Lokale Installation und Updates mit vorkonfigurierten Paketen....38
Bereitstellung von Informationen....40
Verwalten von Richtlinien....40
Einstellungen....41
Verwerfen nicht verteilter Änderungen an den Einstellungen....41
Beschränkungen....41
Konfigurieren von Einstellungen....41
Richtlinienvererbung....42
Verwaltung von Vorgängen und Aufgaben....43
Alarme....43
Anzeigen von Alarmen und Berichten....43
Konfigurieren der Alarmweiterleitung....44
Dienstprogramm zur Berichterstellung....44
Fensterbereich "Auswahl der Domäne/des Hosts"....45
Fensterbereich "Auswahl des Berichtstyps"....45
Fensterbereich "Bericht"....46
Unterer Fensterbereich....46
Anzeigen und Exportieren eines Berichts....46
Voreinstellungen....47
Verbindungsspezifische Voreinstellungen....47
Gemeinsame Voreinstellungen....48

Kapitel 4: Verwalten von Policy Manager Server....49

Sichern und Wiederherstellen von Daten Policy Manager....50
Erstellen einer Sicherungskopie....50
Wiederherstellen einer Sicherungskopie....50
Exportieren und Importieren von Signaturschlüsseln....51
Replizieren von Software mithilfe von Image-Dateien....51

Kapitel 5: Aktualisieren der Virendefinitionsdatenbank....53

Automatische Updates mit Automatic Update Agent....54
Funktionsbeschreibung von Automatic Update Agent....54
Die Vorteile der Verwendung von Automatic Update Agent....54
Verwenden von Automatic Update Agent....55
Konfigurieren von Automatic Update Agent....55
Vorgehensweise zum Lesen der Protokolldatei....56
Erzwingen der sofortigen Suche nach neuen Updates durch Automatic Update Agent....57
Manuelles Aktualisieren der Datenbanken....57
Problembehandlung....57

Kapitel 6: Verwenden des Produkts unter Linux....59

Übersicht....60
Installation....60
Installieren von Automatic Update Agent und Policy Manager Server....61
Installieren von Policy Manager Console....62
das Produkt deinstallieren....63
Häufig gestellte Fragen (FAQ)....64

Kapitel 7: Web Reporting....69
Erstellen und Anzeigen von Berichten....70
Erstellen eines Berichts....70
Erstellen eines druckbaren Berichts....70
Automatische Berichterstellung....71
Verwalten von Web Reporting....71
Web ReportingFehlermeldungen von und Fehlerbehebung....71
Fehlermeldungen....71
Problembehandlung....72
Ändern des Ports für Web Reporting....72

Kapitel 8: Policy Manager Proxy....73
Übersicht....74

Kapitel 9: Problembehandlung....75
Policy Manager Server und Policy Manager Console....76
Policy ManagerWeb Reporting....79
Richtlinienverteilung....79

Kapitel 10: ILAUNCHR-Fehlercodes....81
Fehlercodes....82

Kapitel 11: Fehlercodes bei der Remote-Installation von FSII....85
Fehlercodes....86

Kapitel 12: NSC-Notation für Netzmasken....89
Details zur NSC-Notation....90

Kapitel

1

Einführung

Themen:

- *Systemanforderungen*
- *Hauptkomponenten*
- *Funktionen*
- *Produktregistrierung*
- *Verwaltung auf Richtlinienbasis*

Policy Manager bietet eine skalierbare Methode zur zentralen Verwaltung der Sicherheit verschiedener Anwendungen auf unterschiedlichen Betriebssystemen.

Mit Policy Manager können folgende Aufgaben ausgeführt werden:

- Definieren und Verteilen von Sicherheitsrichtlinien,
- Installieren von Anwendungssoftware auf lokalen und entfernten Systemen,
- Überwachen der Aktivitäten aller Systeme innerhalb des gesamten Unternehmens, um die Einhaltung der unternehmensinternen Sicherheitsrichtlinien und eine zentrale Kontrolle zu gewährleisten.

Nach der Einrichtung des Systems können Sie Statusinformationen aus der gesamten verwalteten Domäne von einem Standort aus abrufen. Auf diese Weise lässt sich sehr bequem gewährleisten, dass die gesamte Domäne geschützt ist. Ebenso einfach und schnell können Sie die Schutzeinstellungen bei Bedarf ändern. Sie können auch verhindern, dass Benutzer selbständig Änderungen an den Sicherheitsrichtlinien vornehmen. So können Sie sicher sein, dass der Schutz stets aktuell ist.

Systemanforderungen

Dieser Abschnitt enthält die Systemanforderungen für Policy Manager Server und für Policy Manager Console.

Policy Manager Server

Für die Installation von Policy Manager Server muss Ihr System die hier angegebenen Mindestvoraussetzungen erfüllen.

Betriebssystem:	Microsoft Windows: • Microsoft Windows Server 2003 SP1 oder höher (32-Bit); Standard, Enterprise, Web Edition oder Small Business Server Editionen • Windows Server 2003 SP1 oder höher (64-Bit); Standard oder Enterprise Editionen • Windows Server 2008 SP1 (32-Bit); Standard, Enterprise oder Web Server Editionen • Windows Server 2008 SP1 (64-Bit); Standard, Enterprise, Web Server, Small Business Server oder Essential Business Server Editionen • Windows Server 2008 R2 mit oder ohne SP1; Standard, Enterprise oder Web Server Edition Linux: • Red Hat Enterprise Linux 4, 5 und 6 • CentOS 5 • openSUSE Linux 11 • SUSE Linux Enterprise Server 10 und 11 • SUSE Linux Enterprise Desktop 11 • Debian GNU Linux 5 • Ubuntu 8.04, 10.04
Prozessor:	P4-2-Ghz- oder Multicore-3-GHz-CPU, abhängig vom Betriebssystem und der Größe der verwalteten Umgebung.
Arbeitsspeicher:	1 - 2 GB RAM, abhängig vom Betriebssystem und der Größe der verwalteten Umgebung.
Speicherplatz:	6 bis 10 GB freier Festplattenspeicher, abhängig von der Größe der verwalteten Umgebung.
Netzwerk	100-Mbit-Netzwerk.

Policy Manager Console

Für die Installation von Policy Manager Console muss Ihr System die hier angegebenen Mindestvoraussetzungen erfüllen

Betriebssystem:	Microsoft Windows: • Windows XP Professional (SP2 oder höher) • Windows Vista (32-Bit oder 64-Bit) mit oder ohne SP1; Business, Enterprise oder Ultimate Editionen • Windows 7 (32-Bit oder 64-Bit) mit oder ohne SP1; Professional, Enterprise oder Ultimate Editions • Microsoft Windows Server 2003 SP1 oder höher (32-Bit); Standard, Enterprise, Web Edition oder Small Business Server Editionen • Windows Server 2003 SP1 oder höher (64-Bit); Standard oder Enterprise Editionen • Windows Server 2008 SP1 (32-Bit); Standard, Enterprise oder Web Server Editionen • Windows Server 2008 SP1 (64-Bit); Standard, Enterprise, Web Server, Small Business Server oder Essential Business Server Editionen • Windows Server 2008 R2 mit oder ohne SP1; Standard, Enterprise oder Web Server Edition Linux: • Red Hat Enterprise Linux 4, 5 und 6 • CentOS 5 • openSUSE Linux 11 • SUSE Linux Enterprise Server 10 und 11 • SUSE Linux Enterprise Desktop 11 • Debian GNU Linux 5 • Ubuntu 8.04, 10.04
Prozessor:	P4-2-GHz-Prozessor
Arbeitsspeicher:	512 MB - 1 GB RAM, abhängig vom Betriebssystem und der Größe der verwalteten Umgebung.
Speicherplatz:	200 MB freier Festplattenspeicher.
Anzeige:	16-Bit-Grafik mit einer Auflösung von 1024 x 768 (32-Bit-Farbe bei einer Auflösung von 1280 x 1024 oder höher wird empfohlen).
Netzwerk:	100-Mbit-Netzwerk.

Hauptkomponenten

Die Stärke von Policy Manager liegt in der dreistufigen Verwaltungsarchitektur von F-Secure, die eine umfassende Skalierbarkeit für eine weitgehend dezentralisierte, mobile Arbeitswelt bietet.

Policy Manager Console	Policy Manager Console stellt eine zentrale Verwaltungskonsole bereit, mit der alle Sicherheitsaspekte der verwalteten Hosts kontrolliert und gesteuert werden können. Mit dieser Komponente kann der Administrator das Netzwerk in logische Einheiten für

übergreifende Richtlinien strukturieren. Diese Richtlinien werden auf Policy Manager Console definiert und danach über den Policy Manager Server an die Arbeitsstationen verteilt. Policy Manager Console ist eine *Java*-basierte Anwendung, die auf verschiedenen Plattformen installiert werden kann. Hiermit können Sie Management Agent von einem entfernten Standort ohne jegliche Eingriffe durch den Endbenutzer, Anmeldeskripts oder Neustarts auf anderen Arbeitsstationen installieren.

Policy Manager Console verfügt über zwei Benutzeroberflächen:

- Die Benutzeroberfläche im **Anti-Virus-Modus** ist für die zentrale Verwaltung von Client Security und Anti-virus for Workstations optimiert.
- Über die Benutzeroberfläche im **Erweiterten Modus** können andere F-Secure-Produkte verwaltet werden.

Policy Manager Server

Policy Manager Server fungiert als Datenbank für Richtlinien und Softwarepakete, die vom Administrator verteilt werden, und sendet darüber hinaus Statusinformationen und Alarmmeldungen an die verwalteten Hosts. Die Kommunikation zwischen Policy Manager Server und den verwalteten Hosts erfolgt durch das Standard-*HTTP-Protokoll*, das einen störungsfreien Betrieb im *LAN* und *WAN* ermöglicht.

Management Agent

Management Agent implementiert die Sicherheitsrichtlinien, die vom Administrator für die verwalteten Hosts festgelegt werden, und stellt für die Endbenutzer eine Benutzeroberfläche und weitere Dienste bereit. Er steuert alle Verwaltungsfunktionen auf einer lokalen Arbeitsstation, bietet eine gemeinsame Schnittstelle für alle F-Secure-Anwendungen und arbeitet innerhalb der Verwaltungsinfrastruktur auf Richtlinienbasis.

Web Reporting

Web Reporting ist ein unternehmensweites webbasiertes System zur Erstellung von grafischen Berichten, das im Lieferumfang von Policy Manager Server enthalten ist. Mit Web Reporting können Sie mühelos grafische Berichte anhand historischer Trenddaten erstellen und ungeschützte und für Virusausbrüche anfällige Computer identifizieren.

Update Server & Agent

Update Server & Agent werden zur Aktualisierung der Viren- und Spyware-Definitionen auf den verwalteten Hosts verwendet und sind in Policy Manager Server enthalten. Mit Automatic Update Agent können Benutzer Virendefinitions-Updates und Informationen über neue Bedrohungen empfangen, ohne ihre Arbeit unterbrechen oder Dateien aus dem Internet herunterladen zu müssen. Der Update-Agent lädt die Dateien automatisch herunter und verwendet dabei nur die Bandbreite, die nicht von anderen Internet-Anwendungen beansprucht wird. Wenn Automatic Update Agent immer mit dem Internet verbunden ist, werden die aktualisierten Virendefinitionen automatisch innerhalb von zwei Stunden empfangen, nachdem sie von F-Secure veröffentlicht wurden.

Funktionen

Hier werden einige der Hauptfunktionen von Policy Manager beschrieben.

Software-Verteilung

- Installation von F-Secure-Produkten auf den Hosts von einem zentralen Standort aus und Aktualisierung der Programm- und Datendateien inkl. der Virendefinitions-Updates.
- Updates können unter Zuhilfenahme mehrerer Methoden bereitgestellt werden:
  - Von einer F-Secure-CD.
  - Von der F-Secure-Website zum Kunden. Diese Updates können automatisch vom Automatic Update Agent installiert (Push-Installation) oder manuell von der F-Secure-Website abgerufen werden.

	• Mit Policy Manager Console können vorkonfigurierte Installationspakete exportiert werden, die auch über Fremdanbietersoftware, wie SMS oder ähnliche Tools, bereitgestellt werden können.
Konfiguration und Richtlinienverwaltung	• Zentrale Konfiguration von Sicherheitsrichtlinien. Die Richtlinien werden vom Administrator über den Policy Manager Server an die Arbeitsstationen der Benutzer verteilt. Die Integrität der Richtlinien wird mithilfe digitaler Signaturen gewährleistet.
Ereignisverwaltung	• Berichterstattung an Event Viewer (lokale Protokolle und Remote-Protokolle), SNMP-Agent, E-Mail, Berichtdateien und die Erstellung von Ereignisstatistiken.
Leistungsmanagement	• Verarbeitung und Berichterstellung für Statistiken und Leistungsdaten.
Aufgabenverwaltung	• Verwaltung der Aufgaben zur Virenüberprüfung und anderer Vorgänge.

Produktregistrierung

Sie haben die Möglichkeit, Informationen über die Verwendung von Policy Manager an F-Secure weiterzugeben, indem Sie Ihr Produkt registrieren.

Folgende Fragen und Antworten enthalten weitere Informationen zur Registrierung Ihrer Installation von Policy Manager. Zudem sollten Sie die Lizenzbestimmungen von F-Secure (*http://www.f-secure.com/en_EMEA/estore/license-terms/*) und die Datenschutzrichtlinie (*http://www.f-secure.com/en_EMEA/privacy.html*) lesen.

Warum erfasst F-Secure Daten?

Um unseren Service zu verbessern, erfassen wir statistische Daten in Bezug auf die Verwendung von F-Secure-Produkten. Wenn Sie F-Secure helfen möchten, das Service- und Supportangebot zu verbessern, können Sie uns erlauben, diese Informationen mit Ihren Kontaktinformationen zu verknüpfen. Geben Sie hierfür bei der Installation von Policy Manager die Kundennummer aus Ihrem Lizenzvertrag ein.

Welche Informationen werden gesendet?

Wir erfassen Informationen, die nicht mit dem Endbenutzer des Computers in Verbindung gebracht werden können. Erfasst werden zum Beispiel F-Secure-Produktversionen, Betriebssystemversionen, die Anzahl der verwalteten Hosts und die Anzahl der nicht verbundenen Hosts. Die Informationen werden in einem sicheren und verschlüsselten Format übertragen.

Welchen Vorteil habe ich davon, wenn ich Informationen an F-Secure weitergebe?

Wenn Sie sich an unseren Support wenden, können wir mithilfe der erfassten Informationen schneller eine Lösung für Ihr Problem finden. Darüber hinaus können wir mit diesen Informationen unser Produkt und unsere Dienstleistungen noch besser an die Bedürfnisse unserer Kunden anpassen.

Wo werden die Informationen gespeichert, und wer kann auf sie zugreifen?

Die Daten werden im streng gesicherten Rechenzentrum von F-Secure gespeichert und sind nur für die hierfür zuständigen Mitarbeiter von F-Secure zugänglich.

Verwaltung auf Richtlinienbasis

Eine Sicherheitsrichtlinie besteht aus einer Anzahl genau festgelegter Regeln, die bestimmen, wie vertrauliche Daten und andere Ressourcen verwaltet, geschützt und verteilt werden sollen.

Die Verwaltungsarchitektur von F-Secure verwendet Richtlinien, die vom Administrator zentral konfiguriert werden, um eine optimale Sicherheitskontrolle in einer Unternehmensumgebung zu gewährleisten. Zur Verwaltung auf Richtlinienbasis werden zahlreiche Funktionen implementiert:

- Steuerung und Überwachung der Produkte von einem Remote-Computer aus.
- Überwachung der Statistiken durch die Produkte und den Management Agent.
- Starten vordefinierter Vorgänge von einem Remote-Computer.
- Übertragung von Alarmen und Benachrichtigungen von den Produkten an den Systemadministrator.

Der Informationsfluss zwischen Policy Manager Console und den Hosts erfolgt durch die Übertragung von Richtliniendateien. Es gibt drei Arten von Richtliniendateien:

- *Standardrichtliniendateien* (`.dpf`)
- *Basisrichtliniendateien* (`.bpf`)
- *Inkrementelle Richtliniendateien* (`.ipf`)

Die aktuellen Produkteinstellungen bestehen aus allen drei Richtliniendateitypen:

Standardrichtliniendateien	Die Standardrichtliniendatei enthält die Standardwerte (Werkseinstellungen) für ein einzelnes Produkt, die während der Installation eingerichtet werden. Standardrichtlinien werden nur auf dem Host verwendet. Wenn weder die Basisrichtliniendatei noch die inkrementelle Richtliniendatei einen Eintrag für eine Variable enthält, wird der Wert aus der Standardrichtliniendatei verwendet. Neue Produktversionen enthalten auch immer neue Versionen der Standardrichtliniendatei.
Basisrichtliniendateien	Basisrichtliniendateien enthalten die Verwaltungseinstellungen und Beschränkungen für alle Variablen des F-Secure-Produkts auf einem bestimmten Host (bei Richtlinien auf Domänenebene können mehrere Hosts dieselbe Richtliniendatei verwenden). Eine Basisrichtliniendatei wird von Policy Manager Console signiert. Dadurch ist die Datei vor Änderungen geschützt, während sie im Netzwerk übertragen wird und während sie im Dateisystem des Hosts gespeichert ist. Diese Dateien werden von Policy Manager Console an Policy Manager Server gesendet. Der Host überprüft in regelmäßigen Abständen, ob neue Richtlinien von Policy Manager Console erstellt wurden.
Inkrementelle Richtliniendateien	Inkrementelle Richtliniendateien werden zum Speichern lokaler Änderungen an der Basisrichtlinie verwendet. Es sind nur solche Änderungen erlaubt, die gemäß den in der Basisrichtlinie festgelegten Einschränkungen zulässig sind. Die inkrementellen Richtliniendateien werden in regelmäßigen Abständen an Policy Manager Console gesendet, damit der Administrator die aktuellen Einstellungen und Statistiken anzeigen kann.

Management Information Base

Bei der *Management Information Base* (*MIB*) handelt es sich um eine hierarchische Management-Datenstruktur, die vom *SNMP*-Protokoll (*Simple Network Management Protocol*) verwendet wird.

Bei Policy Manager wird die Struktur der MIB verwendet, um den Inhalt der Richtliniendateien zu definieren. Jede Variable verfügt über eine Objektkennung (*OID* = *Object Identifier*) und einen Wert, auf den über die *Richtlinien-API* zugegriffen werden kann. Neben den grundlegenden SNMP-MIB-Definitionen beinhaltet das

F-Secure-MIB-Konzept zahlreiche Erweiterungen, die für eine vollständige richtlinienbasierte Verwaltung erforderlich sind.

Die folgenden Kategorien sind in einer Produkt-MIB definiert:

Einstellungen	Werden für die Verwaltung der Arbeitsstation entsprechend dem SNMP verwendet. Die verwalteten Anwendungen müssen die hier festgelegten Grenzwerte einhalten.
Statistiken	Dient zur Übertragung der Produktstatistiken an Policy Manager Console.
Vorgänge	Vorgänge werden mithilfe von zwei Richtlinienvariablen verwaltet: (1) einer Variable für die Übertragung der Vorgangskennung an den Host und (2) einer Variable, um Policy Manager Console über die ausgeführten Vorgänge zu informieren. Die zweite Variable wird unter Verwendung normaler Statistiken übertragen. Dabei werden alle vorherigen Vorgänge gleichzeitig quittiert. Der Unterstruktur ist ein benutzerdefinierter Editor zum Bearbeiten von Vorgängen zugeordnet. Dieser Editor blendet die beiden Variablen aus.
Privat	Die MIBs für das Verwaltungskonzept können außerdem Variablen enthalten, die das Produkt für die interne Verwendung zwischen Sitzungen speichert. Dadurch ist das Produkt unabhängig von externen Diensten wie den Windows-Registrierungsdateien.
Traps	Traps sind Meldungen (einschließlich Alarmen und Ereignissen), die an die lokale Konsole, an Protokolldateien, an Remote-Verwaltungsprozesse usw. gesendet werden. Die folgenden Trap-Typen werden am häufigsten von F-Secure-Produkten gesendet:
	Info. Normale Informationen eines Hosts über einen Arbeitsvorgang.
	Warnung. Eine Warnung vom Host.
	Fehler. Ein behebbarer Fehler auf dem Host.
	Schwerwiegender Fehler. Ein unbehebbarer Fehler auf dem Host.
	Sicherheitsalarm. Ein Sicherheitsrisiko auf dem Host.

Kapitel

2

Installieren von das Produkt.

Themen:

- *Sicherheitsprobleme*
- *Installieren von Policy Manager in hochsicheren Umgebungen*
- *Installationsreihenfolge*
- *Installieren von Policy Manager Server*
- *Ändern des Pfads für den Webbrowser*
- *das Produkt deinstallieren.*

In diesem Abschnitt werden die zur Installation von Policy Manager erforderlichen Schritte erläutert.

Hier finden Sie Anweisungen zur Installation der Hauptkomponenten des Produkts, Policy Manager Server und Policy Manager Console.

Sicherheitsprobleme

Policy Manager Servernutzt *Jetty Web Server*-Technologie und auch wenn wir unser Möglichstes tun, um eine sichere und aktuelle Technologie zu liefern, empfehlen wir, die folgende Website zu Informationen über Jetty-Technologie und Sicherheit aufzurufen.

Eine Liste mit Jetty-Sicherheitsberichten kann unter *http://docs.codehaus.org/display/JETTY/Jetty+Security* abgerufen werden.

Hinweis: Wichtige Informationen zur Installation und Sicherheit finden Sie in den Versionshinweisen. Lesen Sie diese sorgfältig durch.

Installieren von Policy Manager in hochsicheren Umgebungen

Policy Manager wurde für den Einsatz in internen Unternehmensnetzwerken als Verwaltungsprogramm für Anti-Virus-Produkte von F-Secure entwickelt und sollte nicht über öffentliche Netze wie das Internet eingesetzt werden.

Hinweis: Bei der Installation von Policy Manager in hochsicheren Umgebungen sollten Sie sicherstellen, dass der *Administrations-Port* (standardmäßig Port 8080) und der *Host-Port* (standardmäßig Port 80) im Internet nicht sichtbar sind.

Integrierte Sicherheitsfunktionen

Zugriff auf Policy Manager ist auf Benutzer beschränkt, die über ein Konto verfügen. Ein nicht autorisierter Benutzer kann daher keine Änderungen an den verwalteten Hosts vornehmen.

Alternativ zur separaten Installation der Komponenten können Policy Manager Console und Policy Manager Server auf dem gleichen Rechner mit auf den Localhost beschränktem Zugriff installiert werden. Der Remote-Zugriff durch den Administrator auf Policy Manager Console kann über ein sicheres Remote-Desktopprodukt erfolgen.

Die Kommunikation zwischen Policy Manager Server und Policy Manager Console wird über das HTTPS-Protokoll gesichert.

Web Reporting in hochsicheren Umgebungen

Web Reporting wurde für den Einsatz in internen Unternehmensnetzwerken entwickelt und eignet sich z.B. zur Erstellung grafischer Berichte zum Virenschutzstatus und den Alarmen von Client Security. F-Secure empfiehlt, Web Reporting nicht über öffentliche Netze wie das Internet einzusetzen.

Eine Alternative für hochsichere Umgebungen besteht darin, den Zugriff auf Web Reporting nur während der Installation auf den lokalen Host zu beschränken. Anschließend kann Web Reporting nur von dem Benutzer verwendet werden, der über physischen Zugriff auf den lokalen Host verfügt.

Installationsreihenfolge

Wenn Sie Policy Manager-Komponenten auf verschiedenen Computern installieren, sollte dies in einer bestimmten Reihenfolge geschehen.

Befolgen Sie für die Installation von Policy Manager diese Installationsreihenfolge (es sei denn Sie installieren Policy Manager Server und Policy Manager Console auf dem gleichen Rechner. In diesem Fall werden über die Einrichtung beide Komponenten während des Installationsvorgangs installiert):

1. Policy Manager Server,
2. Policy Manager Console,
3. Verwaltete Punktanwendungen.

Installieren von Policy Manager Server

Dieser Abschnitt enthält Anweisungen zur Installation von Policy Manager Server.

Zur Installation von Policy Manager Server benötigen Sie physischen Zugriff auf den Server-Computer.

Die Kommunikation zwischen Policy Manager Server und anderen Komponenten wird über das HTTPS-Protokoll gesichert.

Policy Manager Server speichert u.a. folgende Dateien:

- Struktur der Richtliniendomäne.
- Richtliniendaten, bei denen es sich um die eigentlichen Richtlinieninformationen handelt, die jeder Richtliniendomäne oder jedem Host zugeordnet sind.
- Benutzerkonteninformationen.
- Aus den Richtliniendaten erzeugte Basisrichtliniendateien.
- Statusinformationen, einschließlich inkrementeller Richtliniendateien, Alarme und Berichte.
- Autoregistrierungs-Anfragen, die von den Hosts gesendet wurden.
- Updatepakete für die Programminstallation und die Virendefinitionsdatenbanken.
- Statistiken und historische Trenddaten über die Hosts.

Herunterladen und Ausführen des Installationspakets

Im ersten Schritt der Installation von Policy Manager muss das Installationspaket heruntergeladen und ausgeführt werden.

So beginnen Sie mit der Installation des Produkts:

1. Laden Sie das Installationspaket unter *www.f-secure.com/webclub* herunter.
   Sie finden die Datei im Abschnitt **Download** der Seite **Policy Manager**.
2. Doppelklicken Sie auf die ausführbare Datei, um mit der Installation zu beginnen.
   Das Installationsprogramm wird gestartet.
3. Wählen Sie die Installationssprache und klicken auf **Weiter**, um fortzufahren.
4. Lesen Sie die Lizenzvereinbarung, wählen Sie dann **Lizenz annehmen** und klicken Sie auf **Weiter**, um fortzufahren.

Auswählen der zu installierenden Komponenten

Als Nächstes müssen Sie die zu installierenden Produktkomponenten auswählen.

So fahren Sie mit der Installation des Produkts fort:

1. Wählen Sie die Komponenten, die installiert werden sollen, und klicken Sie auf **Weiter**, um fortzufahren.
   - Wählen SiePolicy Manager Server und Policy Manager Console, um beide Komponenten auf demselben Computer zu installieren.

- Wählen Sie Policy Manager Server, wenn Sie Policy Manager Console auf einem anderen Computer installieren möchten.

2. Wählen Sie den Zielordner, und klicken Sie dann auf **Weiter**.

   Es wird empfohlen, das Standardinstallationsverzeichnis zu wählen. Wenn Sie das Produkt in einem anderen Verzeichnis installieren möchten, klicken Sie auf **Durchsuchen**, und wählen Sie ein neues Verzeichnis aus.

   Hinweis: Wenn Sie Management Agent auf demselben Computer installiert haben, wird dieses Fenster nicht angezeigt.

3. Geben Sie Ihre Kundennummer ein, und klicken Sie auf **Weiter**.

   Ihre Kundennummer finden Sie im Lizenzvertrag, der dem Produkt beigefügt ist.

4. Geben Sie ein Kennwort für Ihr admin-Benutzerkonto ein und bestätigen Sie dieses. Klicken Sie auf **Weiter**.

   Nutzen Sie dieses Kennwort für die Anmeldung bei Policy Manager Console mit dem Benutzernamen `admin`.

5. Wählen Sie die Policy Manager Server-Module, die aktiviert werden sollen:

   - Das **Host**-Modul wird für die Kommunikation mit den Hosts benötigt. Der Standard-Port ist Port 80.
   - Das **Verwaltungs-Modul** wird für die Kommunikation mit Policy Manager Console verwendet. Der Standard-HTTP-Port ist 8080.

     Hinweis: Wenn Sie den Standard-Port für die Kommunikation ändern möchten, müssen Sie außerdem die neue Port-Nummer in der URL **Verbindungen** bei der Anmeldung Policy Manager Console angeben.

     Standardmäßig ist der Zugriff auf das **Verwaltungs-Modul** auf den lokalen Computer beschränkt. Dies gewährleistet die größte Sicherheit für die Verwendung des Produkts. Wenn jedoch eine Verbindung über das Netzwerk verwendet wird, empfiehlt es sich, die Datenkommunikation mit F-Secure SSH zu sichern.
   - Das Modul für die **Web-Berichterstellung** wird für die Kommunikation mit Web Reporting verwendet. Geben Sie an, ob das Modul aktiviert werden soll. Bei der Web-Berichterstellung werden Serverdaten über eine lokale Socket-Verbindung zum **Verwaltungs-Modul** abgerufen. Der Standard-Port ist Port 8081.

     Der Zugriff auf Web Reporting ist standardmäßig auch von anderen Computern aus möglich. Wenn Sie den Zugriff auf diesen Computer beschränken möchten, wählen Sie **Schränken Sie den Zugriff auf den lokalen Computer ein**.

6. Klicken Sie auf **Weiter**, um fortzufahren.

Abschließen des Migrationsassistenten

Der Migrationsassistent wird während der Installation automatisch gestartet, damit Sie Daten aus einer vorherigen Version von Policy Manager importieren können.

Der Migrationsassistent wird nur bei der Aktualisierung von einer älteren Version von Policy Manager geöffnet. Können keine älteren Policy Manager-Daten gefunden werden, wird der Assistent nicht angezeigt.

Wird der Migrationsassistent nicht angezeigt, schlägt er fehl oder wenn Sie Migrationsdaten später importieren möchten, können Sie den Migrationsassistenten auch zu einem anderen Zeitpunkt über die ausführbare Datei `<F-Secure>\Management Server 5\bin\fspms-migration-wizard.exe` öffnen.

1. Geben Sie die Pfade zum Kommunikationsverzeichnis und Schlüsselpaar der älteren Version ein und klicken Sie auf **Weiter**.

2. Lesen Sie sich die unten angegebenen Informationen über Richtliniendomänen durch und klicken Sie auf **Start**.
3. Warten Sie, bis der Datenimport abgeschlossen ist, und klicken Sie auf **Schließen**, um den Assistenten zu beenden.

Der Migrationsassistent wird geschlossen und der Installationsassistent wird wieder angezeigt.

Hinweis: Die commdir-Daten und Signaturschlüssel aus einer vorherigen Version von Policy Manager werden nach der Aktualisierung nicht gelöscht und können weiter verwendet werden, wenn Sie wieder auf eine ältere Version abrüsten müssen.

Hinweis: Bei der Aktualisierung werden auf Richtlinien basierende Installationsvorgänge und die Zeitdauer, nach der die Verbindung eines Hosts als aufgehoben angesehen wird, nicht mit übernommen. Sie können die Zeitdauer im Dialogfeld **Tools** > **Serverkonfiguration** einrichten.

Abschließen der Produktinstallation

Als nächster Schritt muss die Installation des Produkts abgeschlossen werden.

1. Überprüfen Sie alle Änderungen, die das Installationsprogramm ausführen wird, und klicken Sie dann auf **Starten**, um die ausgewählten Komponenten zu installieren.
   Nach Abschluss der Installation wird angezeigt, ob alle Komponenten erfolgreich installiert wurden.
2. Klicken Sie auf **Fertig stellen**, um die Installation abzuschließen.
3. Starten Sie den Computer neu, wenn Sie dazu aufgefordert werden.

Überprüfen, dass die Installation erfolgreich war

Als nächster Schritt ist zu überprüfen, ob das Produkt korrekt installiert wurde.

So stellen Sie fest, ob die Installation erfolgreich war:

1. Öffnen Sie einen Webbrowser auf dem Computer, auf dem Policy Manager Server installiert wurde.
2. Geben Sie `https://localhost:8080` als Adresse ein (wenn Sie die standardmäßige Admin-Port-Nummer während der Installation verwenden) und betätigen Sie die Eingabetaste.
   Wenn die Server-Installation erfolgreich war, wird eine Begrüßungsseite angezeigt.

Ändern des Pfads für den Webbrowser

Policy Manager Console ermittelt während der Installation den Pfad zum Standard-Webbrowser.

Gehen Sie wie folgt vor, um den Pfad zum Webbrowser zu ändern:

1. Wählen Sie **Extras** > **Voreinstellungen** aus dem Menü.
2. Öffnen Sie die Registerkarte **Verzeichnisse**, und geben Sie den neuen Pfad ein.

das Produkt deinstallieren.

Führen Sie die folgenden Schritte aus, um Policy Manager-Komponenten zu deinstallieren.

So deinstallieren Sie Policy Manager-Komponenten:

1. Öffnen Sie das **Start**-Menü von Windows, und rufen Sie die **Systemsteuerung** auf.

2. Wählen Sie **Software**.
3. Wählen Sie die Komponente aus, die Sie deinstallieren möchten (Policy Manager Console oder Policy Manager Server), und klicken Sie auf **Ändern/Entfernen**.
   Das Dialogfeld zur **Deinstallation** von F-Secure wird angezeigt.
4. Klicken Sie auf **Starten**, um mit der Deinstallation zu beginnen.
5. Klicken Sie nach Abschluss der Deinstallation auf **Schließen**.
6. Wiederholen Sie die oben aufgeführten Schritte, wenn Sie weitere Komponenten von Policy Manager deinstallieren möchten.
7. Schließen Sie das Applet **Software**, wenn Sie die jeweiligen Komponenten deinstalliert haben.
8. Es wird empfohlen, den Computer nach der Deinstallation neu zu starten.

   Beim Neustart werden alle auf dem Computer verbliebenen Produktdateien gelöscht. Dies ist notwendig, wenn Sie die gleichen F-Secure-Produkte anschließend erneut installieren möchten.

Kapitel

3

Verwenden von Policy Manager Console

Themen:

- *Übersicht*
- *Grundlegende Informationen und Aufgaben*
- *Verwalten von Domänen und Hosts*
- *Software-Verteilung*
- *Verwalten von Richtlinien*
- *Verwaltung von Vorgängen und Aufgaben*
- *Alarme*
- *Dienstprogramm zur Berichterstellung*
- *Voreinstellungen*

Dieser Abschnitt enthält Informationen über die Policy Manager Console Komponente und deren Verwendung.

Policy Manager Console ist ein Dienstprogramm zur Remote-Verwaltung der am häufigsten eingesetzten Sicherheitsprogramme von F-Secure. Die Konsole wurde entwickelt, um eine gemeinsame Plattform für alle Sicherheitsverwaltungsfunktionen bereitzustellen, die in einem Unternehmensnetzwerk benötigt werden.

Übersicht

Dieser Abschnitt enhält einige allgemeine Informationen über Policy Manager Console.

Die Konzeption von Policy Manager Console besteht aus Hosts, die in Richtliniendomänen gruppiert werden können. Die Richtlinien sind host-orientiert, d. h. auch in Mehrbenutzerumgebungen gelten für alle Benutzer eines bestimmten Hosts dieselben Einstellungen.

Ein Administrator kann unterschiedliche Sicherheitsrichtlinien für jeden Host oder eine einzelne Richtlinie für mehrere Hosts erstellen. Die Richtlinie kann über ein Netzwerk an die Arbeitsstationen, Server und Sicherheits-Gateways verteilt werden.

Mit Policy Manager Console kann ein Administrator Folgendes durchführen:

- die Attributwerte der verwalteten Programme festlegen.
- die Benutzerrechte festlegen, die bestimmen, ob die Benutzer Attributwerte anzeigen oder ändern dürfen, die zuvor vom Administrator remote festgelegt wurden.
- verwaltete Hosts in Richtliniendomänen mit gemeinsamen Attributwerten gruppieren.
- Host- und Domänenhierarchien ohne großen Aufwand verwalten.
- signierte Richtliniendefinitionen erstellen, die Attributwerte und Beschränkungen enthalten.
- Statusangaben anzeigen.
- Alarme verarbeiten.
- F-Secure Berichte zur Anti-Virus-Überprüfung verwalten.
- Remote-Installationen verwalten
- Berichte im HTML-Format anzeigen oder Berichte in verschiedene Formate exportieren.

Policy Manager Console erstellt die Richtliniendefinition und zeigt Status- sowie Warnmeldungen an. Jeder verwaltete Host verfügt über ein Modul (Management Agent), das die Richtlinie auf dem Host durchsetzt.

Benutzer mit Nur-Lese-Berechtigungen können Folgendes durchführen:

- Richtlinien, Statistiken, Betriebsstatusangaben, Versionsnummern der installierten Programme, Alarme und Berichte anzeigen
- Policy Manager Console Einstellungen ändern, da diese Installation benutzerabhängig ist und sich die Änderungen durch einen Benutzer daher nicht auf andere Benutzer auswirken.

Folgende Aktionen können von Benutzern im schreibgeschützten Modus nicht ausgeführt werden:

- Domänenstruktur oder Eigenschaften von Domänen oder Hosts ändern
- Programmeinstellungen ändern
- Vorgänge ausführen
- Programme installieren
- Richtliniendaten speichern
- Richtlinien verteilen
- Alarme oder Berichte löschen

Grundlegende Informationen und Aufgaben

In den folgenden Abschnitten werden das Anmeldungsverfahren, Menübefehle und grundlegende Aufgaben von Policy Manager Console beschrieben.

Anmelden

Beim Starten von Policy Manager Consolewird das Dialogfeld **Anmeldung** geöffnet.

Tipp: Sie können auf **Optionen** klicken, um das Dialogfeld zu erweitern und weitere Optionen anzuzeigen.

Im Dialogfeld **Anmeldung** können Sie definierte Verbindungen auswählen. Für jede Verbindung werden eigene Einstellungen festgelegt. Dadurch wird die Verwaltung mehrerer Server mit einer einzigen Instanz von Policy Manager Console vereinfacht.

Darüber hinaus ist es möglich, mehrere Verbindungen zu einem einzigen Server aufzubauen. Geben Sie nach der Auswahl der Verbindung Ihren Policy Manager Console-Benutzernamen und das zugehörige Kennwort ein. Benutzername und Kennwort sind für Ihr Policy Manager-Benutzerkonto spezifisch. Sie sind nicht mit Ihrem Netzwerk- oder Netzwerk-Administrator-Kennwort verbunden. Das Kennwort für den Benutzer `admin` wird bei der Installation des Programms festgelegt und andere Benutzer (entweder mit admin- oder Nur-Lese-Zugriffsrechten) werden über Policy Manager Console erstellt.

Der Setup-Assistent baut eine erste Verbindung auf, die standardmäßig im Feld **Verbindungen:** erscheint. Wenn Sie weitere Verbindungen hinzufügen möchten, klicken Sie auf **Hinzufügen**, oder klicken Sie auf **Bearbeiten**, um eine vorhandene Verbindung zu bearbeiten. (Diese Optionen sind nur verfügbar, wenn das Dialogfeld erweitert wird.)

Verbindungseigenschaften

Die Verbindungseigenschaften werden beim Hinzufügen einer neuen Verbindung oder beim Bearbeiten einer vorhandenen Verbindung festgelegt.

Der Link zum Datenrepository ist als HTTPS-URL von Policy Manager Server definiert.

Im Feld **Anzeigen als** wird festgelegt, wie die Verbindung im Feld **Verbindung:** im Dialogfenster **Anmeldung** genannt wird. Bleibt das Feld **Name** leer, wird die URL angezeigt.

Neue Benutzer hinzufügen

Sie können Benutzer mit Administrator- oder Nur-Lese-Zugriff auf Policy Manager hinzufügen.

1. Wählen Sie **Tools** > **Benutzer** aus dem Menü aus.
   Das Dialogfenster **Benutzer** wird geöffnet. Hier sind alle aktuellen Benutzer aufgelistet.
2. Klicken Sie auf **Hinzufügen**, um einen neuen Benutzer hinzuzufügen.
3. Geben Sie einen Benutzernamen und ein Kennwort für den neuen Benutzer ein.
4. Wählen Sie **Nur-Lese-Zugriff** aus, wenn Sie den Zugriff des Benutzers beschränken möchten, und klicken Sie auf **OK**.
   Der neue Benutzer wird auf der Benutzerliste angezeigt. Dieser kann nun auf Policy Manager zugreifen.

Hinweis: Jeder Benutzer mit Administrator-Zugriffsrechten kann andere Benutzer löschen, aber es muss mindestens einen Benutzer mit vollständigem Administrator-Zugriff geben. Wird ein Benutzerkonto gelöscht, während dieser Benutzer angemeldet ist, wird dieser abgemeldet und erhält eine Meldung, sich bei der nächsten Verbindung mit Policy Manager wieder anzumelden.

Ändern des Kennworts

Sie können das Kennwort für Ihre Benutzerkonto ändern, wenn Sie bei Policy Manager angemeldet sind.

1. Wählen Sie **Tools** > **Kennwort ändern** aus dem Menü aus.
2. Geben Sie Ihr neues Kennwort in beide Felder ein und klicken Sie auf **OK**.
   Ihr Kennwort wurde nun geändert.

Client SecurityVerwaltung von

Beim ersten Start von Policy Manager Console öffnet sich die Benutzeroberfläche des **Anti-Virus**-Modus.

Dieser Modus wurde für die Verwaltung von Client Security optimiert. Über die Benutzeroberfläche des **Anti-Virus**-Modus können Sie die meisten Aufgaben rund um die Verwaltung von Client Security, Anti-virus for Workstations und Anti-virus for Windows Servers vornehmen.

Sie können die meisten Aufgaben über die Benutzeroberfläche des **Anti-Virus-Modus** durchführen. Wenn Sie jedoch andere Programme als Client Security verwalten müssen, müssen Sie die Benutzeroberfläche des **erweiterten Modus** verwenden.

Benutzeroberfläche des erweiterten Modus

Um die Einstellungen zu konfigurieren, die im Modus **Anti-Virus** nicht verfügbar sind, müssen Sie die Benutzeroberfläche von **Erweiterten Modus** ändern.

Wählen Sie **Ansicht** > **Erweiterter Modus**, um zur Benutzeroberfläche **Erweiterter Modus** zu wechseln.

Richtliniendomänen-Baum

Sie können Vorgänge für Richtliniendomänen und Hosts in der Baumstruktur **Richtliniendomäne** durchführen.

In der Baumstruktur **Richtliniendomäne** können Sie folgende Vorgänge durchführen:

- Fügen Sie eine neue Richtliniendomäne hinzu (klicken Sie auf das Symbol in der Symbolleiste). Eine neue Richtliniendomäne kann nur erstellt werden, wenn eine übergeordnete Domäne gewählt wurde.
- Fügen Sie einen neuen Host hinzu (klicken Sie auf das Symbol).
- Einen Host suchen.
- Zeigen Sie die Eigenschaften einer Domäne oder eines Host-Rechners an. Alle Hosts und Domänen sollten eindeutige Namen haben.
- Importieren Sie neue Hosts.
- Hosts aus einer Windows-Domäne automatisch erkennen.
- Hosts oder Domänen löschen.
- Hosts oder Domänen mit Hilfe der Funktionen zum Ausschneiden und Einfügen verschieben.
- Richtliniendateien exportieren.

Nachdem Sie eine Domäne oder einen Host ausgewählt haben, können Sie auf die oben beschriebenen Optionen über das Menü **Bearbeiten** zugreifen.

Die Domänen, auf die sich die Befehle beziehen, sind keine Windows NT- oder DNS-Domänen. Richtliniendomänen sind Host- oder Subdomänen-Gruppen mit einer ähnlichen Sicherheitsrichtlinie.

Inhalte der Benutzeroberfläche "Erweiterter Modus"

Die Funktion des Hauptbereichs der Anwendung in der Benutzeroberfläche **Erweiterter Modus** ändert sich je nachdem, welche Registerkarte geöffnet ist.

- Registerkarte **Richtlinie**: Sie können den Wert einer Richtlinienvariablen einrichten. Alle Änderungen haben Auswirkungen auf die ausgewählte Richtliniendomäne oder den ausgewählten Host. Für jeden Typ an Richtlinienvariable stehen vordefinierte Einstellungen zur Verfügung.
- Registerkarte **Status**: Sie können Einstellungen, bei denen es sich um lokale Änderungen handelt, die vom Host gemeldet wurden, und Statistiken anzeigen.
- Registerkarte **Alarme**: Wenn auf der Registerkarte **Alarme** ein Alarm gewählt wird, werden Einzelheiten des Alarms angezeigt.
- Registerkarte **Scan-Berichte**: Wird auf der Registerkarte **Berichte** ein Bericht ausgewählt, werden die Einzelheiten zum Bericht angezeigt.
- Registerkarte **Installation**: Sie können Informationen zur Installation anzeigen und bearbeiten.

Die traditionelle **MIB-Struktur** von Policy Manager Console enthält alle Einstellungen/Vorgänge (Richtlinie) und lokalen Einstellungen/Statistiken (Status) in einer komponentenspezifischen **MIB-Struktur**.

Verwenden der Hilfe

Wenn Sie einen **MIB**-Baumknoten auf der Registerkarte **Richtlinie** auswählen, wird der verfügbare Hilfetext im Hauptanwendungsbereich angezeigt.

Bearbeiten der Richtlinieneinstellungen

Sie können häufige Richtlinieneinstellungen im Hauptbereich der Anwendung bearbeiten.

Wählen Sie ein Produkt (z. B. Management Agent) auf der Registerkarte **Richtlinie** aus und klappen Sie die Baumstruktur auf, um die verfügbaren Einstellungen und Vorgänge für das Produkt anzusehen. Wenn Sie auf einen Baumknoten klicken, erfolgt über Policy Manager Console die Anzeige des Feldes, in dem Sie die ausgewählten Einstellung ändern können.

Sie können die Richtlinieneinstellungen normal ändern und Änderungen durch den Benutzer entweder zulassen oder nicht zulassen.

Definieren von Richtlinieneinstellungen

Die meisten Seiten für die Richtlinieneinstellung nutzen entweder ein Textfeld oder ein Dropdown-Feld zur Definition der Einrichtung.

Zusätzlich zu dem Feld für die Eingabe oder Auswahl des Wertes für die Richtlinienvariable verfügen die meisten Einstellungen über drei Schaltflächen: **Bereinigen**, **Wert erzwingen** und **Domänenwerte anzeigen**.

Bereinigen

Über die Schaltfläche **Bereinigen** wird der aktuelle Wert bereinigt. Hiernach wird im Feld entweder der geerbte Wert (grauer Text) oder gar kein Text angezeigt. **Bereinigen** ist nur verfügbar, wenn für die aktuell ausgewählte Domäne oder den aktuell ausgewählten Host ein Wert definiert wurde.

Wert erzwingen

Wert erzwingen ist nur verfügbar, wenn eine Richtliniendomäne ausgewählt ist. Sie können erzwingen, dass die aktuelle Domäneneinstellung ebenfalls in allen Unterdomänen und Hosts aktiv ist. In der Praxis löscht dieser Vorgang die entsprechende Einstellung in allen Unterdomänen und Hosts unterhalb der aktuellen Domäne. So wird die Vererbung des aktuellen Wertes auf alle Unterndomänen und Hosts ermöglicht. Verwenden Sie diese Funktion mit Bedacht: Alle in den Unterdomänen oder Hosts definierten Werte unter der ausgewählten Domäne werden verworfen und können nicht mehr wiederhergestellt werden.

Domänenwerte anzeigen

Domänenwerte anzeigen ist nur verfügbar, wenn eine Richtliniendomäne ausgewählt ist. Sie können eine Liste alle Richtliniendomänen und Hosts unter der ausgewählten Richtliniendomäne zusammen mit dem Wert des ausgewählten Felds anzeigen.

Klicken Sie auf eine beliebige Domäne oder einen beliebigen Host-Namen, um die Domäne oder den Host schnell auszuwählen. Es ist möglich, gleichzeitig mehrere Dialogfelder vom Typ **Domänenwert** zu öffnen.

Anzeigen des Status

Sie können die Einstellungen und Statistiken einer Richtliniendomäne im Hauptbereich der Anwendung anzeigen.

So zeigen Sie den Status an:

1. Öffnen Sie die Registerkarte **Status**.
2. Wählen Sie das Programm aus.
   Policy Manager Console erstellt eine Produktansicht für das gewählte Programm, in der Sie die wichtigeren lokalen Einstellungen und Statistiken einsehen können.

Hinweis: In dieser Ansicht können keine Werte geändert werden. Sie können jedoch die **MIB-Hilfetexte** anzeigen, indem Sie auf ein Feld oder dessen Bezeichnung klicken.

Bei Richtliniendomänen wird auf der Registerkarte **Status** eine Statusübersicht auf Domänenebene angezeigt: die Anzahl der Hosts in der Domäne und die Anzahl der Hosts, die gegenwärtig nicht verbunden sind.

3. Klicken Sie auf einen beliebigen getrennten Host, um die Auswahl der Richtliniendomäne schnell zu ändern und den Host auszuwählen.

   Auf diese Weise lässt sich leicht nachprüfen, ob der getrennte Host vor dem Abbruch der Verbindung in der Lage war, einige Alarme und nützliche Statistiken zu übertragen. Anhand dieser Informationen lässt sich unter Umständen ermitteln, warum die Verbindung zum Host getrennt wurde. Wenn der Grund offensichtlich ist, z. B. weil die F-Secure Software auf dem Host deinstalliert wurde, können Sie den Host normal löschen.

4. Nachdem Sie einen getrennten Host überprüft haben, können Sie zur zuvor gewählten Domänenebene zurückkehren, indem Sie auf der Symbolleiste auf die Schaltfläche klicken.
   Die Ansicht **Domänenstatus** bietet darüber hinaus zwei verknüpfte Vorgänge, um eine höhere Anzahl getrennter Hosts zu verwalten: Auswählen aller getrennten Hosts und Löschen aller getrennten Hosts. Auf beide Vorgänge kann über das Kontextmenü des Root-Knotens der Struktur **Getrennte Hosts** zugegriffen werden.

   Vorsicht: Alle nicht verbundenen Hosts zu löschen, ist risikobehaftet,da es möglich ist, dass die Verbindung einiger vorhandener Hosts aus natürlichen Gründen temporär länger als die zugewiesenen Schwellwerttage aufgehoben wird. Prüfen Sie immer den Trennungsschwellwert in **Tools** > **Serverkonfiguration** > **Hosts**, bevor Sie Hosts löschen. Wird ein noch vorhandener Host versehentlich gelöscht, gehen alle für den Host spezifischen Alarm-, Bericht-, Status- und Richlinieneinstellungen verloren. Der Host jedoch sendet eine Meldung zur automatischen Registrierung, sobald erkannt wurde, dass ein Entfernen von Policy Manager stattgefunden hat. Der Host kann wieder in den Domänenbaum importiert werden, aber von Policy Manager wird dieser wie jeder andere neu hinzugefügte Host behandelt.

Fensterbereich "Meldung"

Policy Manager Consoleprotokolliert Meldungen zu verschiedenen Ereignissen im Fensterbereich **Meldungen**.

Im Gegensatz zu den Registerkarten **Warnungen** und **Scan-Berichte** werden Ereignisse im Fenster **Meldung** nur von Policy Manager Console generiert.

Es gibt drei Kategorien von Meldungen: **Informationen**, **Warnungen** und **Fehler**. Jede Registerkarte in der Ansicht **Meldungen** kann Meldungen aller drei Schweregrade enthalten. Über das Kontextmenü, das Sie durch Klicken mit der rechten Maustaste auf die Registerkarte öffnen, können Sie eine Kategorie löschen. Wenn Sie mit der rechten Maustaste auf eine einzelne Meldung klicken, wird ein Kontextmenü mit den Optionen **Ausschneiden**, **Kopieren** und **Löschen** angezeigt.

Standardmäßig werden Meldungen in beiden Dateien im Meldungsunterverzeichnis des lokalen Policy Manager Console-Installationsverzeichnisses protokolliert. Protokolle der Meldungen werden sowohl in Englisch als auch in der Sprache, die Sie für Policy Manager Console eingerichtet haben, aufbewahrt. Es wird eine separate Protokolldatei für jede Meldungskategorie erstellt (Registerkartennamen im Fensterbereich **Meldungen**). Sie können über die Seite **Einstellungen** > **Speicherorte** das Verzeichnis für die Protokolldatei festlegen.

Die Symbolleiste

Die Symbolleiste enthält Schaltflächen für die wichtigsten Aufgaben von Policy Manager Console.

	Verteilt die Richtlinie.

	Wechselt zur vorherigen Domäne oder zum vorherigen Host in der Auswahlhistorie der Domänenstruktur.
	Wechselt zur nächsten Domäne oder zum nächsten Host in der Auswahlhistorie der Domänenstruktur.
	Wechselt in die übergeordnete Domäne.
	Schneidet einen Host oder eine Domäne aus.
	Fügt einen Host oder eine Domäne ein.
	Fügt der derzeit ausgewählten Domäne eine Domäne hinzu.
	Fügt der derzeit ausgewählten Domäne einen Host hinzu.
	Zeigt das Feld **Eigenschaften** eines Hosts oder einer Domäne an.
	Startet das Dienstprogramm **Windows-Hosts automatisch feststellen**. Neue Hosts werden zu der momentan ausgewählten Richtliniendomäne hinzugefügt.
	Beginnt damit, eine Installation an die Windows-Hosts zu übertragen.
	Hierüber erfolgt der Import neuer Hosts zur aktuell ausgewählten Domäne. Die grüne Farbe weist darauf hin, dass der Host eine Anfrage auf automatische Registrierung gesendet hat.
	Zeigt die zur Verfügung stehenden Installationspakete an.
oder	Zeigt alle Alarme an. Wenn neue Alarme vorliegen, wird das Symbol hervorgehoben. Wenn Policy Manager Console gestartet ist, ist das Symbol generell hervorgehoben.

Menübefehle

Dieser Abschnitt bietet einen Überblick über die verfügbaren Menübefehle in Policy Manager Console.

Menü	Befehl	Aktion
Datei	Richtlinien verteilen	Hierüber erfolgt die Verteilung der Richtlinien.
	Richtlinienänderungen verwerfen	Hierüber werden nicht verteilte Änderungen an der Richtlinie verworfen, die seit der letzten Verteilung der Richtlinie vorgenommen wurden.
	Host-Richtliniendatei exportieren	Exportiert die Richtliniendateien.
	Beenden	Beendet Policy Manager Console.
Bearbeiten	Ausschneiden	Schneidet die ausgewählten Elemente aus.
	Einfügen	Fügt ein oder mehrere zuvor kopierte oder ausgeschnittene Elemente an der ausgewählten Position ein.

Menü	Befehl	Aktion
	Löschen	Löscht die ausgewählten Elemente.
	Neue Richtliniendomäne	Fügt eine neue Domäne hinzu.
	Neuer Host	Fügt einen neuen Host hinzu.
	Active Directory-Struktur importieren	Hierüber wird der Active Directory-Importassistent geöffnet.
	Neue Hosts importieren	Hierüber werden neue Hosts importiert, die eine Anfrage auf Hinzufügen zur Richtliniendomäne gesendet haben.
	Windows-Hosts automatisch erkennen	Importiert Hosts aus der Windows-Domänenstruktur.
	Installationspakete auf Windows-Hosts übertragen	Führt eine Remote-Installation der Software durch und importiert die durch ihre IP-Adresse oder WINS-Namen festgelegten Hosts.
	Suchen	Sucht in den Host-Eigenschaften nach einer Zeichenfolge. Es werden alle Hosts in der ausgewählten Domäne durchsucht.
	Eigenschaften von Domäne/Host	Zeigt die Seite **Eigenschaften** des ausgewählten Hosts oder der ausgewählten Domäne an.
Ansicht	Fensterbereich "Meldung"	Zeigt den Fensterbereich **Meldung** im unteren Teil des Bildschirms an oder blendet ihn aus.
	Neue Meldung automatisch öffnen	Wenn diese Option ausgewählt ist, wird der Fensterbereich **Meldung** automatisch geöffnet, wenn eine neue Meldung empfangen wird.
	Zurück	Wechselt zur vorherigen Domäne oder zum vorherigen Host in der Auswahlhistorie der Domänenstruktur.
	Weiter	Wechselt zur nächsten Domäne oder zum nächsten Host in der Auswahlhistorie der Domänenstruktur.
	Übergeordnete Domäne	Wechselt zur übergeordneten Domäne.
	Alle Alarme	Öffnet die Seite **Alarme**, auf der alle Alarme angezeigt werden.
	Erweiterter Modus	Zeigt die Benutzeroberfläche **Erweiterter Modus** an.
	Anti-Virus-Modus	Zeigt die Benutzeroberfläche des **Anti-Virus-Modus** an, der für die zentrale Verwaltung von Client Security optimiert ist.
	<Element> aktualisieren	Aktualisiert die Ansicht für den Status, Alarme oder Berichte manuell. Dieser Menübefehl ändert sich entsprechend der ausgewählten Seite.
	Alle aktualisieren	Aktualisiert alle Daten, die momentan auf der Benutzeroberfläche angezeigt werden: Richtlinien, Status, Alarme, Berichte, Installationspakete und Anfragen zur automatischen Registrierung.
Tools	Installationspakete	Hierüber werden Informationen über Installationspakete in einem Dialogfenster angezeigt.
	Berichterstellung	Erlaubt die Auswahl von Berichterstellungsmethoden sowie der Domänen/Hosts und Programme, die in den Berichten enthalten sein sollen.

Menü	Befehl	Aktion
	Benutzer	Hierüber wird das Dialogfenster **Benutzer** geöffnet. Hier können Policy Manager-Benutzer hinzugefügt und gelöscht werden.
	Kennwort ändern	Hierüber wird das Dialogfenster **Kennwort ändern** geöffnet, in dem Sie das Kennwort für Ihr Benutzerkonto ändern können.
	Serverkonfiguration	Hierüber wird das Dialogfenster **Serverkonfiguration** geöffnet, in dem Sie Signaturschlüssel exportieren/importieren, die Zeitdauer für die Aufhebung der Verbindung des Hosts einrichten und nicht verbundene Hosts entfernen können.
	Voreinstellungen	Legt die lokalen Voreinstellungen für Policy Manager Console fest. Diese Eigenschaften gelten nur für die lokale Installation von Policy Manager Console.
Hilfe	Inhalt	Zeigt den Index für die **Hilfe** an.
	Registrieren	Öffnet einen Dialog, in dem Sie das Programm registrieren können.
	Kontaktinformationen	Zeigt Kontaktinformationen für F-Secure an.
	Info über F-Secure Policy Manager Console	Zeigt Informationen zur Version an.

Verwalten von Domänen und Hosts

Wenn Sie verschiedene Sicherheitsrichtlinien für unterschiedliche Hosts (Laptops, Desktop-PC, Server), für Benutzer in unterschiedlichen Unternehmensbereichen oder mit unterschiedlichen Computerkenntnissen einsetzen möchten, ist es empfehlenswert, die Domänenstruktur auf Grundlage dieser Kriterien zu planen.

Dies erleichtert die spätere Verwaltung der Hosts. Wenn Sie bereits im Vorfeld eine richtlinienbasierte Domänenstruktur definiert haben, können Sie die Hosts direkt in diese Struktur importieren. Wenn Sie möglichst schnell beginnen möchten, können Sie auch alle Hosts zunächst in die Root-Domäne importieren und die Domänenstruktur je nach Bedarf nachträglich erstellen. Die Hosts können anschließend durch Ausschneiden und Kopieren in die neuen Domänen eingefügt werden.

Alle Domänen und Hosts müssen in dieser Struktur einen eindeutigen Namen haben.

Eine andere Möglichkeit besteht darin, die Niederlassungen in den verschiedenen Ländern als Subdomänen zu erstellen.

Hinzufügen von Richtliniendomänen

In diesem Thema wird das Hinzufügen neuer Richtliniendomänen beschrieben.

So fügen Sie eine neue Richtliniendomäne hinzu:

1. Wählen Sie **Bearbeiten** > **Neue Richtliniendomäne** aus dem Menü.
   Alternativ:
   - Klicken Sie in der Symbolleiste auf .
   - Drücken Sie Strg+Einfg.

   Die neue Richtliniendomäne wird als Unterdomäne der ausgewählten übergeordneten Domäne eingerichtet.
2. Geben Sie einen Namen für die Richtliniendomäne ein.
   Ein Symbol wird für die Domäne erstellt.

Hinzufügen von Hosts

In diesem Abschnitt werden unterschiedliche Methoden zum Hinzufügen von Hosts zu einer Richtliniendomäne beschrieben.

Zum Hinzufügen von Hosts zu einer Richtliniendomäne stehen je nach dem verwendeten Betriebssystem folgende Hauptmethoden zur Verfügung:

- Sie können die Hosts direkt aus der Windows-Domäne importieren.
- Sie können Hosts mithilfe der Autoregistrierung importieren. (In diesem Fall ist es erforderlich, dass Management Agent auf dem importierten Host installiert ist.) Sie können außerdem unterschiedliche Kriterien festlegen, um automatisch registrierte Hosts in unterschiedliche Subdomänen zu importieren.
- Sie können die Hosts mit dem Befehl **Neuer Host** manuell erstellen.

Importieren von Hosts aus einer Active Directory-Struktur

Sie können eine Richtliniendomänenstruktur und Hosts in Policy Manager aus einer Active Directory-Struktur importieren.

1. Wählen Sie **Bearbeiten** > **Active Directory-Struktur importieren** aus dem Menü aus.
   Der Assistent für den **Import der Active Directory-Struktur** wird geöffnet.
2. Geben Sie den Speicherort Ihres Active Directory-Servers und den Benutzernamen und das Kennwort ein, über die Sie zumindest Lese-Zugriff erhalten, und klicken Sie auf **Weiter**.
3. Wählen Sie die Active Directory-Domäne, die Container, die Sie importieren möchten, und die Zielrichtliniendomäne aus, die Sie darin importieren möchten, und klicken Sie auf **Weiter**.

   Container, die Hosts enthalten, werden hervorgehoben.
4. Prüfen Sie die Importregeln, wählen Sie die Regeln aus, die Sie erstellen wollen und klicken Sie auf **Start**.
   Die ausgewählten Regeln werden auf die Hosts aus der Active Directory-Struktur angewandt, die eine Verwaltungsanfragen an Policy Manager gesandt haben.
5. Warten Sie, bis der Importvorgang abgeschlossen ist, und klicken Sie auf **Schließen**, um den Assistenten zu beenden.

Die Hosts aus Active Directory werden zusammen mit allen neuen Posten der Richtlinienstruktur in Policy Manager angezeigt.

Hinzufügen von Hosts in Windows-Domänen

In einer Windows-Domäne fügen Sie Hosts am einfachsten einer Richtliniendomäne hinzu, indem Sie sie mithilfe der intelligenten Installation importieren.

Beachten Sie, dass dabei auch Management Agent auf den importierten Hosts installiert wird. So werden Hosts aus einer Windows-Domäne importiert:

1. Wählen Sie die Zieldomäne.
2. Wählen Sie **Bearbeiten** > **Windows-Hosts automatisch feststellen** aus dem Menü.
   Nach Abschluss der automatischen Erkennung wird der neue Host automatisch in die Struktur der **Richtliniendomäne** aufgenommen.

Importieren neuer Hosts

Eine weitere Option zum Hinzufügen von Hosts in Policy Manager Console ist das *Importieren neuer Hosts*.

Dies ist nur möglich, nachdem Management Agent auf den Hosts installiert wurde und die Hosts eine Anfrage zur automatischen Registrierung gesendet haben. Management Agent muss von einer CD-ROM, einem Anmeldeskript oder anderweitig installiert werden.

So importieren Sie neue Hosts:

1. Klicken Sie auf der Symbolleiste auf .

   Alternativ:

   - Wählen Sie **Bearbeiten** > **Neue Hosts importieren** aus dem Menü aus.
   - Wählen Sie **Neue Hosts importieren** aus der Ansicht **Installation** aus.

   Wenn der Vorgang abgeschlossen ist, wird der Host zum Domänenbaum hinzugefügt. Die neuen Hosts können basierend auf unterschiedlichen Kriterien in unterschiedliche Domänen importiert werden. Zu diesen Kriterien gehören die Host-IP oder die DNS-Adresse. Die Ansicht **Neue Hosts** enthält eine tabellarische Ansicht der Daten, welche vom Host in der Meldung zur automatischen Registrierung gesendet werden. Hierzu gehören benutzerdefinierte Eigenschaften, die während der Installation in das Remote-Installationspaket eingebunden wurden.
2. Sie können die folgenden Aktionen für die Ansicht **Neue Hosts** durchführen:

   - Sie können Meldungen gemäß den Werten der Spalte sortieren, indem Sie auf die entsprechende Tabellenüberschrift klicken.
   - Sie können auch die Reihenfolge der Spalten ändern. Ziehen Sie dazu die Spalten an die entsprechende Position. Die Spaltenbreite kann nach Belieben eingestellt werden.
   - Sie können das Kontextmenü der Tabelle (rechter Mausklick auf die Leiste der Tabellüberschrift) verwenden, um festzulegen, welche Eigenschaften in der Tabelle sichtbar sind.

Einsatz von Importregeln

Sie können die Importregeln für neue Hosts auf der Registerkarte **Importregeln** im Fenster **Neue Hosts importieren** festlegen.

Importregeln können automatisch auf neue Hosts angewandt werden, die eine Verbindung zum Server aufbauen. Dies bedeutet, dass es nicht notwendig ist, die Importregeln manuell auszuführen, wenn neue Hosts eine Verbindung zum Policy Manager Server aufbauen. Die neuen Hosts werden gemäß der vorhandenen Importregeln zur Domänenstruktur hinzugefügt.

Die folgenden Daten eignen sich als Importkriterien, die in den Regeln festgelegt werden können:

- WINS-Name, DNS-Name, benutzerdefinierte Eigenschaften
  - Als Platzhalter wird hier das `*` (Sternchen) unterstützt. Das Sternchen `*` kann für eine beliebige Anzahl von Zeichen stehen. Beispiele: `host_test*` oder `*.example.com`.
  - Beim Abgleich wird die Groß-/Kleinschreibung nicht berücksichtigt, d. h., Groß- und Kleinschreibung eines Buchstabens werden als dasselbe Zeichen ausgewertet.
- IP-Adresse
  - Hier wird eine exakte Übereinstimmung der IP-Adresse (Beispiel: `192.1.2.3`) und der IP-Unterdomäne (Beispiel: `10.15.0.0/16`) unterstützt.

1. Sie können Spalten in der Tabelle ein- oder ausblenden. Öffnen Sie dazu im Fenster **Regeln für den Import** das Kontextmenü, indem Sie mit der rechten Maustaste auf einen beliebigen Spaltenkopf klicken.

   Beim Importieren von Hosts in die Richtliniendomäne werden nur die Werte aus den angezeigten Spalten als Kriterien für den Abgleich berücksichtigt. Die Werte in den gegenwärtig ausgeblendeten Spalten werden ignoriert.
2. Beim Importieren von Hosts können Sie neue benutzerdefinierte Eigenschaften hinzufügen.

   Ein Beispiel für den Einsatz benutzerdefinierter Eigenschaften ist die Erstellung von separaten Installationspaketen für unterschiedliche Abteilungen in einem Unternehmen, die unter abteilungsspezifischen Richtliniendomänen gruppiert wurden. In diesem Fall könnten Sie den Gerätenamen als benutzerdefinierte Eigenschaft verwenden und anschließend Regeln für den Import definieren, die Gerätenamen als Importkriterien verwenden. Beachten Sie, dass Namen von ausgeblendeten

benutzerdefinierten Eigenschaften verloren gehen, sobald Policy Manager Console geschlossen wird. So fügen Sie eine neue benutzerdefinierte Eigenschaft hinzu:

a) Klicken Sie mit der rechten Maustaste auf einen Spaltenkopf, und wählen Sie **Benutzerdefinierte Eigenschaft hinzufügen**.
Das Dialogfeld **Neue benutzerdefinierte Eigenschaft** wird geöffnet.

b) Geben Sie einen Namen für die benutzerdefinierte Eigenschaft ein, z. B. den Abteilungsnamen, und klicken Sie dann auf **OK**.
Die neue benutzerdefinierte Eigenschaft wird nun in der Tabelle angezeigt und Sie können neue Importregeln erstellen, in denen diese als Importkriterium verwendet wird.

3. Erstellen Sie eine neue Importregel

a) Klicken Sie auf der Registerkarte **Regeln für den Import** auf **Hinzufügen**.
Das Dialogfeld **Ziel-Richtliniendomäne für die Regel auswählen** wird mit einer Liste der vorhandenen Domänen und Subdomänen angezeigt.

b) Wählen Sie die Domäne aus, für die Sie die Regel erstellen möchten, und klicken Sie auf **OK**.

c) Wählen Sie die neu erstellte Zeile aus und klicken Sie auf die Zelle, der der Wert hinzugefügt werden soll.

d) Geben Sie den Wert in die Zelle ein.
Die Importkriterien sind definiert.

e) Wählen Sie **Regeln automatisch bei Verbindung des Hosts zum Server anwenden** aus, wenn Sie möchten, dass die Regeln automatisch für jeden neuen Host, der eine Verbindung aufbaut, angewandt werdenn sollen.

Diese Option ist für neue Installationen von Policy Manager standardmäßig aktiviert und für aktualisierte Versionen deaktiviert, um das Verhalten der vorherigen Version nachzuahmen.

- Wenn die neuen Hosts importiert werden, werden die Regeln in der Reihenfolge von oben nach unten verifiziert und es wird die erste passende Regel angewandt. Sie können die Reihenfolge der Regeln ändern, indem Sie auf **Nach unten** oder **Nach oben** klicken.
- Mithilfe der Option **Klonen** können Sie mehrere Regeln für eine Domäne erstellen. Beginnen Sie, indem Sie zunächst eine Regel für die Domäne definieren. Wählen Sie anschließend die Zeile aus, und klicken Sie auf **Klonen**. Jetzt können Sie die Kriterien in der neuen duplizierten Zeile bearbeiten.

4. Wenn Sie den Importvorgang starten möchten, wählen Sie die Registerkarte **Neue Hosts** aus und klicken auf **Importieren**.

Die definierten Importregeln werden validiert, bevor der Import beginnt.

Nachdem die Hosts importiert wurden, wird ein Dialogfenster mit einer Zusammenfassung angezeigt, in dem die Anzahl der erfolgreich installierten Hosts und die Anzahl der fehlgeschlagenen Importvorgänge angegeben werden. Beachten Sie, dass ein leerer Satz an Bedingungen immer als Übereinstimmung angesehen wird.

Manuelle Definition von Hosts

In diesem Thema wir die manuelle Definition von Hosts beschrieben.

So definieren Sie einen Host manuell:

1. Wählen Sie die Zieldomäne.

2. Wählen Sie **Bearbeiten** > **Neuer Host** aus dem Menü.

Alternativ:

- Klicken Sie in der Symbolleiste auf .
- Drücken Sie Einfg.

Dieser Vorgang ist in den folgenden Fällen nützlich:

- Kennen lernen und Testen - Sie können einen Teil der Funktionen von Policy Manager Console ausprobieren, ohne neben Policy Manager Console weitere Software installieren zu müssen.Policy Manager Console.
- Vorabdefinition von Richtlinien - Sie können für einen Host eine Richtlinie definieren und erzeugen, bevor die Software auf dem Host installiert wurde.
- Spezialfälle - Sie können Richtlinien für Hosts erstellen, die nie direkt auf den Server zugreifen werden (d. h., wenn es nicht möglich ist, diese Hosts zu importieren). So ist es zum Beispiel möglich, Basis-Richtliniendateien für einen Computer zu erstellen, der nicht auf den F-Secure Policy Manager Server zugreift. Sie müssen in diesem Fall die Basis-Richtliniendatei entweder manuell oder mittels einer anderen externen Übertragungsmethode übermitteln. Wählen Sie dazu **Bearbeiten** > **Richtliniendatei exportieren** aus dem Menü.

Hinweis: Hosts, auf denen Management Agent nicht installiert wurde, können nicht über Policy Manager Console verwaltet werden, da es für diese Hosts keine Möglichkeit zum Abrufen der Richtlinien gibt. In diesem Fall sind auch keine Statusinformationen verfügbar. Alle Änderungen, die Sie an der Domänenstruktur vornehmen, werden auch dann umgesetzt, wenn Sie Policy Manager Console beenden, ohne die Änderungen an den aktuellen Richtliniendaten zu speichern.

Automatische Behandlung von nicht verbundenen Hosts

Sie können festlegen, wann die Verbindung von Hosts als aufgehoben angesehen werden soll und wann nicht verbundene Hosts aus der Richtliniendomäne entfernt werden sollen.

1. Wählen Sie **Tools** > **Serverkonfiguration** aus dem Menü aus.
2. Wählen Sie **Hosts** aus.
3. Geben Sie in **Verbindung von Host als aufgehoben ansehen nach** die Anzahl der Tage an, nach denen der Hoststatus auf **Getrennt** gesetzt werden soll.
4. Geben Sie in **Nicht verbundene Host entfernen nach** die Anzahl der Tage an, nach denen nicht verbundene Hosts aus der Richtliniendomäne entfernt werden sollen.
5. Klicken Sie auf **OK**, um das Dialogfeld zu schließen.

Host-Eigenschaften

Dieser Abschnitt bietet einen Überblick über die Host-Eigenschaften, die in Policy Manager Console angezeigt und bearbeitet werden können.

Um Host-Eigenschaften anzusehen, klicken Sie mit der rechten Maustaste auf den entsprechenden Host und in dem Menü, das sich öffnet, wählen Sie **Eigenschaften** aus (alternativ können Sie Alt + Eingabetaste betätigen).

Jeder Host verfügt über eine UID zur Identifikation. Dies ist ein eindeutiger Bezeichner, der direkt aus dem Host-Status abgerufen wird und in Policy Manager Console nicht bearbeitet werden kann.

In das Feld **Anzeigen als** können Sie einen Namen Ihrer Wahl eingeben, über den der Host identifiziert wird. Hierdurch wird die eigentliche Bezeichnung des Hosts bei der Anzeige im Domänenbaum ersetzt.

Software-Verteilung

Policy Manager stellt mehrere Methoden zur Installation und Aktualisierung von verwalteten Anwendungen bereit.

Push-Installationen	Policy Manager kann Software auf neue Hosts installieren, die noch nicht zentral verwaltet werden. Über die Funktion **Windows-Hosts automatisch feststellen** können Hosts aus Windows-Domänen

	gesucht werden. Alternativ können Sie den Ziel-Host auch direkt durch Eingabe des WINS-Namens oder der IP-Adresse angeben. Dazu verwenden Sie die Funktion **Installationspakete auf Windows-Hosts übertragen**. Die Push-Installationsfunktionen eignen sich nicht nur zur Erstinstallation, sondern können auch zur Aktualisierung und Reparatur von Installationen eingesetzt werden, wenn richtlinienbasierte Installationen nicht praktikabel sind.
Installationen auf Richtlinienbasis	Policy Manager kann Installations- und Aktualisierungsvorgänge über richtlinienbasierte Anweisungen initiieren. Dabei ist es erforderlich, dass der Host bereits zentral verwaltet wird, d. h. bereits in eine Richtliniendomäne in Policy Manager Console einbezogen ist.
Lokale Installationen und Updates von CD-ROM	Die Installation kann unabhängig auf dem Host durchgeführt werden, indem die Einrichtung direkt von der CD-ROM ausgeführt wird. Nach der Installation sendet Management Agent eine Registrierungsmeldung an Policy Manager. Der Administrator kann den neuen Host dann ansehen und annehmen, indem er den Befehl **Neue Hosts importieren** aus dem Menü **Bearbeitern** in Policy Manager Console auswählt.
Lokale Installation und Updates mit vorkonfigurierten Paketen	Anstatt die Installation mithilfe des Installationsprogramms von der CD-ROM auszuführen, können Sie mit Policy Manager ein benutzerdefiniertes Installationspaket (JAR oder MSI) vorbereiten, das Informationen zu den Einstellungen für diese Installation enthält. Bei Auswahl dieser Methode kann die Einrichtung auf dem Computer des Endbenutzers im Hintergrund, d. h. ohne Benutzereingriffe, durchgeführt werden, da das vorkonfigurierte Paket alle Einstellungen enthält, die der Benutzer normalerweise festlegen muss.
Updates der F-Secure-Virendefinitions-Datenbank	kann die Anti-Virus-Datenbanken aktualisieren, indem es die neuesten Updates von der automatischen Update-Site von F-Secure herunterlädt. Verwaltete Hosts rufen die Updates von Policy Manager entsprechend der Host-Richtlinie automatisch oder durch remote ausgelöste Vorgänge ab.

Verknüpfungen zu allen installationsbezogenen Funktionen finden Sie auf der Registerkarte **Installation**.

Wenn bei der Verteilung von Software zu Hosts der Zugriff auf den öffentlichen Schlüssel erforderlich ist, kann dieser von der Begrüßungsseite von Policy Manager Server heruntergeladen werden.

Push-Installationen

In diesem Abschnitt wird beschrieben, wie Installationspakete auf Hosts übertragen werden.

Der einzige Unterschied zwischen den Funktionen **Windows-Hosts automatisch feststellen** und **Installationspakete auf Windows-Hosts übertragen** besteht in der Methode, mit der die Ziel-Hosts ausgewählt werden: Die Funktion zur automatischen Feststellung durchsucht die Windows-Domänen, und der Benutzer wählt die Ziel-Hosts aus einer Host-Liste aus. Die Push-Installation ermöglicht dagegen die direkte Eingabe der Windows-Ziel-Hosts in Form von IP-Adressen und Host-Namen. Nachdem die Ziel-Hosts ausgewählt wurden, wird die Installation auf den Host-Computern bei beiden Methoden auf dieselbe Weise durchgeführt.

Hinweis: Bevor Sie mit der Installation von F-Secure auf den Hosts beginnen, stellen Sie zunächst sicher, dass sich auf den Ziel-Computern keine Virenschutz- oder Firewall-Programme befinden, die Konflikte auslösen können.

Windows-Hosts automatisch erkennen

Ziel-Hosts können mit der Funktion *Automatische Feststellung* ausgewählt werden.

Wählen von Ziel-Hosts:

1. Wählen Sie die Zieldomäne.
2. Wählen Sie **Bearbeiten** > **Windows-Hosts automatisch feststellen** aus dem Menü.

   Wahlweise können Sie auch auf die Schaltfläche klicken.
3. Wählen Sie aus der Liste **NT-Domänen** eine Domäne aus, und klicken Sie auf **Aktualisieren**.

   Die Host-Liste wird nur aktualisiert, wenn Sie auf **Aktualisieren** klicken. Andernfalls werden aus Gründen der Leistungsfähigkeit Daten aus dem Zwischenspeicher angezeigt. Vor dem Klicken auf **Aktualisieren** können Sie die folgenden Optionen ändern:

   - **Bereits verwaltete Hosts ausblenden**. Aktivieren Sie dieses Kontrollkästchen, um nur solche Hosts anzuzeigen, auf denen keine F-Secure Anwendungen installiert sind.
   - **Hosts mit allen Details auflösen (langsamer)**. Bei dieser Auswahl werden alle Details zu den Hosts angezeigt, z. B. die Versionen des Betriebssystems und Management Agent.
   - **Nur Host-Namen und Kommentare auflösen (schneller)**. Wenn in der detaillierten Ansicht nicht alle Hosts angezeigt werden oder wenn das Abrufen der Liste zu lange dauert, können Sie diese Option verwenden. Hinweis: Unter Umständen dauert es eine Weile, bis im **Haupt-Browser** ein neuer, soeben im Netzwerk installierter Host angezeigt werden kann.
4. Wählen Sie die Hosts aus, auf denen die Software installiert werden soll:

   Drücken Sie die Leertaste, um ausgewählte Hosts zu überprüfen. Sie können ohne großen Aufwand mehrere Hosts auswählen. Halten Sie dazu die Umschalttaste gedrückt, und führen Sie dann eine der folgenden Aktionen durch:

   - Klicken Sie mit der Maus auf mehrere Host-Zeilen
   - Markieren Sie durch Ziehen mit der Maus mehrere Host-Zeilen
   - Wählen Sie die Hosts mit den nach oben und unten weisenden Pfeiltasten aus

   Wahlweise können Sie auch mit der rechten Maustaste klicken. Daraufhin erscheint das Kontextmenü der Host-Liste mit folgenden Optionen:

   - **Aktivieren** - versieht die ausgewählten Hosts mit Häkchen (entspricht dem Drücken der Leertaste).
   - **Deaktivieren** - entfernt die Häkchen von den ausgewählten Hosts (entspricht dem Drücken der Leertaste).
   - **Alle aktivieren** - versieht alle Hosts in der ausgewählten Windows-Domäne mit Häkchen.
   - **Alle deaktivieren** - entfernt die Häkchen von allen Hosts, die in der ausgewählten Windows-Domäne markiert waren.
5. Klicken Sie auf **Installieren**, um fortzufahren.

Nach der Auswahl der Ziel-Hosts müssen Sie noch die Anwendungen auf den Hosts remote installieren.

Installationspakete auf Windows-Hosts übertragen

Sie können Ziel-Hosts auch über die Funktion **Installationspakete auf Windows-Hosts übertragen** auswählen.

Wählen von Ziel-Hosts:

1. Wählen Sie die Zieldomäne.
2. Wählen Sie **Bearbeiten** > **Installationspakete auf Windows-Hosts übertragen** aus dem Menü.

   Wahlweise können Sie auch auf die Schaltfläche klicken.

3. Geben Sie die Namen der Ziel-Hosts ein, auf denen eine Push-Installation der Software durchgeführt werden soll, und klicken Sie auf **Weiter**, um fortzufahren.

   Sie können auf **Durchsuchen** klicken, wenn Sie die Versionsnummer von Management Agent auf den Hosts überprüfen möchten.

Nach der Auswahl der Ziel-Hosts müssen Sie noch die Anwendungen auf die Hosts übertragen und installieren.

Push-Installation nach Auswahl des Ziel-Hosts

Nach dem Auswählen der Ziel-Hosts müssen Sie die Installationspakete übertragen und installieren.

Gehen Sie folgendermaßen vor, um die Installationspakete auf die gewählten Ziel-Hosts zu übertragen und auf diesen zu installieren:

1. Wählen Sie das Installationspaket aus, und klicken Sie auf **Weiter**, um fortzufahren.

   Sie können auf dieser Seite neue Installationspakete importieren, wenn dies notwendig ist.`Erzwungene Neuinstallation`Die Option ist in allen Installationspaketen immer aktiv. Daher wird die Anwendung erneut installiert, wenn der Host bereits über die gleiche Versionsnummer der installierten Anwendung verfügt.

2. Übernehmen Sie die Standardrichtlinie, oder geben Sie an, welche Host- bzw. Domänenrichtlinie als anonyme Richtlinie verwendet werden soll. Klicken Sie dann auf **Weite**, um fortzufahren
3. Wählen Sie Benutzerkonto und Passwort für die Push-Installation, indem Sie entweder **Dieses Konto** (das aktuelle Konto) oder **Anderer Benutzer** wählen.

   Hinweis: Für die Push-Installation sind auf dem Zielcomputer während der Installation Administratorrechte notwendig. Wenn das Konto nicht über Administratorrechte auf einem der Remote-Hosts verfügt, wird eine Fehlermeldung **Zugriff verweigert** für diesen Host angezeigt, während die Installation auf den anderen Hosts fortgeführt wird.

   Wenn Sie **Dieses Konto** auswählen, werden die Sicherheitsrechte des momentan angemeldeten Kontos verwendet. Verwenden Sie diese Option in den folgenden Fällen:

   - Sie sind bereits als Domänenadministrator angemeldet; oder
   - Sie sind als lokaler Administrator mit einem Passwort angemeldet, das dem Passwort für den lokalen Administrator des Ziel-Hosts entspricht.

   Anderer Benutzer: Geben Sie Konto und Passwort ein. Der Administrator kann ein beliebiges Domänen-Administratorkonto mit dem entsprechenden Passwort eingeben, um die Remote-Installation auf den ausgewählten Hosts bequem abzuschließen.

   - Wenn Sie die Installation in vertrauenswürdigen und nicht vertrauenswürdigen Domänen mit einem Domänen-Konto durchführen, achten Sie bei der Eingabe der Kontodaten darauf, dass das Format `DOMAIN\ACCOUNT` eingehalten wird.
   - Wenn Sie ein lokales Administratorkonto verwenden, nutzen Sie das Format `KONTO`. (Geben Sie den Host-Namen nicht als Teil der Kontobezeichnung ein, sonst wird das Konto nur von dem betreffenden Host akzeptiert.)

   Hinweis: Wenn bei der Installation auf dem Computer des Administrators eine offene Netzwerkverbindung zu einem Ziel-Rechner besteht und für diese Verbindung ein anderes Benutzerkonto eingegeben wurde, wird Fehler **1219** angezeigt, d. h., dass ein NT-Berechtigungskonflikt vorliegt. In diesem Fall müssen Sie alle aktiven Verbindungen schließen, bevor Sie mit der **Push-Installation** beginnen.

4. Installationszusammenfassung prüfen.
5. Um den **Assistenten für die Remote-Installation** zu starten, klicken Sie auf **Starten**.

   Der **Assistent für die Remote-Installation** führt Sie durch die einzelnen Installationsschritte und zeigt mehrere Dialogfelder mit Fragen an. Abhängig von Ihren Antworten legt der Assistent die Einstellungen

für die Installation fest. Klicken Sie im letzten Dialogfeld auf **Fertig stellen**, und fahren Sie mit dem nächsten Schritt fort.

Policy Manager installiert Management Agent und die ausgewählten Programme auf den Hosts. Während dieses Vorgangs wird auf der **Statusleiste** der Fortschritt der Installation angezeigt. Sie können jederzeit auf **Abbrechen** klicken, um die Installation zu stoppen.

6. Wenn die **Statuszeile** vollständig ist, ist der Prozess abgeschlossen, und Sie können über die Einstellungen für den Import die Domäne für die neuen Hosts auswählen.
7. Klicken Sie auf **Fertig stellen**.

   Policy Manager ConsoleWenn Sie in diesem Dialogfeld keine andere Domäne angeben, legt für den neuen Host die Domäne fest, die Sie in Schritt 1 ausgewählt haben. Sie können auch festlegen, dass keine automatische Zuordnung der Hosts zu Domänen stattfinden soll. Die neuen Hosts senden Anforderungen für eine automatische Registrierung und können auf diese Weise importiert werden.

   Nach wenigen Minuten werden die installierten Programme aufgelistet.
8. Zum Anzeigen der Liste wählen Sie die Registerkarte **Installation** (alternativ können Sie die obere Domäne in der Struktur **Richtliniendomäne** wählen).

Installation auf Richtlinienbasis

Installationsvorgänge auf Hosts, auf denen Management Agent installiert ist, können über Richtlinien in Policy Manager zentral verwaltet werden.

Über die auf Richtlinie basierende Installation erfolgt eine Erstellung und Speicherung des vorgangsspezifischen Installationspaketes und ein Schreiben einer Installationsaufgabe in die grundlegenden Richtliniendateien (daher ist eine Richtlinienverteilung für den Start der Installationen erforderlich). Sowohl die grundlegenden Richtliniendateien als auch das Installationspaket werden vom Verwaltungsschlüsselpaar signiert, sodass nur echte Informationen von den Hosts angenommen werden.

Management Agent auf dem Host ruft die neuen Richtlinien aus Policy Manager Server ab und ermittelt die Installationsaufgabe. Daraufhin ruft Management Agent das in den Aufgabenparametern angegebene Installationspaket vom Server ab und beginnt mit der Installation der Programme.

Nach Abschluss der Installation sendet Management Agent das Ergebnis des Vorgangs in einer inkrementellen Richtliniendatei an den Server. Die Ergebnisse der neuen Statusinformationen werden in Policy Manager Console angezeigt.

Bei einer Deinstallation wird derselbe Mechanismus verwendet. Die Ergebnisse der Deinstallation werden nicht gemeldet.

Verwenden von richtlinienbasierter Installation

Richtlinienbasierte Installation muss auf Hosts verwendet werden, auf denen bereits Management Agent installiert ist.

Sie können die richtlinienbasierte Installation nutzen, um Installationsvorgänge auf einer ausgewählten Domäne oder ausgewählten Hosts durchzuführen. Zusätzlich zur Installation von Produkten können Sie Hotfixes, Upgrades, Reparaturen und Deinstallationen vornehmen.

Ist der Installationsvorgang erfolgreich abgeschlossen, können Sie den Vorgang in der Tabelle **Richtlinienbasierte Installationen** belassen, sodass der gleiche Installationsvorgang automatisch auf alle neuen Hosts angewandt wird, die zur entsprechenden Domäne hinzugefügt werden.

So verwenden Sie richtlinienbasierte Installation:

1. Öffnen Sie die Registerkarte **Installation**.
   Auf der Registerkarte **Installation** wird in der Tabelle **Richtlinienbasierte Installationen** der Status der aktuellen Installationsvorgänge angezeigt. In der Tabelle **Zusammenfassung installierter Produkte** werden die Produkte aufgelistet, die aktuell auf verwalteten Hosts installiert sind.

2. Klicken Sie auf **Installieren** unter der Tabelle **Richtlinienbasierte Installationen**, um den Assistenten für die Remote-Installation zu starten.
3. Führen Sie die Anweisungen des Assistenten für die Remote-Installation aus, indem Sie die notwendigen Details angeben.

   Die Informationen, die in den Assistenten für die Remote-Installation eingegeben werden, werden verwendet, um das benutzerdefinierte Paket vorzubereiten, das für diesen Installationsvorgang spezifisch ist. Das Installationspaket wird dann an die ausgewählte Domäne oder die ausgewählten Hosts verteilt, sobald die Richtlinie verteilt wird.

   Nach Abschluss des Assistenten für die Remote-Installation werden der Installationsvorgang und der Status in der Tabelle **Richtlinienbasierte Installatione** als neue Zeile angezeigt.
4. Verteilen Sie die Richtlinie.
   Sobald der Installationsvorgang abgeschlossen ist, werden der Produktname, die Version und die Nummer der Hosts, auf denen das Produkt ausgeführt wird, in der Tabelle **Zusammenfassung installierter Produkte** angezeigt.

   Hinweis: Der Installationsvorgang kann länger dauern. Dies ist beispielsweise der Fall, wenn ein betroffener Host keine Verbindung zum Netzwerk hat oder wenn der aktive Installationsvorgang erfordert, dass der Benutzer seinen Host neu startet, bevor die Installation abgeschlossen werden kann. Sind die Hosts mit dem Netzwerk verbunden und senden und empfangen sie die Richtliniendateien richtig, liegt wahrscheinlich ein größeres Problem vor. Der Host quittiert ggf. den Installationsvorgang nicht richtig. Es ist möglich, den Installationsvorgang aus der Richtlinie zu entfernen, indem man auf **Zeile löschen** klickt und dann die Richtlinie verteilt. Hierdurch wird der Installationsvorgang abgebrochen. Es ist möglich, die Installationsaufgabe in der ausgewählten Domäne und allen Unterdomänen zu löschen, indem man die Option **Installation für Unterdomänen und Hosts rekursiv abbrechen** im Bestätigungsfenster auswählt.

Für andere Installationsvorgänge, beispielsweise Upgrades oder Deinstallationen, können Sie die Links neben dem Produkt in der Tabelle **Zusammenfassung installierter Produkte** verwenden. Diese Links werden automatisch angezeigt, wenn die Installationspakete, die für die entsprechende Aktion notwendig sind, verfügbar sind. Die Optionen sind: **Hotfix**, **Upgrade**, **Reparatur** und **Deinstallation**.

Wird der Link für den Vorgang, den Sie ausführen möchten, nicht in der Tabelle **Zusammenfassung installierter Produkte** angezeigt, können Sie, je nachdem, was Sie durchführen möchten, entweder auf **Installieren** oder **Deinstallieren** unter der Tabelle **Richtlinienbasierte Installationen** klicken. Prüfen Sie dann, ob das entsprechende Paket verfügbar ist. Unterstützt das Produkt beispielsweise die Remote-Deinstallation nicht, wird diese Option für die Deinstallation nicht angezeigt.

Beim Deinstallieren von Management Agent werden keine statistischen Informationen gesendet, mit denen angegeben wird, dass die Deinstallation erfolgreich ausgeführt wurde, da Management Agententfernt wurde und keine Informationen mehr senden kann. Beispiel: Deinstallieren von F-Secure Anti-Virus und Management Agent:

1. Deinstallieren Sie F-Secure Anti-Virus.
2. Warten Sie, bis der Erfolg oder Misserfolg der Deinstallation in Policy Manager Console angezeigt wird.
3. Wenn F-Secure Anti-Virus erfolgreich deinstalliert wurde, deinstallieren Sie Management Agent.
4. Schlägt die Deinstallation von Management Agent fehl, zeigt Policy Manager Console einen Statistikbericht über den Fehler an. Eine erfolgreiche Deinstallation kann nicht gemeldet werden, wird aber durch die eingestellte Kommunikation deutlich. Der endgültige Bericht für Management Agent gibt an:`Wird ausgeführt....`

Lokale Installation und Updates mit vorkonfigurierten Paketen

Sie können vorkonfigurierte Pakete in das MSI- (Microsoft Installer) oder JAR-Format exportieren.

MSI-Pakete können beispielsweise über die Windows-Gruppenrichtlinie in Active Directory-Umgebungen verteilt werden.

Der Exportvorgang ist bei beiden Formaten gleich und wird unten beschrieben. Sie können das Dateiformat für das benutzerdefinierte Paket im Dialogfenster **Installationspaket exportieren** auswählen.

Verwendung des angepassten Remote-Installationspakets

Es gibt zwei Möglichkeiten Anmeldeskripts auf Windows-Plattformen zu verwenden: zum einen durch die Nutzung eines benutzerdefinierten MSI-Pakets oder durch ein benutzerdefiniertes Remote-Installations-JAR-Paket.

So verwenden Sie ein benutzerdefiniertes Installationspaket:

1. Führen Sie Policy Manager Console aus.
2. Wählen Sie **Extras** > **Installationspakete** aus dem Menü
   Damit wird das Dialogfeld **Installationspakete** geöffnet.
3. Wählen Sie das Installationspaket mit den Programmen aus, die installiert werden sollen, und klicken Sie auf **Exportieren**.
4. Legen Sie das Dateiformat, MSI oder JAR, und den Speicherort für das benutzerdefinierte Installationspaket fest und klicken Sie dann auf **Exportieren**.
5. Legen Sie den Dateispeicherort für das benutzerdefinierte Installationspaket fest und klicken Sie auf **Speicher**.
6. Wählen Sie die zu installierenden Programme aus, und klicken Sie auf **Weiter**, um fortzufahren.
7. Übernehmen Sie die Standardrichtlinie, oder geben Sie an, welche Host- bzw. Domänenrichtlinie als anonyme Richtlinie verwendet werden soll, und klicken Sie dann auf **Weiter**, um fortzufahren.
8. Wählen Sie den Installationstyp aus.

   Die Standardeinstellung **Zentralverwaltungs-Installation** wird empfohlen. Sie können auch ein Paket für einen Einzelplatzhost vorbereiten.

   Auf einer Zusammenfassungsseite werden Ihre Installationseinstellungen angezeigt.
9. Überprüfen Sie die Zusammenfassung, und klicken Sie auf **Starten**, um die nächste Seite des Installations-Assistenten anzuzeigen.

   Policy Manager Console zeigt die **Assistenten für die Ferninstallation** an, über die alle notwendigen Einrichtungsinformationen für die ausgewählten Produkte gesammelt werden. Es ist möglich, eine beliebige Anzahl an benutzerdefinierten Eigenschaften in das Installationspaket einzubinden. Ein Host fügt diese benutzerdefinierten Eigenschaften zu einer Meldung hinzu, die nach der lokalen Installation an Policy Manager gesendet wird. Diese kundenspezifischen Eigenschaften werden zusammen mit den standardmäßigen Host-Identifikationseigenschaften in der Ansicht **Neue Hosts** angezeigt. Der Name der benutzerdefinierten Eigenschaft ist auch der Name der Spalte und der Wert wird als Zellenwert angegeben.

   Ein Beispiel für die Art der Nutzung benutzerdefinierter Eigenschaften ist die Erstellung eines separaten Installationspakets für unterschiedliche organisatorische Einheiten, die unter der Einheit spezifischen Richtliniendomänen gruppiert werden sollten. Der Name der Eigenschaft könnte `Einheit` lauten und der Wert ist für jedes Installationspaket anders. Nun können Hosts aus jeder Einheit in der neuen Host-Ansicht unterschieden werden. Darüber hinaus können über die Spaltensortierung und eine Mehrfachauswahl alle Hosts aus einer Einheit zu ihrer Zieldomäne importiert werden. Beachten Sie, dass die Zieldomäne direkt über die Ansicht **Neue Hots** geändert werden kann. Danach können die Hosts aus einer anderen Einheit in ihre Zieldomäne importiert werden.
10. Wenn Sie die letzte Seite des Assistenten erreichen, klicken Sie auf **Fertig stellen**, um fortzufahren.
11. Darüber hinaus können Sie eine exportierte JAR-Datei auf den Hosts installieren, indem Sie die Datei `ilaunchr.exe` ausführen.

    Das Programm `ilaunchr.exe` befindet sich im Policy Manager Console-Installationsverzeichnis unter `...\Administrator\Bin`. Gehen Sie wie folgt vor:

    a) Kopieren Sie die Datei `ilaunchr.exe` und das exportierte JAR-Paket in ein Verzeichnis, in dem das Anmeldeskript auf die Dateien zugreifen kann.
    b) Geben Sie folgenden Befehl ein:`ilaunchr <paketname>.jar` wobei Sie anstelle von `paketname` den Namen des zu installierenden JAR-Pakets eingeben.

Während der Installation wird der Verlauf der Installation angezeigt. Falls nach der Installation ein Neustart erforderlich ist, erhält der Benutzer gemäß den Festlegungen beim Export des Installationspakets eine entsprechende Aufforderung. Wenn die Installation unbeaufsichtigt im Hintergrund ablaufen soll, geben Sie den Befehl wie folgt ein: `ilaunchr <package name>.jar /Q`. Selbst im Hintergrundmodus wird der Benutzer nach der Installation unter Umständen aufgefordert, den Computer neu zu starten, und sollte es während der Installation zu einem schwerwiegenden Fehler kommen, erhält er eine entsprechende Meldung.

Für **ILAUNCHR** gelten die folgenden Befehlszeilenparameter:

`/U` — Unbeaufsichtigte Installation. Es werden keine Meldungen angezeigt, auch nicht bei einem schwerwiegenden Fehler.

`/F` — Erzwungene Installation. Schließt die Installation ab, auch wenn Management Agent bereits installiert ist.

Geben Sie in der Befehlszeile `ILAUNCHR /?` ein, um die vollständige Hilfe anzuzeigen.

Bei einer Installation unter Windows XP oder einer neueren Windows-Version können Sie auch die folgenden Parameter einsetzen:

- `/Benutzer:Domaene\Benutzername` (Variation: `/Benutzer:Benutzername`) — Bestimmt das Benutzerkonto und den Domänennamen. Sie können den Domänennamen wahlweise auslassen.
- `/Passwort:geheim` (Variation: `Passwort:"geheim mit Leerzeichen"`) — Bestimmt das Passwort für das Benutzerkonto.

An der Funktionalität von ILAUNCHR ändert sich nichts, wenn Sie beide Parameter auslassen. Wird jedoch nur ein Parameter angegeben, gibt ILAUNCHR einen Fehlercode zurück. Wenn beide Parameter angegeben werden, startet ILAUNCHR das**Setup-**Programm. Befehlsbeispiel:

```
ILaunchr <JAR-Datei> /Benutzer:Domaene\Benutzername /Passwort:Geheimwort
```

Bereitstellung von Informationen

Alle Installationsinformationen werden in Form einer Datei über Policy Manager Server bereitgestellt.

Bei den Installationspaketen handelt es sich um JAR-Archive, die mit einem geeigneten Komprimierungsprogramm (z. B. WinZip) angezeigt werden können. Andere Dateitypen (z. B. Richtliniendateien und `INI`-Dateien) werden zur Auslösung des eigentlichen Installationsvorgangs eingesetzt.

Bevor Policy Manager Console mit einer Installation beginnen kann, muss das erste Installationspaket an Policy Manager Server übertragen werden. Die Installationspakete sind über zwei Quellen verfügbar:

- Installations-CD-ROM oder
- F-Secure Website.

Normalerweise werden neue Remote-Installationspakete von der CD-ROM installiert und über die Einrichtung von Policy Manager erfolgt ein automatisches Verschieben der Pakete auf den Server. Wird ein Remote-Installationspaket aus einer anderen Quelle bezogen, können Sie das Paket importieren, indem Sie auf die Option **Importieren** im Dialogfenster **Installationspakete** klicken.

Policy Manager Console überprüft daraufhin, ob das neue Installationspaket mit dem privaten Schlüssel von F-Secure signiert ist, bevor das neue Paket zur Verwendung freigegeben wird.

Verwalten von Richtlinien

In diesem Abschnitt wird die Konfiguration und Verteilung von Richtlinien beschrieben.

Es können mehrere Benutzer gleichzeitig angemeldet sein und Änderungen an Richtlinien vornehmen. Alle Änderungen, die von Benutzern vorgenommen werden, werden automatisch in deren eigenem Arbeitsplatz gespeichert. Die Änderungen müssen also nicht manuell gespeichert werden. Änderungen, die von einem

beliebigen Benutzer vorgenommen worden, sind nur für andere Benutzer sichtbar und treten in Kraft, wenn der Benutzer die Richtlinienänderungen verteilt.

Hinweis: Es gibt keine Konfliktlösung für Richtlinienänderungen, die von unterschiedlichen Benutzern vorgenommen wurden. Die letzten verteilten Änderungen überschreiben die vorherigen Änderungen an den Richtlinienvariablen.

Wenn Richtlinienänderungen verteilt werden, werden die Richtliniendateien automatisch für jeden Host auf Anfrage generiert. Dies bedeutet, dass eine Rückverteilung der Richtlinie bei Änderung der Domänenstruktur, beispielsweise bei Hinzufügen neuer Hosts oder nach einem Upgrade der verwalteten Software auf vorhandenen Hosts, nicht notwendig ist.

Einstellungen

Zum Konfigurieren der Einstellungen durchsuchen Sie die Richtlinienstruktur, und ändern Sie die Werte der Richtlinienvariablen.

Eventuell existiert für eine Richtlinienvariable ein im Vorfeld definierter Standardwert. Standardwerte verhalten sich so, als wären sie aus der Standarddomäne vererbt worden. Das heißt, dass die Werte als übernommene Werte angezeigt werden, auch wenn die oberste Domäne (Stamm) ausgewählt ist. Standardwerte können wie alle anderen Werte überschrieben werden.

Werte in der ausgewählten Richtliniendomänenebene sind wie folgt farbcodiert:

- Schwarz - Werte, die auf der ausgewählten Richtliniendomäne oder auf dem ausgewählten Host geändert wurden
- Grau - geerbte Werte
- Rot - ungültige Werte
- Abgedunkeltes Rot - ungültige geerbte Werte

Verwerfen nicht verteilter Änderungen an den Einstellungen

Sie können Änderungen an den Einstellungen, die Sie noch nicht angewandt haben, rückgängig machen.

Wählen Sie **Datei** > **Richtlinienänderungen verwerfen** aus dem Menü aus.
Die Einstellungen werden auf die Werte zurückgesetzt, die zum Zeitpunkt der letzten Verteilung gültig waren. Wurden die Änderungen bereits verteilt, müssen Sie die Änderungen manuell rückgängig machen und die Richtlinie erneut verteilen.

Beschränkungen

Mittels Einschränkungen kann ein Administrator den Zugriff auf eine beliebige Richtlinienvariable durch den Benutzer beschränken.

Richtlinienvariablen, die auf **Benutzeränderungen nicht zulassen** eingerichtet sind, erzwingen immer die Einrichtung: Die Richtlinienvariable überschreibt jeden loakeln Host-Wert und der Endbenutzer kann den Wert nicht ändern, solange die Beschränkung **Benutzeränderungen nicht zulassen** aktiv ist.

Konfigurieren von Einstellungen

Einstellungen werden über die Modifikation von Richtlinienvariablen geändert.

So konfigurieren Sie Einstellungen:

1. Durchsuchen Sie die Richtlinien-Baumstruktur.
2. Ändern Sie die Werte der Richtlinienvariablen.
3. Verteilen Sie die Richtlinien:

Im Anschluss an die Konfiguration der Domänen und Hosts müssen Sie die neuen Konfigurationsdaten an die Hosts verteilen. Gehen Sie dazu wie folgt vor:

- Klicken Sie in der Symbolleiste auf .
- Wählen Sie **Datei** > **Verteilen** aus dem Menü.
- Drücken Sie CTRL + D.

Sobald Sie die Änderungen verteilen, werden die aktualisierten Richtlinien in der Datenbank gespeichert, in der die F-Secure-Software auf den Hosts automatisch nach Updates sucht.

Hinweis: Es werden keine Änderungen übernommen, bevor Sie nicht die Richtlinie verteilt haben und der Host diese abgerufen hat. Dies gilt auch für Vorgänge, da diese über den auf der Richtlinie basierenden Mechanismus eingebunden werden.

Richtlinienvererbung

In Policy Manager Console erbt jede Richtliniendomäne automatisch die Einstellungen der übergeordneten Domäne. Auf diese Weise lassen sich große Netzwerke bequem und effizient verwalten.

Die vererbten Einstellungen können auf einzelnen Hosts oder Domänen geändert werden. Wenn die vererbten Einstellungen einer Domäne geändert werden, werden diese Änderungen von allen Hosts und untergeordneten Domänen der jeweiligen Domäne übernommen. Alle überschriebenen Einstellungen können mithilfe des Vorgangs **Löschen** erneut vererbt werden. Da die Einstellung aus der gegenwärtig ausgewählten Richtliniendomäne oder vom ausgewählten Host gelöscht wird, wird sie durch die Einstellung in der übergeordneten Domäne ersetzt.

Durch das Vererben von Richtlinien wird die Definition einer gemeinsamen Richtlinie vereinfacht. Eine Richtlinie kann für untergeordnete Domänen oder sogar für einzelne Hosts genauer bestimmt werden. Die Anzahl der festgelegten Richtlinien für die einzelnen Installationen kann stark variieren. Manche Administratoren legen unter Umständen nur wenige Richtlinien für große Domänen fest, während andere Administratoren eventuell an jeden Host eine Richtlinie anhängen.

Durch die Kombination dieser Strategien vereinen Sie die Vorteile beider Verfahren. Einige Programme können ihre Richtlinien von großen Domänen erben, während andere Programme ihre Richtlinien von Subdomänen erben und manche sogar spezifische, auf den Host zugeschnittene Richtlinien erhalten.

Wenn Richtlinienänderungen auf mehreren Ebenen in der Hierarchie der Richtliniendomäne implementiert werden, kann sich die Verfolgung und Protokollierung von Änderungen als recht komplex erweisen. Eine bequeme Methode besteht im Einsatz der Operation **Domänenwerte anzeigen**, um festzustellen, welche Änderungen an einer spezifischen Richtlinieneinstellung vorgenommen wurden.

Wenn die Subdomänen- oder Host-Werte auf die aktuellen Domänenwerte zurückgesetzt werden müssen, können Sie mithilfe der Operation **Wert erzwingen** die Subdomänen- und Host-Werte bereinigen.

Tipp: Sie können auch das **Dienstprogramm zur Berichterstellung** verwenden, um **Vererbungsberichte** zu erstellen, in denen angezeigt wird, wo vererbte Einstellungen überschrieben wurden.

Indexvererbung in Tabellen

Wenn Sie auf die Schaltfläche **Zeile löschen** klicken, werden die Werte in der ausgewählten Reihe gelöscht. Das Ergebnis hängt von der Art der Standardzeilen ab, die in den übergeordneten Domänen in der MIB als Standardzeilen gespeichert sind.

- Wenn es eine Zeile mit denselben Indexwerten wie die gelöschte Zeile gibt, werden die Werte neu geerbt.
- Wenn es keine Zeile mit denselben Indexwerten gibt, bleibt die bereinigte Zeile nach dem Löschen der Zeile leer.

Hinweis: Der Inhalt einer Zeile kann von einer übergeordnete Domäne oder aus einer MIB (eine Definition der Einstellungen, die außerdem die Standardwerte für alle Einstellungen enthält) als eine

Standardzeile geerbt werden. Die MIB kann am besten als eine "Domäne oberhalb der Stammdomäne" in Relation zum Blattwert oder zur Zeilenvererbung verstanden werden. Die MIB-Standardwerte werden an die Subdomänen vererbt, es sei denn, die Werte werden auf Domänenebene vererbt. Um eine geerbte Zeile zu überschreiben, definieren Sie eine Zeile mit denselben Indexspaltenwerten. MIB-Standardwerte werden auf der Grundlage der auf den Hosts installierten Programmversion abgerufen. In einer Domäne werden die Werte der neuesten Programmversion verwendet.

Verwaltung von Vorgängen und Aufgaben

Mit Policy Manager Console können diverse produktspezifische Vorgänge durchgeführt werden.

So starten Sie einen Vorgang aus Policy Manager Console:

1. Wählen Sie eine der Aktionen der Registerkarte **Vorgänge** aus.

   Weiterhin können Sie verfügbare Vorgänge in der Ansicht **Erweiterter Modus** im Zweig **Vorgänge** des ausgewählten Produkts auf der Registerkarte **Richtlinie** ansehen.
2. Klicken Sie auf **Starten**, um den gewählten Vorgang zu starten.
3. Der Vorgang beginnt auf dem Host, wenn Sie die neue Richtlinie verteilt haben und die Richtliniendatei vom Host abgerufen wurde.

   Sie können jederzeit auf **Abbrechen** klicken, um den Vorgang rückgängig zu machen.

Alarme

In diesem Abschnitt wird beschrieben, wie Alarme und Berichte angezeigt und Alarm-Weiterleitungen konfiguriert werden.

Anzeigen von Alarmen und Berichten

Wenn Probleme mit einem Programm oder einem Vorgang auftreten, können Hosts Alarme und Berichte senden.

Wenn ein Alarm empfangen wird, leuchtet die Schaltfläche auf. So zeigen Sie die Alarme an:

1. Klicken Sie auf geändert.

   Die Registerkarte **Alarme** wird geöffnet. Die empfangenen Alarme werden in folgendem Format angezeigt:

Quittieren	Klicken Sie auf die Schaltfläche **Quittieren**, um einen Alarm zu quittieren. Wenn alle Alarme bestätigt wurden, wird die Schaltfläche **Quittieren** abgeblendet.		
Schweregrad	Der Schweregrad des Problems. Für jeden Schweregrad gibt es ein eigenes Symbol:		
		Info	Normale Informationen eines Hosts über einen Arbeitsvorgang.
		Warnung	Eine Warnung vom Host.
		Fehler	Behebbarer Fehler auf dem Host.
		Schwerwiegender Fehler	Unbehebbarer Fehler auf dem Host.
		Sicherheitsalarm	Sicherheitsrisiko auf dem Host.

Datum/Uhrzeit	Datum und Uhrzeit des Alarms.
Beschreibung	Beschreibung des Problems.
Host/Benutzer	Name des Hosts bzw. des Benutzers.
Programm	Das F-Secure-Programm, das den Alarm gesendet hat.

Bei Auswahl eines Alarms aus der Liste werden nähere Informationen zum Alarm angezeigt.F-Secure Alarme der Anti-Virus-Überprüfug können über einen angehängten Bericht verfügen, der ebenfalls angezeigt wird.

2. Um Berichte anzusehen, klicken Sie auf die Registerkarte **Scan-Berichte** oder wählen Sie **Produktansicht** > **Meldungen** aus dem Menü aus.

   Die Registerkarte **Scan-Berichte** hat die gleiche Struktur wie die Registerkarte **Warnungen**. Die Tabellen **Warnungen** und **Scan-Berichte** können per Klick auf die Spaltenüberschrift sortiert werden.

Konfigurieren der Alarmweiterleitung

Sie können Alarme konfigurieren, indem Sie die Tabelle **Alarm-Weiterleitung** bearbeiten. Diese Tabelle befindet sich unter **F-Secure Management Agent** > **Einstellungen** > **Alarmausgabe** > **Alarm-Weiterleitung**.

Dieselbe Tabelle finden Sie in der Produktansicht von Management Agent auf der Registerkarte **Alarm-Weiterleitung**.

So konfigurieren Sie die Alarm-Weiterleitung:

1. Wählen Sie **F-Secure Management Agent** > **Einstellungen** > **Alarmausgabe** > **Alarm-Weiterleitung** aus dem Menü.
2. Bestimmen Sie abhängig vom Schweregrad, wohin die Alarme gesendet werden.

   Beim Ziel kann es sich um die Policy Manager Console, die lokale Benutzeroberfläche, einen Alarmagenten (wie die **Ereignisansicht**, eine Protokolldatei oder SMTP) oder eine Management-Erweiterung handeln.

   Die Tabelle **Alarm-Weiterleitung** verfügt über eigene Standardwerte.

   Alarme mit dem Schweregrad "Info" oder "Warnung" werden standardmäßig nicht an Policy Manager Console gesendet oder auf der Benutzeroberfläche angezeigt. Diese Alarme niedriger Priorität und Benachrichtigungen können sehr nützliche Informationen zur Fehlerbehebung enthalten. Wenn Sie diese Alarme aktivieren, kommt es jedoch zu einer drastischen Erhöhung der Anzahl der übertragenen Alarme. Wenn Sie bei einer großen Domänenstruktur strenge Regeln zur Alarm-Weiterleitung auf der Stammdomänenebene festlegen, wird Policy Manager Console unter Umständen durch zu viele Alarme überflutet.
3. Konfigurieren Sie das Alarmziel ggf. durch die Festlegung von Richtlinienvariablen unter zielspezifischen Verzweigungen weiter .
   Über die Befehlsfolge **Einstellungen** > **Alarmausgabe** > **F-Secure Policy Manager Console** > **Sendewiederholungsintervall** legen Sie z. B. fest, wie oft ein Host versucht, Alarme an Policy Manager Console zu senden, wenn der vorherige Versuch fehlgeschlagen ist.

Dienstprogramm zur Berichterstellung

Mit dem **Dienstprogramm zur Berichterstellung** können Benutzer Berichte über verwaltete Daten von Policy Manager Console anzeigen und exportieren.

Über die Funktionen zum Anzeigen und Exportieren können Sie die Daten von verschiedenen Hosts/Domänen gleichzeitig untersuchen.

Fensterbereich "Auswahl der Domäne/des Hosts"

Im Fensterbereich **Auswahl der Domäne/des Hosts** können Sie die Domänen und/oder Hosts auswählen, zu denen Sie Berichte erstellen möchten.

Die im Richtliniendomänen-Baum des Hauptbereichs der Anwendung ausgewählte Domäne wird standardmäßig vom **Dienstprogramm zur Berichterstellung** ausgewählt.

Wenn Sie das Kontrollkästchen **Rekursiv** aktivieren, werden alle Hosts, die sich unter den ausgewählten Domänen in der Domänenhierarchie befinden, ebenso in den Bericht aufgenommen.

Fensterbereich "Auswahl des Berichtstyps"

Hier können Sie den Berichtstyp auswählen, der in diesem Fensterbereich ausgeführt werden soll.

Im Fensterbereich **Auswahl des Berichtstyps** können Sie:

- den Typ des zu erstellenden Berichts auswählen.
- die Filterung nach Programm aktivieren (es werden nur Informationen zu ausgewählten Programmen in den Bericht aufgenommen).

Zurzeit sind folgende Berichtstypen verfügbar:

Berichtstyp	Beschreibung
Richtlinie	Berichte mit den Werten aller Richtlinienvariablen der ausgewählten Programme aus den ausgewählten Domänen werden exportiert/angezeigt. Sie können auch das Kontrollkästchen **Vererbung** aktivieren, wenn Sie Vererbungsinformationen in den Bericht aufnehmen möchten.
Vererbung	Berichte mit den Werten aller Richtlinienvariablen der ausgewählten Programme aus den ausgewählten Domänen, die nicht aus einer übergeordneten Domäne übernommen wurden, d. h. Werte aller Richtlinienvariablen, die in den ausgewählten Domänen überschrieben werden, werden exportiert/angezeigt.
Status	Berichte mit den Werten aller lokalen Einstellungen und Statusvariablen der ausgewählten Programme aus den ausgewählten Domänen werden exportiert/angezeigt.
Eigenschaften	Berichte mit den Werten aus allen Eigenschaftsfeldern der Domänen-Komponenten werden exportiert/angezeigt. Über die **Kontrollkästchen** zur Auswahl der Eigenschaften können Sie die Eigenschaftsfelder festlegen, die in den Bericht aufgenommen werden sollen.
Alarm	Berichte mit Informationen zu allen Alarmen aus den ausgewählten Domänen werden exportiert/angezeigt. Sie können auch die Auswahl**Sortierreihenfolge** verwenden, um die Sortierreihenfolge der Felder mit den Alarmbeschreibungen festzulegen. Über die Auswahl **Schweregrad** können Sie die Schweregrade der Alarme bestimmen, die in den Bericht aufgenommen werden sollen.

Berichtstyp	Beschreibung
Konfiguration	Berichte mit Informationen zu den installierten Programmen der ausgewählten Produkte aus den ausgewählten Domänen werden exportiert/angezeigt.
Anti-Virus	Berichte mit den Werten für den Domänenstatus der Programmversionen und Updates der Virendefinitionen werden exportiert/angezeigt.

Fensterbereich "Bericht"

Nach der Auswahl eines Berichtstyps können Sie in diesem Fensterbereich typenabhängige Konfigurationen vornehmen.

Im Fensterbereich **Bericht** können Sie:

- die vom Berichtstyp abhängige Konfiguration für den aktuell ausgewählten Berichtstyp auswählen. Bei den vom Berichtstyp abhängigen Konfigurationen können Sie weitere Filterfunktionen für den Bericht anpassen.
- eine Beschreibung zum gegenwärtig ausgewählten **Berichtstyp** suchen.

Die derzeit bekannten Berichtstypen weisen folgende Konfigurationen auf:

- Mit den **Konfigurationen für Richtlinienberichte** können Sie Vererbungsinformationen der Richtlinienwerte auswählen, die in den Bericht aufgenommen werden sollen.
- Mit den **Konfigurationen für Eigenschaftsberichte** können Sie basierend auf Identitäten, Plattform, Verschiedenes und Abfrageeigenschaften festlegen, welche Informationen in den Bericht aufgenommen werden.
- Mit den **Konfigurationen für Alarmberichte** können Sie Alarme nach den Alarmbeschreibungsfeldern sortieren und die Schweregrade von Alarmen wählen, die in den Bericht aufgenommen werden sollen.

Unterer Fensterbereich

Nach der Konfiguration eines Berichts können Sie eine zu ergreifende Maßnahme im unteren Fensterbereich des **Dienstprogramms zur Berichterstellung** wählen.

Im unteren Fensterbereich können Sie:

- die Standardeinstellungen für alle Komponenten der Benutzeroberfläche wiederherstellen,
- den Prozess zum Exportieren der Berichte starten,
- den Prozess zum Anzeigen der Berichte starten,
- den Prozess zur Berichterstellung anhalten.
- die Benutzeroberfläche des **Dienstprogramms zur Berichterstellung** schließen. Dadurch wird die Erstellung des zu exportierenden Berichts nicht angehalten, da dieser Prozess im Hintergrund läuft. Die Generierung von Berichten, die auf dem Bildschirm angezeigt werden sollen, kann über das angezeigte Dialogfeld angehalten werden.

Anzeigen und Exportieren eines Berichts

Berichte können mithilfe des **Dienstprogramms zur Berichterstellung** angezeigt und exportiert werden.

So verwenden Sie das **Dienstprogramm zur Berichterstellung**:

1. Wählen Sie **Extras** > **Berichterstellung...** aus dem Menü.

   Alternativ:

   - Rufen Sie das **Dienstprogramm zur Berichterstellung** aus dem Kontextmenü im Hauptbereich der Anwendung auf.

Das **Dienstprogramm zur Berichterstellung** wird geöffnet.

2. Wählen Sie die Domänen und/oder Hosts, die Sie in den Bericht einbeziehen möchten.
   - Wählen Sie **Rekursiv**, wenn Sie alle Hosts in den gewählten Domänen in den Bericht einbeziehen möchten.
3. Wählen Sie den Berichtstyp aus.
4. Wählen Sie ggf. die Programme aus, die Sie in den Bericht einbeziehen möchten.
5. Wählen Sie ggf. vom Berichtstyp abhängige Konfigurationen für den aktuell gewählten Bericht.
6. Zeigen Sie den Bericht an, oder exportieren Sie ihn:
   - Klicken Sie im unteren Fensterbereich auf **Ansicht**, um den Bericht zu erzeugen und mit dem Standard-Webbrowser im HTML-Format anzuzeigen. Wenn auf Ihrem Computer kein Standard-Webbrowser definiert wurde, wird ein Dialogfeld angezeigt, in dem Sie aufgefordert werden, den Webbrowser zu definieren.
   - Klicken Sie im unteren Fensterbereich auf **Exportieren**, um den Bericht zu erzeugen und als Datei zu speichern. Der Dateipfad und das Berichtsformat werden im Dialogfeld **Datei speichern** definiert, das nach dem Klicken auf **Exportieren** angezeigt wird.

Voreinstellungen

Voreinstellungen werden gemeinsam genutzt oder auf eine bestimmte Verbindung angewendet.

Verbindungsspezifische Voreinstellungen

Wählen Sie zur Bearbeitung dieser Einstellungen den Eintrag **Voreinstellungen** aus dem Menü **Extras**. Nur das aktuelle Verbindungsobjekt ist betroffen.

Registerkarte	Einstellung	Bedeutung
Warnungen und Berichte		Mit diesen Optionen werden folgende Vorgänge gesteuert: • die Zeitdauer, aus der Warnungen angezeigt werden sollen. • die Zeitdauer, aus der Berichte angezeigt werden sollen.
Push-Installation	**Zeitlimit für Installation**	Die Zeit, die Policy Manager Console höchstens auf die Ergebnisse eines Installationsvorgangs wartet.
	Zeitlimit für Suchläufe	Nur wichtig, wenn die Option **Bereits verwaltete Hosts ausblenden** aktiviert ist. Dabei handelt es sich um den maximalen Zeitraum, in dem auf die Registrierung des Hosts zugegriffen werden kann.
	Maximale Anzahl gleichzeitig ablaufender Netzwerkoperationen	Sie können die Anzahl der Netzwerkoperationen ändern. Beim Standardwert handelt es sich um die empfohlene Einstellung. Wenn Sie aber eine langsame Netzwerkverbindung verwenden, die bei der Push-Installation Probleme verursacht, verringern Sie die Anzahl der gleichzeitig aktiven Netzwerkverbindungen entsprechend.
	Fortschrittsanzeige	Sie können festlegen, ob die Fortschrittsanzeige während der Remote-Installation für Endbenutzer angezeigt werden soll.

Gemeinsame Voreinstellungen

Diese Einstellungen werden auf alle Verbindungen angewendet, die in bestimmten Installationen von Policy Manager Console definiert wurden.

Registerkarte	Einstellung	Bedeutung
Darstellung > Allgemeine Optionen	Sprache	Sprachauswahl. Sie können die lokale Spracheinstellung des Betriebssystems oder die Standardeinstellung "Englisch" wählen. Alle Objekte, die die lokale Sprache des Betriebssystems nicht unterstützen, werden in englischer Sprache dargestellt. Sie müssen Policy Manager Console neu starten, damit die Änderungen wirksam werden.
	Schriftart	In Policy Manager Console verwendete Schriftart. Die Schriftarteinstellung wird nach einem Neustart des Programms übernommen.
	Look & Feel	Definiert das Aussehen und das Verhalten der Komponenten der Benutzeroberfläche. Die Änderung wird nach einem Neustart des Programms übernommen.
Push-Installation	Cache löschen	Sie können alle zwischengespeicherten Informationen zu durchsuchten Hosts und installierter Software löschen, um Festplattenspeicherplatz freizugeben.
Standort	HTML-Browser-Pfad	Der vollständige Pfad zur Programmdatei des HTML-Browsers. Der Browser wird zum Anzeigen der Online-Hilfe und der Anti-Virus-Berichte benötigt.
	Pfad für Meldungsprotokolle	Geben Sie den Pfad zu einem Verzeichnis ein, in dem die Protokolldateien für die einzelnen Registerkarten aus der Ansicht Meldung angelegt werden sollen. Jede Protokolldatei enthält den Namen der entsprechenden Registerkarte. Darüber hinaus enthält jede Zeile eine Meldung mit Angabe des Schweregrades sowie der Erstellungszeit.
Anti-Virus	Virendefinitionen	Über diesen Wert können Sie die Zeitspanne definieren, nach deren Ablauf Virendefinitionen im Anti-Virus-Modus als veraltet angezeigt werden.

Kapitel

4

Verwalten von Policy Manager Server

Themen:

- *Sichern und Wiederherstellen von Daten Policy Manager*
- *Erstellen einer Sicherungskopie*
- *Wiederherstellen einer Sicherungskopie*
- *Exportieren und Importieren von Signaturschlüsseln*
- *Replizieren von Software mithilfe von Image-Dateien*

Dieser Abschnitt enthält Themen in Bezug auf die Sicherstellung einer zuverlässigen Ausführung von Policy Manager Server.

Sie finden hier detaillierte Anleitungen zur Sicherung und Wiederherstellung von Konsolendaten in Policy Manager Server.

Sichern und Wiederherstellen von Daten Policy Manager

Policy Manager Server kann durch die routinemäßige Sicherung der Daten auf dem Server gepflegt werden. So ist eine Wiederherstellung möglich.

Es wird dringend empfohlen, die wichtigsten Verwaltungsinformationen regelmäßig zu sichern. Sowohl die Domänen- und Richtliniendaten als auch die Signaturschlüssel werden in der H2-Datenbank gespeichert.

Hinweis: Bevor Sie Daten sichern, müssen Sie den Policy Manager Server-Dienst anhalten.

Darüber hinaus können Sie Signaturschlüssel, die bei Ihrer Installation von Policy Manager Server verwendet werden, in einen Netzwerkspeicherort exportieren, von wo aus sie bei Bedarf auch wieder importiert werden können.

Wenn Sie auch die Voreinstellungen von Policy Manager Console sichern möchten, fertigen Sie eine Sicherungskopie der Datei `lib\Administrator.properties` aus dem lokalen Installationsverzeichnis an.

Hinweis: Die Datei `Administrator.properties` wird während der ersten Ausführung von Policy Manager Console erstellt. Sie enthält sitzungsbezogene Daten, z. B. die Fenstergröße oder die Server-URL.

Erstellen einer Sicherungskopie

Hier finden Sie Informationen darüber, wie Sie eine Sicherung von Richtliniendaten und Domänenstruktur erstellen.

1. Stoppen Sie den Policy Manager Server-Dienst.
2. Sichern Sie das Verzeichnis `<F-Secure-Installationsordner>\Management Server 5\data\h2db`.
3. Starten Sie den Policy Manager Server-Dienst neu.
4. Öffnen Sie die Policy Manager Console-Verwaltungssitzungen erneut.

Wiederherstellen einer Sicherungskopie

Im Falle eines Verlusts von Policy Manager-Daten können Sie die zuletzt gesicherten Daten wiederherstellen.

So stellen Sie gesicherte Policy Manager-Daten wieder her:

1. Stoppen Sie den Policy Manager Server-Dienst.
2. Kopieren Sie die Sicherung des Verzeichnisses `<F-Secure-Installationsordner>\Management Server 5\data\h2db` an den richtigen Speicherort.
3. Starten Sie den Policy Manager Server-Dienst neu.
4. Öffnen Sie die Policy Manager Console-Verwaltungssitzungen erneut.

Exportieren und Importieren von Signaturschlüsseln

Sie können Ihre Signaturschlüssel in einen externen Speicherort exportieren oder vorhandene Signaturschlüssel importieren, um die während der Installation generierten zu ersetzen.

Sie müssen ggf. die Signaturschlüssel exportieren, beispielsweise wenn Sie mehrere Installationen von Policy Manager nutzen, um eine große Umgebung zu verwalten, aber die gleichen Signaturschlüssel für die gesamte Umgebung nutzen möchten.

1. Wählen Sie **Tools** > **Serverkonfiguration** aus dem Menü aus.
2. Wählen Sie **Schlüssel** aus.

   So exportieren Sie aktuelle Signaturschlüssel:

   a) Klicken Sie auf **Exportieren**.
   b) Wählen Sie den Zielordner oder den Netzwerkspeicherort für die exportierten Schlüssel aus und klicken Sie auf **Speichern**.
   c) Geben Sie eine Passphrase für die exportierten privaten Schlüssel ein und wiederholen Sie die Eingabe. Klicken Sie dann auf **OK**.

   So importieren Sie vorhandene Signaturschlüssel, um aktuell verwendete zu ersetzen:

   a) Klicken Sie auf **Ersetzen**.
   b) Navigieren Sie zum Speicherort der Schlüssel, die Sie importieren möchten, und klicken Sie auf **OK**.
   c) Geben Sie die Passphrase für die importierten Signaturschlüssel ein und klicken Sie dann auf **OK**.

   Es wird eine Meldung angezeigt, in der bestätigt wird, dass die Signaturschlüssel erfolgreich exportiert oder ersetzt wurden.
3. Klicken Sie auf **OK**, um das Dialogfenster **Serverkonfiguration** zu schließen.

Replizieren von Software mithilfe von Image-Dateien

Wenn Sie Image-Dateien zur Verteilung von Installationen des Programms verwenden, müssen Sie sicherstellen, dass keine Konflikte hinsichtlich der eindeutigen Kennung bestehen.

Anti-virus kann eingeschlossen werden, wenn die Software mithilfe von Disk-Image-Dateien repliziert wird. Jede Programminstallation enthält jedoch einen eindeutigen Identifikations-Code (UID), der von Policy Manager verwendet wird. Wenn die Disk-Image-Software zur Installation neuer Computer genutzt wird, versuchen unter Umständen mehrere Computer, dieselbe eindeutige Kennung (UID) zu verwenden. Dadurch wird die ordnungsgemäße Funktion von Policy Manager beeinträchtigt.

Bitte führen Sie die folgenden Schritte aus, um sicherzustellen, dass jeder Computer eine personalisierte eindeutige Kennung (UID) verwendet, selbst wenn Disk-Image-Software eingesetzt wurde:

1. Installieren Sie das System und die gesamte Software, einschließlich Anti-virus, die Sie in die Image-Datei aufnehmen möchten.
2. Konfigurieren Sie Anti-virus zur Verwendung der richtigen Policy Manager Server.

   Hinweis: Importieren Sie den Host nicht in Policy Manager Console, wenn er eine Anfrage zur automatischen Registrierung an Policy Manager Server gesendet hat. Nur Hosts, auf denen die Image-Datei installiert wird, sollten importiert werden.

3. Führen Sie den Befehl `fsmautil resetuid` aus der Eingabeaufforderung aus.

   Dieses Dienstprogramm befindet sich in der Regel im Verzeichnis `C:\Program Files\F-Secure\Common` (das Verzeichnis kann abweichen, wenn Sie eine lokalisierte Version von Windows verwenden oder nicht den vorgegebenen Standard-Installationspfad übernommen haben).

4. Fahren Sie den Computer herunter.

   Hinweis: Führen Sie in diesem Stadium keinen Neustart durch.

5. Erstellen Sie die Disk-Image-Datei.
   Das Dienstprogramm setzt die eindeutige Kennung (UID) in der Anti-virus-Installation zurück. Beim Neustart des Systems wird automatisch eine neue eindeutige Kennung erstellt. Dies geschieht individuell auf jedem Computer, auf dem die Image-Datei installiert wird. Diese Computer senden automatische Registrierungsanforderungen an Policy Manager, und die Anforderung kann normal verarbeitet werden.

Kapitel

5

Aktualisieren der Virendefinitionsdatenbank

Themen:

- *Automatische Updates mit Automatic Update Agent*
- *Verwenden von Automatic Update Agent*
- *Erzwingen der sofortigen Suche nach neuen Updates durch Automatic Update Agent*
- *Manuelles Aktualisieren der Datenbanken*
- *Problembehandlung*

In diesem Abschnitt wird beschrieben, wie man die Virendefinitionsdatenbank auf dem aktuellen Stand hält.

Virendefinitionsdatenbanken müssen immer auf dem aktuellen Stand sein, um einen sachgemäßen Schutz gegen die neuesten Bedrohungen sicherzustellen.

Automatische Updates mit Automatic Update Agent

Mit Automatic Update Agent erhalten Sie automatische Updates und informative Inhalte, ohne dass Sie Ihre Arbeit unterbrechen müssen, um zu warten, bis die Dateien aus dem Internet heruntergeladen werden.

Automatic Update Agent lädt die Dateien automatisch im Hintergrund herunter. Dabei wird nur die Bandbreite genutzt, die nicht von anderen Internet-Anwendungen beansprucht wird. Ohne im Internet nach den entsprechenden Dateien suchen zu müssen, haben Benutzer so jederzeit die Gewissheit, dass auf ihren Rechnern die aktuellen Updates installiert sind.

Bei einer ständigen Verbindung von Automatic Update Agent mit dem Internet werden neue automatische Updates innerhalb von etwa zwei Stunden nach der Veröffentlichung durch F-Secure automatisch an diesen Client gesendet. Mögliche Verzögerungen hängen davon ab, wann eine Verbindung zum Internet möglich ist.

Automatic Update Agent wird zur Aktualisierung zentral verwalteter oder eigenständiger F-Secure Programme verwendet. Standardmäßig lädt der Agent auch die neuesten Nachrichten über Viren herunter. Das Herunterladen der Nachrichten kann wahlweise deaktiviert werden. Sie können Automatic Update Agent zusammen mit lizenzierten Anti-virus- und Sicherheitsprogrammen installieren und verwenden.

Funktionsbeschreibung von Automatic Update Agent

Automatic Update Agent fragt regelmäßig den Server ab, um festzustellen, ob neue Inhalte vorliegen, und lädt diese dann ggf. herunter.

Wenn der Dienst Automatic Update Agent gestartet wird, stellt er eine Verbindung zum F-Secure-Update-Server her. Der Agent fragt regelmäßig den Server ab, um festzustellen, ob neue Inhalte vorliegen. Neue Inhalte werden automatisch heruntergeladen. Das Abrufintervall wird auf dem Server festgelegt und kann nicht vom Client geändert werden.

In Policy Manager 6.0 und höheren Versionen versucht der mit Programmen von F-Secure installierte Automatic Update Agent für automatische Updates, die automatischen Updates in der folgenden Reihenfolge von den konfigurierten Update-Quellen herunterzuladen:

1. Falls im Unternehmensnetzwerk Policy Manager Proxy-Server verwendet werden, versucht der Client, nacheinander über die einzelnen Policy Manager Proxys eine Verbindung mit Policy Manager Server aufzubauen.
2. Falls der Client für HTTP-Proxy-Server konfiguriert ist, versucht er, die Updates über den HTTP-Proxy von Policy Manager Server herunterzuladen.
3. Danach versucht der Client, die Updates direkt von Policy Manager Server herunterzuladen.
4. Falls im Unternehmensnetzwerk Policy Manager Proxy-Server verwendet werden, versucht der Client, nacheinander über die einzelnen Policy Manager Proxys eine Verbindung mit dem Policy Manager Server-Update-Server aufzubauen.
5. Falls der Client für HTTP-Proxy-Server konfiguriert ist, versucht er, die Updates über den HTTP-Proxy vom Policy Manager Server-Update-Server herunterzuladen.
6. Danach versucht der Client, die Updates direkt vom Policy Manager Server-Update-Server herunterzuladen.

Die Vorteile der Verwendung von Automatic Update Agent

Automatic Update Agent lädt Updates automatisch herunter und nutzt die Bandbreite effektiv.

Optimierte Downloads von Virendefinitions-Updates

Automatic Update Agent erkennt, wenn die Virendefinitionsdatenbank geändert wurde. Durch den Einsatz eines ausgereiften Algorithmus auf Byte-Ebene werden nur die Änderungen heruntergeladen. Es ist somit nicht erforderlich, vollständige Dateien oder ganze Datenbanken herunterzuladen. Bei den Änderungen handelt es sich im Normalfall um Bruchteile des kompletten Updates. Nutzer einer langsamen DFÜ-Verbindung

erhalten auf diese Weise ihre täglichen Updates schnell und bequem, und Benutzer mit einer ständigen Verbindung profitieren ebenso von der geringen Ausnutzung der Bandbreite.

Datenübertragungen können nach einem Abbruch fortgesetzt werden

Automatic Update Agent lädt Inhalte über mehrere Sitzungen hinweg herunter. Wenn der Download unterbrochen wird, speichert Automatic Update Agent die bereits heruntergeladenen Daten und setzt den Download fort, wenn Sie sich das nächste Mal anmelden.

Automatische Updates

Sie müssen nicht nachprüfen, ob Updates vorliegen, und diese manuell herunterladen. Mit Automatic Update Agent erhalten Sie automatisch die Updates der Virendefinitionen, wenn diese von F-Secure veröffentlicht wurden.

Verwenden von Automatic Update Agent

Sie können Automatic Update Agent über eine Bearbeitung der Konfigurationsdatei `fsaua.cfg` konfigurieren.

Konfigurieren von Automatic Update Agent

Bei Policy Manager 7.0 und höheren Versionen wird Automatic Update Agent durch Bearbeiten der Konfigurationsdatei `fsaua.cfg` konfiguriert, wenn Policy Manager installiert ist.

> **Wichtig:** Diese Anweisungen sind nur bei einer Installation mit Policy Manager Server auf Automatic Update Agent anzuwenden. Sie sollten nur die unten angegebenen Einstellungen bearbeiten. Ändern Sie keine anderen Einstellungen in der Konfigurationsdatei.

Konfigurieren von Automatic Update Agent:

1. Öffnen Sie die Konfigrationsdatei `fsaua.cfg`, die sich im Verzeichnis `C:\Program Files\F-Secure\FSAUA\program\fsaua.cfg` befindet.
2. Geben Sie HTTP-Proxys an:

   Die Richtlinie `http_proxies` steuert, welche HTTP-Proxys von Automatic Update Agent verwendet werden. Verwenden Sie dabei das folgende Format:

   ```
   http_proxies=[http://][[Domäne\]Benutzer[:Kennwort]@]<Adresse>[:Port]
   [,[http://][[Domäne\]Benutzer[:Kennwort]@]<Adresse>[:Port]]
   ```

   Beispiele:

   ```
   http_proxies=http://proxy1:8080/,http://backup_proxy:8880/,
   http://Domäne\Benutzername:Benutzerkennwort@ntlmproxy.Domäne.com:80
   ```

3. Geben Sie das Abfrageintervall an:

   Die Richtlinie `poll_interval` steuert, mit welcher Häufigkeit Automatic Update Agent nach neuen Updates sucht. Der Standardwert liegt bei 1800 Sekunden, also einer halben Stunde.

   ```
   poll_interval=1800
   ```

   > **Hinweis:** Wenn das minimale auf dem F-Secure-Update-Server definierte Abfrageintervall beispielweise 2 Stunden beträgt, kann diese Beschränkung nicht durch die Einstellungen in der Konfigurationsdatei von Automatic Update Agent überschrieben werden.

4. Speichern und schließen Sie die Datei.
5. Sie müssen den **fsaua**-Dienst anhalten und neu starten, damit die Änderungen wirksam werden.

Geben Sie dazu die folgenden Befehle in der Befehlszeile ein:

```
net stop fsaua
net start fsaua
```

Vorgehensweise zum Lesen der Protokolldatei

Die Datei `fsaua.log` wird zum Speichern von Meldungen verwendet, die von Automatic Update Agent erzeugt wurden.

Einige dieser Meldungen bieten Informationen zu normalen Vorgängen wie Starten und Herunterfahren. In anderen Meldungen werden Fehler angegeben.

Die Datei `fsaua.log` befindet sich im Verzeichnis `C:\Program Files\F-Secure\FSAUA\program`.

Alle Nachrichten im Protokoll enthalten die folgenden Informationen:

- Das Datum und den Zeitpunkt, zu dem die Meldung generiert wurde.

  ```
  [ 3988]Thu Oct 26 12:40:39 2006(3): Downloaded'F-Secure Anti-Virus Update
  2006-10-26_04' - 'DFUpdates' version '1161851933' from fsbwserver.f-secure.com,
   12445450 bytes (download size 3853577)
  ```

- Eine kurze Beschreibung des Geschehnisses. Beim Herunterladen eines Updates werden der Name und die Version des Updates angezeigt.

  ```
  [ 3988]Thu Oct 26 12:40:39 2006(3): Downloaded 'F-Secure Anti-Virus Update
  2006-10-26_04' - 'DFUpdates' version '1161851933' from fsbwserver.f-secure.com,
   12445450 bytes (download size 3853577)
  ```

- Bei Updates werden in der Meldung außerdem die Quelle des Updates und die Größe des Downloads angezeigt.

  ```
  [ 3988]Thu Oct 26 12:40:39 2006(3): Downloaded 'F-Secure Anti-Virus Update
  2006-10-26_04' - 'DFUpdates' version '1161851933' from fsbwserver.f-secure.com,
   12445450 bytes (download size 3853577)
  ```

Meldungen in "fsaua.log"

Nachfolgend sind Beispiele für Meldungen aufgeführt, die Sie in der Protokolldatei finden können.

Nachricht	Bedeutung
`Update check completed successfully`	Die Verbindung zur Update-Quelle wurde erfolgreich hergestellt.
`Update-Prüfung erfolgreich abgeschlossen.`	Die Verbindung zur Update-Quelle wurde erfolgreich hergestellt, aber es waren keine neuen Dateien zum Herunterladen verfügbar.
`Downloaded 'F-Secure Anti-Virus Update 2006-10-26_04' - 'DFUpdates' version '1161851933' from fsbwserver.f-secure.com, 12445450 bytes (download size 3853577)`	Die Verbindung wurde erfolgreich hergestellt und es wurden einige Dateien heruntergeladen.
`Installation von 'F-Secure Anti-Virus-Update 2006-10-26_04' : erfolgreich`	Die Dateien wurden im Zielverzeichnis abgelegt (und die vorhandenen Dateien wurden gelöscht). Beachten Sie, dass über Automatic Update Agent keine Anzeige darüber erfolgt, ob die neuen Dateien vom/von (den) Host(s) verwendet werden oder nicht.

Nachricht	Bedeutung
`Update-Prüfung fehlgeschlagen. Während der Verbindung mit fsbwserver.f-secure.com (DNS-Lookup-Fehler) ist ein Fehler aufgetreten.`	Eine Fehlermeldung, in der angegeben wird, dass bei der Update-Überprüfung ein Fehler aufgetreten ist.

Vorgehensweise beim Überprüfen des Protokolls auf eine ordnungsgemäße Funktionsweise

Wenn alles ordnungsgemäß ausgeführt wird, sollte das letzte Installationsergebnis für jedes heruntergeladene Update wie folgt angezeigt werden:`Erfolg`. Beispiel:

```
Installation of 'F-Secure Anti-Virus Update 2006-10-26_04' : Success
```

Sie können auch eine Zusammenfassung zum Status der Virus-, Spyware- und DeepGuard-Updates anzeigen. Wechseln Sie dazu auf dem Server in Policy Manager Console zur Registerkarte **Zusammenfassung**.

Wechseln Sie zum Überprüfen des Update-Status auf einem zentral verwalteten Host in Policy Manager Console zur Seite **Status** > **Allgemeiner Schutz**.

Erzwingen der sofortigen Suche nach neuen Updates durch Automatic Update Agent

Wenn Sie die sofortige Suche nach neuen Updates durch Automatic Update Agent erzwingen müssen, können Sie dies in der Automatic Update Agent Oberfläche durchführen.

Gehen Sie wie folgt vor:

1. Wählen Sie **Start** > **Programme** > **F-Secure Policy Manager** > **F-Secure Automatic Update Agent**, um die Automatic Update Agent-Benutzeroberfläche aufzurufen.
2. Klicken Sie auf **Jetzt prüfen**, um zu ermitteln, ob aktuell Updates verfügbar sind.
   In der **Kommunikationszeile** wird der aktuelle Update-Status angezeigt.

Manuelles Aktualisieren der Datenbanken

Wenn für Ihren Computer keine Verbindung zum Internet besteht, können Sie die Datenbanken manuell aktualisieren.

1. Stellen Sie auf einem anderen Computer eine Verbindung zu http://support.f-secure.com/ her.
2. Laden Sie das Programm `fsdbupdate.exe` herunter.
3. Übertragen Sie das Programm `fsdbupdate.exe` beispielsweise mit einem Speicherstick oder anderen Wechseldatenträgern auf Ihren Computer, und führen Sie es aus.

Problembehandlung

Nachfolgend sind einige Beispiele zu Problemen aufgeführt, die in der Datei `fsaua.log` als Fehlermeldungen protokolliert sein können.

Problem	Grund	Lösung
Es ist ein Fehler beim DNS-Lookup oder Herstellen einer Verbindung aufgetreten, oder eine Verbindung wurde unterbrochen oder verweigert.	Netzwerkprobleme	Überprüfen Sie, ob das Netzwerk ordnungsgemäß konfiguriert ist.
Fehler bei der Proxy-Authentifizierung	Das für den HTTP-Proxy eingegebene Passwort ist falsch.	Überprüfen und korrigieren Sie das Passwort für den HTTP-Proxy in der Richtlinie `http_proxies` in der Datei `fsaua.cfg`.
Der Datenträger ist voll, oder es ist ein E/A-Fehler aufgetreten.	Auf dem Laufwerk mit dem Zielverzeichnis ist nicht genügend freier Speicherplatz vorhanden.	Geben Sie Speicherplatz frei, damit das Update gespeichert werden kann.
Es ist ein Server-Fehler oder ein nicht spezifizierter Fehler aufgetreten.	Unbekannt	-

Kapitel

6

Verwenden des Produkts unter Linux

Themen:

- *Übersicht*
- *Installation*
- *das Produkt deinstallieren.*
- *Häufig gestellte Fragen (FAQ)*

Policy Manager kann auch auf Linux installiert werden.

Policy Manager funktioniert unter Linux genauso wie unter Windows, allerdings stehen einige Funktionen nicht zur Verfügung und das Installationsverfahren unterscheidet sich.

Übersicht

Im Folgenden finden Sie einige allgemeine Informationen über die Verwendung und Installation des Produkts unter Linux.

Unterschiede zwischen Windows und Linux

Nicht verfügbare Dienste, wenn Policy Manager Console unter Linux ausgeführt wird:

- Push-Installationsfunktionen
- Windows Installer-Paket-(MSI-)Export
- Automatische Erkennung von Arbeitsstationen im Netzwerk

Unterstützte Verteilungen

Policy Manager unterstützt viele der Linux-Verteilungen, die auf dem Debian Package Management-(DEB)-System und dem Redhat Package Management-(RPM)-System basieren. Sowohl die 32-Bit- als auch die 64-Bit-Versionen der Distributionen werden unterstützt.

Unterstützte Verteilung	Packaging-System
Red Hat Enterprise Linux 4, 5 und 6	RPM
CentOS 5	RPM
SUSE Linux Enterprise Server 10 und 11	RPM
SUSE Linux Enterprise Desktop 11	RPM
openSUSE 11	RPM
Debian GNU Linux 5	DEB
Ubuntu 8.04, 10.04	DEB

Installation

Eine Policy Manager-Installation umfasst drei Komponenten.

Die Komponenten sind in der folgenden Reihenfolge zu installieren:

1. Automatic Update Agent
2. Policy Manager Server
3. Policy Manager Console

Policy Manager Server und Automatic Update Agent müssen auf demselben Computer installiert werden.

Policy Manager Console kann auf demselben oder einem anderen Computer installiert werden.

Hinweis: Wenn Sie eine frühere Version vonPolicy Manager aktualisieren, bei der Web Reporting installiert war, müssen Sie Web Reporting vor der Aktualisierung von Policy Manager Server zuerst deinstallieren.

Hinweis: Nähere Informationen über den Installationsvorgang und die Aktualisierung einer früheren Version von Policy Manager finden Sie in den Freigabehinweisen.

Hinweise zur Installation

Red Hat- und Suse-Verteilungen:

- Für einige Plattformen wird die Kompatibilitäts-Bibliothek `libstdc++` enötigt. Installieren Sie vor der Installation von Policy Manager Server die folgenden Pakete:
  - Installieren Sie für Red Hat Enterprise Linux 4, 5 und 6 das Paket `compat-libstdc++-33`.
  - Installieren Sie für 32-bit openSuse 11 das Paket `libstdc++33`.
  - Installieren Sie für 32-bit openSuse 11 die Pakete `libstdc++33` und `libstdc++33-32bit`.
- Für die Installation von Policy Manager Server und Policy Manager Console auf einer 64-Bit-Plattform müssen Sie die 64-Bit-Version der Installationspakete verwenden.

Debian- und Ubuntu-Verteilungen:

- Für Policy Manager Server wird die Kompatibilitäts-Bibliothek `libstdc++` benötigt. Installieren Sie das Paket `libstdc++5` vor der Installation von Policy Manager Server. Wenn die Installation nicht abgeschlossen wurde, weil die Kompatibilitäts-Bibliothek nicht gefunden wurde, installieren Sie die Bibliothek, und verwenden Sie dann den Befehl `apt-get install -f`, um die Installation des Produkts abzuschließen.
- Bei der Installation von Policy Manager Server und Policy Manager Console auf einer 64-Bit-Plattform müssen Sie die 64-Bit-Version der Installationspakete verwenden. Außerdem:
  - Installieren Sie das Paket `ia32-libs` mit Laufzeit-Bibliotheken für die ia32/i386-Architektur, bevor Sie Policy Manager Server installieren.
  - Installieren Sie das Paket Automatic Update Agent mit der Option `--force-architecture`.

Installieren von Automatic Update Agent und Policy Manager Server

Der erste Schritt besteht in der Installation von F-SecureAutomatic Update Agent und Policy Manager Server.

1. Melden Sie sich als `root` an.

   Wenn Sie das Produkt auf einer Ubuntu-Verteilung installieren, sollten Sie sich als normaler Benutzer anmelden, der zu `/etc/sudoers` hinzugefügt wurde.
2. Öffnen Sie ein Terminal.
3. Geben Sie zur Installation die folgenden Befehle ein:

Verteilungstyp	Befehl
Auf Debian basierende Verteilungen	`dpkg -i f-secure-automatic-update-agent_<Versionsnummer>.<Build-Nummer>_i386.`
	`dpkg -i f-secure-policy-manager-server_<Versionsnummer>.<Build-Nummer>_i386.d`
Auf RPM basierende Verteilungen	`rpm -i f-secure-automatic-update-agent-<Versionsnummer>.<Build-Nummer>-1.i386`
	`rpm -i f-secure-policy-manager-server-<Versionsnummer>.<Build-Nummer>-1.i386`
Ubuntu-Verteilungen	`sudo dpkg -i f-secure-automatic-update-agent_<Versionsnummer>.<Build-Nummer>_i386.`
	`sudo dpkg -i f-secure-policy-manager-server_<Versionsnummer>.<Build-Nummer>_i386.d`

4. Geben Sie zur Konfiguration `/opt/f-secure/fsaua/bin/fspms-config` ein, und beantworten Sie die Fragen.

Geben Sie für Ubuntu-Verteilungen `sudo /opt/f-secure/fsaua/bin/fspms-config` ein.

Drücken Sie die Eingabetaste, um die Standardeinstellung zu wählen (wird in eckigen Klammern angezeigt).

5. Melden Sie sich als normaler Benutzer an, und geben Sie die folgenden Befehle ein, um den Status der Komponenten zu überprüfen:

   - `/etc/init.d/fsaua status`
   - `/etc/init.d/fspms status`

   Alternativ können Sie Ihren Browser öffnen und die folgenden URLs aufrufen:

   - `http://localhost` - Status von Policy Manager Server
   - `http://localhost/B` - Status von Automatic Update Server
   - `http://localhost:8081` - Status von Web Reporting

Nachdem das Konfigurationsskript durchgelaufen ist, werden Automatic Update Agent und Policy Manager Server ausgeführt und starten automatisch immer dann, wenn der Computer neu gestartet wird.

Installieren von Policy Manager Console

Als Nächstes müssen Sie Policy Manager Console installieren.

1. Melden Sie sich als `root` an.

   Wenn Sie das Produkt auf einer Ubuntu-Verteilung installieren, sollten Sie sich als normaler Benutzer anmelden, der zu `/etc/sudoers` hinzugefügt wurde.

2. Öffnen Sie ein Terminal.
3. Geben Sie zur Installation Folgendes ein:

Verteilungstyp	Befehl
Auf Debian basierende Verteilungen	`dpkg -i f-secure-policy-manager-console_<Versionsnummer>.<Build-Nummer>_i386.`
Auf RPM basierende Verteilungen	`rpm -i f-secure-policy-manager-console-<Versionsnummer>.<Build-Nummer>-1.i386`
Ubuntu-Verteilungen	`sudo dpkg -i f-secure-policy-manager-console_<Versionsnummer>.<Build-Nummer>_i386.`

   Policy Manager Console wird installiert in `/opt/f-secure/fspmc/`. Eine neue Benutzergruppe namens `fspmc` wird automatisch erstellt.

4. Fügen Sie Benutzer zur Benutzergruppe `fspmc` hinzu.

   Bevor diese Benutzer Policy Manager Console ausführen können, muss Folgendes durchgeführt werden:

   a) Überprüfen Sie, zu welchen Gruppen der Benutzer gehört:

      ```
      groups <benutzer-id>
      ```

      Wenn der Benutzer zum Beispiel Tom heißt:

      ```
      groups Tom
      ```

   b) Fügen Sie diesen Benutzer zur Gruppe `fspmc` hinzu:

      ```
      /usr/sbin/usermod -G fspmc,<Gruppen, denen der Benutzer momentan angehört
      (als kommagetrennte Liste)> <benutzer-id>
      ```

      Wenn Tom beispielsweise den Gruppen `normal_users` und `administrators` angehört, lautet der Befehl:

      ```
      /usr/sbin/usermod -G fspmc,normal_users,administrators Tom
      ```

Hinweis: Die kommagetrennte Liste der Gruppen ersetzt die Gruppen, denen der Benutzer zuvor angehört hat.

5. Wählen Sie Policy Manager Console im F-Secure-Untermenü im Menü **Programme**.

   Sie können Policy Manager Console auch von der Befehlszeile starten, indem Sie `sg fspmc -c /opt/f-secure/fspmc/fspmc` eingeben.

   Hinweis: Unter Red Hat Enterprise Linux 4 müssen Sie sich vor Verwendung des Menüelements **Programme** abmelden und dann wieder anmelden. Der Befehl `sg` akzeptiert außerdem das Argument `<command>` nicht. Sie können aber `newgrp` auf der Befehlszeile verwenden:

   - `newgrp fspmc`
   - `/opt/f-secure/fspmc/fspmc`

Beim erstmaligen Start von Policy Manager Console werden Sie aufgefordert, einige Fragen zu beantworten, um die Konfiguration abzuschließen. Diese Fragen sind die gleichen wie bei der Windows-Version.

das Produkt deinstallieren.

Für die Deinstalltion von Policy Manager unter Linux müssen Sie die Komponenten in einer festen Reihenfolge deinstallieren.

Sie müssen die drei Komponenten in der folgenden Reihenfolge deinstallieren:

1. Policy Manager Server
2. Automatic Update Agent
3. Policy Manager Console

1. Melden Sie sich als `root` an.

   Wenn das Produkt auf einer Ubuntu-Verteilung installiert ist, sollten Sie sich als normaler Benutzer anmelden, der zu `/etc/sudoers` hinzugefügt wurde.
2. Öffnen Sie ein Terminal.
3. Geben Sie die folgenden Befehle in der angegebenen Reihenfolge ein:

Verteilungstyp	Befehl
Auf Debian basierende Verteilungen	**1.** `dpkg -r f-secure-policy-manager-server` **2.** `dpkg -r f-secure-automatic-update-agent` **3.** `dpkg -r f-secure-policy-manager-console`
Auf RPM basierende Verteilungen	**1.** `rpm -e f-secure-policy-manager-server` **2.** `rpm -e f-secure-automatic-update-agent` **3.** `rpm -e f-secure-policy-manager-console`
Ubuntu-Verteilungen	**1.** `sudo dpkg -r f-secure-policy-manager-server` **2.** `sudo dpkg -r f-secure-automatic-update-agent` **3.** `sudo dpkg -r f-secure-policy-manager-console`

Hinweis: Um versehentliches Löschen unwiederbringlicher Daten zu vermeiden, die von Policy Manager-Komponenten erstellt wurden, z. B. MIB-Dateien, Domänenstruktur, Richtlinien, Konfigurationsdateien und Einstellungen , werden bei der Deinstallation die unten aufgeführten

Verzeichnisse nicht entfernt. Löschen Sie keine Schlüssel, die möglicherweise in Zukunft benötigt werden. Wenn Sie das Produkt komplett entfernen möchten, melden Sie sich als `root` an, und geben Sie die folgenden Befehle ein:

```
rm -rf /var/opt/f-secure/fspms
rm -rf /var/opt/f-secure/fsaus
rm -rf /etc/opt/f-secure/fspms
rm -rf /etc/opt/f-secure/fsaus
rm -rf /opt/f-secure/fspmc
```

Häufig gestellte Fragen (FAQ)

Hier finden Sie Antworten auf häufig gestellte Fragen.

Frage	Antwort
Wo befinden sich bei der Linux-Version die Protokoll- und Konfigurationsdateien?	Sie können alle Dateien und deren Pfade auflisten, indem Sie die folgenden Befehle als normaler Benutzer eingeben: • RPM-basierte Verteilungen: `rpm -ql f-secure-<component_name>`. • Debian-basierte Verteilungen: `dpkg -L f-secure-<component_name>`. Sie finden die Protokolldateien in den folgenden Verzeichnissen: • Policy Manager Console: `/opt/f-secure/fspmc/lib/Administrator.error.log`. • Der Automatic Update Agent protokolliert Laufzeitfehler, Warnungen und sonstige Informationen in der Datei `syslog`, die sich typischerweise unter `/var/log/messages` befindet. • Policy Manager Server: `/var/opt/f-secure/fspms/logs` und `/var/opt/f-secure/fsaus/log`. Sie finden die Konfigurationsdateien in den folgenden Verzeichnissen: • Policy Manager Console: `/opt/f-secure/fspmc/lib/Administrator.properties` • Automatic Update Agent: `/etc/opt/f-secure/fsaua/fsaua_config` • Policy Manager Server: `/etc/opt/f-secure/fspms/fspms.conf`
Warum sind die Dateien so ungewöhnlich verteilt?	Alle Dateien für den Policy Manager haben Ihren eigenen Speicherort entsprechend dem File Hierarchy Standard (Dateihierarchiestandard, FHS). Weitere

Frage	Antwort
	Informationen über den FHS finden Sie unter *http://www.pathname.com/fhs/*.
Warum wird der Policy Manager Server nicht gestartet?	Überprüfen Sie, ob Sie das Konfigurationsskript ausgeführt haben: `/opt/f-secure/fspms/bin/fspms-config`. Sie können auch überprüfen, ob die Ports, die für den Policy Manager Server konfiguriert sind, aktiv sind, indem Sie sich als `root` anmelden und den Befehl `netstat -lnpt` ausführen.
Wie kann ich Komponenten von Policy Manager starten, stoppen und neu starten bzw. deren Status überprüfen?	Automatic Update Agent: `/etc/init.d/fsaua {start|stop|restart|status}` Policy Manager Server: `/etc/init.d/fspms {start|stop|restart|status}`
Wie kann ich einen HTTP Proxy angeben?	Sie können das Konfigurationsskript `/opt/f-secure/fsaua/bin/fsaua-config` ausführen oder die Konfigurationsdatei manuell bearbeiten. Die Vorgabe ist `http_proxies=http://address:port/`. Vergessen Sie nicht, Automatic Update Agent neu zu starten, damit die neuen Einstellungen wirksam werden.
Wie kann ich die Standard-Ports (80 und 8080) ändern, die Policy Manager Server auf Anforderungen abhört?	Diese Ports werden mit dem Konfigurationsskript konfiguriert: `/opt/f-secure/fspms/bin/fspms-config`.
Wie kann ich den Standard-Port (8081) ändern, den Web Reporting auf Anforderungen abhört?	Der Port für Web Reporting wird mit dem Policy Manager Server-Konfigurationsskript konfiguriert: `/opt/f-secure/fspms/bin/fspms-config`.
Kann ich einen eigenen Zeitplan für die Aktualisierung von F-Secure-Virendefinitionen einrichten?	Ja. Automatische Aktualisierungen werden mithilfe des eigenen Planungsdämons des Betriebssystems durchgeführt (`cron`). Bearbeiten oder fügen Sie Ihren eigenen Zeitplan in der Datei `/etc/crontab` hinzu. Um beispielsweise alle 10 Minuten eine Aktualisierung der Virendefinitionen durchzuführen, fügen Sie der Datei `/etc/crontab` folgende Zeile hinzu: `*/10 * * * * fspms /opt/f-secure/fspms/bin/fsavupd` Weitere Informationen über die Konfiguration automatischer Aktualisierungen mit `cron` finden Sie in `man cron` und `man 5 crontab`. In den meisten Fällen können Sie die planmäßige Aktualisierung der F-Secure-Virendefinitionen mit dem Befehl `/opt/f-secure/fspms/bin/fspms-config` ändern.

Frage	Antwort
Wie kann ich die F-Secure-Virendefinitionen manuell aktualisieren?	Melden Sie sich als Benutzer `fspms` an, und führen Sie das Aktualisierungstool aus, indem Sie Folgendes eingeben: `sudo -u fspms /opt/f-secure/fspms/bin/fsavupd --debug` Mit dem optionalen Flag `--debug` erhalten Sie ausführlichere Diagnosemeldungen.

Wie kann ich F-Secure-Virendefinitionen manuell aus dem letzten `fsdbupdate`-Paket veröffentlichen?	Laden Sie das neueste Tool `fsdbupdate.run` unter *http://download.f-secure.com/latest/fsdbupdate.run* herunter. Melden Sie sich als `root` an, und führen Sie dieses Tool aus:
	`./fsdbupdate.run`
	Damit werden alle Datenbanken im Automatic Update Agent aktualisiert. Anschließend müssen Sie diese Updates im Update-Server und im Policy Manager Server veröffentlichen, entweder über die Einplanung von `fsavupd` in `crontab` oder durch manuelle Ausführung des Befehls `fsavupd`:
	`sudo -u fspms /opt/f-secure/fspms/bin/fsavupd`

Gibt es ein Diagnosetool, das ich verwenden kann?	Ja. Verwenden Sie `fsdiag`, um Informationen zu Ihrem System und den zugehörigen Paketen zu erfassen. Wenn Sie als 'root' angemeldet sind, führen Sie Folgendes aus: `/opt/f-secure/fspms/bin/fsdiag` Sämtliche relevanten Informationen werden im Archiv `fsdiag.tar.gz` gespeichert, das sich im aktuellen Verzeichnis befindet. Diese Datei können Sie auf Anforderung an den F-Secure-Kundensupport senden.
Ich erhalte die Warnung:`...Es wurde ein weiterer Server mit automatischer Aktualisierung gefunden...` während des Starts. Was soll ich tun?	**1.** Überprüfen Sie, ob ein weiterer Automatic Update Server noch immer ausgeführt wird und die TCP-Sockets verwendet: `netstat -anp | grep bwserver` `ps axuww | grep bwserver` **2.** Stoppen Sie den anderen Automatic Update Server, indem Sie Folgendes ausführen: `kill `pidof bwserver`` `kill -9 `pidof bwserver`` **3.** Starten Sie Policy Manager Server neu: `/etc/init.d/fspms stop` `rm -f /var/lock/subsys/fsaus /var/run/fsaus.pid`

Frage	Antwort
	`/etc/init.d/fspms start`
Wie kann ich in Policy Manager Console Software auf Remote-Hosts unter Linux installieren?	Sie können Installationspakete in JAR-Dateien exportieren und das Tool `ilaunchr.exe` zur Installation von Software auf Hosts verwenden, indem Sie beispielsweise Anmeldeskripts nutzen. Folgen Sie den Beschreibungen im Handbuch. Sie finden das Tool `ilaunchr.exe` im Verzeichnis `/opt/f-secure/fspmc/bin`.
Wie kann ich Policy Manager für die Verwendung in großen Umgebungen konfigurieren?	• Erhöhen Sie die Werte für `Abfrageintervall für eingehende Pakete` und `Aktualisierungsintervall für ausgehende Pakete` in Policy Manager Console auf 30-60 Minuten. • Nutzen Sie eine oder mehrere Policy Manager Proxy-Installationen, um die Belastung von Policy Manager Server durch die Lieferung von Datenbankaktualisierungen an Clients zu minimieren.

Kapitel

7

Web Reporting

Themen:

- *Erstellen und Anzeigen von Berichten*
- *Verwalten von Web Reporting*
- *Web ReportingFehlermeldungen von und Fehlerbehebung*

Web Reporting ist ein grafisches Berichtssystem, das in Policy Manager Server enthalten ist.

Anhand der detaillierten grafischen Berichte in Web Reporting können Sie Computer identifizieren, die ungeschützt oder anfällig für Vireninfektionen sind. Mit Web Reporting können Sie mithilfe einer internetbasierten Oberfläche schnell grafische Berichte auf der Grundlage historischer Trenddaten erstellen. Sie können anhand von Client Security-Alarmen und Statusinformationen, die von Management Agent an Policy Manager Server gesendet wurden, eine Vielzahl von nützlichen Berichten und Abfragen erstellen. Die Berichte können in das HTML-Format exportiert werden.

Für die Anzeige der Berichte, die von Web Reporting erstellt wurden, muss auf dem Computer ein Internet-Browser installiert sein, zum Beispiel Internet Explorer oder Mozilla Firefox.

Erstellen und Anzeigen von Berichten

Zu den allgemeinen Berichtstypen, die erstellt werden können, gehören Balken- und Tortendiagramme für die gegenwärtige Sicherheitssituation, Trendberichte und detaillierte Listenberichte.

Um anzuzeigen, welche Berichte und Berichtsvorlagen verfügbar sind, wählen Sie eine der folgenden Seiten (**Virenschutz-Zusammenfassung**, **Zusammenfassung für Internet Shield**, **Alarme**, **Installierte Software** und **Host-Eigenschaften**) auf der Web Reporting-Benutzeroberfläche.

Erstellen eines Berichts

Mit Web Reporting können Sie ohne großen Aufwand mithilfe einer internetbasierten Oberfläche grafische Berichte anhand historischer Trenddaten erstellen.

Sie können einen Web-Bericht wie folgt generieren:

1. Öffnen Sie die Hauptseite von Web Reporting.
2. Geben Sie den Namen oder die IP-Adresse von Policy Manager Server gefolgt von der Port-Adresse für Web Reporting (getrennt durch einen Doppelpunkt) in die Adresszeile des Browsers ein.
   Zum Beispiel `fspms.example.com:8081`.

   Wenn Sie auf Web Reporting lokal zugreifen, können Sie Web Reporting wahlweise auch über das Menü **Start** aufrufen: **Start** > **F-Secure Policy Manager Server** > **Web Reporting**.
3. Warten Sie, bis die Web Reporting-Seite geladen ist.

   In großen Umgebungen dauert dies unter Umständen sehr lange.

   Wenn die Seite Web Reporting geöffnet wird, wird ein Standardbericht für die derzeit ausgewählte Berichtskategorie angezeigt. Standardmäßig ist **Stamm** in der Baumstrukture **Richtliniendomänen** ausgewählt.
4. Zum Anzeigen eines neuen Berichts wählen Sie zunächst die Domäne, Subdomäne oder den Host aus, für die bzw. den der Bericht erstellt werden soll.
5. Wählen Sie eine Berichtskategorie (**Virenschutz-Zusammenfassung**, **Zusammenfassung für Internet Shield**, **Alarme**, **Installierte Software** und **Host-Eigenschaften**) sowie den genauen zu erstellenden Berichtstyp aus.
6. Warten Sie, bis der Bericht im unteren Teil des Hauptfensters angezeigt wird.

Erstellen eines druckbaren Berichts

Sie können Berichte auch ausdrucken.

So erhalten Sie eine Druckversion der Seite:

1. Klicken Sie in der oberen rechten Ecke der Seite auf den Link **Druckversion**.
   Die Seite wird in einem neuen Browser-Fenster mit dem Inhalt des Haupt-Frames in einem druckbaren Format angezeigt.
2. Drucken Sie die Seite anschließend über die normale Druckfunktion des Browsers aus.

Sie können den Bericht auch für eine spätere Nutzung speichern. Wählen Sie dazu die herkömmliche Browser-Option **Speichern unter** oder **Seite speichern unter**. Achten Sie bei der Auswahl der Speicheroption darauf, dass die komplette Seite, einschließlich der Bilder, gespeichert wird:

- Wählen Sie bei Verwendung des Microsoft Internet Explorers die Einträge **Datei** > **Speichern** aus dem Menü. Wenn das Dialogfeld **Webseite speichern** angezeigt wird, wählen Sie **Webseite, vollständig** aus dem Dropdown-Menü **Dateityp**.
- Wenn Sie Mozilla verwenden, wählen Sie **Datei** > **Seite speichern unter** aus dem Menü.

Automatische Berichterstellung

Sie können auch die URL eines druckbaren Berichts speichern, um automatische Berichte zu erstellen.

Bei der Nutzung der automatischen Berichterstellung müssen Sie die Berichtskategorie, den Berichtstyp oder die gewünschte Richtliniendomäne nicht auswählen, wenn Sie denselben Bericht erneut erstellen möchten, da diese Informationen bereits in der berichtsspezifischen URL gespeichert sind.

Sie haben zwei Möglichkeiten:

- Generieren Sie einen druckbaren Bericht mit allen gewünschten Einstellungen, die Sie überwachen möchten, und speichern Sie anschließend einen Link zu diesem Bericht auf Ihrem Computer (auf dem Desktop, als Lesezeichen oder an einer anderen Position). Wenn Sie das nächste Mal über diesen Link auf Web Reporting zugreifen, wird der Bericht mit den aktuellen Daten neu erstellt.
- Sie können außerdem den generierten Bericht speichern, damit Sie die gegenwärtige Situation mit den zukünftigen Berichten vergleichen können. Erstellen Sie zunächst eine Druckversion der Seite, und speichern Sie anschließend die gesamte Seite im Browser. Auf dieser Seite wird immer der "alte" Bericht angezeigt.

Verwalten von Web Reporting

Dieser Abschnitt behandelt die häufigsten Wartungsaufgaben von Web Reporting.

Hinweis: Web Reporting wird während der Installation von Policy Manager Server aktiviert und deaktiviert. Darüber hinaus wird während der Installation auch die Zugriffsbeschränkung auf den lokalen Computer eingerichtet. Sie können Web Reporting über die Registry oder durch erneute Installation von Policy Manager Server aktivieren oder deaktivieren.

Alle Web Reporting-Daten werden in der H2-Datenbank gespeichert, die von Policy Manager Server genutzt wird. Immer wenn Sie diese Datenbank sichern, werden daher auch die Web Reporting-Daten gesichert.

Web ReportingFehlermeldungen von und Fehlerbehebung

Dieser Abschnitt behandelt Fehlermeldungen von Web Reporting und die Fehlerbehebung für die Web Reporting-Datenbank.

Fehlermeldungen

Im Folgenden werden häufige Fehlermeldungen aufgelistet, die bei der Verwendung von Web Reporting aufteten können.

- Browser-Fehlermeldung: **Beim Versuch, auf <URL> zuzugreifen, wurde die Verbindung verweigert.**

  Der Browser konnte keine Verbindung zu Policy Manager Server aufbauen. Der verwendete Link verweist auf einen falschen Computer oder falschen Port, oder Policy Manager Server ist nicht auf diesem Computer installiert, oder der Policy Manager Server-Dienst ist nicht aktiv. Überprüfen Sie diese Punkte in der angegebenen Reihenfolge. Eventuell wird die Verbindung auch durch die Firewall blockiert.
- Fehlermeldung: **Die Datenbankverbindung von Web Reporting wurde unterbrochen. Eventuell ist ein Neustart des Dienstes Policy Manager Server erforderlich.**

  Wenn Web Reporting nicht auf die Datenbank zugreifen kann, sollten Sie den Dienst Policy Manager Server neu starten. Wenn sich das Problem dadurch nicht beheben lässt, sollten Sie Policy Manager Serverneu installieren und dabei die vorhandene Datenbank beibehalten.

Problembehandlung

Im Allgemeinen sollten Sie die nachstehend aufgeführten Schritte durchführen, wenn Web Reporting nicht funktioniert.

Führen Sie die Schritte in der folgenden Reihenfolge durch:

1. Laden Sie die Seite neu.
2. Wenn das Problem dadurch verursacht wird, dass noch nicht alle Prozesse gestartet wurden, warten Sie einen Moment ab, und versuchen Sie anschließend, die Seite neu zu laden.

   Darüber hinaus können Sie die Startdauer durch Löschen der unnötigen Alarme verringern.
3. Starten Sie den Web Reporting-Dienst neu.
4. Starten Sie Policy Manager Server neu.
5. Starten Sie den Computer neu.
6. Installieren Sie Policy Manager Server unter Beibehaltung der vorhandenen Konfiguration neu.
7. Wenn alle anderen Versuche fehlschlagen, setzen Sie die Web Reporting-Datenbank zurück, oder stellen Sie sie über eine Sicherungskopie wieder her.

Ändern des Ports für Web Reporting

Es wird empfohlen, den Port für Web Reportingdurch erneutes Ausführen des Installationsprogramms von Policy Manager zu ändern.

Sie können den Port für Web Reporting auch über die Bearbeitung des Registrierungsschlüssels `HKEY_LOCAL_MACHINE\SOFTWARE\Data Fellows\F-Secure\Management Server 5` ändern:

1. Beenden Sie Policy Manager Server.
2. Öffnen Sie den Registrierungsschlüssel `HKEY_LOCAL_MACHINE\SOFTWARE\Data Fellows\F-Secure\Management Server 5`.
3. Bearbeiten Sie den Wert `WRPortNum`, und geben Sie die neue Port-Nummer ein.

   Achten Sie bei der Eingabe der neuen Port-Nummer darauf, dass **Dezimal** als Option unter **Basis** gewählt ist.
4. Starten Sie Policy Manager Server.

   Bei einem Port-Konflikt kann Policy Manager Server nicht gestartet werden. Stattdessen wird eine Fehlermeldung in die Protokolldatei geschrieben. Geben Sie in diesem Fall einen anderen Port ein, der von keinem anderen Dienst verwendet wird.

Kapitel

8

Policy Manager Proxy

Themen:

- *Übersicht*

In diesem Abschnitt wird eine kurze Einführung in Policy Manager Proxy gegeben.

In diesem Abschnitt finden Sie einige grundlegende Informationen zu Policy Manager Proxy.

Übersicht

Der Policy Manager Proxy bietet eine Lösung für Bandbreitenprobleme in verteilten Installationen von Client Security, indem die Netzwerkbelastung bei langsamen Verbindungen deutlich reduziert wird.

Der Policy Manager Proxy legt die vom Policy Manager Server oder F-Secure-Update-Server empfangenen Updates der Virendefinitionsdatenbanken in einem Zwischenspeicher ab. Er befindet sich dabei auf demselben Remote-Netzwerk wie die Hosts, die die Datenbank als Verteilungspunkt nutzen. In jedem Netzwerk mit langsamen Netzwerkleitungen sollte sich ein Policy Manager Proxy befinden. Der Policy Manager Proxy ruft die Updates der Virendefinitionsdatenbanken direkt vom F-Secure-Verteilungsserver herunter. Die Hosts, auf denen Anti-virus ausgeführt wird, rufen die Updates lokal vom Policy Manager Proxy ab. Arbeitsstationen in den dezentralen Niederlassungen tauschen ebenfalls Daten mit dem Policy Manager Server in der Zentrale aus, diese Kommunikation ist jedoch auf die Remote-Verwaltung von Richtlinien, die Statusüberwachung und Alarmierung beschränkt.

Kapitel

9

Problembehandlung

Themen:

- *Policy Manager Server und Policy Manager Console*
- *Policy ManagerWeb Reporting*
- *Richtlinienverteilung*

Dieses Kapitel enthält Informationen zur Fehlerbehebung sowie häufig gestellte Fragen zu Policy Manager.

Wenn bei der Verwendung des Programms Probleme auftreten, können Sie in diesem Abschnitt nach Lösungen suchen.

Policy Manager Server und Policy Manager Console

Im Folgenden werden Fragestellungen zu Policy Manager Server und Policy Manager Console beschrieben.

Frage	Antwort
Warum startet Policy Manager Server nicht?	Laufzeitfehler, Warnungen und andere Informationen finden Sie in den Dateien: `<F-Secure>\Management Server 5\logs\fspms-webapp-errors.log` und `<F-Secure>\Management Server 5\logs\fspms-sersvice.log` Stellen Sie sicher, dass die Zugriffsrechte (`properties/security/permissions`) das Benutzerkonto "Local Service" umfassen. Wenn Local Service nicht als autorisierter Benutzer aufgeführt wird, fügen Sie diesen manuell hinzu und richten Sie die Zugriffsrechte auf **Vollständige Kontrolle** ein. Übernehmen Sie die Zugriffsrechte für das `Management Server 5`-Verzeichnis (standardmäßig `C:\Programme\F-Secure\Management Server 5`) und alle Unterverzeichnisse. Starten Sie nach Vornahme dieser Änderungen den Policy Manager Server-Dienst oder den Computer neu. Das Konto "Lokaler Dienst" ist das Windows-Systemkonto und der Policy Manager Server-Dienst wird unter diesem Benutzerkonto gestartet. Bei einer normalen Installation werden die Verzeichniszugriffsrechte für das Verzeichnis `Management Server 5` automatisch korrekt eingestellt. Wenn das Verzeichnis manuell kopiert oder beispielsweise aus einer Sicherungskopie wiederhergestellt wird, können die Zugriffsrechte gelöscht werden. In diesem Fall müssen Sie die im vorherigen Absatz beschriebenen Schritte ausführen.

Wo befinden sich die Protokolldateien und die Konfigurationsdateien für Policy Manager Server?	Die Protokolldateien befinden sich in:
	`<F-Secure>\Management Server 5\logs`
	Die Konfigurationsdateien befinden sich in:
	`<F-Secure>\Management Server 5\conf`

Wo befinden sich die Policy Manager Console Protokolldateien?	Die Protokolldatei ist:
	`<F-Secure>\Administrator\lib\administrator.error.log`
	Richtlinienänderungen, die mit dem Vorgang **Richtlinie verteilen** angewandt werden, werden protokolliert in:
	`fspms-policy-audit.log`

Frage	Antwort
Der Migrationsassistent wurde während der Installation nicht geöffnet. Kann ich ihn unabhängig von der Installation separat aufrufen?	Sie können den Migrationsassistenten öffnen, indem Sie diese ausführbare Datei ausführen: `<F-Secure>\Management Server 5\bin\fspms-migration-wizard.exe`
Ich habe mein admin-Kennwort verloren. Kann ich das Kennwort abfragen oder zurücksetzen?	Wenn Sie das Kennwort für den Benutzer `admin` verloren haben oder wenn das Konto versehentlich gelöscht wurde, können Sie das Benutzerkonto über das folgende Tool zurücksetzen: `<F-Secure>\bin\reset-admin-account.bat` **Hinweis:** Sie müssen Policy Manager Server manuell beenden, bevor Sie das Tool zum Zurücksetzen ausführen.
Wie kann eine Änderung der Serverrolle bewirken, dass Policy Manager Server nicht mehr funktioniert?	Domänencontroller-Server und Mitglieds-/Einzelplatz-Server verwenden verschiedene Kontotypen: Domänenkonten auf Domänencontrollern und lokale Konten auf Mitgliedsservern. Da Policy Manager Server zur Ausführung ein eigenes Konto verwendet, wird dieses Konto durch eine Rollenänderung ungültig. Die einfachste Methode zur Wiederherstellung von Policy Manager Server nach einer Serverrollenänderung ist eine Neuinstallation von Policy Manager Server mit aktivierter Option **Vorhandene Einstellungen beibehalten**. Dadurch wird das Policy Manager Server-Konto neu erstellt, und alle Dateizugriffsrechte werden auf die richtige Einstellung zurückgesetzt.

Wie kann eine Erhöhung der Windows-Sicherheit bewirken, dass Policy Manager Server nicht mehr funktioniert?	Zugriffsrechtsbeschränkungen, besonders Beschränkungen im `%SystemRoot%`-Verzeichnis (`C:\\Windows` oder `C:\\winnt`), können verhindern, dass Policy Manager Server ausgeführt wird, da dessen eigenes Konto (Lokaler Dienst) in der Lage sein muss, die netzwerkbezogenen DLL- und SYS-Dateien zu lesen.
	Sie müssen daher dem Konto "Lokaler Dienst" das 'Lesen' der folgenden Verzeichnisse gestatten:
	`%SystemRoot%`
	`%SystemRoot%\system32`
	`%SystemRoot%\system32\drivers`
	Bestimmte Dienstbeschränkungen können auch verhindern, dass der Policy Manager Server-Dienst gestartet wird. Weitere Informationen hierzu finden Sie in der Dokumentation zu Microsoft Windows Server.

Frage	Antwort
Warum verliert Policy Manager Console die Verbindung mit Policy Manager Server?	Wenn Policy Manager Console auf einem anderen Computer ausgeführt wird als Policy Manager Server, kann die Verbindung durch Netzwerkprobleme beeinträchtigt werden. Es gibt zahlreiche Berichte, denen zufolge beispielsweise eine Netzwerk-Switch-Änderung Verbindungsprobleme zwischen Policy Manager Console und dem Policy Manager Server verursacht hat. In der Regel werden diese Probleme durch Aktualisierung der Netzwerktreiber auf die neueste Version oder durch Neukonfiguration des neuen Switch und der Netzwerkkarten auf den Computern mit Policy Manager Console und dem Policy Manager Server behoben. Wenn Policy Manager Console auf demselben Computer installiert ist wie Policy Manager Server, besteht die Gefahr, dass Policy Manager Server vom Netzwerk so ausgelastet ist, dass keine freien Netzwerkverbindungen verfügbar sind. Policy Manager Console und alle Hosts konkurrieren um dieselben Netzwerkressourcen. Mögliche Lösungen bestehen darin, die Abfrage-Intervalle der Hosts zu erhöhen, die Zeiten für die Windows-Netzwerkzeitüberschreitungen zu verkürzen oder die Anzahl der Windows-Netzwerkports zu erhöhen. Hilfreiche Windows-Netzwerkeinstellungen sind: `HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\MaxUserPort` (maximale Anzahl an Netzwerkports, Standardwert = 5000) `HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\TcpTimedWaitDelay` (Zeit, die gewartet wird, bis eine inaktive Netzwerkverbindung geschlossen wird, Standardwert = 240 Sekunden). Mithilfe des Befehls `netstat -an` können Sie überprüfen, ob zu viele Verbindungen zum Server geöffnet sind.
Wie kann ich die Ports ändern, die der Server auf Anforderungen abhört?	Standardmäßig empfängt das Verwaltungs-Modul von Policy Manager Server (die Komponente, die Anfragen von Policy Manager Console verarbeitet) Daten über Port 8080, und das Host-Modul von Policy Manager Server (die Komponente, die Anfragen von den Arbeitsstationen verarbeitet) verwendet dazu Port 8. Diese Einstellungen können während der Installation geändert werden. Für den Fall, dass Sie die Portnummern nach der Installation ändern müssen.

Frage	Antwort
	1. Beenden Sie Policy Manager Server. **2.** Öffnen Sie den Registrierungsschlüssel `HKEY_LOCAL_MACHINE\SOFTWARE\Data Fellows\F-Secure\Management Server 5`. **3.** Geben Sie als Werte für `AdminPortNum` (Admin-Modul) und `HttpPortNum` (Host-Modul) die neuen Port-Nummern ein. Achten Sie bei der Eingabe der neuen Port-Nummer darauf, dass **Dezimal** als Option unter **Basis** gewählt ist. **4.** Starten Sie Policy Manager Server. **Vorsicht:** Wenn Sie die Arbeitsstationen bereits für den Zugriff auf Policy Manager Server (über das Host-Modul von Policy Manager Server konfiguriert haben, sollten Sie die Einstellung für den Host-Port (d. h., den Port für die Kommunikation mit den Agenten) von Policy Manager Server nicht ändern, da sich daraus eine Situation ergeben kann, in der kein Verbindungsaufbau zwischen den Arbeitsstationen und dem Server mehr möglich ist.

Policy ManagerWeb Reporting

Im Folgenden werden die Speicherorte der Protokoll- und Konfigurationsdateien angegeben.

Frage	Antwort

Wo befinden sich die Protokoll- und Konfigurationsdateien für Web Reporting?	Die Protokolldateien befinden sich in:
	`<F-Secure>\Management Server 5\Web Reporting\logs`
	Die Konfigurationsdateien befinden sich in:
	Der Registrierungsschlüssel `HKEY_LOCAL_MACHINE\SOFTWARE\Data Fellows\F-Secure\Management Server 5`
	Außerdem beinhaltet Policy Manager Server die folgenden Konfigurationsdateien:
	`<F-Secure>\Management Server 5\conf`

Richtlinienverteilung

Hier finden Sie Informationen über häufige Fehlermeldungen in Bezug auf die Richtlinienverteilung.

Frage	Antwort
Beim Verteilen einer Richtlinie zeigt Policy Manager Console eine Fehlermeldung zu einem ungültigen Richtlinienwert an. Was ist zu tun?	Nachfolgend finden Sie Informationen zu Fehlermeldungen, die möglicherweise während einer Richtlinienverteilung angezeigt werden, sowie Gründe und Lösungen für die jeweiligen Probleme.

Fehlermeldung	Grund	Lösung

`"<Einstellungsname>" hat einen Wert, der sich außerhalb des eingeschränkten Wertebereichs befindet`
`"<Einstellungsname>" hat eine ungültige Einschränkung`
`"<Einstellungsname>" hat einen ungültigen Wert: "<Wert>"`
	Grund 1:
	Der in einer Auswahlliste ausgewählte Wert befindet sich nicht in der Auswahl für eine Subdomäne oder einen Host, es wurden zu hohe oder zu niedrige Werte als Grenzen für die Bereichseinschränkung angegeben, oder es wurde eine leere Auswahlliste angegeben.
	Wenn eine Domäne Hosts enthält, auf denen unterschiedliche Programmversionen installiert sind, werden zum Bearbeiten der Richtlinienwerte die MIB-Einstellungen der neuesten Programmversion verwendet. Folglich treten bei der Richtlinienverteilung auf Hosts, auf denen ältere Versionen der Software installiert sind, möglicherweise Fehler auf, da die neuen Richtlinieneinstellungen oder -werte von den älteren Versionen nicht unterstützt werden.
	
	Grund 2:
	Sie haben einen Ganzzahlwert eingegeben, der außerhalb der Bereichseinschränkung liegt.
		Unterteilen Sie die Hosts in Subdomänen, damit Sie die neuen Werte für Hosts, auf denen die neue Software installiert ist, festlegen und ältere Richtlinienwerte für andere Hosts verwenden können. Gehen Sie wie folgt vor:
		1. Gruppieren Sie die Hosts basierend auf den installierten Programmversionen in Subdomänen. Gruppieren Sie beispielsweise Hosts, auf denen Client Security 6.x installiert ist, in einer Subdomäne und Hosts, auf denen Client Security 7.x installiert ist, in einer anderen Subdomäne.
		2. Legen Sie die meisten Einstellungen in der Stammdomäne fest, und erstellen Sie Subdomänen für Ausnahmen. Diese Lösung eignet sich, wenn Sie nur über ein paar Hosts verfügen, auf denen ältere Versionen der Software installiert sind.

`"<Einstellungsname>" ist erforderlich, aber nicht definiert`	Diese Einstellung ist erforderlich, aber derzeit ist kein Wert angegeben.	Geben Sie einen Wert ein, oder wenden Sie den Vorgang **Löschen** an, um den Wert aus der übergeordneten Domäne oder MIB neu zu erben. Wenn der Wert auf mehreren Ebenen der Domäne nicht angegeben ist, müssen Sie den Vorgang **Löschen** möglicherweise mehrfach anwenden.

Kapitel
10

ILAUNCHR-Fehlercodes

Themen:

- *Fehlercodes*

Falls in der **ILAUNCHR**-Komponente Fehler auftreten, können Sie mithilfe der in diesem Abschnitt aufgeführten Fehlercodes die Ursache des Fehlers ermitteln.

Dieser Abschnitt enthält Informationen zu den Fehlercodes, die sich auf die **ILAUNCHR**-Komponente beziehen.

Fehlercodes

Wenn `Ilaunchr.exe` im Hintergrund ohne Benutzereingriffe ausgeführt wird, werden die Installationsergebnisse mit den Standardabschlusscodes gemeldet.

Über das Anmeldeskript können Sie Tests durchführen, um die Problemursache zu ermitteln. Hier ist ein Beispiel, das Sie in Ihr Anmeldeskript einfügen können:

```
Start /Wait ILaunchr.exe \\server\share\mysuite.jar /U if errorlevel 100 Go to
Some_Setup_Error_occurred if errorlevel 5 Go to Some_Ilaunchr_Error_occurred if
 errorlevel 3 Go to Problem_with_JAR_package if errorlevel 2 Go to
User_does_not_have_admin_rights if errorlevel 1 Go to FSMA_was_already_installed
 if errorlevel 0 Echo Installation was OK!
```

Fehlercodes:

Fehlercode	Beschreibung
0	Installation OK.
1	FSMA ist bereits installiert.
2	Benutzer verfügt nicht über Administratorrechte.
3	JAR wurde nicht gefunden.
4	JAR ist beschädigt.
6	Fehler beim Dekomprimieren eines Installationspakets aufgetreten.
7	Für die Installation ist nicht genügend freier Speicherplatz auf dem Zieldatenträger vorhanden.
8	Daeti `package.ini` wurde nicht in der JAR-Datei gefunden.
9	Datei `package.ini` enthält keine Arbeitsanweisungen.
10	Falsche Parameter in der Befehlszeile oder `INI`-Datei.
11	Beim Initialisieren eines neuen Arbeitsvorgangs ist ein Fehler aufgetreten.
12	Beim Erstellen des Installationsvorgangs für Setup ist ein Fehler aufgetreten.
13	Das `TEMP`-Verzeichnis konnte nicht angelegt werden.
14	Nicht definierter Fehler.
100	Erforderliche Daten für die "unbemerkte" Installation fehlen. Ungültige JAR-Datei.
101	Update ist deaktiviert. (Setup hat versucht, die Installation zu aktualisieren.)
102	Setup konnte die Datei `product.ini` nicht lesen.
103	Die Datei `prodsett.ini` enthält ungültige Daten.
104	Management Agent hat die Installation abgebrochen, oder es wurden Programme gefunden, die Konflikte verursachen. Installation abgebrochen.
105	Der Lizenzschlüssel wurde falsch eingegeben oder fehl. Installation abgebrochen.
110	Nicht genügend Speicherplatz.

Fehlercode	Beschreibung
111	Beim Ziellaufwerk handelt es sich nicht um ein lokales Laufwerk.
120	Der Benutzer verfügt nicht über Administratorrechte auf diesem Computer.
130	Setup konnte nicht gepackte Dateien nicht in das Zielverzeichnis kopieren.
131	Setup konnte das Deinstallations-Plugin nicht in das Zielverzeichnis für das Produkt kopieren.
132	Setup konnte die Datei `product.ini` nicht in das `TEMP`-Verzeichnis kopieren.
133	Beim Kopieren der Programmdatei in das Zielverzeichnis ist ein Fehler aufgetreten.
134	Die Datei `prodsett.ini` kann nicht kopiert werden.
140	Eine neuere Version der Suite wurde festgestellt.
150	Setup konnte die Programm-Plugin-DLL nicht laden.
151	Setup konnte die DLL zur Installationsunterstützung nicht laden.
152	Setup konnte die Wrapper-DLL nicht laden.
160	Setup konnte eine CAB-Datei nicht initialisieren.
170	Management Agent Setup-Plugin hat einen Fehler zurückgegeben.
171	Ein unerwarteter Code wurde vom Plugin zurückgegeben.
172	Ein Wrapper-Code wurde vom Plugin zurückgegeben.
173	Einer der vorherigen Installations-/Deinstallationsvorgänge wurde nicht abgeschlossen. Um den Vorgang abzuschließen, ist ein Neustart erforderlich.
174	Der Ziel-Computer wurde neu gestartet, um einen früheren Installations-/Deinstallationsvorgang abzuschließen. Führen Sie die Push-Installation erneut aus.
200	Teilerfolg. Die Installation einiger Programme ist fehlgeschlagen.

Kapitel

11

Fehlercodes bei der Remote-Installation von FSII

Themen:

- *Fehlercodes*

Falls bei Remote-Installationsvorgängen Probleme auftreten sollten, können Sie mithilfe der hier aufgeführten Informationen nach der Ursache suchen.

In diesem Abschnitt werden die häufigsten Fehlercodes und -meldungen beschrieben, die bei Verwendung der Funktion **Windows-Hosts automatisch feststellen** angezeigt werden können.

Fehlercodes

Hier finden Sie eine Beschreibung der häufigsten Fehlercodes und Fehlermeldungen, die bei Remote-Installationsvorgängen angezeigt werden können.

Windows-Fehlercodes

Fehlercode	Beschreibung
1057	Der Name des Benutzerkontos ist ungültig oder nicht vorhanden.
5	Zugriff verweigert. Wenn **Dieses Konto** verwendet wird, muss der Administrator auf dem Computer mit Policy Manager Console mit Rechten eines Domänen-Administrators angemeldet sein. Bei **Domain Trusts**sollten Sie sicherstellen, dass Sie sich mit einem Konto einer vertrauensvollen Domäne bei Policy Manager Console angemeldet haben.
1069	Anmeldung fehlgeschlagen. In den meisten Fällen wurde ein falsches Passwort eingegeben.
1722	RPC-Server ist nicht verfügbar. Diese Fehlermeldung wird unter Umständen angezeigt, wenn der Host direkt nach der Installation neu gestartet wurde und Policy Manager Console nicht genügend Zeit hatte, um zu überprüfen, ob die Installation erfolgreich abgeschlossen wurde.
1219	Policy Manager Console hat offene Netzwerkverbindungen zur Zielarbeitsstation. Schließen Sie die Verbindungen, bevor Sie versuchen, Verbindungen unter Verwendung eines anderen Benutzerkontos zu öffnen.

Fehlermeldungen

Fehlermeldung	Beschreibung
Die erforderliche Berechtigung wird dem aktuellen Konto nicht gewährt und sollte manuell hinzugefügt werden.	Standardmäßig verfügen selbst Administratoren nicht über die erforderliche Berechtigung **Einsetzen als Teil des Betriebssystems** auf dem Computer mit Policy Manager Console. Ohne diese Berechtigung kann FSII die eingegebenen Benutzerkonten unter Windows NT nicht authentifizieren. Um diese Berechtigung zu einem Administratorkonto auf Policy Manager Console, hinzuzufügen, klicken Sie auf **Windows NT Benutzer-Manager** > **Richtlinien** > **Benutzerrechte**.
Management Agent hat die Installation abgebrochen, oder es wurden Programme gefunden, die Konflikte verursachen. Installation abgebrochen.	Die Setup-Komponente Management Agent bricht die gesamte Installation in folgenden Situationen ab: • Es wurde Fremdanbietersoftware gefunden, die Konflikte verursacht. • Es gibt verschiedene weitere Ursachen, unter anderem: Falsche URL zu Policy Manager Server.

Fehlermeldung	Beschreibung
Der CD-Schlüssel wurde falsch eingegeben oder fehlt. Installation abgebrochen.	Die Installation auf dem Remote-Host kann nicht gestartet werden, da der Lizenzschlüssel nicht korrekt eingegeben wurde. Überprüfen Sie die Syntax.
Der Speicherplatz auf dem Ziel-Host reicht nicht aus	Auf dem Ziel-Host befindet sich nicht genügend Festplattenspeicher. Normalerweise sind mindestens 20 MB erforderlich.
Aufgrund eines schwerwiegenden FSMAINST-Fehlers ist die Installation von Management Agent fehlgeschlagen. Weitere Informationen finden Sie in den Host-Protokolldateien.	Während der Management Agent-Installation aufgetretene schwerwiegende Fehler. Es wird empfohlen, Management Agent manuell auf dem Host zu installieren. Darüber hinaus ist es möglich, zu versuchen, `FEHLER` das Schlüsselwort aus der `fswssdbg.log` Datei herauszufinden, die sich im Windows-Verzeichnis befindet.
Eine neuere Version des F-Secure-Produkts wurde festgestellt. Die Installation wurde abgebrochen.	Wenn auf dem Ziel-Host bereits eine neuere Produktversion installiert wurde, kann die Installation erst nach einer Deinstallation abgeschlossen werden.
Die Datei prodsett.ini enthält ungültige Daten.	Die Konfigurationsdatei `prodsett.ini` enthält ungültige Daten. Wenn Sie die Datei manuell bearbeitet haben, vergewissern Sie sich, dass die Syntax korrekt ist. Anstelle der direkten Bearbeitung von `prodsett.ini` wird empfohlen, JAR-Dateien zu exportieren und diese mit **ILAUNCHR** zu installieren.

Kapitel
12

NSC-Notation für Netzmasken

Themen:

- *Details zur NSC-Notation*

Dieser Abschnitt enthält Details zum NSC-Notationsstandard.

Sie finden hier Informationen über die Verknüpfung einer Netzwerkadresse mit der zugeordneten Netzmaske.

Details zur NSC-Notation

Bei der NSC-Notation handelt es sich um die Standard-Kurznotation, bei der Netzwerkadressen mit der zugehörigen Netzmaske kombiniert werden.

Die NSC-Notation definiert die Anzahl der zusammenhängenden 1-Bit-Werte in der Netzmaske in Form eines Schrägstrichs und einer Zahl, gefolgt von der Netzwerkadresse. Hier ist ein einfaches Beispiel:

Netzwerkadresse	Netzmaske	NSC-Notation
192.168.0.0	255.255.0.0	192.168.0.0/16
192.168.1.0	255.255.255.0	192.168.1.0/24
192.168.1.255	255.255.255.255	192.168.1.255/32

Die NSC-Notation ist nicht mit Netzwerken kompatibel, die Netzmasken im "Kammstil" verwenden, d. h., dass bei den Netzmasken nicht alle 1-Bit-Werte aufeinander folgen. Der folgenden Tabelle können Sie die Anzahl der Bits für die einzelnen zulässigen Netzmasken entnehmen.

.0.0.0/0 ist eine spezielle Netzwerkdefinition, die für die Standardroute reserviert ist.

Netzmaske	Bit
128.0.0.0	1
192.0.0.0	2
224.0.0.0	3
240.0.0.0	4
248.0.0.0	5
252.0.0.0	6
254.0.0.0	7
255.0.0.0	8
255.128.0.0	9
255.192.0.0	10
255.224.0.0	11
255.240.0.0	12
255.248.0.0	13
255.252.0.0	14
255.254.0.0	15
255.255.0.0	16
255.255.128.0	17
255.255.192.0	18
255.255.224.0	19
255.255.240.0	20
255.255.248.0	21
255.255.252.0	22
255.255.254.0	23
255.255.255.0	24
255.255.255.128	25

Netzmaske	Bit
255.255.255.192	26
255.255.255.224	27
255.255.255.240	28
255.255.255.248	29
255.255.255.252	30
255.255.255.254	31
255.255.255.255	32