F-Secure Linux Security

Inhalt

Kapitel 1: Willkommen.....7

Funktionsweise des Produkts.....8
Schutz vor Malware.....8
Host Intrusion Prevention System.....8
Wichtige Funktionen und Vorteile.....9
Erhöhter Schutz vor Viren und Würmern.....9
Transparenz für Endbenutzer.....9
Schutz von wichtigen Systemdateien.....9
Einfache Bereitstellung und Verwaltung.....9
Umfassende Alarmausgabeoptionen.....10

Kapitel 2: Bereitstellung.....11

Bereitstellung auf mehreren eigenständigen Linux-Arbeitsstationen.....12
Bereitstellung auf mehreren zentral verwalteten Linux-Arbeitsstationen.....12
Zentrale Bereitstellung mithilfe von Image-Dateien.....12

Kapitel 3: Installation.....15

Systemanforderungen.....16
Liste der verwendeten Systemressourcen.....16
Einzelplatzinstallation.....17
Zentral verwaltete Installation.....18
Update.....19
Update ausgehend von einer früheren Version des Produkts.....19
Update der Testversion.....20
Benutzerdefinierte Installationen.....20
Vorbereitung der benutzerdefinierten Installation.....20
Unbeaufsichtigte Installation.....20
Ausschließliche Installation des Befehlszeilen-Scanners.....21
Verwenden des Produkts auf Samba-Servern.....22
Erstellen einer Sicherungskopie.....23
Deinstallation.....23

Kapitel 4: Verwaltung des Produkts.....25

Grundlegendes zur Verwendung von F-Secure Policy Manager.....26
Zugriff auf die Webbenutzerschnittstelle.....26
Überprüfen der Virenschutzfunktionen.....27

Kapitel 5: Verwendung des Produktes.....29

Zusammenfassung.....30
Allgemeine Aufgaben.....30
Scannen auf Viren.....32
Was versteht man unter Viren und sonstiger Malware?.....33
Viren und andere Malware stoppen.....35
Verfahren zum Schutz des Computers vor Malware.....36
Schutz durch Firewall.....43
Was ist eine Firewall?.....43
Was sind Sicherheitsprofile?.....43
Firewall-Regeln.....45
Firewall-Einstellungen.....47
Integritätsprüfung.....48
Liste "Bekannte Dateien".....48
Softwareinstallationsmodus.....50
Baseline.....51
Allgemeine Einstellungen.....52
Alarmmeldungen.....52
Automatische Updates.....54
F-Secure Anti-Virus-Proxies.....55
Info.....55

Kapitel 6: Fehlerbehebung.....57

Manuelles Installieren der erforderlichen Kernel-Module.....58
Benutzeroberfläche.....58
F-Secure Policy Manager.....59
Integritätsprüfung.....59
Firewall.....60
Virenschutz.....61
Kompatibilität mit anderen Sicherheitsprodukten.....62
Allgemeine Probleme.....62

Anhang A: Befehlszeilen -Tools.....65

fsav.....66
fsav-config.....66
dbupdate.....67
fsfwc.....67
fsic.....68
fsims.....68
fsma.....68
fssetlanguage.....69
fschooser.....70

Anhang B: Vor der Installation.....71

64-Bit-Produkte.....72
Distributionen mit Prelink.....72
Red Hat Enterprise Linux, Asianux, CentOS.....72
Debian.....73
SUSE.....74
Turbolinux.....74
Ubuntu.....75

Anhang C: Benutzeroberflächen-Referenz.....77

Einfache Webbenutzer-Oberfläche.....78
"Ich möchte".....78
Erweiterte Benutzeroberfläche.....78
Zusammenfassung.....78
Alarmmeldungen.....79
Virenschutz.....79
Firewall.....85
Integritätsprüfung.....86
Allgemeine Einstellungen.....87

Anhang D: Liste von Traps.....91

Anhang E: Weitere Hilfe.....97

Kapitel

1

Willkommen

Themen:

- *Funktionsweise des Produkts*
- *Wichtige Funktionen und Vorteile*

Willkommen bei F-Secure Anti-Virus Linux Security.

Computerviren gehören zu den schlimmsten Gefahren für die Sicherheit von Daten auf Computern. Die Anzahl der Viren hat sich von nur einer Hand voll vor ein paar Jahren auf gegenwärtig mehrere tausend erhöht. Obwohl einige Viren harmlose Streiche sind, können andere Viren Daten zerstören und eine wirkliche Bedrohung darstellen.

Das Produkt umfasst eine integrierte, sofort einsatzfähige Sicherheitslösung mit einem starken Echtzeit-Virenschutz und einer Funktionalität zur Host Intrusion Prevention (HIPS), die Schutz vor unbefugten Verbindungsversuchen aus Netzwerken, unbefugten Systemänderungen, Userspace- und Kernel-Rootkits bietet. Die Lösung kann auf einfache Weise bereitgestellt und verwaltet werden - entweder mit der Webbenutzeroberfläche oder mit F-Secure Policy Manager.

F-Secure Policy Manager bietet eine eng integrierte Infrastruktur für die Definition und Verteilung von Sicherheitsrichtlinien sowie für die Überwachung der Sicherheit verschiedener Anwendungen von einem zentralen Standort aus.

Funktionsweise des Produkts

Das Produkt erkennt und verhindert unberechtigte Zugriffe und schützt vor Malware.

Mit den Standardeinstellungen sind Computer sofort nach der Installation geschützt. Es geht somit keine Zeit durch die Konfiguration des Produkts verloren.

Schutz vor Malware

Das Produkt schützt das System vor Viren und potenziell bösartigen Dateien.

Wenn der Benutzer eine Datei aus dem Internet herunterlädt, beispielsweise durch Klicken auf einen Link in einer E-Mail-Nachricht, wird die Datei gescannt, sobald der Benutzer versucht, sie zu öffnen. Wenn die Datei infiziert ist, wird das System durch das Produkt vor der Malware geschützt.

- Das *Echtzeit-Scanning* gewährleistet einen lückenlosen Schutz vor Viren und Riskware, sobald Dateien geöffnet, kopiert und aus dem Internet heruntergeladen werden. Das Echtzeit-Scanning wird transparent im Hintergrund ausgeführt. Es wird aktiviert, wenn Sie auf Dateien auf der Festplatte, Disketten oder Netzwerklaufwerke zugreifen. Wenn Sie versuchen, auf eine infizierte Datei zuzugreifen, wird die Ausführung des Virus automatisch durch den Echtzeitschutz verhindert.
- Wenn das Echtzeit-Scanning so konfiguriert wurde, dass eine begrenzte Anzahl von Dateien gescannt wird, kann das *manuelle Scanning* dazu verwendet werden, das gesamte System zu scannen. Mit dem geplanten Scanning können Sie das gesamte System in regelmäßigen Zeitabständen scannen.
- *Automatische Updates* sorgen dafür, dass die Virendefinitionen stets aktuell bleiben. Nachdem das Produkt installiert wurde, werden die Virendefinitionsdatenbanken automatisch aktualisiert. Die Virendefinitions-Updates werden vom F-Secure AntiVirus Research Team veröffentlicht und mit einer digitalen Signatur versehen.

Host Intrusion Prevention System

Das Host Intrusion Prevention System (*HIPS*) erkennt alle böswilligen Aktivitäten auf dem Host. Damit wird das System auf mehreren Ebenen geschützt.

- Mit der *Integritätsprüfung* wird das System vor nicht autorisierten Änderungen geschützt. Sie basiert auf dem Konzept einer als funktionierend bekannten Konfiguration - das Produkt muss installiert werden, bevor eine Verbindung zwischen dem Server bzw. der Arbeitsstation und dem Netzwerk hergestellt wird, damit sichergestellt ist, dass sich das System in einer als funktionierend bekannten Konfiguration befindet.

  Sie können eine Baseline der Systemdateien erstellen, die geschützt werden sollen, und Änderungsversuche von geschützten Dateien für alle Benutzer blockieren.
- *Die Firewall*-Komponente ist eine Stateful-Paketfilterungsfirewall, die auf Netfilter und Iptables basiert. Sie schützt den Computer vor unbefugten Verbindungsversuchen. Sie können vordefinierte Sicherheitsprofile verwenden, die für allgemeine Anwendungsfälle so angepasst werden, dass der zulässige und unzulässige Datenverkehr ausgewählt werden kann.
- Wenn ein Hacker Shell-Zugriff auf das System erlangt und versucht, ein Benutzerkonto zum späteren Anmelden im System hinzuzufügen, erkennt das Host Intrusion Prevention System (*HIPS*) geänderte Systemdateien, und gibt eine Alarmmeldung an den Administrator aus.
- Wenn ein Hacker Zugriff auf das System erlangt hat und versucht, ein Userspace-Rootkit zu installieren, indem er verschiedene Systemprogramme ersetzt, erkennt *HIPS* geänderte Systemdateien und gibt eine Alarmmeldung an den Administrator aus.

Wichtige Funktionen und Vorteile

Das Produkt bietet erhöhten Schutz vor Viren und Würmern und ist für Endbenutzer transparent.

Erhöhter Schutz vor Viren und Würmern

Mit dem Produkt können Dateien auf einem beliebigen, von Linux unterstützten Dateisystem gescannt werden. Dies ist die optimale Lösung für Computer mit mehreren Betriebssystemen, die über ein Multi-Boot-Programm gestartet werden.

- Überprüft Dateien auf beliebigen von Linux unterstützten Dateisystemen.

  Hinweis: Das Echtzeit-Scannen wird bei der Verwendung von NFS-Servern nicht unterstützt. Es können jedoch anderen Scan-Methoden verwendet werden.

- Erhöhte Erkennungsrate mit mehreren Scan-Modulen.
- Ein heuristisches Scanning-Modul erkennt verdächtige, potenziell bösartige Dateien.
- Das Produkt erkennt und kategorisiert Riskware.
- Das Produkt kann so konfiguriert werden, dass die Benutzer den Schutz nicht umgehen können.
- Dateien werden auf Viren gescannt, sobald sie geöffnet oder geschlossen oder ausgeführt werden.
- Sie können angeben, welche Dateien gescannt werden sollen, wie sie gescannt werden sollen, welche Maßnahmen ergriffen werden sollen, wenn böswillige Inhalte gefunden werden, und auf welche Weise Alarmmeldungen zu den Infektionen ausgegeben werden sollen.
- Rekursives Scannen von Archivdateien.
- Updates der Virendefinitionsdatenbanken werden zur Sicherheit mit einer Signatur versehen.
- Integrierte Firewall-Komponente mit vordefinierten Sicherheitsstufen.Jede Sicherheitsstufe umfasst Regeln, mit denen der Netzwerkdatenverkehr aufgrund der verwendeten Protokolle zugelassen bzw. blockiert wird.

Transparenz für Endbenutzer

Das Produkt arbeitet völlig transparent für die Endbenutzer.

- Das Produkt verfügt über eine benutzerfreundliche Benutzeroberfläche.
- Virendefinitionsdatenbanken werden ohne die Notwendigkeit von Maßnahmen seitens des Endbenutzers automatisch aktualisiert.

Schutz von wichtigen Systemdateien

Wichtige Informationen zu Systemdateien werden gespeichert und automatisch überprüft, bevor der Zugriff gewährt wird.

- Der Administrator kann Dateien vor Änderungen schützen, sodass es beispielsweise nicht möglich ist, eine Trojanerversion zu installieren.
- Es wird eine Alarmmeldung an den Administrator gesendet, wenn eine geänderte Systemdatei gefunden wird.

Einfache Bereitstellung und Verwaltung

Die Standardeinstellungen gelten für die meisten Systeme und das Produkt ist ohne zusätzliche Konfiguration einsatzbereit.

- Sicherheitsrichtlinien können ausgehend von einem zentralen Standort konfiguriert und verteilt werden.

Umfassende Alarmausgabeoptionen

Das Produkt verfügt über umfassende Überwachungs- und Alarmausgabefunktionen, die zum Benachrichtigen von Administratoren im Netzwerk eines Unternehmens über infizierte Inhalte verwendet werden können.

- Alarmmeldungen können an die F-Secure Policy Manager-Konsole, E-Mail und Syslog weitergeleitet werden.

Kapitel

2

Bereitstellung

Themen:

- *Bereitstellung auf mehreren eigenständigen Linux-Arbeitsstationen*
- *Bereitstellung auf mehreren zentral verwalteten Linux-Arbeitsstationen*
- *Zentrale Bereitstellung mithilfe von Image-Dateien*

Das Produkt kann auf eigenständigen oder auf zentral verwalteten Linux-Arbeitsstationen bereitgestellt werden.

Bereitstellung auf mehreren eigenständigen Linux-Arbeitsstationen

Es wird eine zentral verwaltete Installation mit F-Secure Policy Manager empfohlen, der auf einem separaten Computer installiert ist.

Im zentral verwalteten Installationsmodus wird der F-Secure Policy Manager zur Verwaltung der Linux-Arbeitsstationen verwendet. Die empfohlene Bereitstellungsmethode besteht darin, die Installationsverantwortlichkeit auf die Benutzer der einzelnen Arbeitsstationen zu übertragen und den Installationsverlauf über die F-Secure Policy Manager-Konsole zu überwachen. Nachdem die Installation auf einem Host abgeschlossen ist, sendet der Host eine automatische Registrierungsanforderungen an F-Secure Policy Manager. Mithilfe der F-Secure Policy Manager-Konsole kann überwacht werden, welche Hosts eine automatische Registrierungsanforderung gesendet haben.

Wenn das Unternehmen mehrere Linux-Arbeitsstationen bereitstellt, die jedoch nicht zentral verwaltet werden, können die Benutzer der jeweiligen Arbeitsstation die Software selbst installieren.

In Unternehmen mit nur wenigen Linux-Maschinen können die Linux-Arbeitsstationen über die grafische Benutzeroberfläche verwaltet werden, statt den F-Secure Policy Manager zu verwenden.

Bereitstellung auf mehreren zentral verwalteten Linux-Arbeitsstationen

Wenn Arbeitsstationen über ein vorhandenes Verwaltungssystem verwaltet werden, können sie verwendet werden, um die Software an Arbeitsstationen zu verschieben.

Wenn das Unternehmen mehrere Linux-Arbeitsstationen bereitstellt, die über ein Red Hat-, Ximian Red Carpet- oder ein ähnliches Netzwerk verwaltet werden, kann die Software an Arbeitsstationen verschoben werden, die das vorhandene Verwaltungssystem verwenden.

Zentrale Bereitstellung mithilfe von Image-Dateien

Wenn das Unternehmen über eine zentrale IT-Abteilung verfügt, in der Computer installiert und gewartet werden, kann die Software zentral auf allen Arbeitsstationen installiert werden.

Wenn Sie beabsichtigen, das Produkt auf mehreren Computern zu installieren, können Sie eine Disk-Image-Datei erstellen, die das Produkt enthält. Mit diesem Image können Sie die Software auf den Computern replizieren. Stellen Sie sicher, dass für jeden Computer, auf dem die Software installiert wird, ein neuer, eindeutiger Identifizierungscode erstellt wird.

Führen Sie die folgenden Schritte aus, um sicherzustellen, dass jeder Computer eine personalisierte eindeutige Kennung (UID) verwendet, wenn eine Disk-Image-Software verwendet wird.

1. Installieren Sie das System und die gesamte Software, die Sie in die Image-Datei aufnehmen möchten, einschließlich des Produkts.
2. Konfigurieren Sie das Produkt so, dass es den richtigen F-Secure Policy Manager-Server verwendet. Sie sollten den Host jedoch nicht in die F-Secure Policy Manager-Konsole importieren, wenn der Host eine automatische Registrierungsanforderung an den F-Secure Policy Manager-Server gesendet hat. Nur Hosts, auf denen die Image-Datei installiert wird, sollten importiert werden.
3. Führen Sie folgenden Befehl aus: `/etc/init.d/fsma clearuid`
   Das Hilfsprogramm setzt die eindeutige Kennung (UID) in der Produktinstallation zurück.

4. Fahren Sie den Computer herunter und starten Sie den Computer erst neu, nachdem die Image-Datei erstellt wurde.
5. Erstellen Sie die Disk-Image-Datei.

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 F-Secure Policy Manager, wenn sie neu gestartet werden. Diese Anforderungen können normal verarbeitet werden.

Kapitel

3

Installation

Themen:

- *Systemanforderungen*
- *Einzelplatzinstallation*
- *Zentral verwaltete Installation*
- *Update*
- *Benutzerdefinierte Installationen*
- *Erstellen einer Sicherungskopie*
- *Deinstallation*

Das Produkt kann im Standaonemodus oder im zentral verwalteten Modus installiert werden.

Systemanforderungen

Eine Liste der Systemanforderungen.

Betriebssystem:	Die Liste der unterstützten Distributionen finden Sie in den Versionsinfos des Produkts.
Prozessor:	686
Arbeitsspeicher:	Vollständige Installation: 1024 MB RAM oder mehr Reine Befehlszeileninstallation: 512 MB RAM (1024 MB werden empfohlen) **Hinweis:** Sie sollten unbedingt für eine ausreichende Kapazität des Auslagerungsspeichers sorgen.
Festplattenspeicher:	3 GB
Erforderliche Komponenten	Linux-Kernel 2.6 oder höher Glibc 2.3.4 oder höher 32-Bit-Kompatibilitätsbibliotheken auf 64-Bit-Distributionen

Hinweis: Die Verwendung der Webbenutzeroberfläche wird von den Browsern Firefox 2 oder höher und Internet Explorer 6 und 7 unterstützt.

Hinweis zur Version für Dazuko

Für das Produkt ist das Kernel-Modul Dazuko für den Echtzeit-Virenschutz, für die Integritätsprüfung und den Rootkit-Schutz erforderlich. Dazuko ist ein Open-Source-Kernel-Modul, das eine Schnittstelle für die Dateizugriffssteuerung bietet. Weitere Informationen finden Sie unter *http://www.dazuko.org*.

Das Produkt installiert den Dazuko-Treiber während der Produktinstallation.

Das Produkt wurde umfassend mit der Dazuko-Version getestet, die im Lieferumfang des Produkts enthalten ist. Die Verwendung mit anderen Dazuko-Versionen oder durch Linux bereitgestellten Dazuko-Versionen wird nicht unterstützt bzw. nicht empfohlen.

Liste der verwendeten Systemressourcen

Eine Zusammenfassung der vom Produkt verwendeten Systemressourcen.

Installierte Dateien

Alle vom Produkt installierten Dateien befinden sich in den folgenden Verzeichnissen:

- `/opt/f-secure`
- `/etc/opt/f-secure`
- `/var/opt/f-secure`

Zusätzlich werden bei der Installation die folgenden Symlinks erstellt:

- `/usr/bin/fsav` -> `/opt/f-secure/fssp/bin/fsav`
- `/usr/bin/fsic` -> `/opt/f-secure/fsav/bin/fsic`
- `/usr/bin/fsui` -> `/opt/f-secure/fsav/bin/fsui`
- `/usr/share/man/man1/fsav.1` -> `/opt/f-secure/fssp/man/fsav.1`

- `/usr/share/man/man8/fsavd.8` -> `/opt/f-secure/fssp/man/fsavd.8`

logrotate-Konfigurationsdatei installiert in:

- `/etc/logrotate.d/fs-linux-security`

init-Skript installiert in:

- `/etc/init.d/fsma`

Geänderte Systemdateien

- `/etc/passwd`: Zwei neue Benutzerkonten (fsma und fsaua) werden während der Installation erstellt.
- `/etc/group`: Eine neue Gruppe (fsc) wird während der Installation erstellt.
- Cron-Tabelle von Root-Benutzer: Geplante Überprüfungsaufgaben werden bei ihrer Erstellung zur Cron-Tabelle hinzugefügt.

Netzwerkressourcen

Das Produkt reserviert die folgenden IP-Ports, während es ausgeführt wird:

Schnittstelle	Protokoll	Port	Kommentar
lo	tcp	28005	Interner Kommunikations-Port von Web User Interface
lo	tcp	28078	PostgreSQL-Alarmdatenbank
lo	tcp	28080	Lokaler Webbenutzerschnittstellen-Zugang
alle	tcp	28082	Remote SSL Webbenutzerschnittstellen-Zugang (falls aktiviert)

Hauptspeicher

Web User Interface nimmt mehr als 200 MB Arbeitsspeicher in Anspruch, aber da WebUI nicht ständig verwendet wird, ist der Arbeitsspeicher für gewöhnlich anderweitig verfügbar. Die anderen Produktkomponenten benötigen gemeinsam etwa 50 MB Arbeitsspeicher, wobei der On-Access-Scanner den größten Teil davon beansprucht.

Die Arbeitsspeicherauslastung hängt davon ab, wie viele Dateizugriffe im System ausgeführt werden. Wenn mehrere Benutzer im System angemeldet sind und auf viele Dateien zugreifen, steigt die Arbeitsspeicherauslastung.

CPU

Die Auslastung des Prozessors hängt von der Anzahl der Dateizugriffe im System ab, da der On-Access-Scanner jede Datei überprüft, die geöffnet, geschlossen und ausgeführt wird.

Die CPU-Auslastung steigt, wenn viele Benutzer gleichzeitig im System angemeldet sind.

Einige Softwareprodukte sind darauf ausgelegt, auf viele Dateien zuzugreifen und der On-Access-Scanner kann diese Produkte merklich verlangsamen.

Einzelplatzinstallation

Der Einzelplatzinstallationsmodus ist für die Verwendung zu Testzwecken und für Umgebungen mit wenigen Linux-Arbeitsstationen oder -Servern vorgesehen, bei denen die zentrale Administration mit F-Secure Policy Manager nicht notwendig ist.

Ein Compiler und die Kernel-Quelle müssen installiert sein. Informationen dazu, wie Sie überprüfen können, dass die erforderlichen Tools installiert sind, finden Sie in der Dokumentation zu Ihrer Distribution.

Sie müssen das Produkt über ein Konto mit Root-Berechtigungen installieren.

1. Kopieren Sie die Installationsdatei auf Ihre Festplatte. Verwenden Sie folgenden Befehl zum Extrahieren der Installationsdatei: `tar zxvf f-secure-linux-security-<version>.<build>.tgz`
2. Vergewissern Sie sich, dass die Installationsdatei ausgeführt werden kann: `chmod a+x f-secure-linux-security-<version>.<build>`
3. Führen Sie folgenden Befehl aus, um die Installation zu starten:`./f-secure-linux-security-<version>.<build>`
4. Während der Installation wird die Lizenzvereinbarung angezeigt. Wenn Sie der Vereinbarung zustimmen, antworten Sie mit "`yes`" und drücken Sie die Eingabetaste, um fortzufahren.

Die Installation ist angeschlossen.

Nach der Installation können Sie die Produkteinstellungen mit Hilfe des Webbrowsers konfigurieren. Öffnen Sie die folgende Webseite: http://localhost:28080/fsecure/webui/

Wenn Sie einen Remote-Zugriff auf die Webbenutzerschnittstelle benötigen, führen Sie das Befehlszeilenprogramm `fsav-config` aus, um ihn zu aktivieren. Öffnen Sie nach der Aktivierung des Remote-Zugriffs die folgende Webseite: https://host.domain:28082/fsecure/webui

Wobei host.domain entweder der Hostname oder die IP-Adresse des Computers ist, auf dem das Produkt läuft.

Weitere Informationen über das Programm `fsav-config` und die Einstellungen, die Sie dabei konfigurieren können, finden Sie in Abschnitt "fsav-config" in Anhang A.

Hinweis: Wenn Sie einige Funktionen des Produkts vollständig deaktivieren möchten, starten Sie das Befehlszeilenprogramm `fschooser`.

Zentral verwaltete Installation

Im zentral verwalteten Modus wird das Produkt lokal installiert und mit F-Secure Policy Manager verwaltet, der auf einem separaten Computer installiert ist. Wenn das Produkt in einer großen Netzwerkumgebung eingesetzt wird, ist die zentral verwaltete Installation der empfohlene Installationsmodus.

Ein Compiler und die Kernel-Quelle müssen installiert sein. Distributionsspezifische Anweisungen zur Überprüfung, ob erforderliche Tools installiert wurden, finden Sie im Anhang des Handbuchs.

Vor der Installation des Produkts muss F-Secure Policy Manager auf einem separaten Computer installiert sein. Eine Installationsanleitung für die F-Secure Policy Manager-Konsole finden Sie im Administratorhandbuch für F-Secure Policy Manager.

Hinweis: Wenn Sie das Produkt mit F-Secure Policy Manager Windows Version 9.1 verwenden, die nicht standardmäßig über den Kanal aqualnx32 verfügt, müssen in `C:\Programme\F-Secure\FSAUA\program\fsauarep.cfg` die folgenden Zeilen einfügen: `subscribe 0,aqualnx32`.

Hinweis: Linux-Produkte können nicht mit dem Antivirusmodus der F-Secure Policy Manager-Konsole verwaltet werden. Verwenden Sie den Modus "**Erweitert**".

Sie müssen das Produkt über ein Konto mit Root-Berechtigungen installieren.

1. Kopieren Sie die Installationsdatei auf Ihre Festplatte. Verwenden Sie folgenden Befehl zum Extrahieren der Installationsdatei: `tar zxvf f-secure-linux-security-<version>.<build>.tgz`
2. Vergewissern Sie sich, dass die Installationsdatei ausgeführt werden kann: `chmod a+x f-secure-linux-security-<version>.<build>`

3. Führen Sie folgenden Befehl aus, um die Installation zu starten:
   `./f-secure-linux-security-<version>.<build>`
4. Während der Installation wird die Lizenzvereinbarung angezeigt. Wenn Sie der Vereinbarung zustimmen, antworten Sie mit "`yes`" und drücken Sie die Eingabetaste, um fortzufahren.

Die Installation ist abgeschlossen.

Nach der Installation können Sie die Produkteinstellungen mit Hilfe des Webbrowsers konfigurieren. Öffnen Sie die folgende Webseite: http://localhost:28080/fsecure/webui/

Wenn Sie einen Remote-Zugriff auf die Webbenutzerschnittstelle benötigen, starten Sie die Befehlszeile `fsav-config`, um ihn zu aktivieren. Öffnen Sie nach der Aktivierung des Remote-Zugriffs die folgende Webseite: https://host.domain:28082/fsecure/webui/

Wobei host.domain entweder der Hostname oder die IP-Adresse des Computers ist, auf dem das Produkt läuft.

Weitere Informationen über das Programm `fsav-config` und die Einstellungen, die Sie dabei konfigurieren können, finden Sie in Abschnitt "fsav-config" in Anhang A.

Hinweis: Wenn Sie einige Funktionen des Produkts vollständig deaktivieren möchten, starten Sie das Befehlszeilenprogramm `fschooser`.

Update

Sie können die neue Version installieren, ohne die Testversion oder eine frühere Version zu deinstallieren.

Update ausgehend von einer früheren Version des Produkts

Wenn Sie F-Secure Linux Server Security Version 7 oder höher einsetzen, können Sie die neue Version installieren, ohne zuvor die Vorversion zu deinstallieren. Wenn Sie eine ältere Version einsetzen, deinstallieren Sie sie, bevor Sie die neueste Version installieren.

Bei der Deinstallation werden alle Einstellungen und die Host-Identität beibehalten, sodass Sie den Host nicht erneut in F-Secure Policy Manager importieren müssen. Beachten Sie, dass während des Updates alle Alarmmeldungen gelöscht werden, die durch die frühere Version generiert worden sind.

Wichtig: Denken Sie bei zentral verwalteten Installationen daran, die MIB für Ihre F-Secure Policy Manager-Installation zu aktualisieren.

Deinstallieren von früheren Versionen

Eine frühere Version des Produkts kann entweder durch den Deinstallationsbefehl oder durch Löschen der Programmdateien und -verzeichnisse deinstalliert werden.

1. Wenn Sie über Version 5.x verfügen, führen Sie den folgenden Befehl von der Befehlszeile aus, um sie zu deinstallieren: `/opt/f-secure/fsav/bin/uninstall-fsav`
2. Wenn Sie über Version 4.x verfügen, entfernen Sie die folgenden Verzeichnisse und Dateien, um das Programm zu deinstallieren:

   `/opt/f-secure/fsav/`

   `/var/opt/f-secure/fsav/`

   `/etc/opt/f-secure/fsav/`

   `/usr/bin/fsav`

   `/usr/share/man/man1/fsav.1`

```
/usr/share/man/man5/fsav.conf.5
/usr/share/man/man5/fsavd.conf.5
/usr/share/man/man8/dbupdate.8
/usr/share/man/man8/fsavd.8
/usr/share/man/man8/fsavschedule.8
```

Update der Testversion

Die Testversion des Produkts kann auf die lizenzierte Vollversion des Produkts aktualisiert werden.

Wenn Sie eine frühere Version des Produktes getestet haben und die Testzeit abgelaufen ist, deinstallieren Sie zuerst die vorherige Version.

Folgen Sie der Anleitung, wenn Sie die Testversion auf die lizenzierte Vollversion des Produkts aufrüsten möchten.

1. Öffnen Sie die Webbenutzerschnittstelle.
2. Öffnen Sie die Seite "**Info**".
3. Geben Sie den Schlüsselcode ein, um auf die lizenzierte Version des Produkts zu aktualisieren. Geben Sie den Schlüsselcode in dem Format ein, in dem Sie ihn erhalten haben, einschließlich der Bindestriche, die Buchstaben- und Zahlengruppen trennen.

Nachdem Sie den Schlüsselkode eingegeben haben, wurde die Testversion auf eine Vollversion aktualisiert.

Um die Testversion über die Befehlszeile zu aktualisieren, führen Sie den folgenden Befehl aus: `/opt/f-secure/fsav/sbin/convert_to_full_installation.sh`

Hinweis: Wenn die Testversion der aktuellen Version des Produktes abgelaufen ist, bevor Sie ein Upgrade auf eine vollständige Version durchgeführt haben, müssen Sie das Produkt neu starten, nachdem SIe den Schlüsselcode eingegeben haben.

Benutzerdefinierte Installationen

Wenn Sie kein eigenständiges oder zentral verwaltetes Produkt mit den Standardoptionen installieren möchten, können Sie eine benutzerdefinierte Installation durchführen.

Vorbereitung der benutzerdefinierten Installation

Die RPM-Dateien können aus dem Installationspaket extrahiert werden, falls Sie ein benutzerdefiniertes Installationspaket erstellen möchten.

Das Produktinstallationspaket ist ein selbstextrahierendes Paket, das die Software als RPMs enthält. Die RPMs können wie folgt aus dem Paket extrahiert werden:

1. Geben Sie folgenden Befehl ein: `./f-secure-linux-security-<version>.<build> rpm`
2. Installieren Sie RPM-Pakete.
3. Führen Sie folgendes Skript aus: `/opt/f-secure/fsav/fsav-config`

Unbeaufsichtigte Installation

Im unbeaufsichtigten Installationsmodus können Sie einen Satz mit Standardinformationen in die Befehlszeile des Installationsprogramms eingeben. Auf diese Weise können Sie erzwingen, dass die Baseline für die Integritätsprüfung als Teil des Installationsprozesses generiert wird.

Verwenden Sie bei der Installation die folgende Befehlszeilenoption:

```
--auto MODE [fspms=FSPMSURL adminkey=/PATH/TO/ADMIN.PUB] lang=en|de|ja
[no]remotewui [no]locallogin user=USER kernelverify|nokernelverify pass=PASSPHRASE
keycode=KEYCODE
```

Dabei erhält "`MODE`" den Wert "standalone" für eine Einzelplatzinstallation oder "managed" für eine zentral verwaltete Installation.

Wenn für "`MODE`" der Wert "managed" festgelegt ist, müssen Sie die URL für den F-Secure Policy Manager-Server und den Speicherort des *öffentlichen Schlüssels* des Administrators angeben. Beispiel:

```
fspms=http://fspms.company.com/ adminkey=/root/admin.pub
```

Verwenden Sie die folgenden Optionen in der Befehlszeile:

lang	Sprache der Webbenutzerschnittstelle wählen.
remotewui	Remote-Zugriff auf die Webbenutzerschnittstelle zulassen.
noremotewui	Kein Remote-Zugriff auf die Webbenutzerschnittstelle.
nolocallogin	Lokalen Zugriff auf die Webbenutzerschnittstelle ohne Anmeldung zulassen.
locallogin	Anmeldung für lokalen Zugriff auf die Webbenutzerschnittstelle erforderlich.
user=USER	Lokales Konto für die Verwendung der Webbenutzerschnittstelle festlegen.
pass=PASS	Passphrase für die Baseline-Generierung festlegen.
keycode=KEYCODE	Schlüsselcode für Lizenzüberprüfungen festlegen. Wird kein Schlüsselcode angegeben, wird das Produkt als Testversion installiert.
nofirewall	Deaktivieren Sie die Firewall-Komponente des Produkts.

Mit der folgenden Version können Sie das Produkt im eigenständigen Modus mit englischer Webbenutzeroberfläche installieren. Sie haben dann keinen Remote-Zugriff auf die Benutzeroberfläche und benötigen keine Anmeldung für den lokalen Zugriff auf die Benutzeroberfläche.

```
./f-secure-linux-security-<version>.<build> --auto standalone lang=en noremotewui
nolocallogin
```

Ausschließliche Installation des Befehlszeilen-Scanners

Bei der Nur-Befehlszeilen-Installation werden nur der Befehlszeilen-Scanner und der Automatic Update Agent installiert.

Der Installationsmodus ist für Benutzer konzipiert, die von F-Secure Anti-Virus für Linux 4.6x wechseln, und für Benutzer, die keinen Echtzeitschutz, keine Integritätsprüfung, Webbenutzerschnittstelle oder zentrale Verwaltung benötigen, beispielsweise diejenigen, die über einen AMaViS-E-Mail-Virenscanner verfügen.

Verwenden Sie folgende Befehlszeile, wenn Sie das Installationsprogramm ausführen, um die Nur-Befehlszeilen-Version des Produkts zu installieren:

```
./f-secure-linux-security-<version>.<build> --command-line-only
```

Wenn Sie über eine frühere Version verfügen und auf die aktuelle Version aktualisieren, aber nur den Befehlszeilen-Scanner installieren möchten, müssen Sie die frühere Version zuerst deinstallieren.

Verwenden Sie die Konfigurationsdatei "`/etc/opt/f-secure/fssp/fssp.conf`", um die ausschließliche Installation des Befehlszeilen-Scanners zu konfigurieren. Detaillierte Beschreibungen der verfügbaren Einstellungen finden Sie in der Datei.

Verwenden des Produkts auf Samba-Servern

Das Produkt kann über die Daten auf den gemeinsamen Verzeichnissen hinaus den gesamten Samba-Server schützen.

Alle Schutzfunktionen des Produktes können auf Samba-Servern verwendet werden.

1. Wenn Sie F-Secure Anti-Virus für Samba-Server installiert haben, deinstallieren Sie dies, bevor Sie das Produkt installieren. Verwenden Sie den folgenden Befehl:
   `/opt/f-secure/fsav/bin/uninstall-fsav`
2. Folgen Sie den allgmeinen Installationsanweisungen.
   Nach der Installation werden Samba-Freigaben von dem Produkt geschützt, es ist kein weiteres Setup erforderlich.
3. Ändern Sie die Firewallregeln, um den Samba-Datenverkehr zuzulassen.
   - Verwenden Sie den Firewallregelassistenten auf der Webbenutzeroberfläche.
     1. Öffnen Sie die Seite **Ich möchte**, und klicken Sie auf **eine Firewallregel erstellen**.
     2. Wählen Sie **einem auf diesem Rechner ausgeführten Dienst Zugriff gewähren** aus.
     3. Wählen Sie **Windows-Netzwerk (1)** aus.
     4. Beenden Sie den Assistenten.
     5. Rufen Sie den Assistenten erneut auf, und fügen Sie eine weitere Regel für den **Windows-Netzwerk (2)**-Dienst hinzu.
   - Verwenden Sie den Editor für Firewallregeln im erweiterten Modus der Webbenutzeroberfläche.
     1. Gehen Sie auf der Webbenutzeroberfläche in den **Erweiterter Modus**.
     2. Wählen Sie **Firewall** aus.
     3. Wählen Sie auf der Seite **Firewall** das Profil aus, dass Sie im Feld **Zu bearbeitendes Profil** verwenden möchten.
     4. Klicken Sie auf **Regel hinzufügen**.
     5. Geben Sie beispielsweise `[myNetwork]` in das Feld**Remotehost** ein, und fügen Sie eine kurze Beschreibung der Regel hinzu.
     6. Wählen Sie im Dropdownmenü **Windows-Netzwerk** aus, und klicken Sie auf **Dienst zu dieser Regel hinzufügen**, um dies als Dienst hinzuzufügen.
     7. Wählen Sie im Dropdownmenü **Windows-Netzwerk (2)** aus, und klicken Sie auf **Dienst zu dieser Regel hinzufügen**, um dies als Dienst hinzuzufügen.
     8. Verwenden Sie die Pfeile auf der rechten Seite der Tabelle, um die Regel oberhalb der Verweigerungsregeln in der Firewallregelliste zu platzieren.
     9. Klicken Sie auf **Speichern**, um die neuen Regeln zur Verwendung bereitzustellen.
   - Verwenden Sie den Editor für Firewallregeln in der F-Secure Policy Manager-Konsole.
     1. Wählen Sie im erweiterten Modus der F-Secure Policy Manager-Konsole den Host oder die Richtliniendomäne aus, die Sie verwalten möchten.
     2. Wählen Sie "**Linux Security**" aus, und öffnen Sie die Registerkarte "**Firewall**".
     3. Überprüfen Sie im Abschnitt "**Regeln**", ob Sie die Sicherheitsstufe ausgewählt haben, die Sie bearbeiten möchten.
     4. Klicken Sie auf "**Hinzufügen vor**".
     5. Lassen Sie im Regelassistenten für **Windows-Netzwerk** eingehenden Verkehr zu.
     6. Rufen Sie den Regelassistent erneut auf, um **Windows-Netzwerk (2)** hinzuzufügen.
     7. Veröffentlichen Sie die Richtlinie.

Hinweis: Wenn die Firewallregeln lokal bearbeitet wurden, konfigurieren Sie die Einstellung als **Endgültig**, bevor Sie die Richtlinie verteilen.

Wenn Sie neue Regeln hinzufügen möchten, müssen Sie die Firewall vorübergehend deaktivieren:

1. Ändern Sie **Firewallschutz** in **Deaktiviert** , oder führen Sie den folgenden Befehl aus: `/opt/f-secure/fsav/bin/fsfwc --mode bypass`.
2. Wählen Sie die Sicherheitsstufe aus, die Sie bearbeiten möchten, und bearbeiten Sie die Firewallregeln gemäß den Anweisungen.
3. Wenn Sie in der Webbenutzerschnittstelle fertig sind, aktivieren Sie die Firewall, oder führen Sie den folgenden Befehl aus: `/opt/f-secure/fsav/bin/fsfwc --mode your_profile`, wobei es sich bei `your_pfofile` um das bearbeitete Profil handelt ("Blockieren", "Mobil", "Home", "Office", "Strikt" oder "Normal").

Erstellen einer Sicherungskopie

Sie können alle Produktdaten sichern und wiederherstellen.

Führen Sie die folgenden Befehle aus, um alle relevanten Daten zu sichern:

```
# /etc/init.d/fsma stop
# /etc/init.d/fsaua stop
# tar cpsf <backup-filename>.tar /etc/init.d/fsma /etc/init.d/fsaua
/etc/opt/f-secure /var/opt/f-secure /opt/f-secure
# /etc/init.d/fsaua start
# /etc/init.d/fsma start
```

Führen Sie die folgenden Befehle aus, um Daten aus der Sicherungsdatei wiederherzustellen:

```
# /etc/init.d/fsma stop
# /etc/init.d/fsaua stop
# cd /
# rm -rf /var/opt/f-secure
# tar xpsf <backup-filename>.tar
# /etc/init.d/fsaua start
# /etc/init.d/fsma start
```

Stellen Sie sicher, dass fsma- und fsaua-Benutzer und die fsc-Gruppe auch nach der Wiederherstellung der Sicherung noch bestehen, beispielsweise indem Sie auch "`/etc/passwd`"-, "`/etc/shadow`"- und "`/etc/group`"-Dateien sichern.

Deinstallation

Sie können das Produkt mit dem Befehlszeilenbefehl "`uninstall-fsav`" deinstallieren.

Führen Sie als Root-Benutzer folgendes Skript aus, um das Produkt zu deinstallieren: `/opt/f-secure/fsav/bin/uninstall-fsav`

Das Deinstallationsskript entfernt keine Konfigurationsdateien. Wenn Sie sicher sind, dass Sie sie nicht mehr benötigen, entfernen Sie alle Dateien unter dem Pfad "`/etc/opt/f-secure/fsma`".

Kapitel

4

Verwaltung des Produkts

Themen:

- *Grundlegendes zur Verwendung von F-Secure Policy Manager*
- *Zugriff auf die Webbenutzerschnittstelle*
- *Überprüfen der Virenschutzfunktionen*

Abhängig vom Installationsmodus können Sie die Software entweder über die F-Secure Policy Manager-Konsole oder über die Webbenutzerschnittstelle verwalten.

Grundlegendes zur Verwendung von F-Secure Policy Manager

Im zentralisierten Verwaltungsmodus wird die F-Secure Policy Manager-Konsole verwendet, um Einstellungen zu ändern und Statistiken für die F-Secure-Produkte anzuzeigen.

Wenn Ihr Unternehmensnetzwerk F-Secure Policy Manager zum Konfigurieren und Verwalten von F-Secure-Produkten verwendet, können Sie das Produkt zur vorhandenen F-Secure Policy Manager-Umgebung hinzufügen.

Hinweis: Der Antivirusmodus der F-Secure Policy Manager-Konsole kann nicht zur Verwaltung von Linux-Produkten verwendet werden. Verwenden Sie den Modus "**Erweitert**".

Verwenden Sie die Einstellungen auf der Registerkarte **F-Secure Linux Security** > **Einstellungen**, um das Produkt zu konfigurieren.

Hinweis: Sie können die Einstellungen auch mithilfe von **F-Secure Security Platform für Linux**, **F-Secure Management Agent** und **F-Secure Automatic Update Agent** bearbeiten, um das Verhalten des Produktes zu verändern.

Weitere Informationen über F-Secure Policy Manager finden Sie im Administratorhandbuch von F-Secure Policy Manager.

Zugriff auf die Webbenutzerschnittstelle

Sie können über die Systemleiste oder über eine Webadresse auf die Webbenutzerschnittstelle zugreifen.

Die Webbenutzerschnittstelle ist lokal unter folgender Adresse erhältlich:

```
http://localhost:28080/fsecure/webui/
```

Wenn Sie den Remote-Zugriff auf die Webbenutzerschnittstelle zulassen, können Sie unter folgender HTTPS-Adresse darauf zugreifen:

```
https://<host.domain>:28082/
```

Folgen Sie diesen Anweisungen, um das Produktsymbol zur Systemleiste hinzuzufügen.

1. Installieren Sie das Produktsymbol.
   - Wenn Sie GNOME verwenden, folgen Sie dieser Anleitung:
     1. Klicken Sie mit der rechten Maustaste auf das GNOME-Panel.
     2. Wählen Sie **Panel-Applet hinzufügen**.
     3. Wählen Sie das F-Secure-Panel-Applet in der Liste der installierten GNOME-Panel-Applets aus.
   - Wenn Sie GNOME nicht verwenden, geben Sie den Befehl "`fsui`" in der Befehlszeile ein.
2. Doppelklicken Sie auf das Produktsymbol in der Systemleiste, um die Webbenutzeroberfläche zu öffnen.

Nachdem das Produktsymbol in der Symbolleiste installiert ist, können Sie darüber auf die Webbenutzerschnittstelle zugreifen.

Es ist möglich, den F-Secure Policy Manager und die Webbenutzeroberfläche gleichzeitig zu verwenden.

Hinweis: Der Benutzer kann die mit dem F-Secure Policy Manager festgelegten Einstellungen lokal überschreiben, sofern der Administrator dies nicht ausgeschlossen hat, indem er in den F-Secure Policy Manager-Einstellungen das Kontrollkästchen "**Endgültig**" aktiviert hat.

Überprüfen der Virenschutzfunktionen

Um zu testen, ob das Produkt richtig funktioniert, können Sie eine spezielle Testdatei verwenden, die als Virus erkannt wird.

Die Standard-Antiviren-Testdatei EICAR (EICAR ist die Abkürzung für das Europäische Institut für Computer-Antiviren-Forschung (European Institute of Computer Anti-Virus Research)) wird auch von einigen anderen Antivirenprogrammen erkannt. Die Eicar-Infoseite finden Sie unter *http://www.europe.f-secure.com/virus-info/eicar_test_file.shtml*.

1. Laden Sie die EICAR-Testdatei herunter oder erstellen Sie sie.

- Laden Sie die EICAR-Testdatei unter *http://www.europe.f-secure.com/virus-info/eicar_test_file.shtml*herunter oder
- Sie können die Datei "eicar.com" mit einem beliebigen Texteditor erstellen, indem Sie ausschließlich folgende Zeile einfügen:
  `X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*`

2. Führen Sie folgenden Befehl aus: `fsav eicar.com`

Das Produkt sollte die EICAR-Testdatei als Virus erkennen.

Kapitel

5

Verwendung des Produktes

Themen:

- *Zusammenfassung*
- *Scannen auf Viren*
- *Schutz durch Firewall*
- *Integritätsprüfung*
- *Allgemeine Einstellungen*

Verwenden Sie die Web-Benutzeroberfläche, um den Status und Berichte zu überprüfen und um die Produkteinstellungen zu ändern.

Die Webbenutzerschnittstelle ist lokal unter folgender Adresse erhältlich:

```
http://localhost:28080/fsecure/webui/
```

Wenn Sie den Remote-Zugriff auf die Webbenutzerschnittstelle zulassen, können Sie unter folgender HTTPS-Adresse darauf zugreifen:

```
https://<host.domain>:28082/
```

Wobei host.domain entweder der Hostname oder die IP-Adresse des Computers ist, auf dem das Produkt läuft. Anweisungen zum Aktivieren des Remote-Zugriffs für die Webbenutzerschnittstelle finden Sie auf der man-Seite von `fsav-config`.

Zusammenfassung

Auf der Zusammenfassungsseite werden der Produktstatus sowie die letzten Berichte angezeigt.

Mit dem Produktstatus werden der Schutzstatus sowie alle möglichen Fehler und Fehlfunktionen angezeigt.

Über die Zusammenfassungsseite können Sie den Virenschutz und Integritätsschutz auf Wunsch aktivieren und deaktivieren sowie die Firewall-Schutzstufe ändern.

Im Berichtsabschnitt finden Sie Anweisungen zu Problemen, die Sie umgehend beheben sollten.

Allgemeine Aufgaben

Auf der Seite "**Allgemeine Aufgaben**" können Sie die manuellen Scan-Vorgänge und Firewall-Einstellungen konfigurieren und die neuesten Updates der Virendefinitionsdatenbanken einsehen.

Hinweis: Klicken Sie auf "**Erweiterte Einstellungen ändern...**", um die erweiterten Einstellungen anzuzeigen und zu konfigurieren.

Manuelles Scanning des Computers

Sie können den gesamten Computer über die Webbenutzerschnittstelle manuell auf Malware scannen.

Wenn das Produkt Dateien scannt, muss zumindest der Schreibzugriff auf die Dateien möglich sein. Wenn das Produkt infizierte Dateien desinfizieren soll, muss zumindest der Schreibzugriff auf die Dateien möglich sein.

Prüfen und bearbeiten Sie die Einstellungen für das manuelle Scanning, bevor Sie das manuelle Scanning starten.

1. Um das vollständige Scannen des Computers zu starten, wählen Sie im Standardbenutzeroberflächenmodus "**Ich möchte...**" aus.
2. Klicken Sie auf "**Computer auf Malware scannen**".

Hinweis: Wenn Sie das Paket `nautilus-actions` installiert haben, sind Scan-Aktionen im Kontextmenü des GNOME-Dateimanagers enthalten.

Erstellen von Firewall-Diensten und -Regeln

Wenn Sie blockierten Datenverkehr zulassen möchten oder wenn Sie bestimmten Datenverkehr blockieren möchten, können Sie neue Firewall-Dienste und -Regeln erstellen. Wenn Sie Firewall-Regeln erstellen oder bearbeiten, sollten Sie nur die erforderlichen Dienste zulassen und den Rest verweigern, um Sicherheitsrisiken zu minimieren.

Um den Firewall-Assistenten zu verwenden, wechseln Sie zu "**Allgemeine Aufgaben**", klicken Sie auf "**Eine Firewall-Regel erstellen**, befolgen Sie die Anweisungen auf dem Bildschirm und beenden Sie den Assistenten.

Befolgen Sie diese Anweisungen, um einen neuen Dienst und eine neue Regel über die erweiterte Benutzeroberfläche zu erstellen:

1. Erstellen Sie einen neuen Dienst.
   a) Wählen Sie die **Netzwerkdienste** im Menü "**Erweiterter Modus**" aus.
   b) Definieren Sie im Feld "**Dienstname**" einen eindeutigen Namen für den Dienst.
   c) Geben Sie im Feld "**Beschreibung**" einen beschreibenden Kommentar ein, um eine Abgrenzung zu ermöglichen.
   d) Wählen Sie aus der Dropdown- Liste "**Protokoll**" eine Protokollnummer für den Dienst aus.

      Falls Ihr Dienst keines der Protokolle ICMP, TCP oder UDP verwendet, wählen Sie "Numerisch" aus und geben Sie die Protokollnummer in dem dafür vorgesehenen Feld ein.

e) Wenn Ihr Dienst das TCP- oder UDP-Protokoll verwendet, definieren Sie die "**Initiatorports**, die der Dienst verwendet.
f) Wenn Ihr Dienst das TCP- oder UDP-Protokoll verwendet, müssen Sie die **Antwortpartei-Ports** festlegen, die der Dienst abdeckt.
g) Klicken Sie auf "**Als neuen Dienst hinzufügen**", um den Dienst zur Liste der Netzwerkdienste hinzuzufügen.
h) Klicken Sie auf "**Speichern**".
Der neue Dienst wird in der Dienstliste gespeichert.

2. Erstellen Sie eine neue Regel für den Dienst.
   a) Wählen Sie im Menü "**Erweiterter Modus**" den Eintrag "**Firewall-Regeln**" aus, um eine Firewall-Regel zu erstellen, die den von Ihnen definierten Dienst verwendet.
   b) Wählen Sie das Profil aus, dem Sie eine neue Regel hinzufügen möchten, und klicken Sie auf "**Neue Regel hinzufügen**", um eine neue Regel zu erstellen.
   c) Wählen Sie "**Annehmen**" oder "**Ablehnen**" als **Typ** für die Regel aus, um festzulgegen, ob der Dienst von der Regel zugelassen oder abgelehnt wird.
   d) Geben Sie Details zu Zieladressen in das Feld "**Remote-Host**" ein. Geben Sie die IP-Adressen und das Teilnetz im Bit-Netzmaskenformat ein.
   Beispiel: `192.168.88.0/29`

   Sie können folgende Alisase als Zieladresse verwenden:

   - `[myNetwork]` - Das lokale Netzwerk.
   - `[myDNS]` - Alle konfigurierten DNS-Server.

   e) Geben Sie im Feld "**Beschreibung**" einen beschreibenden Kommentar ein, um eine Abgrenzung zu ermöglichen.
   f) Wählen Sie den neu erstellten Dienst im Feld "**Dienst**" aus und geben Sie die Richtung an, für die diese Regel angewendet wird.

   - eingehend = Sämtlicher eingehender Verkehr, der aus dem Internet auf Ihrem Computer eingeht.
   - ausgehend = Sämtlicher ausgehender Verkehr, der von Ihrem Computer stammt.

   g) Wählen Sie die Netzwerkschnittstellen, für die die Regel gilt. Geben Sie die Netzwerkschnittstellen, für die die Regel gelten soll in das Feld "**Flag**" ein. Die Regel wird für alle Netzwerkschnittstellen angewendet, wenn Sie das Feld "**Flag**" leer lassen.
   Beispiel: `[if:eth0]`, `[if:eth3]`.
   h) Klicken Sie auf "**Dienst zu dieser Regel hinzufügen**".
   Der Dienst wird zu der neuen Regel hinzugefügt.
   i) Wenn Sie einer Regel keine weiteren Dienste hinzufügen möchten, klicken Sie auf "**Zu Firewall-Regeln hinzufügen**".

   Für jede Regel muss mindestens ein Dienst vorliegen. Wenn die Regel einen neuen Dienst enthält, müssen Sie sicherstellen, dass sie die Dienstliste auf der Seite "**Netzwerkdienste**" gespeichert haben.

   Die Regel wird zum aktiven Regelsatz der Tabelle "**Firewall-Regeln**" hinzugefügt.
   j) Klicken Sie auf "**Speichern**", um die neue Regelliste zu speichern.

Baseline überprüfen

Sie können die Baseline manuell überprüfen, um sicherzustellen, dass Ihr System sicher ist und alle als Baseline verwendeten Dateien unverändert sind.

1. Geben Sie zur Überprüfung der Baseline Ihre Passphrase ein.
2. Achten Sie darauf, keine weiteren Integritätsprüfvorgänge zu starten, während das Produkt die Baseline überprüft.

Falls ein Hacker Zugriff auf der Root-Ebene erlangt und die Baseline neu generiert hat, stimmt die Baseline bei der Überprüfung nicht mit Ihrer Passphrase überein.

Automatische Updates

Der F-Secure Automatic Update Agent sorgt dafür, dass der Schutz Ihres Computers aktuell bleibt.

Der F-Secure Automatic Update Agent lädt die neuesten Updates auf Ihren Computer herunter, wenn Sie mit dem Internet verbunden sind.

Informationen zum neuesten Update der Virendefinitionsdatenbank finden Sie unter:
http://www.F-Secure.com/download-purchase/updates.shtml

Softwareinstallationsmodus

Verwenden Sie den Softwareinstallationsmodus, wenn Sie die Systemdateien und Programme ändern möchten.

Durch die Integritätsprüfung werden nicht autorisierte oder ungewollte Änderungen an Systemdateien oder Programmen verhindert. Wenn Sie Ihr Betriebssystem aktualisieren, ein Sicherheits-Update anwenden oder neue Versionen der Software installieren, ist es erforderlich, die Dateien zu ändern, die durch die Integritätsprüfung überwacht werden.

Wenn Sie den Software-Installationsmodus aktivieren, bleiben Echtzeit-Scanning und Warnmeldungen für Malware während der Installation aktiviert.

Nach Abschluss der Installation und Verlassen des Software-Installationsmodus aktualisiert das Produkt die Liste "Bekannte Dateien" mit den neuen Dateien und generiert die neue Baseline. Die Integritätsprüfung und der Rootkit-Schutz werden nach der Generierung der neuen Baseline wieder aktiviert, wenn sie zuvor deaktiviert wurden.

Wichtig: Wenn Sie Software nicht im Softwareinstallationsmodus installieren, ist es möglich, dass Sie die neue Software bei der Überwachung der aktualisierten Dateien durch die Integritätsprüfung nicht installieren oder verwenden können. Die Integritätsprüfung kann beispielsweise verhindern, dass ein Kernel-Update ordnungsgemäß gebootet wird, da neue Treiber nicht in der Baseline vorhanden sind.

Baseline

Die Integritätsprüfung wird eingerichtet, indem Sie eine Baseline der Systemdateien erstellen, die Sie schützen möchten.

Während der Installation wird ein Standardsatz mit Systemdateien zu der *Liste "Bekannte Dateien"* hinzugefügt. Die Baseline für diese Dateien wird durch diese Standard-Installationsoptionen jedoch nicht automatisch generiert. Verwenden Sie den Parameter `pass=PASS`, um die Baseline während der Installation zu generieren oder generieren Sie sie nach der Installation mithilfe der Webbenutzeroberfläche oder des Befehlszeilenclients (`fsic`).

Alle Dateien, die der Baseline während der Installation hinzugefügt werden, erhalten den Schutzmodus "**Zulassen**" oder "**Alarm**".

Hinweis: Die Standardliste der bekannten Dateien wird bei der Installation generiert und enthält die wichtigsten Systemdateien. Die Dateiliste ist je nach Version unterschiedlich. Führen Sie `/opt/f-secure/fsav/bin/fslistfiles` aus, um die exakte Dateiliste abzurufen.

Scannen auf Viren

Das Produkt stoppt *Viren* und andere *Malware*.

Was versteht man unter Viren und sonstiger Malware?

Unter Malware werden Programme zusammengefasst, die gezielt entwickelt wurden, um Schäden an Computern zu verursachen, Computer ohne Wissen des Benutzers für illegale Zwecke einzusetzen oder um Informationen von Computern zu stehlen.

Malware kann:

- Kontrolle des Webbrowsers übernehmen,
- Websuchanfragen umleiten,
- unerwünschte Werbung anzeigen,
- besuchte Websites verfolgen,
- persönliche Informationen stehlen, wie z. B. Bankdaten,
- den Computer zum Senden von Spam verwenden
- den Computer für Angriffe auf andere Computer verwenden.

Malware-Programme können auch dafür sorgen, dass der Computer langsam und instabil wird.

Viren

Ein Virus ist meist ein Programm, das sich selbstständig an Dateien anhängen kann und sich ständig selbst repliziert. Ein Virus kann den Inhalt von Dateien so verändern oder ersetzen, dass diese den Computer beschädigen.

Ein *Virus* ist ein Programm, das in der Regel ohne Wissen des Benutzers auf dem Computer installiert wird. Sobald er installiert ist, versucht der Virus, sich selbst zu replizieren. Der Virus:

- verwendet Systemressourcen
- kann auf dem Computer Dateien verändern oder beschädigen
- versucht den Computer zu benutzen, um andere Computer zu infizieren
- lässt eventuell eine Verwendung des Computers zu illegalen Zwecken zu

Riskware

Riskware ist keine Malware; sie wurde nicht in der Absicht entwickelt, dem Computer zu schaden, sie besitzt aber sicherheitskritische Funktionen, die eine Gefahr für den Computer darstellen, wenn sie missbraucht werden.

Diese Programme führen einige nützliche, aber potenziell schädliche Funktionen durch. Beispiele für diese Art von Programmen:

- Programme für Instant Messaging (wie IRC, Internet Relay Chat),
- Programme zur die Übertragung von Dateien über das Internet von einem Computer auf einen anderen oder
- Programme für Internet-Telefonie (VoIP, *VoIP - Voice Over Internet Protocol*).

Wenn das Prorgamm als Riskware erkannt wird, es aber explizit installiert und korrekt eingerichtet wurde, ist es weniger wahrscheinlich, dass es sich um ein schädliches Programm handelt.

Riskware-Typen

Riskware-Kategorien und Plattformen.

Liste der Kategorien

- Adware
- AVTool
- Client-IRC
- Client-SMTP
- CrackTool

- Dialer
- Downloader
- Effect
- FalseAlarm
- Joke
- Monitor
- NetTool
- Porn-Dialer
- Porn-Downloader
- Porn-Tool
- Proxy
- PSWTool
- RemoteAdmin
- RiskTool
- Server-FTP
- Server-Proxy
- Server-Telnet
- Server-Web
- Tool

Liste der Plattformen

- Apropos
- BAT
- Casino
- ClearSearch
- DOS
- DrWeb
- Dudu
- ESafe
- HTML
- Java
- JS
- Linux
- Lop
- Macro
- Maxifiles
- NAI
- NaviPromo
- NewDotNet
- Palm
- Perl
- PHP
- Searcher
- Solomon
- Symantec
- TrendMicro
- UNIX
- VBA
- VBS
- Win16

- Win32
- Wintol
- ZenoSearch

Rootkits

Rootkits sind Programme, die dafür sorgen, dass *Malware* nur schwer erkannt wird.

Rootkit-Programme untergraben die Kontrolle des Betriebssystems über seine rechtmäßigen Funktionen. In der Regel versucht ein Rootkit, seine Installation zu verschleiern und eine Entfernung zu verhindern, indem es laufende Prozesse, Dateien oder Systemdaten vor dem Betriebssystem verbirgt. Im Allgemeinen erfolgt dies mit der Absicht, böswillige Aktivitäten auf dem Computer zu verbergen.

Schutz vor Userspace-Rootkits

Wenn ein Hacker Zugriff auf das System erlangt hat und versucht, ein Userspace-Rootkit zu installieren, indem er verschiedene Systemprogramme ersetzt, erkennt *HIPS* geänderte Systemdateien und gibt eine Alarmmeldung an den Administrator aus.

Viren und andere Malware stoppen

Das Produkt schützt den Computer vor Programmen, die Dateien beschädigen, persönliche Informationen stehlen oder für illegale Zwecke verwenden können.

Standardmäßig schützt das Produkt den Computer im Hintergrund in Echtzeit vor *Malware*. Der Computer ist jederzeit gegen *Malware* geschützt.

Das Produkt kann angegebene Dateien und Verzeichnisse, alle Wechselmedien (wie portable Laufwerke) und heruntergeladene Inhalte automatisch scannen. Das Produkt verhindert sämtliche Änderungen auf dem Computer, die auf *Malware* hinweisen können.

Wie schützt das Scannen in Echtzeit Ihren Computer?

Das Echtzeit-Scanning schützt den Computer, indem Dateien in dem Moment geprüft werden, in dem ein Zugriff erfolgt, und indem der Zugriff auf Dateien blockiert wird, die *Malware* enthalten.

So arbeitet das Echtzeit-Scanning:

1. Der Computer versucht auf eine Datei zuzugreifen.
2. Die Datei wird sofort auf *Malware* gescannt, bevor der Computer darauf zugreifen darf.
3. Wenn in einer Datei *Malware* gefunden wird, blockiert das Echtzeit-Scanning die Datei, sodass die *Malware* auf dem Computer keinen Schaden anrichten kann.
4. Auf der Grundlage der Echtzeit-Scanning-Einstellungen benennt das Echtzeit-Scanning infizierte Dateien entweder um, löscht oder desinfiziert diese.

Beeinträchtigt das Echtzeit-Scanning die Systemleistung?

Wie lange das Echtzeit-Scanning dauert und wie viele Systemressourcen dazu benötigt werden, hängt vom Inhalt, vom Speicherort und vom Typ der gescannten Dateien ab.

Dateien, bei denen das Scannen länger dauert:

- Komprimierte Dateien, wie .zip-Archive. Beachten Sie, dass diese Dateien standardmäßig nicht gescannt werden.
- Dateien in Netzwerkdateisystemen.
- Große Dateien.

Das Echtzeit-Scanning kann zu einer Verlangsamung Ihres Computers führen, wenn gleichzeitig auf eine Vielzahl von Dateien zugegriffen wird.

Manuelles Scanning des Computers

Sie können den gesamten Computer über die Webbenutzerschnittstelle manuell auf Malware scannen.

Wenn das Produkt Dateien scannt, muss zumindest der Schreibzugriff auf die Dateien möglich sein. Wenn das Produkt infizierte Dateien desinfizieren soll, muss zumindest der Schreibzugriff auf die Dateien möglich sein.

Prüfen und bearbeiten Sie die Einstellungen für das manuelle Scanning, bevor Sie das manuelle Scanning starten.

1. Um das vollständige Scannen des Computers zu starten, wählen Sie im Standardbenutzeroberflächenmodus "**Ich möchte...**" aus.
2. Klicken Sie auf "**Computer auf Malware scannen**".

Hinweis: Wenn Sie das Paket `nautilus-actions` installiert haben, sind Scan-Aktionen im Kontextmenü des GNOME-Dateimanagers enthalten.

Verfahren zum Schutz des Computers vor Malware

Es gibt verschiedene Verfahren, um den Computer vor *Malware* zu schützen; die Entscheidung für ein konkretes Verfahren sollte von der Leistungsfähigkeit des Computers und von der erforderlichen Schutzstufe abhängig gemacht werden.

Wenn alle Schutzfunktionen aktiviert sind, kann sich dies spürbar bei der Geschwindigkeit des Computers bemerkbar machen.

Scannen des Computers in Echtzeit

Das Echtzeit-Scanning scannt den Computer in Echtzeit auf *Malware* und sorgt dafür, dass dieser jederzeit geschützt ist.

Aktion bei Infektion mit Viren

Wählen Sie die primären und sekundären Aktionen aus, die durchgeführt werden, wenn ein Virus gefunden wird.

Klicken Sie auf der Seite "**Ich möchte...**" in der Webbenutzerschnittstelle auf "**Erweiterte Einstellungen ändern...**", um die erweiterten Virenscan- Einstellungen anzuzeigen und zu konfigurieren.

1. Wählen Sie die primäre Aktion aus, die durchgeführt wird, wenn ein Virus gefunden wird. Wählen Sie eine der folgenden Aktionen aus:
   - Wählen Sie "**Bericht und Zugriff sperren**" aus, um eine Alarmmeldung für den gefundenen Virus anzuzeigen und den Zugriff auf die Datei zu blockieren. Für die infizierte Datei wird keine weitere Aktion unternommen. Die Sicherheitsalarmmeldungen können Sie auf der Seite "**Alarmmeldungen**" prüfen.
   - Wählen Sie "**Desinfizieren**" aus, um Viren aus infizierten Dateien zu entfernen. Beachten Sie, dass bei einigen Viren keine Desinfektion möglich ist. Falls ein Virus nicht aus einer Datei entfernt werden kann, bleibt der Zugriff auf die infizierte Datei blockiert.
   - Wählen Sie "**Umbenennen**" aus, um die infizierte Datei umzubenennen und ihre Ausführungsberechtigungen zu entfernen. Umbenannte infizierte Dateien bleiben auf dem Computer, können aber keinen Schaden anrichten. Die umbenannte Datei hat die Erweiterung "`.virus`".
   - Wählen Sie "**Löschen**" aus, um die infizierte Datei zu löschen.
   - Wählen Sie "**Zugriff sperren**" aus, um den Zugriff auf die infizierte Datei zu sperren, ohne eine Alarmmeldung zu senden oder einen Bericht zu erstellen.

   Standardmäßig ist die primäre Aktion bei Infektionen "**Desinfizieren**".
2. Wählen Sie die sekundäre Aktion aus. Die sekundäre Aktion wird durchgeführt, wenn die primäre Aktion nicht durchgeführt werden kann.
   Standardmäßig ist die sekundäre Aktion "**Umbenennen**".

Nach der Konfiguration der Aktionen bei Infektionen müssen Sie auf der Seite "**Alarmmeldungen**" festlegen, wie Alarmmeldungen und Berichte eingesetzt werden.

Verdächtige Dateien

Legen Sie die primären und sekundären Aktionen fest, die getroffen werden, wenn das heuristische Scan-Modul verdächtige Dateien findet.

Klicken Sie auf der Seite "**Ich möchte...**" in der Webbenutzerschnittstelle auf "**Erweiterte Einstellungen ändern...**", um erweiterte Einstellungen für den Virenscan-Vorgang anzuzeigen und zu konfigurieren.

1. Wählen Sie die primäre Aktion aus, die ausgeführt wird, wenn das heuristische Scan-Modul eine verdächtige Datei findet. Wählen Sie eine der folgenden Aktionen aus:
   - Wählen Sie "**Bericht und Zugriff sperren**" aus, um eine Warnmeldung über die verdächtige Datei anzuzeigen und den Zugriff darauf zu blockieren. Weitere Maßnahmen werden nicht getroffen. Zeigen Sie die "**Alarmmeldungen**" an, um die Sicherheitswarnungen zu prüfen.
   - Wählen Sie "**Umbenennen**" aus, um den Namen der verdächtigen Datei zu ändern und ihre Ausführungsrechte zu entfernen. Umbenannte verdächtige Dateien bleiben auf dem Computer, können aber keinen Schaden mehr anrichten. Die umbenannte Datei hat die Erweiterung "`.suspected`".
   - Wählen Sie "**Löschen**" aus, damit die verdächtige Datei gelöscht wird.
   - Wählen Sie "**Zugriff sperren**" aus, um den Zugriff auf die verdächtige Datei zu sperren, ohne eine Warnmeldung zu senden oder einen Bericht zu erstellen.

   Als primäre Aktion für verdächtige Dateien ist standardmäßig "**Nur Bericht**" festgelegt.
2. Wählen Sie die sekundäre Aktion aus. Die sekundäre Aktion wird durchgeführt, wenn die primäre Aktion nicht durchgeführt werden kann.
   Als sekundäre Aktion ist standardmäßig "**Zugriff sperren**" festgelegt.

Nach der Konfiguration der Einstellungen für verdächtige Dateien müssen Sie auf der Seite "**Alarmmeldungen**" festlegen, wie Warnmeldungen und Berichte behandelt werden.

Wählen Sie aus, was gescannt wird

Geben Sie die Dateien und Verzeichnisse an, die Sie auf Malware scannen möchten.

Klicken Sie auf der Seite "**Ich möchte...**" in der Webbenutzerschnittstelle auf "**Erweiterte Einstellungen ändern...**", um erweiterte Virenscan-Einstellungen anzuzeigen und zu konfigurieren.

1. Aktivieren Sie "**Vom Scannen ausgenommene Dateien und Verzeichnisse**", um Verzeichnisse zu definieren, die vom Virenscan-Vorgang ausgeschlossen sind. Geben Sie jedes Verzeichnis in eine neue Zeile ein, jeweils ein Verzeichnis pro Zeile.

   Wenn das Scannen eines bestimmten Verzeichnisses lange dauert und Sie wissen, dass Benutzer darin keine infizierten Dateien erstellen oder als Kopie ablegen können, oder wenn während des Scan-Vorgangs falscher Alarm ausgegeben wird, können Sie das Verzeichnis aus dem Virenscan-Vorgang ausschließen.

   Tipp: Die Liste kann auch Dateien enthalten, wenn Sie spezielle Dateien aus dem Scan-Vorgang ausschließen möchten.

2. Wenn Sie ausschließlich ausführbare Dateien auf Viren scannen möchten, aktivieren Sie "**Nur ausführbare Dateien scannen**". Deaktivieren Sie das Kontrollkästchen, um alle angegebenen Dateien auf Viren zu scannen.

   Hinweis: Wen die Optionen "**Beim Öffnen scannen**" und "**Beim Ausführen scannen**" deaktiviert sind, werden keine Dateien gescannt. Dies gilt auch dann, wenn "**Nur ausführbare Dateien scannen**" aktiviert ist.

3. Definieren Sie "**Ausführbare Dateien auf der Weißliste**", die auf beliebige Dateien zugreifen können. Der Virenscan blockiert keinen Dateizugriff, der von ausführbaren Dateien erfolgt, die in der Weißliste aufgeführt sind.

Hinweis: Stellen Sie sicher, dass die ausführbare Datei, die Sie als Anwendung der Weißliste hinzufügen, vertrausenswürdig ist. Es wird empfohlen, den Dateizugriff für Anwendungen der Weißliste einzuschränke. Das Hinzufügen einer Anwendung zur Weißliste ist immer ein Sicherheitsrisiko und sollte mit Vorsicht eingesetzt werden.

4. Wenn Sie die Weißlisteneinstellung mit *Integritätsprüfung* verwenden möchten, aktivieren Sie "**Ausführbare Dateien auf der Weißliste müssen mit der Grundlinie übereinstimmen**", um festzulegen, dass in der Weißliste aufgeführte ausführbare Dateien unverändert in der *Liste "Bekannte Dateien"* vorhanden sein müssen. Wenn diese Einstellung aktiviert ist und die ausführbare Datei nicht in der Baseline der Integritätsprüfung gefunden wird, wird sie nicht auf der Weißliste aufgeführt.

   Hinweis: Wenn Sie Anwendungen für die Weißliste definiert haben, wird dringend empfohlen, diese Option zu aktivieren.

5. Wenn Sie Dateien immer scannen möchten, wenn sie geöffnet werden, aktivieren Sie "**Scannen beim Öffnen einer Datei**".
6. Wenn Sie Dateien immer scannen möchten, wenn sie geschlossen werden, aktivieren Sie "**Scannen beim Schließen einer Datei**".
7. Wenn Sie Dateien immer scannen möchten, sobald sie ausgeführt werden, aktivieren Sie "**Scannen beim Ausführen einer ausführbaren Datei**".

Hinweis: Es können nur reguläre Dateien auf gemounteten Dateisystemen gescannt werden. Besondere Dateien wie beispielsweise von CD-ROM oder von DAT-Geräten (/dev/st0, /dev/hda u. Ä.) können erst als gemountete Dateisysteme gescannt werden. Die Dateien können auch zuerst vom Band auf ein Dateisystem extrahiert werden.

Scannen von Archiven

Beim Scannen von Archiven werden Dateien gescannt, die in komprimierten Archiven vom Typ `ZIP`, `ARJ`, `LZH`, `RAR`, `CAB`, `TAR`, `BZ2`, `GZ`, `JAR` und `TGZ` enthalten sind.

Klicken Sie auf der Seite "**Ich möchte...**" in der Webbenutzerschnittstelle auf "**Erweiterte Einstellungen ändern...**", um erweiterte Virenscan-Einstellungen anzuzeigen und zu konfigurieren.

1. Aktivieren Sie "**Archive scannen**", wenn in Archiven enthaltene Dateien gescannt werden sollen.

   Hinweis: Wenn das Scannen von Archiven aktiviert ist, unterbrechen einige E-Mail-Clients möglicherweise die Verarbeitung weiterer E-Mails, wenn eine infizierte E-Mail geöffnet wird.

2. Legen Sie unter "**Maximalzahl verschachtelter Archive**" die Anzahl der Verschachtelungsebenen fest, die das Produkt in Archiven scannt. Verschachtelte Archive sind Archive, die in anderen Archiven enthalten sind.
3. Wählen Sie aus, wie passwortgeschützte Archive behandelt werden. Passwortgeschützte Archive können nicht auf Viren gescannt werden.
   - Deaktivieren Sie "**Passwortgeschützte Archive als sicher behandeln**", um den Zugriff auf passwortgeschützte Archive zu sperren. Der Benutzer, der das passwortgeschützte Archiv öffnet, sollte über einen aktuellen Virenschutz auf der Arbeitsstation verfügen, wenn passwortgeschützte Archive als sicher behandelt werden.
   - Aktivieren Sie "**Passwortgeschützte Archive als sicher behandeln**", damit Benutzer auf Archive zugreifen können.
4. Wenn das Scannen eines Archivs sofort angehalten werden soll, sobald eine infizierte Datei gefunden wird, aktivieren Sie "**Bei der ersten Infektion im Archiv anhalten**". Wenn diese Einstellung deaktiviert ist, scannt das Produkt das gesamte Archiv.

Riskware-Scanning

Legen Sie die primären und sekundären Aktionen fest, die durchgeführt werden, wenn Riskware gefunden wird.

Klicken Sie auf der Seite "**Ich möchte...**" in der Webbenutzerschnittstelle auf "**Erweiterte Einstellungen ändern...**", um erweiterte Virenscan-Einstellungen anzuzeigen und zu konfigurieren.

1. Wählen Sie die primäre Aktion aus, die durchgeführt wird, wenn Riskware gefunden wird. Wählen Sie eine der folgenden Aktionen aus:
   - Wählen Sie "**Bericht und Zugriff sperren**" aus, um eine Alarmmeldung über die gefundene Riskware anzuzeigen und den Zugriff auf die Datei zu blockieren. Für die infizierte Datei werden keine weiteren Maßnahmen getroffen. Zeigen Sie die "**Alarmmeldungen**" an, um die Sicherheitsalarmmeldungen zu prüfen.
   - Wählen Sie "**Umbenennen**" aus, um die Riskware-Datei umzubenennen und die Berechtigungen zum Ausführen zu entfernen. Die umbenannte Datei bleibt auf dem Computer, kann aber keinen Schaden anrichten. Die umbenannte Datei hat die Erweiterung "`.riskware`".
   - Wählen Sie "**Löschen**" aus, um die Riskware-Datei zu löschen.
   - Wählen Sie "**Zugriff sperren**" aus, um den Zugriff auf die Riskware-Datei zu blockieren, ohne eine Warnmeldung zu senden oder einen Bericht zu erstellen.
   - Wählen Sie "**Nur Bericht**" aus.

   Standardmäßig ist die primäre Aktion bei infizierten Dateien "**Nur Bericht**".
2. Wählen Sie die sekundäre Aktion aus. Die sekundäre Aktion wird durchgeführt, wenn die primäre Aktion nicht durchgeführt werden kann.
   Standardmäßig ist die sekundäre Aktion "**Zugriff sperren**".
3. Geben Sie im Feld "**Ausgeschlossene Riskware**" Riskware-Typen an, die das Produkt nicht scannen soll.

   Verwenden Sie folgendes Format, um Riskware anzugeben, die Sie ausschließen möchten, und trennen Sie die Einträge durch einen Strichpunkt (;)`Category.Platform.Family`, wo Kategorie, Plattform oder Familie der Platzhalter * sein kann.

   "`Client-IRC.*.*`" schließt z. B. sämtliche Riskware-Einträge in der Kategorie "Client-IRC" aus.

Nach der Konfiguration der Einstellungen für das Riskware-Scanning müssen Sie auf der Seite "**Alarmmeldungen**" konfigurieren, wie Alarmmeldungen und Berichte behandelt werden.

Manuelles Scannen des Computers

Sie können den Computer manuell auf Viren scannen und so sicherstellen, dass alle angegebenen Dateien oder alle prüfbaren Dateien auf Viren geprüft werden.

Maßnahme bei Vireninfektion während manuellem Scan

Wählen Sie die primäre und sekundäre zu ergreifende Maßnahme aus, wenn ein Virus während eines manuellen Scans gefunden wird.

Klicken Sie auf der Seite "**Ich möchte...**" auf der Webbenutzeroberfläche auf "**"Erweiterte Einstellungen" ändern...**", um die erweiterten Virenscan-Einstellungen anzuzeigen und zu konfigurieren.

1. Wählen Sie die primäre zu ergreifende Maßnahme aus, wenn ein Virus gefunden wird. Wählen Sie eine der folgenden Maßnahmen:
   - Wählen Sie **Desinfizieren**, um Viren desinfizieren. Einige Viren können nicht desinfiziert werden. Wenn der Virus nicht desinfiziert werden kann, bleibt der Zugriff auf die infizierte Datei blockiert.
   - Wählen Sie **Umbenennen**, um die infizierte Datei umzubenennen und die Ausführungsbrechtigungen zu löschen. Die umbenannte infizierte Datei bleibt auf dem Computer, kann jedoch keinen Schaden anrichten. Die umbenannte Datei hat die Erweiterung `.virus`.
   - Wählen Sie **Löschen**, um die infizierte Datei zu löschen.

Die standardmäßige primäre Maßnahme für Infektionen ist "**Desinfizieren**".

2. Wählen Sie die sekundäre Maßnahme aus. Die sekundäre Maßnahme wird durchgeführt, wenn die primäre nicht durchgeführt werden kann.
   Die standarmäßig eingestelle sekundäre Maßnahme ist "**Umbenennen**".

Nachdem Sie die Maßnahmen für eine Vireninfektion konfiguriert haben, konfigurieren Sie auf der Seite "**Alarmmeldungen**", wie Alarmmeldungen und Berichte gehandhabt werden.

Bei manuellem Scan erkannte verdächtige Dateien

Wählen Sie die primäre und sekundäre zu ergreifende Maßnahme aus, wenn das heuristische Scan-Modul eine verdächtige Datei bei der manuellen Prüfung findet.

Klicken Sie auf der Seite "**Ich möchte...**" in der Webbenutzeroberfläche auf "**Erweiterte Einstellungen ändern...**", um erweiterte Einstellungen für den Viren-Scan anzuzeigen und zu konfigurieren.

1. Wählen Sie die primäre zu ergreifende Maßnahme aus, wenn ein heuristisches Scan-Modul eine verdächtige Datei finden. Wählen Sie eine der folgenden Maßnahmen:
   - Wählen Sie **Umbenennen** aus, um die verdächtige Datei umzubenennen und ihre Ausführungsberechtigungen zu entfernen. Umbenannte verdächtige Dateien verbleiben auf dem Computer, können jedoch keinen Schaden anrichten. Die umbenannte Datei erhält die Erweiterung `.suspected`.
   - Wählen Sie "**Löschen**" aus, um die verdächtige Datei zu löschen.

   Standardmäßig ist die primäre Maßnahme für verdächtige Dateien "**Nur Berichten**".
2. Wählen Sie die sekundäre Maßnahme aus. Die sekundäre Maßname wird durchgeführte, wenn die primäre nicht durchgeführt werden kann.

Nachdem Sie die Einstellungen für verdächtige Dateien konfiguriert haben, konfigurieren Sie auf der Seite "**Alarmmeldungen**", wie Alarmmeldungen und Berichte gehandhabt werden sollen.

Geben Sie an, was während des manuellen Scanvorgangs überprüft werden soll.

Geben Sie die Dateien und Verzeichnisse an, die Sie auf Malware scannen möchten, wenn Sie einen Scanvorgang manuell ausführen.

Klicken Sie auf der Seite " **Ich möchte...**" in der Webbenutzeroberfläche auf **Erweiterte Einstellungen ändern...**", um erweiterte Einstellungen für den Viren-Scan anzuzeigen und zu konfigurieren.

1. Wählen Sie unter "**Dateien überprüfen**" aus, ob bei einem manuellen Scan alle Dateien oder nur Dateien mit bestimmten Erweiterungen überprüft werden sollen.
   Wenn Sie für den Scan "**Nur Dateien mit bestimmten Erweiterungen**" auswählen, wird das Feld "**Erweiterungen einschließen**" angezeigt. Geben Sie Dateierweiterungen an, die überprüft werden sollen, durch Kommas (,) getrennt ein.
2. Geben Sie "**Vom Scan ausgeschlossene Dateien und Verzeichnisse**" an, um Dateien und Verzeichnisse anzugeben, die vom Scan ausgeschlossen werden sollen. Geben Sie jedes Verzeichnis in eine neue Zeile ein, nur ein Verzeichnis je Zeile.

   Wenn die Überprüfung eines bestimmten Verzeichnisses viel Zeit in Anspruch nimmt und Sie wissen, dass kein Benutzer eine infizierte Datei erstellen oder in das Verzeichnis kopieren kann oder Sie falsche Alarmmeldungen beim Scan bekommen, können Sie das Verzeichnis vom Viren-Scan ausschließen.

   Tipp: Die Liste kann auch Dateien enthalten, wenn Sie bestimmte Datei von dem Scan ausschließen möchten.

3. Wenn Sie neben ausführbaren Dateien keine anderen Dateien auf Viren überprüfen möchten, aktivieren Sie "**Nur ausführbare Dateien überprüfen**". Deaktivieren Sie das Kontrollkästchen, um alle angegebenen Dateien auf Viren zu überprüfen.

   Hinweis: Wenn "**Beim Öffnen überprüfen**" und "**Bei Ausführung überprüfen**" deaktiviert sind, erfolgt kein Scan, selbst wenn "**Nur ausführbare Dateien überprüfen**" aktiviert ist.

4. Wenn Sie nicht möchten, dass durch den manuellen Scan die Zeitangabe für den letzen Zugriff nicht geändert wird, aktivieren Sie das Kontrollkästchen "**Zugriffszeit beibehalten**".

   Hinweis: Es können nur reguläre Dateien auf gemounteten Dateisystemen gescannt werden. Besondere Dateien wie beispielsweise von CD-ROM oder von DAT-Geräten (/dev/st0, /dev/hda u. Ä.) können erst als gemountete Dateisysteme gescannt werden. Die Dateien können auch zuerst vom Band auf ein Dateisystem extrahiert werden.

Scannen von Archiven

Beim Scannen von Archiven werden Dateien gescannt, die in komprimierten Archiven vom Typ `ZIP`, `ARJ`, `LZH`, `RAR`, `CAB`, `TAR`, `BZ2`, `GZ`, `JAR` und `TGZ` enthalten sind.

Klicken Sie auf der Seite "**Ich möchte...**" in der Webbenutzerschnittstelle auf "**Erweiterte Einstellungen ändern...**", um erweiterte Virenscan-Einstellungen anzuzeigen und zu konfigurieren.

1. Aktivieren Sie "**Archive scannen**", wenn in Archiven enthaltene Dateien gescannt werden sollen.

   Hinweis: Wenn das Scannen von Archiven aktiviert ist, unterbrechen einige E-Mail-Clients möglicherweise die Verarbeitung weiterer E-Mails, wenn eine infizierte E-Mail geöffnet wird.

2. Legen Sie unter "**Maximalzahl verschachtelter Archive**" die Anzahl der Verschachtelungsebenen fest, die das Produkt in Archiven scannt. Verschachtelte Archive sind Archive, die in anderen Archiven enthalten sind.
3. Wählen Sie aus, wie passwortgeschützte Archive behandelt werden. Passwortgeschützte Archive können nicht auf Viren gescannt werden.
   - Deaktivieren Sie "**Passwortgeschützte Archive als sicher behandeln**", um den Zugriff auf passwortgeschützte Archive zu sperren. Der Benutzer, der das passwortgeschützte Archiv öffnet, sollte über einen aktuellen Virenschutz auf der Arbeitsstation verfügen, wenn passwortgeschützte Archive als sicher behandelt werden.
   - Aktivieren Sie "**Passwortgeschützte Archive als sicher behandeln**", damit Benutzer auf Archive zugreifen können.
4. Wenn das Scannen eines Archivs sofort angehalten werden soll, sobald eine infizierte Datei gefunden wird, aktivieren Sie "**Bei der ersten Infektion im Archiv anhalten**". Wenn diese Einstellung deaktiviert ist, scannt das Produkt das gesamte Archiv.

Riskware bei manuellem Scan gefunden

Wählen Sie die primäre und sekundäre zu ergreifende Maßnahme, wenn Riskware beim manuellen Scan gefunden wird.

Klicken Sie auf der Seite "**Ich möchte...**" der Webbenutzeroberfläche auf **Erweiterte Einstellungen ändern...**, um erweiterte Einstellungen für den Virenscan anzuzeigen und zu konfigurieren.

1. Wählen Sie die primäre zu ergreifende Maßnahme, wenn Riskware gefunden wird. Wählen Sie eine der folgenden Maßnahmen:
   - Wählen Sie "**Umbenennen**", um die Riskware-Datei umzubenennen und die Ausführungsbrechtigungen zu entfernen. Die umbenannte Datei verbleibt auf dem Computer, kann jedoch keinen Schaden anrichten. Die umbenannte Datei hat die Erweiterung `.riskware`.
   - Wählen Sie "**Löschen**", um die Riskware-Datei zu löschen.
   - Wählen Sie **Nur berichten** aus.

   Die standarmäßige primäre Maßnahme für Infektionen ist "**Nur berichten**".
2. Wählen Sie die sekundäre Maßnahme aus. Die sekundäre Maßnahme wird durchgeführt, wenn die primäre Maßnahme nicht durchgeführt werden kann.
3. Geben Sie im Feld "**Ausgeschlossene Riskware**" die Riskware-Typen an, die nicht gescannt werden sollen.

Verwenden Sie folgendes Format, um Riskware anzugeben, die ausgeschlossen werden soll, und trennen Sie jeden Eintrag durch ein Semikolon (;) `Category.Platform.Family`, wobei Kategorie, Plattform oder Famile der Platzhalter * sein können.

Beispiel: `Client-IRC.*.*` schließt alle Riskware-Einträge in der Kategror "Client-IRC" aus.

Nachdem Sie die Einstellungen für den Scan von Riskware vorgenommen haben, konfigurieren Sie auf der Seite "**Alarmmeldungen**", wie Alarmmeldungen und Berichte gehandhabt werden.

Scannen des Computers zu festgelegten Zeitpunkten

Mit geplanten Scan-Vorgängen können Sie den Computer in regelmäßigen Abständen auf *Malware* scannen - beispielsweise täglich, wöchentlich oder monatlich.

Erstellen einer geplanten Scan-Aufgabe

Erstellen Sie geplante Scan-Aufgaben, um den Computer in regelmäßigen Abständen auf *Malware* zu scannen.

Klicken Sie auf der Seite "**Ich möchte...**" in der Webbenutzerschnittstelle auf "**Erweiterte Einstellungen ändern...**", um erweiterte Virenscan-Einstellungen anzuzeigen und zu konfigurieren.

Beachten Sie, dass für geplante Scan-Aufgaben die Einstellungen für **Manuelles Scanning** verwendet werden. So legen Sie den Scan-Zeitplan fest:

1. Klicken Sie auf "**Neue Aufgabe hinzufügen**".
2. Legen Sie das Datum und die Uhrzeit des Zeitpunkts fest, zu dem der geplante Scan-Vorgang beginnen soll.
   Einstellungen werden auf dieselbe Weise definiert wie reguläre Cron-Tabelleneinträge. Beispiel:
   - Die Aufgabe soll jeden Sonntag um 4:00 Uhr ausgeführt werden:
     `Minute: 0, Hour: 4, Day of the Month: *, Month: *, Day of the Week: sun`
   - Die Aufgabe soll jeden Tag um 5:30 Uhr ausgeführt werden:
     `Minute: 30, Hour: 5, Day of the Month: *, Month: *, Day of the Week: *`

   Hinweis: Benutzen Sie die folgenden Werte für den Wochentag:

   - Mon or 1 = Montag
   - Tue or 2 = Dienstag
   - Wed or 3 = Mittwoch
   - Thu or 4 = Donnerstag
   - Fri oder 5 = Freitag
   - Sat or 6 = Samstag
   - Sun or 7 (or 0) = Sonntag

   Benutzen Sie * für eine Aufgabe, die an jedem Wochentag ausgeführt werden soll.
3. Fügen Sie die Verzeichnisse, gescannt werden sollen, zum Feld "**Zu scannende Verzeichnisse**" hinzu. Fügen Sie ein Verzeichnis pro Zeile hinzu.
4. Klicken Sie auf "**Aufgabe speichern**", um den geplanten Scan-Vorgang zum Zeitplan hinzuzufügen.

Ein geplanter Scan-Vorgang kann mehrere Stunden dauern. Deshalb ist es ratsam, den Vorgang auszuführen, wenn das Verkehrsaufkommen auf den Hosts gering ist, wie beispielsweise nachts. Eine weitere Alternative besteht darin, mehrere geplante Scan-Aufgaben zu konfigurieren und nur einige Verzeichnisse gleichzeitig zu scannen.

Konfigurieren Sie auf der Seite "**Alarmmeldungen**", wie Alarmmeldungen und Berichte behandelt werden.

Schutz durch Firewall

Die Firewall schützt den Computer vor unsicherem Datenverkehr mit dem Internet sowie vor Angriffen aus dem lokalen Netzwerk.

Das Produkt:

- Schützt vor Hackern, die versuchen, unberechtigt auf den Computer zuzugreifen. Dabei kann z. B. versucht werden, persönliche Daten, wie Dateien, Passwörter oder Kreditkartennummern, zu stehlen.
- Bietet Schutz gegen Informationsdiebstahl, da unbefugte Zugriffsversuche verhindert und rechtzeitig erkannt werden.

Die Firewall schützt den Computer automatisch, sobald das Produkt installiert ist.

Was ist eine Firewall?

Die *Firewall* schützt den Computer, indem sie sicheren Datenverkehr mit dem Internet zulässt und unsicheren Datenverkehr blockiert.

In der Regel lässt die *Firewall* den Datenverkehr von Ihrem Computer in das Internet zu, blockiert aber den gesamten Datenverkehr aus dem Internet auf Ihren Computer, sofern Sie diesen nicht ausdrücklich zulassen. Indem eingehender Datenverkehr blockiert wird, verhindert die Firewall, dass *schädliche Software*, z. B. *Würmer*, auf Ihren Computer gelangen oder dass Eindringlinge auf Ihren Computer zugreifen können.

Der Computer wird durch die vordefinierten *Firewall*-Einstellungen geschützt. Diese müssen in der Regel nicht geändert werden. Wenn Sie jedoch eine sehr strenge *Sicherheitsstufe* verwenden oder wenn Sie eigene *Firewall-Regeln* oder Dienste hinzugefügt haben, müssen Sie die Einstellungen möglicherweise anpassen.

Vorsicht: Deaktivieren Sie die *Firewall* nicht. Wenn Sie sie deaktivieren, ist der Computer nicht gegen Netzwerkangriffe geschützt.

Was sind Sicherheitsprofile?

Firewall-*Sicherheitsprofile* legen die Schutzstufe für Ihren Computer fest.

Jedes *Sicherheitsprofil* hat einen vordefinierten Satz *Firewall-Regeln,* die festlegen, welcher Typ von Datenverkehr für Ihren Computer zugelassen oder abgewiesen wird. Zu einigen Stufen können Sie selbst erstellte Regeln hinzufügen.

In der folgenden Tabelle finden Sie eine Liste der Sicherheitsprofile, die Ihnen in diesem Produkt zur Verfügung stehen, sowie die Verkehrstypen, die jeweils zugelassen oder abgelehnt werden.

Sicherheitsprofil	Beschreibung
Alle blockieren	Der gesamte Netzwerkdatenverkehr wird blockiert (mit Ausnahme der Testschleife).
Server	Ermöglicht nur IP-Konfiguration über DHCP, DNS-Lookups und SSH-Protokoll-Ein- und -Ausgang. **Wichtig:** Das Serverprofil muss vor der Verwendung angepasst werden.
Mobil	Lässt normales Web-Browsing und Dateiabrufe (HTTP, HTTPS, FTP) zu sowie E-Mail- und Usenet News-Datenverkehr. Auch verschlüsselte Programme, wie VPN und SSH, werden zugelassen. Alles andere wird blockiert. Nach dem Erkennen von schädlichen Datenpaketen können lokale Regeln hinzugefügt werden.

Sicherheitsprofil	Beschreibung
Home	Erlaubt den gesamten ausgehenden TCP-Datenverkehr und FTP-Dateiabrufe. Alles andere wird blockiert. Es können lokale Regeln hinzugefügt werden, um neue Netzwerkfunktionen zuzulassen.
Office	Lässt ausgehenden TCP-Datenverkehr und FTP-Dateiabrufe zu. Alles andere wird standardmäßig blockiert. Mit diesem Profil sollte zwischen 0.0.0.0/0 und dem Host eine Firewall vorhanden sein.
Strikt	Lässt ausgehendes Web-Browsing, E-Mail- und News-Datenverkehr, verschlüsselte Kommunikation, FTP-Dateiübertragungen und Remote-Updates zu. Alles andere wird blockiert.
Normal	Lässt den gesamten ausgehenden Datenverkehr zu und blockiert bestimmte eingehende Dienste.
Deaktiviert	Lässt den gesamten eingehenden und ausgehenden Netzwerkdatenverkehr zu.

Welcher Zusammenhang besteht zwischen Sicherheitsprofilen und Firewall-Regeln und -Diensten?

Ein *Sicherheitsprofil* besteht aus mehreren *Firewall-Regeln*. Eine *Firewall-Regel* besteht aus mehreren *Firewall-Dienste*. Dienste werden durch die verwendeten *Protokolle* und *Ports* definiert.

Das Sicherheitsprofil "**Normal**" enthält z. B. eine Firewall-Regel namens **Web-Browsing**. Diese Regel erlaubt, dass Sie das Web durchsuchen. Die Regel enthält die Dienste, die für Web-Browsing benötigt werden, wie den Dienst **HTTP (HyperText Transfer Protocol)**. Dieser Dienst verwendet TCP *und Port* Nummer 80.

Firewall-Schutzstufe ändern

Über die Firewall-Schutzstufen können Sie Ihre Firewall-Regeln unmittelbar ändern.

1. Öffnen Sie die Seite "**Ich möchte...**" in der Webbenutzerschnittstelle
2. Wählen Sie die Stufe aus, die für den **Schutz durch Firewall** verwendet wird.

Bearbeiten des Sicherheitsprofils

Für einzelne Benutzer können unterschiedliche Sicherheitsprofile zugewiesen und bearbeitet werden.

Jedes Sicherheitsprofil hat mehrere vorkonfigurierte Firewall-Regeln.

1. Wählen Sie das zu bearbeitende Firewall-Profil aus. Sie können das aktuelle Sicherheitsprofil auf der Seite "**Zusammenfassung**" ändern.

   Das aktuelle Sicherheitsprofil wird oben auf der Seite "**Firewall-Regeln**" angezeigt.
2. In der Liste der Regeln werden die derzeit verwendeten Regeln angezeigt. So können Sie den Regelsatz bearbeiten:
   - Deaktivieren Sie das Kontrollkästchen "**Aktiviert**", um eine Regel vorübergehend zu deaktivieren.
   - Mithilfe der nach oben und unten weisenden Pfeiltasten können Sie die Reihenfolge der Regeln innerhalb dieser Liste ändern.

     Hinweis: Das Ändern der Reihenfolge der Regeln wirkt sich u. U. auf alle anderen Regeln aus.
   - Klicken Sie auf "**X**", um die Regel dauerhaft zu löschen.

- Zur Bearbeitung einer Regel wählen Sie diese aus der Liste der Regeln aus. Die ausgewählte Regel wird nun unterhalb der Regelliste im Fensterbereich "**Regel bearbeiten**" angezeigt.

3. Falls das Profil mehr als 10 Regeln enthält, können Sie mithilfe der Pfeiltasten **<<**, **<**, **>** und **>>** durch die Regeln blättern.

Firewall-Regeln

Firewall-Regeln definieren, welche Arten von Datenverkehr mit dem Internet zugelassen oder blockiert werden.

Jede *Sicherheitsstufe* hat einen vordefinierten Satz von *Firewall-Regeln*, die nicht geändert werden können. Die ausgewählte Sicherheitsstufe wirkt sich auf die Priorität aus, die Ihre eigenen Regeln im Vergleich zu vordefinierten Regeln erhalten.

Eine *Firewall-Regel* kann auf Datenverkehr angewendet werden, der aus dem Internet auf Ihren Computer gelangt (eingehend) oder der von Ihrem Computer in das Internet geht (ausgehend). Eine Regel kann auch gleichzeitig für beide Richtungen angewendet werden.

Eine *Firewall-Regel* besteht aus*Firewalldienste*, die den Typ des Datenverkehrs und die *Ports* festlegen, die der Datenverkehr verwendet. Eine Regel namens **Web-Browsing** hat beispielsweise einen Dienst namens **HTTP**, der TCP und den *Port* Nummer 80 verwendet.

Firewall-Regeln definieren außerdem, ob Firewall-*Alarm*-Popups angezeigt werden, wenn bestimmter Datenverkehr mit den *Firewall-Regeln* übereinstimmt.

Wann muss eine neue *Firewall-Regel* hinzugefügt werden?

Möglicherweise müssen Sie eine neue Firewall-Regel hinzufügen, wenn Sie bestimmten blockierten Datenverkehr zulassen oder bestimmten Datenverkehr mit dem Internet blockieren möchten.

Indem Sie alle von dem Programm oder Gerät benötigten Dienste zu derselben Regel hinzufügen, können Sie problemlos:

- aktivieren oder deaktivieren Sie die Regel später
- entfernen Sie die Regel, wenn Sie das Programm deinstallieren oder das Gerät entfernen.

Sie müssen außerdem eine neue Regel hinzufügen, wenn Sie einen bestimmten Datenverkehrstyp abgelehnt haben, diesen aber für bestimmte IP-Adressen zulassen möchten. In diesem Fall existiert bereits eine allgemeine Ablehnungsregel in den *Firewall-Regeln*. Um den Datenverkehr für bestimmte IP-Adressen zuzulassen, müssen Sie eine spezifischere Zulassungsregel erstellen.

Firewall-Dienste

Firewall-Dienste definieren den Typ des Datenverkehrs, für den eine *Firewall-Regel* angewendet wird.

Netzwerkdienste, wie Web-Browsing,*Dateifreigabe* oder *Remote-Zugriff auf die Konsole*, sind Beispiele für solche Firewall-Dienste.

Ein Dienst verwendet ein bestimmtes *Protokoll* und einen bestimmten *Port*. Beispiel: Der HTTP-Dienst verwendet das *Protokoll* TCP und den *Port* Nummer 80.

Ein Firewall-Dienst verwendet zwei Arten von Ports:

- *Ausgangspartei-Port*: der *Port* auf dem Computer, der die Verbindung startet.
- *Antwortpartei-Port*: der *Port* auf dem Computer, bei dem die Verbindung endet.

Ob der *Port* auf dem Computer ein *Ausgangspartei-Port* oder *Antwortpartei-Port* ist, hängt von der Richtung des Datenverkehrs ab:

- Wenn der *Firewall-Dienst* für ausgehenden Datenverkehr ist, ist der *Ausgangspartei-Port* der *Port* auf Ihrem eigenen Computer. Der *Antwortpartei-Port* ist dann der *Port* auf einem Remote-Computer.
- Wenn der *Firewall-Dienst* für eingehenden Datenverkehr ist, ist der *Ausgangspartei-Port* der *Port* auf einem Remote-Computer. Der *Antwortpartei-Port* ist dann der *Port* auf Ihrem eigenen Computer.

Die *Antwortpartei-Ports* werden in der Regel in der Softwaredokumentation angegeben. Beim *Ausgangspartei-Port* handelt es sich in der Regel um alle *Port*s oberhalb von 1023. Für einige Spiele müssen jedoch bestimmte *Ausgangspartei-Ports* definiert werden. In diesem Fall finden Sie entsprechende Angaben in der Softwaredokumentation.

Wenn Sie eine neue*Firewall-Regel* erstellen, stehen Ihnen verschiedene vordefinierte Dienste zur Verfügung, die Sie zur Regel hinzufügen können. Sie können auch eigene Dienste erstellen und hinzufügen, falls sich der benötigte Dienst nicht in der Liste befindet.

Erstellen von Firewall-Diensten und -Regeln

Wenn Sie blockierten Datenverkehr zulassen möchten oder wenn Sie bestimmten Datenverkehr blockieren möchten, können Sie neue Firewall-Dienste und -Regeln erstellen. Wenn Sie Firewall-Regeln erstellen oder bearbeiten, sollten Sie nur die erforderlichen Dienste zulassen und den Rest verweigern, um Sicherheitsrisiken zu minimieren.

Um den Firewall-Assistenten zu verwenden, wechseln Sie zu "**Allgemeine Aufgaben**", klicken Sie auf "**Eine Firewall-Regel erstellen**, befolgen Sie die Anweisungen auf dem Bildschirm und beenden Sie den Assistenten.

Befolgen Sie diese Anweisungen, um einen neuen Dienst und eine neue Regel über die erweiterte Benutzeroberfläche zu erstellen:

1. Erstellen Sie einen neuen Dienst.
   a) Wählen Sie die **Netzwerkdienste** im Menü "**Erweiterter Modus**" aus.
   b) Definieren Sie im Feld "**Dienstname**" einen eindeutigen Namen für den Dienst.
   c) Geben Sie im Feld "**Beschreibung**" einen beschreibenden Kommentar ein, um eine Abgrenzung zu ermöglichen.
   d) Wählen Sie aus der Dropdown- Liste "**Protokoll**" eine Protokollnummer für den Dienst aus.

      Falls Ihr Dienst keines der Protokolle ICMP, TCP oder UDP verwendet, wählen Sie "Numerisch" aus und geben Sie die Protokollnummer in dem dafür vorgesehenen Feld ein.
   e) Wenn Ihr Dienst das TCP- oder UDP-Protokoll verwendet, definieren Sie die "**Initiatorports**, die der Dienst verwendet.
   f) Wenn Ihr Dienst das TCP- oder UDP-Protokoll verwendet, müssen Sie die **Antwortpartei-Ports** festlegen, die der Dienst abdeckt.
   g) Klicken Sie auf "**Als neuen Dienst hinzufügen**", um den Dienst zur Liste der Netzwerkdienste hinzuzufügen.
   h) Klicken Sie auf "**Speichern**".
      Der neue Dienst wird in der Dienstliste gespeichert.
2. Erstellen Sie eine neue Regel für den Dienst.
   a) Wählen Sie im Menü "**Erweiterter Modus**" den Eintrag "**Firewall-Regeln**" aus, um eine Firewall-Regel zu erstellen, die den von Ihnen definierten Dienst verwendet.
   b) Wählen Sie das Profil aus, dem Sie eine neue Regel hinzufügen möchten, und klicken Sie auf "**Neue Regel hinzufügen**", um eine neue Regel zu erstellen.
   c) Wählen Sie "**Annehmen**" oder "**Ablehnen**" als **Typ** für die Regel aus, um festzulgegen, ob der Dienst von der Regel zugelassen oder abgelehnt wird.
   d) Geben Sie Details zu Zieladressen in das Feld "**Remote-Host**" ein. Geben Sie die IP-Adressen und das Teilnetz im Bit-Netzmaskenformat ein.
      Beispiel: `192.168.88.0/29`

      Sie können folgende Alisase als Zieladresse verwenden:

      - `[myNetwork]` - Das lokale Netzwerk.

- `[myDNS]` - Alle konfigurierten DNS-Server.

e) Geben Sie im Feld "**Beschreibung**" einen beschreibenden Kommentar ein, um eine Abgrenzung zu ermöglichen.

f) Wählen Sie den neu erstellten Dienst im Feld "**Dienst**" aus und geben Sie die Richtung an, für die diese Regel angewendet wird.

- eingehend = Sämtlicher eingehender Verkehr, der aus dem Internet auf Ihrem Computer eingeht.
- ausgehend = Sämtlicher ausgehender Verkehr, der von Ihrem Computer stammt.

g) Wählen Sie die Netzwerkschnittstellen, für die die Regel gilt. Geben Sie die Netzwerkschnittstellen, für die die Regel gelten soll in das Feld "**Flag**" ein. Die Regel wird für alle Netzwerkschnittstellen angewendet, wenn Sie das Feld "**Flag**" leer lassen.
Beispiel: `[if:eth0]`, `[if:eth3]`.

h) Klicken Sie auf "**Dienst zu dieser Regel hinzufügen**".
Der Dienst wird zu der neuen Regel hinzugefügt.

i) Wenn Sie einer Regel keine weiteren Dienste hinzufügen möchten, klicken Sie auf "**Zu Firewall-Regeln hinzufügen**".

Für jede Regel muss mindestens ein Dienst vorliegen. Wenn die Regel einen neuen Dienst enthält, müssen Sie sicherstellen, dass sie die Dienstliste auf der Seite "**Netzwerkdienste**" gespeichert haben.

Die Regel wird zum aktiven Regelsatz der Tabelle "**Firewall-Regeln**" hinzugefügt.

j) Klicken Sie auf "**Speichern**", um die neue Regelliste zu speichern.

Wie funktioniert die Prioritätsreihenfolge der *Firewall-Regeln*?

Firewall-Regeln haben eine Prioritätsreihenfolge, die festlegt, welche Regeln auf Netzwerkdatenverkehr angewendet werden.

Firewall-Regeln werden auf der Seite "**Regeln**" als Liste angezeigt. Die*Regeln* werden von oben nach unten angewendet. Die erste Regel, die zum Datenverkehr passt, wird jeweils angewendet und alle weiteren Regeln werden ignoriert. Das Prinzip basiert darauf, dass nur der erforderliche Datenverkehr zugelassen und jeder andere Datenverkehr blockiert wird. Deshalb ist die letzte Regel einer *Sicherheitsstufe* die "**Alles andere sperren**"-Regel. Sie blockiert den gesamten Datenverkehr, der durch keine der zuvor aufgeführten Regeln explizit zugelassen wurde.

Beispiel für die Arbeitsweise der Prioritätsreihenfolge

Die folgenden Beispiele machen deutlich, wie Sie steuern können, welche Regeln auf bestimmten Datenverkehr angewendet werden, indem Sie die Reihenfolge der Firewall-Regeln ändern.

- Sie haben eine Regel hinzugefügt, die den gesamten ausgehenden *FTP*-Datenverkehr blockiert. Oberhalb der Regel fügen Sie in der Regelliste eine weitere Regel hinzu, die eine *FTP*-Verbindung zur IP-Adresse Ihres Internet Service Providers zulässt. Diese Regel erlaubt Ihnen, eine *FTP*-Verbindung zu dieser IP-Adresse herzustellen.
- Sie haben eine Regel hinzugefügt, die es erlaubt, eine *FTP*-Verbindung zur IP-Adresse Ihres Internet Service Providers herzustellen. Oberhalb der Regel fügen Sie in der Regelliste eine weitere Regel hinzu, die den gesamten *FTP*-Datenverkehr blockiert. Diese Regel verhindert, dass Sie eine *FTP*-Verbindung zur IP-Adresse Ihres Internet Service Providers (oder einer anderen IP-Adresse) herstellen.

Firewall-Einstellungen

Auf der Registerkarte "**Einstellungen**" können Sie Einstellungen für die Protokollierung von Netzwerkpaketen auswählen und vertrauenswürdige Netzwerkschnittstellen konfigurieren.

Protokollieren nicht verarbeiteter Netzwerkpakete

Das Protokollieren nicht verarbeiteter Netzwerkpakete kann sich bei der Problembehebung als nützlich erweisen.

Standardmäßig ist es nicht erforderlich, nicht verarbeitete Netzwerkpakete zu protokollieren.

1. Öffnen Sie die Webbenutzerschnittstelle.
2. Versehen Sie das Kontrollkästchen "**Erweitert**" mit einem Häkchen, um den erweiterten Modus zu aktivieren.
3. Wechseln Sie zu **Schutz durch Firewall** > **Allgemein**.
4. Aktivieren Sie das Kontrollkästchen "**Alle nicht verarbeiteten Netzwerkpakete protokollieren**", damit alle Netzwerkpakete protokolliert werden, die keiner Firewall-Regel entsprechen.

Alle Netzwerkpakete, die nicht mit bestimmten Firewall-Regeln übereinstimmen, werden mithilfe von syslog protokolliert (dies kann je nach verwendeter Linux-Version unterschiedlich sein).

Bearbeiten vertrauenswürdiger Netzwerkschnittstellen

Firewall-Regeln werden auf die erste Netzwerkschnittstelle auf dem Host angewendet; alle anderen Schnittstellen werden blockiert. Wenn weitere Schnittstellen mit vertrauenswürdigen Netzwerken verbunden sind, müssen Sie diese Schnittstellen zur Liste der vertrauenswürdigen Netzwerkschnittstellen hinzufügen.

1. Öffnen Sie die Webbenutzerschnittstelle.
2. Setzen Sie in dem Kontrollkästchen "**Erweitert**" ein Häkchen, um den erweiterten Modus zu aktivieren.
3. Wechseln Sie zu **Schutz durch Firewall** > **Allgemein**.
4. Fügen Sie Netzwerkschnittstellen zur Liste "**Vertrauenswürdige Netzwerkschnittstellen**" hinzu und trennen Sie die einzelnen Einträge durch Kommas.

Jeglicher an vertrauenswürdige Netzwerkschnittstellen gerichtete Datenverkehr ist zulässig.

Integritätsprüfung

Die Integritätsprüfung schützt wichtige Systemdateien vor nicht autorisierten Änderungen.

Mit der Integritätsprüfung können sämtliche Änderungsversuche an geschützten Dateien, unabhängig von den Dateisystemberechtigungen, blockiert werden.

Verwenden Sie die Assistenten für die Integritätsprüfung auf der Seite "**Allgemeine Aufgaben**" zum Generieren und Überprüfen der Dateisystem-Baseline. Die Dateisystem-Baseline schützt Ihren Computer vor nicht autorisierten Dateiänderungen. Für weitere Integritätsprüfungsoptionen können Sie Einstellungen im Modus "**Erweitert**" konfigurieren.

Bei der Integritätsprüfung werden Dateien auf der Festplatte mit den Grunddaten (der so genannten Baseline) verglichen. Dabei handelt es sich um eine kryptografisch gezeichnete Liste von Dateieigenschaften. Die Integritätsprüfung kann so konfiguriert werden, dass Alarmmeldungen bezüglich Änderungsversuchen an überwachten Dateien an den Administrator gesendet werden.

Liste "Bekannte Dateien"

Die *Liste "Bekannte Dateien"* enthält alle Dateien, die vom Produkt überwacht und geschützt werden.

Die Baseline wird anhand der *Liste "Bekannte Dateien"* erstellt. Dazu werden die Eigenschaften der Dateien in der Liste gelesen und das Ergebnis wird kryptografisch gezeichnet. Bei der Integritätsprüfung wird dieses Ergebnis mit dem Echtzeit-Dateizugriff verglichen.

Hinweis: Die *Liste "Bekannte Dateien"* in der Webbenutzeroberfläche zeigt nur den derzeit im Programm gespeicherten Baselinestatus an. Um den tatsächlichen aktuellen Dateisystemstatus anzuzeigen,

verwenden Sie die Operation "Baseline überprüfen" in der Webbenutzeroberfläche oder führen Sie das Befehlszeilenprogramm fsic aus.

Verwenden der Suchfunktion für die Liste "Bekannte Dateien"

Verwenden Sie Suchfilter, um Dateien auszuwählen, die in der *Liste "Bekannte Dateien"* angezeigt werden.

1. Wählen Sie Dateien aus, die in der Liste "Bekannte Dateien" angezeigt werden sollen.
   - Wählen Sie "**Geändert und neu**", um alle Dateien anzuzeigen, die geändert oder zur Baseline hinzugefügt wurden.
   - Wählen Sie "**Geändert**", um alle Dateien anzuzeigen, die geändert wurden.
   - Wählen Sie "**Neu**", um alle Dateien anzuzeigen, die zur Baseline hinzugefügt wurden.
   - Wählen Sie "**Nicht geändert**", um alle Dateien in der Baseline anzuzeigen, die nicht geändert wurden.
   - Wählen Sie "**Alle**", um alle in der Liste "Bekannte Dateien" enthaltenen Dateien anzuzeigen.
2. Wenn Sie die Suche auf den Dateinamen beschränken möchten, geben Sie einen beliebigen Teil des Dateinamens der überwachten Datei, die in der Liste "Bekannte Dateien" angezeigt werden soll, im Feld "**Dateiname**" ein.
3. Klicken Sie auf "**Suchen**".
   Die *Liste "Bekannte Dateien"* enthält die Suchergebnisse.
4. Suchergebnis anzeigen.

Option	Beschreibung
Dateiname	Zeigt den Namen der Datei an.
Erkennungszeitpunkt	Gibt den Zeitpunkt an, zu dem eine Änderung erkannt wurde.
Ermitteltes Änderungsprogramm	Gibt den Dateinamen des Prozesses an, durch den die Datei geändert wurde.
Aktion	Zeigt an, ob die Änderung an der Datei vom Produkt zugelassen oder abgelehnt wird.
Alarm	Zeigt an, ob das Produkt einen Alarm sendet, wenn die Datei geändert wird.
Schutz	Zeigt an, ob die Datei überwacht oder geschützt ist. Geschützte Dateien können nicht geändert werden; überwachte Dateien werden hingegen nur überwacht, können aber geändert werden.

5. Wählen Sie die durchzuführende Aktion aus:
   - Zum erneuten Generieren der Baseline wählen Sie die neuen und geänderten Dateien aus, die Sie als Baseline zusammenfassen möchten, und klicken Sie auf "**Baseline für markierte Dateien neu generieren**".
   - Wenn Sie Dateien aus der Baseline entfernen möchten, klicken Sie zur Auswahl auf die entsprechenden Dateien und klicken Sie auf "**Markierte Dateien entfernen**". Damit werden die ausgewählten Dateien nicht länger überwacht.

Hinweis: Die Integritätsprüfung schützt neue oder bearbeitete Dateien erst nach dem erneuten Generieren der Baseline. Wenn Sie Dateien zur *Liste "Bekannte Dateien"* hinzufügen oder wenn Dateien geändert wurden, müssen Sie die Baseline erneut generieren, um diese Dateien zu schützen.

Hinzufügen von Dateien zur Liste "Bekannte Dateien"

Sie können Dateien zur Liste der bekannten Dateien hinzufügen, um diese vor unerwünschten Änderungen zu schützen.

1. Geben Sie den Namen der Datei, die Sie überwachen möchten, im Feld "**Dateiname**" ein. Bei der Eingabe mehrerer Dateinamen werden diese durch Leerzeichen getrennt.
2. Wählen Sie das gewünschte Schutzverfahren aus.
   - Wählen Sie "**Überwachen**", damit die Datei nur überwacht wird. Eine überwachte Datei kann geändert werden.
   - Wählen Sie "**Schützen**", um alle Änderungen der Datei abzulehnen. Die geschützte Datei kann geöffnet, aber nicht geändert werden.
3. Wählen Sie aus, ob der Zugriff auf die geänderte Datei verhindert wird.
   - Wählen Sie "**Zulassen**", um den Zugriff auf die geänderte Datei zuzulassen, wenn sie ausgeführt oder geöffnet wird.
   - Wählen Sie "**Ablehnen**", um den Zugriff auf die geänderte Datei zu verhindern. Geänderte Dateien können weder geöffnet noch ausgeführt werden.
4. Um Änderungen an bestimmten Attributen der Datei zu ignorieren, aktivieren Sie die entsprechenden Kontrollkästchen unter "**Ignorierte Attribute**":
   - Modus: Änderungen an Dateiberechtigungen werden ignoriert
   - Benutzer: Änderungen des Dateieigentümers werden ignoriert
   - Gruppe: Änderungen an der Dateigruppe werden ignoriert
   - Größe: Änderungen an der Datiegröße werden ignoriert
   - Änderungszeit: Änderungen an der Dateiänderungszeit werden ignoriert
   - Hash: Änderungen am Inhalt der Datei werden ignoriert

   Hinweis: In der Regel ist es nicht wünschenswert, lediglich das Hash-Attribut zu ignorieren, da sich bei einer Änderung des Dateiinhalts meist auch der Änderungskeit und Größe ändern.
5. Klicken Sie auf "**Zu bekannten Dateien hinzufügen**", um den Eintrag zur *Liste "Bekannte Dateien"* hinzuzufügen.

Die Integritätsprüfung schützt neue oder bearbeitete Dateien erst nach dem erneuten Generieren der Baseline. Generieren Sie die Baseline neu, um die hinzugefügten Dateien zu schützen.

Hinweis: Sie können eine einzelne Datei oder mehrere Dateien gleichzeitig zur Baseline hinzufügen.

Softwareinstallationsmodus

Verwenden Sie den Softwareinstallationsmodus, wenn Sie die Systemdateien und Programme ändern möchten.

Durch die Integritätsprüfung werden nicht autorisierte oder ungewollte Änderungen an Systemdateien oder Programmen verhindert. Wenn Sie Ihr Betriebssystem aktualisieren, ein Sicherheits-Update anwenden oder neue Versionen der Software installieren, ist es erforderlich, die Dateien zu ändern, die durch die Integritätsprüfung überwacht werden.

Wenn Sie den Software-Installationsmodus aktivieren, bleiben Echtzeit-Scanning und Warnmeldungen für Malware während der Installation aktiviert.

Nach Abschluss der Installation und Verlassen des Software-Installationsmodus aktualisiert das Produkt die Liste "Bekannte Dateien" mit den neuen Dateien und generiert die neue Baseline. Die Integritätsprüfung und der Rootkit-Schutz werden nach der Generierung der neuen Baseline wieder aktiviert, wenn sie zuvor deaktiviert wurden.

Wichtig: Wenn Sie Software nicht im Softwareinstallationsmodus installieren, ist es möglich, dass Sie die neue Software bei der Überwachung der aktualisierten Dateien durch die Integritätsprüfung nicht installieren oder verwenden können. Die Integritätsprüfung kann beispielsweise verhindern, dass ein Kernel-Update ordnungsgemäß gebootet wird, da neue Treiber nicht in der Baseline vorhanden sind.

Aktivieren des Softwareinstallationsmodus

Aktivieren Sie den Softwareinstallationsmodus, wenn Sie geschützte Dateien aktualisieren oder ändern möchten.

Gehen Sie wie folgt vor, um auf den Softwareinstallationsmodus zuzugreifen.

1. Öffnen Sie die Webbenutzeroberfläche.
2. Wechseln Sie zur Seite "**Ich möchte...**".
3. Klicken Sie auf "**Software installieren**".
   Der Assistent für den Softwareinstallationsmodus wird geöffnet.

Der Assistent für den Softwareinstallationsmodus führt Sie durch die Softwareinstallation und aktualisiert die Baseline mit neuer Software, die Sie auf Ihrem System installieren.

Sie können auch das Befehlszeilentool `fsims` verwenden, um den Software-Installationsmodus über die Shell zu verwenden.

Baseline

Die Integritätsprüfung wird eingerichtet, indem Sie eine Baseline der Systemdateien erstellen, die Sie schützen möchten.

Während der Installation wird ein Standardsatz mit Systemdateien zu der *Liste "Bekannte Dateien"* hinzugefügt. Die Baseline für diese Dateien wird durch diese Standard-Installationsoptionen jedoch nicht automatisch generiert. Verwenden Sie den Parameter `pass=PASS`, um die Baseline während der Installation zu generieren oder generieren Sie sie nach der Installation mithilfe der Webbenutzeroberfläche oder des Befehlszeilenclients (`fsic`).

Alle Dateien, die der Baseline während der Installation hinzugefügt werden, erhalten den Schutzmodus "**Zulassen**" oder "**Alarm**".

Hinweis: Die Standardliste der bekannten Dateien wird bei der Installation generiert und enthält die wichtigsten Systemdateien. Die Dateiliste ist je nach Version unterschiedlich. Führen Sie `/opt/f-secure/fsav/bin/fslistfiles` aus, um die exakte Dateiliste abzurufen.

Baseline-Passphrase

Die Baseline muss gezeichnet werden, um eine Änderung der geschützten Dateien zu verhindern.

Das Produkt führt eine kryptografische Überprüfung der Baseline und der Systemintegrität aus. Es wird ein kryptografischer Algorithmus auf den Inhalt der Baseline und die Passphrase angewendet, um eine Signatur (eine HMAC-Signatur) der als Baseline verwendeten Informationen zu erzeugen.

Wichtig: Gehen Sie bitte sorgfältig mit der Passphrase um. Sie darf nicht vergessen werden, da sie nicht wiederhergestellt werden kann und die Baseline ohne die entsprechende Passphrase nicht auf unerlaubte Änderungen überprüft werden kann.

Hinweis: Alle Administratoren, die die Passphrase kennen, können die Baseline erneut generieren, daher sollte die Weitergabe der Passphrase beschränkt werden.

Baseline überprüfen

Sie können die Baseline manuell überprüfen, um sicherzustellen, dass Ihr System sicher ist und alle als Baseline verwendeten Dateien unverändert sind.

1. Geben Sie zur Überprüfung der Baseline Ihre Passphrase ein.
2. Achten Sie darauf, keine weiteren Integritätsprüfvorgänge zu starten, während das Produkt die Baseline überprüft.

Falls ein Hacker Zugriff auf der Root-Ebene erlangt und die Baseline neu generiert hat, stimmt die Baseline bei der Überprüfung nicht mit Ihrer Passphrase überein.

Allgemeine Einstellungen

In den allgemeinen Einstellungen können Sie die Alarmausgabe und die automatische Aktualisierung der Virendefinitionsdatenbank konfigurieren und die Produktinformationen anzeigen.

Alarmmeldungen

Auf der Seite "Alarmmeldungen" können Sie Alarmmeldungen anzeigen und löschen.

Schweregrade der Alarmmeldungen

Alarmmeldungen werden in verschiedene Schweregrade unterteilt.

Schweregrad	Syslog-Priorität	Beschreibung
Information	Info	Normale Informationen des Hosts über einen Arbeitsvorgang.
Warnung	Warnung	Eine Warnung vom Host. Beispielsweise ein Fehler beim Lesen einer Datei.
Fehler	Fehler	Behebbarer Fehler auf dem Host. Das Update der Virendefinitionsdatenbank ist beispielsweise älter als die vorher zugelassene Version.
Schwerwiegender Fehler	Notfall	Nicht behebbarer Fehler auf dem Host, der die Aufmerksamkeit des Administrators erfordert. Ein Prozess startet beispielsweise nicht oder das Laden eines Kernel-Moduls schlägt fehl.
Sicherheitsalarm	Alarmmeldung	Ein Sicherheitsalarm auf dem Host. Beispielsweise eine Virenalarmmeldung. Die Alarmmeldung enthält Informationen zu der Infektion

Schweregrad	Syslog-Priorität	Beschreibung
		und den durchgeführten Operationen.

Verarbeitung von Alarmmeldungen

Sie können nach bestimmten Alarmmeldungen suchen und diese von bestimmten Hosts löschen.

Befolgen Sie die nachstehenden Anweisungen, um die von Ihnen gesuchten Alarmmeldungen anzuzeigen:

1. Wählen Sie den Status von Sicherheitsalarmmeldungen aus, die Sie anzeigen möchten.
   - Wählen Sie "**Alle**" aus, um alle Alarmmeldungen anzuzeigen.
   - Wählen Sie "**Ungelesen**" aus, um alle ungelesenen Alarmmeldungen anzuzeigen.
   - Wählen Sie "**Gelesen**" aus, um alle bereits angezeigten Alarmmeldungen anzugeben.
2. Wählen Sie den **Schweregrad** von Sicherheitsalarmmeldungen aus, die Sie anzeigen möchten.
3. Sie können gleichzeitig mehrere Meldungen löschen oder als gelesen markieren.
   - Klicken Sie auf "Alarmmeldungen", um diese zu markieren, und klicken Sie auf "**Hervorgehobene Elemente als gelesen markieren**", um sie als gelesene Meldung zu markieren.
   - Klicken Sie auf "**Hervorgehobene Elemente löschen**", um markierte Alarmmeldungen zu löschen.

Hinweis: Sie können gleichzeitig mehrere Meldungen löschen oder als gelesen markieren. Wählen Sie aus, wie alt ein Alarm ist und welchen Schweregrad Alarme aufweisen, die Sie bearbeiten möchten. Klicken Sie auf "Aktion durchführen", um die ausgewählten Nachrichten zu löschen oder als gelesen zu markieren.

Konfiguration von Alarmen

Ändern Sie die Einstellungen für "**Kommunikation**", um zu konfigurieren, wohin die Alarmmeldungen gesendet werden.

Achten Sie im zentral verwalteten Installationsmodus darauf, dass die URL der F-Secure Policy Manager-Server-Adresse im Feld "**Server-Adresse**" richtig angegeben ist. **Zertifikat für Policy Manager Server hochladen**`admin.pub`

1. Geben Sie unter "**Alarmstufe**" an, an wen die Alarme je nach Schweregrad gesendet werden. Sie können einen Alarm senden an:
   - **E-Mail an** - Geben Sie die E-Mail-Adresse an, an die der Alarm in Form einer E-Mail gesendet wird.
   - **Lokal** - Alarm wird in der Webbenutzeroberfläche angezeigt.
   - **Syslog** - Alarm wird im Systemprotokoll vermerkt. Die Syslog-Facility ist LOG_DAEMON und die Alarmpriorität variiert.
   - **Policy Manager** - Alarm wird an F-Secure Policy Manager gesendet.

   Hinweis: Das F-Secure-Panel-Applet in der GNOME-Systemleiste zeigt lokale Alarmmeldungen als Popup-Fenster an.
2. Legen Sie die **E-Mail-Einstellungen** fest.

   Die E-Mail-Einstellungen werden für alle Alarmmeldungen verwendet, die für die Versendung als E-Mail-Alarmmeldung konfiguriert wurden.

   a) Geben Sie im Feld "**Server-Adresse**" die Adresse des SMTP-Servers ein. Sie können entweder den DNS-Namen oder die IP-Adresse des SMTP-Servers verwenden. Als Server-Portnummer wird immer 25 verwendet. Dies kann nicht geändert werden.

> **Hinweis:** Falls der Mail-Server nicht ausgeführt wird oder das Netzwerk nicht funktioniert, können möglicherweise einige E-Mail-Alarmmeldungen verloren gehen. Um dies zu verhindern, konfigurieren Sie den lokalen Mail-Server für Port 25 und verwenden Sie ihn zum Weitergeben von Alarmmeldungen per E-Mail.

b) Geben Sie die vollständige E-Mail-Adresse in das Feld "**Von**" ein (Sender@beispiel.de), die Sie als Absender des Alarms in einer E-Mail-Nachricht verwenden möchten.

c) Geben Sie den **Betreff** der E-Mail-Alarmmeldung an. Verwenden Sie "%DESCRIPTION%" als Betreff, damit eine kurze Beschreibung der Alarmmeldung in der Betreffzeile des Felds "Betreff" ausgegeben wird.

Automatische Updates

Der F-Secure Automatic Update Agent sorgt dafür, dass der Schutz Ihres Computers aktuell bleibt.

Der F-Secure Automatic Update Agent lädt die neuesten Updates auf Ihren Computer herunter, wenn Sie mit dem Internet verbunden sind.

Informationen zum neuesten Update der Virendefinitionsdatenbank finden Sie unter:
http://www.F-Secure.com/download-purchase/updates.shtml

Konfiguration der Optionen für automatische Updates

Konfigurieren Sie automatische Updates, wenn Sie Proxy-Dienste verwenden und steuern möchten, wie das Produkt automatisch Updates der Virendefinitionen abruft.

1. Aktivieren Sie das Kontrollkästchen "**Updates aktiviert**", um automatische Updates der Virendefinitionen zu aktivieren. Automatische Updates sind standardmäßig aktiviert.
2. Konfigurieren von F-Secure Policy Manager-Proxies.

   Die Liste "**Policy Manager-Proxies**" enthält eine Liste mit Update-Quellen für die Virendefinitionsdatenbank und F-Secure Policy Manager-Proxies. Falls keine Update-Server konfiguriert sind, ruft das Produkt die aktuellen Updates der Virendefinitionen automatisch vom F-Secure Update-Server ab.

   a) Zum Hinzufügen einer neuen Adresse in dieser Liste geben Sie im Feld "**PM-Proxy-Adresse**" die URL ein.

   b) Klicken Sie auf "**PM-Proxy hinzufügen** ", um der Liste einen neuen Eintrag hinzuzufügen.
3. Konfigurieren Sie den HTTP-Proxy, wenn Sie für den Zugriff auf das Internet einen Proxy benötigen.

   a) Aktivieren Sie das Kontrollkästchen "**HTTP-Proxy verwenden**", um zum Herunterladen von Datenbank-Updates einen HTTP-Proxy-Server zu verwenden.

   b) Geben Sie im Feld "**HTTP-Proxy-Adresse**" die HTTP-Adresse des Proxy-Servers ein. Verwenden Sie folgendes Format: `http://[username:password@]host[:port]`
   Zum Beispiel: `http://user:password@example.com:8080`
4. Regelmäßige Updates konfigurieren.

   a) Geben Sie im Feld "**Intervall für automatische Updates**" einen Wert (in Minuten) dafür an, wie oft das Produkt die Update-Quellen der Virendefinitionsdatenbank auf neue Updates überprüft.

   b) Geben Sie die Failover-Zeit in Minuten an, zu der eine Verbindung mit den im Feld "**Failover-Zeit (Min.) für Zwischenserver**" angegebenen Update-Servern hergestellt werden soll.

   Falls das Produkt während der angegebenen Zeit keine Verbindung mit den Update-Servern herstellen kann, werden die aktuellen Updates der Virendefinitionen vom F-Secure Update-Server abgerufen, falls die Option "**Abrufen von Updates vom F-Secure Update-Server zulassen**" aktiviert ist.

   c) Aktivieren Sie das Kontrollkästchen für "**Abrufen von Updates vom F-Secure Update-Server zulassen**", damit das Produkt Updates der Virendefinitionen vom F-Secure Update-Server herunterlädt, wenn keine Verbindung zu den angegebenen Update-Servern hergestellt werden kann.

   d) Sie können auswählen, ob nach der Aktualisierung der Virendefinitionsdatenbank automatisch ein Virenscan-Vorgang gestartet werden soll. Beim Virenscan werden alle lokalen Dateien und Verzeichnisse

überprüft, was viel Zeit in Anspruch nehmen kann. Es werden die Einstellungen für manuelles Scanning verwendet. Der Scan-Vorgang wird in der Standardeinstellung nicht automatisch gestartet.

5. Erinnerungen konfigurieren.

a) Falls die Virendefinitionsdatenbank über einen bestimmten Zeitraum nicht aktualisiert wurde, kann das Produkt auch so konfiguriert werden, dass es eine Aufforderung sendet. Zur Aktivierung der Erinnerungen aktivieren Sie das Kontrollkästchen "**Erinnerungen senden**".

Der Schweregrad der Erinnerung ist "Sicherheitsalarmmeldung".

Das Feld für das Datenbankalter wird angezeigt.

b) Legt fest, ab welchem Alter die Virendefinitionsdatenbanken als alt definiert werden (3 bis 30 Tage, der Standardwert liegt bei 7 Tagen). Sobald die Datenbank älter ist als angegeben, wird eine Alarmmeldung als Erinnerung gesendet.

F-Secure Anti-Virus-Proxies

F-Secure Anti-Virus-Proxy bietet eine Lösung für Bandbreitenprobleme in verteilten Installationen des Produkts, indem die Netzwerkbelastung bei langsamen Verbindungen deutlich reduziert wird.

Wenn Sie F-Secure Anti-Virus-Proxy als Update-Quelle verwenden, können F-Secure-Produkte so konfiguriert werden, dass sie Updates der Virendefinitionsdatenbanken von einem lokalen Update-Repository und nicht vom zentralen F-Secure Policy Manager-Server abrufen.

Hinweis: Informationen zur Installation und Konfiguration von F-Secure Anti-Virus-Proxy finden Sie im Kapitel "F-Secure Anti-Virus-Proxy" im Administratorhandbuch für F-Secure Policy Manager.

Info

Auf der Seite "Info" der Webbenutzeroberfläche werden die Lizenzbedingungen, die Nummer der Produktversion und die Datenbankversion angezeigt.

Wenn Sie die Testversion des Produkts verwenden, können Sie auf der Seite "Info" den Schlüsselcode eingeben, um auf die Vollversion zu aktualisieren.

Hinweis: Wenn der Testzeitraum abläuft, bevor Sie auf die Vollversion aktualisieren, müssen Sie das Programm nach Eingabe des Schlüsselcodes neu starten.

Kapitel

6

Fehlerbehebung

Themen:

- *Manuelles Installieren der erforderlichen Kernel-Module*
- *Benutzeroberfläche*
- *F-Secure Policy Manager*
- *Integritätsprüfung*
- *Firewall*
- *Virenschutz*
- *Kompatibilität mit anderen Sicherheitsprodukten*
- *Allgemeine Probleme*

Informationen und Hilfe zu Produkteinrichtung, Problemen und Lösungen für allgemeine Probleme.

Manuelles Installieren der erforderlichen Kernel-Module

Sie müssen die erforderlichen Kernel-Module gegebenenfalls manuell installieren, wenn Sie den Software-Installationsmodus nicht verwendet haben und das System nicht korrekt funktioniert oder wenn einige Hosts bei großen Installationen keine Entwicklungstools oder Kernel-Verzeichnisse enthalten.

Überprüfen Sie, dass die ausgeführte Kernel-Version mit der Version der installierten Kernel-Verzeichnisse übereinstimmt. Die Kernel-Konfiguration muss ebenfalls identisch sein. Bei einigen Ausführungen, wie z. B. älteren SUSE-Ausführungen, müssen Sie möglicherweise `/usr/src/linux` aufrufen und die folgenden Befehle ausführen, damit die Kernel-Verzeichnisse mit dem installierten Kernel übereinstimmen:

```
make cloneconfigmake modules_prepare
```

Befolgen Sie die folgenden Anweisungen für die Installation der erforderlichen Kernel-Module:

Führen Sie als Root-Benutzer folgenden Befehl aus:`/opt/f-secure/fsav/bin/fsav-compile-drivers`
Wenn auf der Zusammenfassungsseite der Benutzeroberfläche keine Fehler angezeigt werden, funktioniert das Produkt ordnungsgemäß.

"fsav-compile-drivers" ist ein Shell-Skript, das den Dazuko-Treiber automatisch für Ihr System und das Produkt konfiguriert und kompiliert. Weitere Informationen zum Dazuko-Treiber finden Sie unter *www.dazuko.org*.

Hinweis: Sie können den Dazuko-Treiber unter *www.dazuko.org* herunterladen und ihn zusammen mit dem Produkt verwenden, dies wird jedoch nicht empfohlen. Das Produkt wurde nur mit der mitgelieferten Dazuko-Version umfassend getestet, die unter "`/opt/f-secure/fsav/dazuko.tar.gz`" installiert ist.

Wenn Ihre Linux-Version über einen vorinstallierten Dazuko-Treiber verfügt, kann dieser nicht verwendet werden, da Dazuko von den beigefügten Patches und Konfigurationsoptionen abhängt, die wahrscheinlich von denen des vorinstallierten Dazuko abweichen. Deinstallieren Sie den vorinstallierten Dazuko-Treiber, stellen Sie sicher, dass er nicht läuft, wenn Sie das System hochfahren, und befolgen Sie die zuvor beschriebenen Installationsanweisungen, um Dazuko mit allen benötigten Patches und Konfigurationsoptionen zu installieren.

Benutzeroberfläche

Schwierigkeiten bei der Fehlerbehebung für die Webbenutzeroberfläche.

Ich kann mich nicht bei der Webbenutzeroberfläche anmelden. Was kann ich tun?

Bei einigen Ausführungen müssen Sie die folgende Zeile in `/etc/pam.d/login` auskommentieren, d. h. am Anfang der Zeile ein Rautenzeichen (#) einfügen:

```
# auth requisite pam_securetty.so
```

Über dem F-Symbol wird ein rotes Kreuz angezeigt. Was bedeutet das?

Wenn über dem F-Symbol in der Systemleiste oder im GNOME-Panel-Applet ein rotes Kreuz angezeigt wird, hat das Programm einen Fehler festgestellt. Öffnen Sie die Webbenutzeroberfläche, um einen detaillierten Bericht zu dem Problem anzuzeigen.

Starten Sie das Programm neu, um das Problem zu beheben. Führen Sie folgenden Befehl aus:

```
/etc/init.d/fsma restart
```

Wie zeige ich das F-Symbol in der Systemleiste an?

Zum Anzeigen des F-Symbols in der Systemleiste müssen Sie sich eventuell abmelden und erneut anmelden. Wenn Sie Gnome Desktop verwenden, stellen Sie sicher, dass im Gnome-Panel ein Benachrichtigungsbereich vorhanden ist, und gehen Sie gemäß den folgenden Anweisungen vor:

1. Klicken Sie mit der rechten Maustaste in das GNOME-Panel.
2. Wählen Sie **Panel-Applet hinzufügen**.
3. Wählen Sie aus der Liste der installierten GNOME-Panel-Applets "F-Secure-Panel-Applet" aus.

Wie kann ich das Debugging-Protokoll für die Webbenutzeroberfläche aktivieren?

Nehmen Sie die folgende Einstellung an `/opt/f-secure/fsav/tomcat/conf/logging.properties`:

```
.level=FINEST
```

Die Protokolldatei befindet sich in `/var/opt/f-secure/fsav/tomcat/catalina.out`.

F-Secure Policy Manager

Schwierigkeiten bei der Fehlerbehebung für F-Secure Policy Manager

Seit der Aktualisierung des Programms funktioniert mein Netzkwerk nicht mehr. Wie lässt sich das Problem beheben?

Sie müssen die MIB-Datei in Ihrer Installation von F-Secure Policy Manager aktualisieren, da das aktualisierte Programm andernfalls das Server-Firewall-Profil verwendet, wodurch praktisch jeglicher Verkehr blockiert wird.

Integritätsprüfung

Bei der Fehlerbehebung sind Schwierigkeiten mit der Integritätsprüffunktion aufgetreten.

Ich habe vergessen, den Softwareinstallationsmodus zu verwenden, und mein System funktioniert nicht ordnungsgemäß. Was kann ich tun?

Erstellen Sie eine neue Baseline. Führen Sie folgende Befehle aus:

```
/opt/f-secure/fsav/bin/fslistfiles | fsic --add -fsic --baseline
```

Kann ich bei Verwendung der Integritätsprüfung den Linux-Kernel aktualisieren?

Verwenden Sie den Softwareinstallationsmodus. Deaktivieren Sie den Softwareinstallationsmodus nach dem Kernel-Update, um die normale Sicherheitsstufe wiederherzustellen:

Es sind zu viele geänderte Dateien vorhanden, die mit der Benutzeroberfläche aktualisiert werden müssen.

Erstellen Sie eine neue Baseline. Führen Sie folgende Befehle aus:

```
/opt/f-secure/fsav/bin/fslistfiles | fsic --add -fsic --baseline
```

Muss ich bei jedem Generieren der Baseline dieselbe Passphrase verwenden?

Nein, Sie müssen zwar beim Überprüfen einer Baseline dieselbe Passphrase verwenden, die Sie zu deren Generierung gewählt haben; bei einer neuen Generierung einer Baseline brauchen Sie jedoch nicht wieder dieselbe Passphrase zu verwenden.

Firewall

Fehlerbehebung bei Problemen mit der Firewall

Ich kann nicht auf Samba-Freigaben auf meinem Computer zugreifen, nachdem ich das Produkt installiert habe. Was kann ich tun?

Im Office-Firewallprofil ist eine Regel enthalten, die das Windows-Netzwerk zulässt. Diese Regel ist jedoch standardmäßig deaktiviert. Aktivieren Sie die Regel, um Zugriffe auf Samba-Freigaben zuzulassen.

Ich kann nach der Installation des Produktes kann ich lokale Netzwerkdomänen und Arbeitsgruppen (SBM) nicht durchsuchen. Was kann ich tun?

Sie müssen der Firewall eine Regel hinzufügen, um das Durchsuchen der Windows-Freigaben auf Ihrem lokalen Bereichsnetzwerk zuzulassen. Folgen Sie diesen Anweisungen:

1. Wechseln Sie zur Seite **Firewall** > **Netzwerkdienste** im erweiterten Modus der Webbenutzeroberfläche.
2. Klicken Sie auf **Neuen Dienst hinzufügen**.
3. Erstellen Sie den folgenden Dienst:
   - **Dienstname**: `Windows Networking Local Browsing`
   - **Protokoll**: `UDP`
   - **Initiatorports**: `137-138`
   - **Responder**: `>1023`
   - **Beschreibung**: `SMB LAN browsing`
4. Klicken Sie auf "Als neuen Dienst hinzufügen" und "**Speichern**.
5. Klicken Sie im Menü "Firewall" auf "**Firewallregeln**".
6. Klicken Sie auf "**Neue Regel hinzufügen**".
7. Erstellen Sie folgende Regel:
   - **Typ**: `ACCEPT`
   - **Remotehost**: `[myNetwork]`
   - **Beschreibung**: `Windows Networking Local Browsing`
   - **Dienst** (Feld auswählen): `Windows Networking Local Browsing`
   - **Richtung**: `in`
8. Klicken Sie auf "**Dienst zu dieser Regel hinzufügen**" und "**Zu Firewallregeln hinzufügen**". Die neue Regel sollte am unteren Rand der Firewallregellisste angezeigt werden. Wenn die Regel nicht angezeigt wird, klicken Sie auf "**>>**", um ans Listenende zu gelangen.
9. Klicken Sie auf den Pfeil nach oben neben der neuen Regel, um diese an eine Stelle über eine eventuell vorhandene "Alles andere sperren"-Regel zu verschieben.
10. Klicken Sie auf "**Speichern**", um den neuen Regelsatz zu speichern und neue Firewallregeln anzuwenden.

Ihr SMB-LAN-Browsing sollte nun funktionieren.

Wie kann ich Firewallregeln für den Zugriff auf NFS-Server einrichten?

Sie müssen folgenden Netzwerkdatenverkehr über die Firewall zulassen:

- Portmapper (tcp- und udp-Port 111)
- nfsd (tcp und udp 2049)
- mountd (variabler Port vom Portmapper)

"Gemountet" ist nur dann erforderlich, wenn die NFS-Freigabe gemountet ist. Wenn der Mountvorgang abgeschlossen ist, wird der gesamte Datenverkehr zu nfsd geleitet.

Da der gemountete Port nicht immer derselbe ist, befolgen Sie zum mounten von NFS-Freigaben diese Anweisungen:

- Deaktivieren Sie die Firewall oder mounten (bzw. unmounten) Sie die NFS-Freigabe und aktivieren Sie die Firewall anschließend wieder oder
- starten Sie "mountd" auf dem NSF-Server mit der Option `--port PORT`, über die erzwungen wird, dass "mountd" statt einem zufälligen Port eine feste Portnummer verwendet.
- Erstellen Sie anschließend eine Firewall-Regel, die UDP- und TCP-Netzwerkverkehr zu dieser Portnummer zulässt.

Virenschutz

Schwierigkeiten bei der Fehlerbehebung für die Virenschutzfunktion.

Wie kann ich das Debugging-Protokoll für den Echtzeit-Virenscanner aktivieren?

Gehen Sie in der Policy Manager Konsole zu **Produkt** > **Einstellungen** > **Erweitert** und legen Sie Folgendes fest: **fsoasd-Protokollierungsebene** to **Debuggen.**

Führen Sie in der Einzelplatzinstallation den folgenden Befehl aus:

```
/opt/f-secure/fsma/bin/chtest s 44.1.100.11 9
```

Die Protokolldatei befindet sich in `/var/opt/f-secure/fsav/fsoasd.log`.

Wie kann ich zum Herunterladen von Datenbank-Updates einen HTTP-Proxy-Server verwenden?

Wechseln Sie in der Policy Manager Konsole zu **F-Secure Automatic Update Agent** > **Einstellungen** > **Kommunikation** > **HTTP-Einstellungen** > **Benutzerdefinierte Proxy-Einstellungen** und legen Sie für **Adresse** Folgendes fest: `http://[[user][:pass]@]proxyhost[:port]`.

Verwenden Sie die Einstellung auf der Seite **Automatische Updates** im erweiterten Modus der Webbenutzeroberfläche.

Kann die Funktion für das Echtzeit-Scanning auf einem NFS-Server verwendet werden?

Wenn das Produkt auf einem NFS-Server installiert ist, scannt die Funktion für Echtzeit-Scanning Dateien nicht automatisch, wenn ein Client auf eine Datei auf dem Server zugreift.

Wie kann ich den Echtzeit-Virenscan vorübergehend deaktivieren?

Während bestimmter administrativer Aufgaben (z. B. bei der Sicherung oder Wiederherstellung) kann es von Vorteil sein, im Hintergrund laufende Virenscans vorübergehend zu deaktivieren.

Führen Sie die folgenden Befehle aus, um den Virenscan und die Integritätsprüfung zu deaktivieren:

```
/opt/f-secure/fsma/bin/chtest s 45.1.40.10 0/opt/f-secure/fsma/bin/chtest s
45.1.70.10 0
```

Um den Echtzeit-Virenscan und die Integritätsprüfung wieder zu aktivieren, führen Sie folgende Befehle aus:

```
/opt/f-secure/fsma/bin/chtest s 45.1.40.10 1/opt/f-secure/fsma/bin/chtest s
45.1.70.10 1
```

Werden beim Echtzeit-Scan Dateien gescannt, wenn sie umbenannt oder verknüpft wurden?

Der Echtzeit-Scan scannt Dateien jedes Mal, wenn sie geöffnet, geschlossen oder ausgeführt werden. Sie werden nicht gescannt, wenn Sie sie umbenennen oder eine Verknüpfung zu einer Datei erstellen oder entfernen.

Kompatibilität mit anderen Sicherheitsprodukten

Mögliche Kompatibilitätsprobleme mit dem Produkt.

Das Produkt verwendet für die On-Access-Dateiüberprüfung Kernel-Funktionen auf niedriger Ebene. Andere Produkte für Sicherheit und Zugriffssteuerung, die eine ähnliche Funktionsweise besitzen, können Konflikte verursachen. Eine gleichzeitige Verwendung dieser Produkte kann zu einer Verringerung der Verarbeitungsleistung und zu einer eventuellen Instabilität des Systems führen.

Die aktuellsten Informationen über bekannte Kompatibilitätsprobleme sowie Links zu verwandten Ressourcen finden Sie in den Versionsinfos.

Allgemeine Probleme

Allgemeine Fehlerbehebung bei Problemen mit diesem Produkt.

Wie kann ich eine unterbrochene Installation bereinigen?

Wenn die Produktinstallation unterbrochen wurde, haben Sie möglicherweise die Produktkomponenten manuell entfernt.

1. Listen Sie alle installierten RPM-Pakete auf:

   ```
   rpm -qa | grep f-securerpm -qa | grep fsav
   ```

2. Entfernen Sie die installierten Pakete. Führen Sie für jedes installierte Paket den folgenden Befehl aus:

   ```
   rpm -e --noscripts <package_name>
   ```

3. Entfernen Sie alle Verzeichnisse der Produktinstallation:

   ```
   rm -rf /var/opt/f-secure/fsavrm -rf /var/opt/f-secure/fsmarm -rf
   /etc/opt/f-secure/fsavrm -rf /etc/opt/f-secure/fsmarm -rf /opt/f-secure/fsavrm
    -rf /opt/f-secure/fsma
   ```

Das System reagiert nur verzögert. Was könnte die Ursache sein?

Das Scannen von Viren in Echtzeit und die Integritätsprüfung können das System verlangsamen.

1. Verwenden Sie die grundlegenden Linux-Tools (top und vmstat), um zu überprüfen, wodurch die Geschwindigkeit des Systems verlangsamt wird.
2. Stellen Sie sicher, dass Sie die Version für Dazuko verwenden, die im Lieferumfang des Produkts enthalten ist.
3. Wenn der Scan-Vorgang für eine Datei, auf die häufig zugegriffen wird, zeitaufwändig ist, können Sie sie eventuell der Ausschlussliste hinzufügen.
4. Wenn Sie den zentralisierten Verwaltungsmodus verwenden, stellen Sie sicher, dass die DNS-Abfragen Adressen schnell zurückgeben oder IP-Adressen mit F-Secure Policy Manager verwenden.

Das Programm kann nicht mit der Datenbank kommunizieren. Wie lässt sich dieses Problem beheben?

Gelegentlich, beispielsweise nach dem Zurücksetzen der Hardware, kann das Produkt möglicherweise die Datenbank nicht kontaktieren. Befolgen Sie diese Anweisungen, um das Problem zu beheben:

1. Melden Sie sich als Root-Benutzer an, und entfernen Sie die PID-Datei der Datenbank:
   ```
   rm /var/opt/f-secure/fsav/pgsql/data/postmaster.pid
   ```
2. Starten Sie als Root-Benutzer das Produkt neu:
   ```
   /etc/init.d/fsma restart
   ```

Ich erhalte Meldungen, dass F-Secure Status Daemon nicht ausgeführt wird. Wie kann ich ihn starten?

In bestimmten Fällen, beispielsweise nach einem Hardware-Reset, kann es vorkommen, dass F-Secure Status Daemon nicht gestartet werden kann. Starten Sie das Programm neu, um dieses Problem zu beheben:

```
/etc/init.d/fsma restart
```

Sie können F-Secure Status Daemon auch manuell starten:

```
/opt/f-secure/fsav/bin/fstatusd
```

Linux Kernel verweigert das Laden des Moduls. Was soll ich tun?

Nachdem Sie Kernel aktualisiert haben, müssen Sie die Kernel-Module erneut kompilieren, da sie nicht automatisch neu erstellt werden. Sie müssen die Kernel-Treiber, die das Produkt benötigt, gegebenenfalls manuell kompilieren, wenn:

- Sie Compiler und andere erforderliche Tools nicht in den Installationsvorgang einbezogen haben,
- Sie Kernel-Header oder -Quellen nicht in den Installationsvorgang einbezogen haben oder
- Sie den Kernel aktualisiert haben und Treiber für den neuen Kernel kompilieren müssen.

Führen Sie zum Kompilieren und Installieren von Treibern den folgenden Befehl aus:

```
/opt/f-secure/fsav/bin/fsav-compile-drivers
```

Anhang

A

Befehlszeilen -Tools

Themen:

- *fsav*
- *fsav-config*
- *dbupdate*
- *fsfwc*
- *fsic*
- *fsims*
- *fsma*
- *fssetlanguage*
- *fschooser*

Sie können das Produkt und die dazugehörigen Funktionen aus der Befehlszeile verwenden.

Weitere Informationen zu Befehlszeilen -Tools und -optionen finden Sie auf den man-Seiten.

fsav

"`fsav`" ist ein Programm, das Dateien nach Viren und anderem bösartigen Code durchsucht.

"fsav" durchsucht die angegebenen Ziele (Dateien oder Verzeichnisse) und meldet jeden bösartigen Code, den es erkennt. Wahlweise kann "fsav" infizierte Dateien auch desinfizieren, umbenennen oder löschen.

Gehen Sie folgendermaßen vor, um Dateien von der Shell aus zu scannen:

- Wenn alle Standarddateitypen in allen lokalen Laufwerken gescannt werden sollen, geben Sie Folgendes ein: `fsav /`
- Wenn alle Dateien in einem Verzeichnis und dessen Unterverzeichnissen gescannt werden sollen, geben Sie den Namen des Verzeichnisses ein. Beispiel: `fsav mydirectory`
- Wenn eine einzelne Datei gescannt werden soll, geben Sie den Dateinamen (ohne Platzhalter) ein. Beispiel: `fsav myfile.exe`

Beim rekursiven Scannen werden gemountete Unterverzeichnisse des Netzwerkdateisystems erkannt und es werden keine Netzwerkdateisysteme gescannt. Das Scannen eines Netzwerkdateisystems von der Client-Workstation aus würde das Netzwerk unnötig beanspruchen und läuft wesentlich langsamer ab als das Scannen des lokalen Dateisystems.

Wenn Sie das Netzwerkdateisystem scannen möchten, führen Sie "`fsav /`" auf dem Server aus.

Wenn Sie "fsav" nicht auf dem Server ausführen können, können Sie das Netzwerkdateisystem von der Client-Workstation aus scannen, indem Sie gemountete Netzwerkdateisystem-Verzeichnisse in der fsav-Befehlszeile angeben.

Wenn eine NFS-Datei beispielsweise in "`/mnt/server1`" gemountet ist, scannen Sie sie mit dem folgenden Befehl: `fsav /mnt/server1`

Hinweis: Es können nur reguläre Dateien auf gemounteten Dateisystemen gescannt werden. Besondere Dateien wie beispielsweise von CD-ROM oder von DAT-Geräten (/dev/st0, /dev/hda u. Ä.) können erst als gemountete Dateisysteme gescannt werden. Die Dateien können auch zuerst von dem Band auf ein Dateisystem extrahiert werden.

Weitere Informationen zu Befehlszeilenoptionen finden Sie auf den man-Seiten zu fsav, oder geben Sie Folgendes ein: `fsav --help`

fsav-config

`fsav-config`-Tool erstellt die ursprüngliche Produktkonfiguration.

Wenn Sie das Programm mit RPM-Paketen installieren, müssen Sie das `fsav-config`-Befehlszeilen-Tool verwenden.

1. Verwenden Sie folgenden Befehl, um die ursprüngliche Produktkonfiguration zu erstellen:
   `/opt/f-secure/fsav/fsav-config`
   Im Skript werden einige Fragen angezeigt. Der Standardwert wird in Klammern nach der Frage angezeigt. Klicken Sie auf`ENTER`, um den Standardwert auszuwählen.
2. Wählen Sie die Sprache aus, die Sie auf der Webbenutzeroberfläche verwenden möchten.

```
Select language to use in Web User Interface [1] English (default) [2] Japanese
 [3] German
```

3. Geben Sie den Schlüsselcode ein, um die vollständige lizensierte Version des Produktes zu installieren. Gegen Sie den Schlüsselkode genauso ein, wie Sie ihn erhalten haben, einschließlich der Bindestriche, mit denen die Folgen von Zahlen und Buchstaben voneinander getrennt sind. Wenn Sie das Produkt testen möchten, aber keinen Schlüsselcode zur Hand haben, klicken Sie auf `ENTER`.
4. Wählen Sie zwischen einer Standaloneinstallation und einer zentral verwalteten Installation aus.
   a) Geben Sie für die zentral verwaltete Installation die Adresse des F-Secure Policy Manager-Servers ein.
   ```
   Address of F-Secure Policy Manager Server: [http://localhost/]:
   ```
   b) Geben Sie für die zentral verwaltete Installation den Speicherort des `admin.pub`-Schlüssels ein. Dies ist der Schlüssel, den Sie während der Installation der F-Secure Policy Manager-Konsole erstellt haben.
5. Wählen Sie aus, ob Sie Remotezugriff auf die Webbenutzeroberfläche zulassen möchten.
   ```
   Allow remote access to the web user interface? [no]
   ```
6. Legen Sie fest, ob die Webbenutzeroberfläche über den lokalen Host ohne Anmeldung geöffnet werden kann.
   ```
   Allow connections from localhost to the web user interface without login? [yes]
   ```
7. Geben Sie den Benutzernamen ein, der für die Verwendung der Webbenutzeroberfläche zugelassen ist.
   ```
   Please enter the user name who is allowed to use the web user interface.
   ```

   Hinweis: Der Benutzername ist ein lokales Linux-Konto. Erstellen Sie ein Konto, wenn noch keins vorhanden ist. Verwenden Sie hierfür nicht das Root-Konto.

dbupdate

`dbupdate` ist ein Shell-Skript zur Aktualisierung der F-Secure Anti-Virus-Virendefinitionsdatenbanken.

Befolgen Sie diese Anweisungen, um Virendefinitionsdatenbanken manuell über die Befehlszeile zu aktualisieren:

1. Laden Sie die Datei `fsdbupdate9.run` von folgender Website herunter:
   http://download.f-secure.com/latest/fsdbupdate9.run
   "`fsdbupdate9.run`" ist eine selbstextrahierende Datei, die den Automatic Update-Daemon stoppt, Datenbanken aktualisiert und den Automatic Update Agent dann erneut startet.
2. Führen Sie als Root-Benutzer folgenden Befehl aus: `dbupdate fsdbupdate9.run`
   wobei `fsdbupdate9.run` der absolute oder relative Pfad zur Datei `fsdbupdate9.run` ist.

Weitere Informationen zu Befehlszeilenoptionen finden Sie auf den man-Seiten zu dbupdate, oder geben Sie Folgendes ein: `dbupdate --help`

fsfwc

`fsfwc` ist ein Befehlszeilen-Tool, mit dem Sicherheitsstufen der Firewall festgelegt werden.

Verwenden Sie folgenden Befehl zum Ändern des aktuellen Sicherheitsprofils:
```
/opt/f-secure/fsav/bin/fsfwc --mode {block, mobile, home, office, strict,
normal, bypass}
```

fsic

Sie können eine Baseline erstellen, der Baseline Dateien hinzufügen und die Baseline mithilfe des Befehlszeilen-Tools `fsic` überprüfen.

1. Gehen Sie wie folgt vor, um die Baseline zu erstellen:
   a) Führen Sie das Befehlszeilentool "fsic" mit der Option "--baseline" aus: `fsic --baseline`
   b) Geben Sie eine Passphrase ein, um eine Signatur zu erstellen.

   Eine neue Baseline wurde erstellt.
2. Befolgen Sie diese Anweisungen, um Dateien zur Baseline hinzuzufügen:
   a) Führen Sie das Befehlszeilentool "fsic" mit den Optionen "--add", "--aler"t und "--protect" aus: `/opt/f-secure/fsav/bin/fsic --add --alert=yes --protect=yes /etc/passwd /etc/shadow`
   b) Berechnen Sie die Baseline neu. Während dieses Vorgangs wird der Update-Verlauf für die Baseline angezeigt und Sie müssen eine Auswahl treffen, ob Sie die neuen Dateien in die Baseline einbinden möchten: `/opt/f-secure/fsav/bin/fsic --baseline`
   c) Geben Sie eine Passphrase ein, um eine Signatur zu erstellen.

   In diesem Beispiel ist das Programm auch so konfiguriert, dass bei nicht autorisierten Änderungsversuchen an den geschützten Dateien ein Alarm gesendet wird.
3. Überprüfen der Baseline:
   a) Führen Sie folgenden Befehl aus:`/opt/f-secure/fsav/bin/fsic`
   b) Geben Sie die Passphrase ein, die Sie beim Erstellen der Baseline verwendet haben.

   Das Programm überprüft die Dateien und gibt an, ob diese korrekt sind.

fsims

Sie können den Befehl `fsims` verwenden, um den Softwareinstallationsmodus von der Shell aus zu verwenden.

Befolgen Sie diese Anweisungen, um neue Software zu installieren:

1. Verwenden Sie den folgenden Befehl, um den Softwareinstallationsmodus zu aktivieren: `/opt/f-secure/fsav/bin/fsims on`
2. Installieren Sie die neue Software.
3. Deaktivieren Sie den Softwareinstallationsmodus, um die normale Sicherheitsstufe wiederherzustellen: `/opt/f-secure/fsav/bin/fsims off`

fsma

Mit dem Befehl `fsma` können Sie den Status der Produktmodule überprüfen.

Führen Sie den folgenden Befehl aus: `/etc/init.d/fsma status`

Modul	Prozess	Beschreibung
F-Secure-Daemon für Alarmdatenbank-Handler	`/opt/f-secure/fsav/sbin/fsadhd`	Speichert Alarmmeldungen in einer lokalen Datenbank. Alarmmeldungen können mithilfe

Modul	Prozess	Beschreibung
		der Webbenutzeroberfläche angezeigt werden.
F-Secure-Daemon für FSAV Policy Manager	`/opt/f-secure/fsav/bin/fsavpmd`	Führt alle Operationen der F-Secure Policy Manager-Konsole aus (z. B. "Alle Festplatten jetzt scannen", "Datenbank jetzt aktualisieren", "Statistiken zurücksetzen")
F-Secure Firewall-Daemon	`/opt/f-secure/fsav/bin/fsfwd.run`	Die Schnittstelle zwischen dem F-Secure Management Agent und der iptables/netfilter-Firewall.
F-Secure FSAV License Alerter	`/opt/f-secure/fsav/libexec/fslmalerter`	Überprüft und informiert Sie darüber, wie viele Tage die Testphase noch dauert, wenn das Produkt im Testmodus installiert ist.
F-Secure-FSAV-Zugriffsscanner-Daemon	`/opt/f-secure/fsav/sbin/fsoasd`	Bietet alle Echtzeitschutzfunktionen: Echtzeit-Virenscan, Echtzeit-Integritätsprüfung und Rootkit-Schutz.
F-Secure-FSAV-Status-Daemon	`/opt/f-secure/fsav/bin/fstatusd`	Überprüft den aktuellen Status jeder Komponente und hält die Desktop-Panel-Anwendungen und die Webbenutzeroberfläche auf dem neuesten Stand.
F-Secure-FSAV-Web-UI	`/opt/f-secure/fsav/tomcat/bin/catalina.sh start`	Verantwortlich für die Webbenutzeroberfläche.
F-Secure-FSAV-PostgreSQL-Daemon	`/opt/f-secure/common/postgresql/bin/startup.sh`	Speichert Alarmmeldungen, die mithilfe der Webbenutzerschnittstelle angezeigt werden können.
F-Secure Updated Daemon	`/opt/f-secure/fssp/libexec/fsupdated`	Führt automatische Produkt-Updates durch.

fssetlanguage

Mit dem Tool `fssetlanguage` können Sie die Sprache der Webbenutzerschnittstelle ändern.

Legen Sie die Sprache mithilfe des folgenden Befehls fest: `/opt/f-secure/fsav/bin/fssetlanguage <language>`

"Language" kann folgende Werte annehmen:

- en - Englisch
- ja - Japanisch
- de - Deutsch

fschooser

Mit `fschooser` können Sie bestimmte Produktfunktionen aktivieren oder deaktivieren.

Sie können einige Produktkomponenten deaktivieren, wenn Sie nicht alle benötigen oder zu deren Ausführung nicht über genügend Systemressourcen verfügen.

1. Führen Sie den folgenden Befehl aus: `/opt/f-secure/fsav/sbin/fschooser`.
   Auf dem Bildschirm werden die Sicherheitskomponenten des Produktes aufgelistet.
2. Folgen Sie den Anweisungen auf dem Bildschirm, um Komponenten zu aktivieren oder zu deaktivieren.

   ```
   Firewall - ENABLED, press f+RET to toggle
   Webbenutzerschnittstelle - AKTIVIERT, drücken Sie w+RET, um umzuschalten.
   ```

3. Klicken Sie auf `RETURN`, um Ihre Auswahl zu bestätigen.

   Hinweis: Klicken Sie auf`ctrl+C`, um Ihre Änderungen zu verwerfen.

Anhang

B

Vor der Installation

Themen:

- *64-Bit-Produkte*
- *Distributionen mit Prelink*
- *Red Hat Enterprise Linux, Asianux, CentOS*
- *Debian*
- *SUSE*
- *Turbolinux*
- *Ubuntu*

Installationsanweisungen für verschiedene Linux-Produkte.

Hinweis: In einigen Bereichen wird `prelink` regelmäßig über `cron` ausgeführt, um verknüpfte Bibliotheken leistungsstärker zu machen. Wenn dies nicht automatisch ausgeführt wird, tun Sie dies manuell, bevor Sie die Integritätsprüfung ativieren.

Sollten Sie das Produkt installiert haben, bevor Sie alle zugehörigen Pakete installiert haben, installieren Sie diese Pakete und führen Sie den folgenden Befehl aus, um alle Module von F-Secure zu initialisieren:

```
/etc/init.d/fsma restart
```

Wenn der Kernel-Interceptor von Linux Security nicht kompiliert werden konnte, führen Sie folgende Befehl aus:

```
/opt/f-secure/fsav/compile-drivers
```

64-Bit-Produkte

Einige 64-Bit-Produkte installieren standardmäßig keine 32-Bit-Kompatibilitätsbibliotheken. Stellen Sie sicher, dass diese Bibliotheken installiert sind.

Der Name des Kompatibilitätsbibliothek-Pakets kann unterschiedlich sein. Informationen zum Paketnamen der 32-Bit-Kompatibilitätsbibliotheken finden Sie in der Dokumentation Ihres Produkts.

Installieren Sie auf 64-Bit Ubuntu `ia32-libs`.

Distributionen mit Prelink

Durch die Verwendung von Prelink kann die Starzeit für Binärdateien verkürzen, führt jedoch zu Konflikten mit der Integritätsprüfung des Programms.

Sie sollten automatisches Prelinking von cron deaktivieren. Unter Asianux, bearbeiten Sie `PRELINKING=yes` in `/etc/sysconfig/prelink` zu `PRELINKING=no` und führen Sie `/etc/cron.daily/prelink`, bevor Sie das Produkt installieren.

Einige Distributionen wie Asianux führen `prelink` regelmäßig von `cron` aus, um die Startzeit von Binärdateien zu verkürzen, die dynamische Bibliotheken nutzen. Durch Prelinking werden Binärdateien und dynamische Bibliotheken auf der Festplatte geändert, was zu einem Konflikt mit der Integritätsprüfung führt, die Änderungen an Systemdateien erkennt.

Wenn Sie F-Secure Linux Security bereits installiert haben, befolgen Sie diese Anweisungen:

1. Führen Sie `/opt/f-secure/fsav/bin/fsims on` über die Befehlszeile aus, um den Software-Installationsmodus zu aktivieren.
   Im Software-Installationsmodus lässt das System Änderungen an Systemdateien zu.
2. Bearbeiten Sie `/etc/sysconfig/prelink` und ändern Sie die Zeile: `PRELINKING=yes` in `PRELINKING=no`.
3. Führen Sie `/etc/cron.daily/prelink` aus.
4. Führen Sie `/opt/f-secure/fsav/bin/fsims off` aus der Befehlszeile aus, um den Software-Installationsmodus auszuschalten.

Wenn der Software-Installationsmodus deaktiviert ist, wird der Status der Systemdateien in der Baseline der Integritätsprüfung gespeichert.

Um Prelinking zu verwenden, müssen Sie den Software-Installationsmodus vor dem Prelinking aktivieren und ihn wieder deaktivieren, wenn das Prelinking abgeschlossen ist. Auf diese Weise kann Prelink die Änderungen an den Systemdateien kontrolliert durchführen. Beispiel:

```
# /opt/f-secure/fsav/bin/fsims on # prelink -a # /opt/f-secure/fsav/bin/fsims
off
```

Hinweis: Dieser Vorgang lässt sich nicht einfach automatisieren. Durch die Deaktivierung des Software-Installationsmodus wird eine neue Baseline erstellt, die mit einer vom Administrator anzugebenden Passphrase signiert werden muss.

Red Hat Enterprise Linux, Asianux, CentOS

Die folgenden Schritte sind notwendig, um das Produkt auf einem Computer zu installieren, auf dem das Red Hat Enterprise Linux-, das Miracle Linux-, das Asianux- oder das CentOS-Betriebsystem läuft.

Red Hat EL 4 / CentOS 4

Im Gegensatz zur Standardinstallation werden folgende zusätzliche RPM Pakete benötigt.

- GCC
- GLIBC-Devel
- GLIBC-Header
- GLIBC-Kernheader

Mindestens eines der folgenden RPM Pakete wird benötigt.

- Kernel-Devel
- Kernel-Hugemem-Devel
- Kernel-SMP-Devel

Um zu sehen, welcher Kernel benutzt wird, geben Sie den folgenden Befehl ein: `uname -r`

Damit das 'F-Icon' Systemleisten-Applet funktioniert, werden folgenden RPM Pakete benötigt:

- kdelibs
- compat-libstdc++

Installieren Sie die RPMs von den System CDs entweder durch den Befehl `rpm -ivh`, **Anwendungen** > **Systemeinstellungen** > **Anwendungen hinzufügen/entfernen** oder verwenden Sie `up2date` Befehlszeilentool in Red Hat.

Red Hat EL 6 / Red Hat EL 5 / Asianux 3.0 / CentOS 5 / CentOS 6

Stellen Sie sicher, dass folgende Pakete installiert sind. Nutzen Sie beispielsweise das Suchfeld **Anwendungen** > **Software hinzufügen/entfernen** oder verwenden Sie den `rpm`-Befehl.

- GCC
- GLIBC-Devel
- GLIBC-Header
- Kernel-Devel

Führen Sie auf CentOS folgenden Befehl als Root aus, um sicherzugehen, dass alle notwendigen Pakete installiert und auf dem neuesten Stand sind:

```
yum install gcc glibc-devel glibc-headers kernel-devel
```

Für Redhat EL 6- und CentOS 6-Plattformen (64-Bit) sind folgende zusätzliche Pakete erforderlich:

- pam.i686
- zlib.i686

Hinweis: Hinweis: Sollte Ihnen während der Installation folgende Fehlermeldung angezeigt werden: `"error: protected multilib versions”: pam-<version>.el6.i686 != pam-<version>.el6.x86_64"`, führen Sie den folgenden Befehl aus und installieren Sie pam.i686 erneut:`yum update`.

Debian

Die folgenden Schritte sind notwendig, um das Produkt auf einem Computer zu installieren, auf dem Debian Linux läuft.

Debian

Sie müssen den Compiler, Kernel-Header, RPM und vermutlich noch zusätzliche Programme installieren, um das Produkt installieren zu können. Um diese zu installieren, verwenden Sie folgende Befehle:

```
sudo apt-get install gcc rpm make libc6-dev psmiscsudo apt-get install
linux-headers-`uname -r`
```

SUSE

Die folgenden Schritte sind notwendig, um das Produkt auf einem Computer zu installieren, auf dem das SUSE Linux Betriebsystem läuft.

Diese Anweisungen wurden auf folgenden SUSE-Versionen getestet: 9.1, 9.2, 9.3, 10.0, 10.1.

Stellen Sie sicher, dass folgende Pakete installiert sind. Sie können YaST oder ein anderes Paketverwaltungsprogramm verwenden.

- Kernel-Verzeichnis
- machen
- Patch
- gcc

Das Installationsprogramm weist Sie darauf hin, falls es nicht die notwendigen Komponenten während des Installationsvorgangs finden kann.

Turbolinux

Die folgenden Schritte sind notwendig, um das Produkt auf einem Computer zu installieren, auf dem das Turbolinux Betriebsystem läuft.

Turbolinux 11

Sie müssen die Turbolinux-Paketgruppe, die Entwicklungstools und das Kernel Recompile Kit installieren, damit Sie das Dazuko Kernel-Modul zusammenstellen können.

Verwenden Sie folgende Liste, wenn Sie einzelne Pakete installieren möchten:

- gcc
- cpp
- GLIBC-Devel
- Kernel-Header
- Kernel-Verzeichnis

Manchmal sind die Turbolinux Kernel-Verzeichnisse nicht konfiguriert und können nicht verwendet werden, um Kernel-Driver zusammenzustellen. Um dies zu beheben, führen Sie die folgenden Befehle aus:

```
cd /usr/src/linux-2.major.minor ./SetupKernelSource.sh architecture make oldconfig
```

major.minor

Beschreibt die Kernel-Version.

architecture

`i686`, `i686smp64G` oder `x86_64`.

Ubuntu

Die folgenden Schritte sind notwendig, um das Produkt auf einem Computer zu installieren, auf dem das Ubuntu Linux Betriebsystem läuft.

Ubuntu 8.04

```
sudo apt-get install rpm libc6-dev patch linux-libc-dev
```

Ubuntu 8.04 Server, Ubuntu 10.04, Ubuntu 10.10

```
sudo apt-get install rpm libc6-dev patch linux-libc-dev make gcc
```

Anhang

C

Benutzeroberflächen-Referenz

Themen:

- *Einfache Webbenutzer-Oberfläche*
- *Erweiterte Benutzeroberfläche*

Eine Liste der Elemente in der Webbenutzer-Oberfläche.

In den folgenden Tabellen werden alle Einstellungen dargestellt, die in der Webbenutzer-Oberfläche verfügbar sind.

Einfache Webbenutzer-Oberfläche

Die Liste der Elemente in der Einfachen Webbenutzer-Oberfläche.

In den folgenden Tabellen werden die Einstellungen dargestellt, die in der Einfachen Webbenutzer-Oberfläche angezeigt werden.

"Ich möchte"

Auf der Seite **Hauptbenutzeroberfläche** > **Ich möchte** werden die folgenden Benutzeroberflächen-Steuerelemente angezeigt.

Element	Beschreibung
Computer auf Malware scannen	Verwenden Sie diesen Assistenten, um manuell auf Malware zu scannen. Sie können Dateien und/oder Verzeichnisse auswählen, die gescannt werden sollen.
Erstellen einer Firewall-Regel.	Verwenden Sie diesen Assistenten, um eine Firewall-Regel zu erstellen. Wenn Sie für die Regel einen neuen Dienst erstellen müssen, verwenden Sie den Bildschirm "Firewall-Regeln" im Erweiterten Modus.
Prüfen der Integrität des Dateisystems	Verwenden Sie diesen Assistenten, um eine Integritätsprüfung des Dateisystems auszuführen. Damit wird verifiziert, dass alle Dateien in der Baseline der Integritätsprüfung unverändert sind.
Aktualisieren der Virusdefinitionen.	Dies ist ein Link zur Seite "Automatische Updates" im Erweiterten Modus, auf der Sie die Einstellungen für die Updates automatischer Virusdefinitionen ändern können.
Software installieren	Verwenden Sie diesen Assistenten, um den Software-Installationsmodus zu aktivieren, wenn Sie ein Upgrade für Ihr System durchführen. Nachdem Sie das Upgrade durchgeführt haben, kehren Sie zum Assistenten zurück und generieren Sie die Integritätsprüfungs-Baseline neu. Dadurch wird sichergestellt, dass die aktualisierten Systemdateien keine unnötigen Warnmeldungen auslösen.
Erstellen einer Baseline	Mit diesem Assistent können Sie eine Integritätsprüfung-Dateisystem-Baseline erstellen.

Erweiterte Benutzeroberfläche

Die Liste der Elemente in der Erweiterten Webbenutzer-Oberfläche.

In den folgenden Tabellen werden die Einstellungen dargestellt, die in der Erweiterten Webbenutzer-Oberfläche angezeigt werden.

Zusammenfassung

Auf der Seite **Erweiterte Benutzeroberfläche** > **Zusammenfassung** werden die folgenden Benutzeroberflächen-Steuerelemente angezeigt.

Element	Beschreibung
Virenschutz	Wenn der Virenschutz aktiviert ist, werden alle Dateizugriffe des Systems auf Malware gescannt. Diese Option muss auch für die On-Access-Integritätsprüfung aktiviert werden. Gibt die aktuell aktive Sicherheitsstufe an. Firewall-Regeln und Anwendungssteuerung werden gemäß der aktuellen Sicherheitsstufe verarbeitet.
Schutz durch Firewall	Wenn die Integritätsprüfung aktiviert ist, entdeckt sie Änderungen an Baselinedateien.

Alarmmeldungen

Auf der Seite **Erweiterte Benutzeroberfläche** > **Alarme** werden die folgenden Benutzeroberfläche-Steuerelemente angezeigt.

Element	Beschreibung
Alarmtabelle	Auf der Seite "Alarme" können Sie Alarmmeldungen lesen und löschen. Befolgen Sie diese Anweisungen, um die Alarmmeldungen zu ermitteln, die Sie anzeigen möchten: 1. Wählen Sie den Status der Sicherheitsalarme aus, die Sie anzeigen möchten. * Wählen Sie "Alle" aus, um alle Alarme anzuzeigen. * Wählen Sie "Ungelesen" aus, um neue Alarme anzuzeigen. * Wählen Sie "Gelesen" aus, um Alarme anzuzeigen, die Sie bereits angezeigt haben. 2. Wählen Sie den Schweregrad der Sicherheitsalarme aus, die Sie anzeigen möchten. Weitere Informationen finden Sie unter "Alarm-Schweregradebenen". 38. Klicken Sie auf Alarme, um sie hervorzuheben und klicken Sie auf "Hervorgehobene Elemente als gelesen markieren", um sie als gelesene Meldungen einzustufen. Klicken Sie auf "Hervorgehobene Elemente löschen", um alle hervorgehobenen Alarme zu löschen.
Pflegen der Alarmdatenbank	Sie können gleichzeitig mehrere Meldungen löschen oder als gelesen markieren. Wählen Sie aus, wie alt ein Alarm ist und welchen Schweregrad Alarme aufweisen, die Sie bearbeiten möchten. Klicken Sie auf "Aktion durchführen", um die ausgewählten Nachrichten zu löschen oder als gelesen zu markieren.

Virenschutz

In den folgenden Tabellen werden die Einstellungen des Virenschutzes dargestellt.

Echtzeit-Scannen

Auf der Seite **Erweiterte Benutzeroberfläche** > **Virenprüfung** > **Echtzeit-Scannen** werden die folgenden Benutzeroberflächen-Steuerelemente angezeigt.

Element	Beschreibung
Primäre Aktion	Geben Sie die primäre Aktion an, die ausgeführt wird, wenn eine Infektion erkannt wird. Bericht und Zugriff sperren = Der Zugriff wird gesperrt. Es wird ein Alarm gesendet. Desinfizieren = Der Zugriff wird gesperrt. Es wird versucht, die Datei zu desinfizieren, wenn ein erfolgreicher Zugriff erlaubt wird. Umbenennen = Der Zugriff wird gesperrt. Die infizierte Datei erhält die Erweiterung .virus. Löschen = Der Zugriff wird gesperrt. Die infizierte Datei wird gelöscht. Zugriff sperren = Der Zugriff wird gesperrt. Es wird kein Alarm gesendet. Wenn die primären und sekundären Aktionen fehlschlagen, wird der Zugriff gesperrt und ein Sicherheitsalarm gesendet.
Primäre Aktion an verdächtigen Dateien	Geben Sie die primäre Aktion an, die ausgeführt wird, wenn eine vermutliche Infektion entdeckt wird. Bericht und Zugriff sperren = Der Zugriff wird gesperrt. Es wird ein Alarm gesendet. Umbenennen = Die verdächtige Datei erhält die Erweiterung .suspected. Löschen = Die infizierte Datei wird gelöscht. Zugriff sperren = Der Zugriff wird gesperrt. Es wird kein Alarm gesendet. Wenn die primäre Aktion fehlschlägt, wird die sekundäre Aktion ausgeführt. Wenn auch die sekundäre Aktion fehlschlägt, wird ein Alarm gesendet, der die fehlgeschlagenen Aktionen beschreibt.
Sekundäre Aktion an verdächtigen Dateien	Geben Sie die sekundäre Aktion an, die ausgeführt wird, wenn eine vermutliche Infektion entdeckt wird und die primäre Aktion fehlgeschlagen ist. Bericht und Zugriff sperren = Der Zugriff wird gesperrt. Es wird ein Alarm gesendet. Umbenennen = Die verdächtige Datei erhält die Erweiterung .suspected. Löschen = Die infizierte Datei wird gelöscht. Zugriff sperren = Der Zugriff wird gesperrt. Es wird kein Alarm gesendet. Wenn die primäre Aktion fehlschlägt, wird die sekundäre Aktion ausgeführt. Wenn auch die sekundäre Aktionen fehlschlagen, wird ein Alarm gesendet, der die fehlgeschlagenen Aktionen beschreibt.
Dateien und Verzeichnisse, die vom Scan-Vorgang ausgeschlossen sind.	Die hier aufgeführten Verzeichnisse werden nicht gescannt. Geben Sie die Namen der Verzeichnisse an, die vom Scan-Vorgang ausgeschlossen werden. Verwenden Sie den vollständigen, absoluten Pfad. Geben Sie jedes Verzeichnis in einer eigenen Zeile ein. Verzeichnisnamen können Leerzeichen enthalten.
Nur ausführbare Dateien scannen	Der Scan-Vorgang kann auf ausführbare Dateien beschränkt werden (= Dateien mit aktiviertem Execute-Bit). Hiervon wird normalerweise abgeraten, da sich Malware auch über nicht ausführbare Dateien ausbreiten kann, beispielsweise Textverarbeitungsmakros.
Ausführbare Dateien auf der Weißliste. Ausführbare Dateien auf der Weißliste müssen mit der Baseline übereinstimmen.	Liste ausführbarer Dateien, für die jederzeit vollständiger Dateizugriff erlaubt ist. Geben Sie den

Element	Beschreibung
	vollständigen Pfad zu den ausführbaren Dateien an, jeweils ein Pfad pro Zeile.
Ausführbare Dateien in der Weißliste müssen mit der Baseline übereinstimmen.	Einer ausführbaren Datei in der Weißliste ist der uneingeschränkte Zugriff nur erlaubt, wenn sie mit der Baseline der Integritätsprüfung übereinstimmt.
Beim Öffnen einer Datei scannen	Geben Sie an, ob Dateien beim Öffnen gescannt werden sollen.
Beim Schließen einer Datei scannen	Geben Sie an, ob Dateien beim Schließen gescannt werden sollen.
Beim Ausführen einer ausführbaren Datei scannen	Geben Sie an, ob Dateien beim Ausführen gescannt werden sollen.
In Archiven scannen	Gibt an, ob Archive in den Echtzeit-Scanvorgang einbezogen werden sollen. Zu den unterstützten Archivformaten gehören beispielsweise .tar, .gz und .zip.
Maximalzahl verschachtelter Archive	Definiert, bis in welche Ebene in verschachtelten Archiven gescannt wird. Es wird davon abgeraten, diesen Wert zu hoch einzustellen, da das Produkt damit anfälliger für DoS-Angriffe (Denial of Service) wird. Wenn die Zahl verschachtelter Archive in einem Archiv über diesem Wert liegt, wird ein Scanfehler generiert. Die Aktion, die das Produkt nach einem Scanfehler ausführt, kann in der Einstellung "Echtzeitschutz/Aktion nach Scanfehler" definiert werden.
Passwortgeschützte Archive als sicher behandeln	Definiert die Vorgehensweise für passwortgeschützte Archive. Mit der Einstellung "Ja" gelten passwortgeschützte Archive als sicher und der Zugriff wird zugelassen. Andernfalls wird der Zugriff nicht zugelassen.
Bei der ersten Infektion im Archiv anhalten	Definiert die Vorgehensweise bei Entdeckung der ersten Infektion in einem Archiv. Mit der Einstellung "Ja" hält der Scan-Vorgang bei der ersten Infektion an. Andernfalls wird das gesamte Archiv gescannt.
Auf Riskware scannen	Wenn Sie diese Option aktivieren, werden Riskware-Entdeckungen gemeldet und bearbeitet. Riskware ist potenzielle Spyware und sonstige Software, die in bösartiger Absicht verwendet werden kann.
Primäre Riskware-Aktion	Gibt die primäre Aktion an, die ausgeführt wird, wenn Riskware entdeckt wird. Bericht und Zugriff sperren = Der Zugriff wird gesperrt. Es wird ein Alarm gesendet. Umbennen = Die infizierte Datei erhält die Erweiterung .riskware. Löschen = Die infizierte Datei wird gelöscht. Zugriff sperren = Der Zugriff wird gesperrt. Es wird kein Alarm gesendet. Wenn die primäre Aktion fehlschlägt, wird die sekundäre Aktion ausgeführt. Wenn auch die sekundäre Aktion fehlschlägt, wird ein Alarm gesendet, der die fehlgeschlagenen Aktionen beschreibt.

Element	Beschreibung
Sekundäre Riskware-Aktion	Geben Sie die sekundäre Aktion an, die ausgeführt wird, wenn Riskware erkannt wird und die primäre Aktion fehlgeschlagen ist. Bericht und Zugriff sperren = Der Zugriff wird gesperrt. Es wird ein Alarm gesendet. Umbenennen = Die infizierte Datei erhält die Erweiterung .riskware. Löschen = Die infizierte Datei wird gelöscht. Zugriff sperren = Der Zugriff wird gesperrt. Es wird kein Alarm gesendet. Wenn die primäre Aktion fehlschlägt, wird die sekundäre Aktion ausgeführt. Wenn auch die sekundäre Aktion fehlschlägt, wird ein Alarm gesendet, der die fehlgeschlagenen Aktionen beschreibt.
Ausgeschlossene Riskware	Riskware, die vom Scan-Vorgang ausgeschlossen werden soll.

Geplanter Scan-Vorgang

Auf der Seite **Erweiterte Benutzeroberfläche** > **Virenschutz** > **Geplanter Scan-Vorgang** werden die folgenden Benutzeroberflächen-Steuerelemente angezeigt.

Element	Beschreibung
Zeitplan	Diese Tabelle enthält die geplanten Scanaufgaben, die auf ähnliche Weise wie in der Cron-Tabelle definiert sind. Der Scan-Vorgang verwendet die Einstellungen, die unter "Manuelles Scanning" definiert sind. Unter "Man Cron-Tabelle" finden Sie die zulässigen Werte für die Felder "Minute", "Stunde", "Monatstag", "Monat" und "Wochentag".

Manuelles Scannen

Auf der Seite **Erweiterte Benutzeroberfläche** > **Virenschutz** > **Manuelles Scannen** werden die folgenden Benutzeroberflächen-Steuerelemente angezeigt.

Element	Beschreibung
Primäre Aktion	Geben Sie die primäre Aktion an, die ausgeführt wird, wenn eine Infektion erkannt wird. Nichts unternehmen = Es wird nichts unternommen. (Dem Benutzer wird nur die Infektion gemeldet.) Nur Bericht = Es wird nur ein Alarm gesendet. Desinfizieren = Es wird versucht, die Datei zu desinfizieren. Umbenennen = Die infizierte Datei erhält die Erweiterung .virus. Bericht und Zugriff sperren = Zugriff sperren. Einen Alarm senden. Desinfizieren = Es wird versucht, die Datei zu desinfizieren. Umbenennen = Die infizierte Datei erhält die Erweiterung .virus. Löschen = Die infizierte Datei wird gelöscht. Benutzerdefiniert = Es wird ein Befehl ausgeführt, der im Feld "Primäre Aktion" definiert ist.. Scan-Vorgang abbrechen = Der Scan-Vorgang wird abgebrochen. Wenn die primären und sekundären Aktionen fehlschlagen, wird ein Alarm gesendet, der die fehlgeschlagenen Aktionen beschreibt.

Element	Beschreibung
Primäre benutzerdefinierte Aktion	Wenn "Benutzerdefiniert" als primäre Aktion ausgewählt wird, muss die benutzerdefinierte Aktion hier angegeben werden. Beachten Sie, dass die benutzerdefinierte Aktion als Superuser des Systems ausgeführt wird. Gehen Sie beim Spezifizieren des Befehls daher umsichtig vor und prüfen Sie ihn sorgfältig. Der benutzerdefinierte Aktionsskript oder das Programm erhalten einen Parameter, den vollständigen Pfadnamen der infizierten Datei.
Sekundäre Aktion	Geben Sie die sekundäre Aktion an, die ausgeführt wird, wenn eine Infektion erkannt wird. Nichts unternehmen = Es wird nichts unternommen. (Dem Benutzer wird nur die Infektion gemeldet.) Nur Bericht = Es wird nur ein Alarm gesendet. Desinfizieren = Es wird versucht, die Datei zu desinfizieren. Umbenennen = Die infizierte Datei erhält die Erweiterung .virus. Löschen = Die infizierte Datei wird gelöscht. Benutzerdefiniert = Es wird ein Befehl ausgeführt, der im Feld "Primäre Aktion" definiert ist. Scan-Vorgang abbrechen = Der Scan-Vorgang wird abgebrochen. Wenn die primären und sekundären Aktionen fehlschlagen, wird ein Alarm gesendet, der die fehlgeschlagenen Aktionen beschreibt.
Sekundäre benutzerdefinierte Aktion	Wenn "Benutzerdefiniert" als sekundäre Aktion ausgewählt wird, muss die benutzerdefinierte Aktion hier angegeben werden. Beachten Sie, dass die benutzerdefinierte Aktion als Superuser des Systems ausgeführt wird. Gehen Sie beim Spezifizieren des Befehls daher umsichtig vor und prüfen Sie ihn sorgfältig. Der benutzerdefinierte Aktionsskript oder das Programm erhalten einen Parameter, den vollständigen Pfadnamen der infizierten Datei.
Primäre Aktion an verdächtigen Dateien	Geben Sie die primäre Aktion an, die ausgeführt wird, wenn eine vermutliche Infektion entdeckt wird. Nichts unternehmen = Es wird nichts unternommen. (Dem Benutzer wird nur die Infektion gemeldet.) Nur Bericht = Es wird nur ein Alarm gesendet. Umbenennen = Die infizierte Datei erhält die Erweiterung .suspected. Löschen = Die infizierte Datei wird gelöscht. Wenn die primäre Aktion fehlschlägt, wird die sekundäre Aktion ausgeführt. Wenn auch die sekundäre Aktion fehlschlägt, wird ein Alarm gesendet, der die fehlgeschlagenen Aktionen beschreibt.
Sekundäre Aktion an verdächtigen Dateien	Geben Sie die sekundäre Aktion an, die ausgeführt wird, wenn eine vermutliche Infektion entdeckt wird und die primäre Aktion fehlgeschlagen ist. Nichts unternehmen = Es wird nichts unternommen. (Dem Benutzer wird nur die Infektion gemeldet.) Nur Bericht = Es wird nur ein Alarm gesendet. Umbenennen = Die infizierte Datei erhält die Erweiterung .suspected. Löschen = Die infizierte Datei wird gelöscht. Wenn die primäre Aktion fehlschlägt, wird die sekundäre Aktion ausgeführt. Wenn auch die sekundäre Aktion

Element	Beschreibung
	fehlschlägt, wird ein Alarm gesendet, der die fehlgeschlagenen Aktionen beschreibt.
Scannen von allen Dateien oder nur den Dateien mit den angegebenen Erweiterungen	Geben Sie an, ob das Produkt alle Dateien oder nur die Dateien scannen soll, die mit den Erweiterungen übereinstimmen, die in der Einstellung "Zu scannende Erweiterungen" angegeben sind.
Einbezogene Erweiterungen	Geben Sie die Liste der Dateinamenerweiterungen an, die gescannt werden sollen. Sie können auch Platzhalter verwenden: "?" entspricht genau einem Zeichen, "*" entspricht einer beliebigen Anzahl von Zeichen, einschließlich null (0) Zeichen. "." (ein einzelner Punkt), der alleinstehend eingegeben wird, entspricht Dateien ohne Erweiterung. Groß- und Kleinschreibung müssen nicht beachtet werden, um eine Übereinstimmung zu erzielen.
Ausschlüsse aktivieren	Legt fest, ob einige Dateien vom Scan-Vorgang ausgeschlossen werden können. Beachten Sie, dass die hier angegeben Dateien vom Scan-Vorgang ausgeschlossen werden, auch wenn sie aufgrund der anderen Scaneinstellungen in den Scan-Vorgang einbezogen werden müssten.
Dateien und Verzeichnisse, die vom Scan-Vorgang ausgeschlossen sind	Legt fest, ob einige Pfade (Dateien oder Verzeichnisse) vom Scan-Vorgang ausgeschlossen werden. Verwenden Sie vollständige, absolute Pfadangaben. Geben Sie jeweils einen Pfad pro Zeile ein. Pfadangaben können Leerzeichen enthalten.
Ausführbare Dateien scannen	Geben Sie an, ob ausführbare Dateien gescannt werden müssen. Wenn für eine Datei Benutzer-, Gruppen- oder andere Executable-Bits festgelegt sind, wird sie unabhängig von der Dateierweiterung gescannt.
In Archiven scannen	Gibt an, ob Archive beim Start eines manuellen Scan-Vorgangs gescannt werden sollen. Zu den unterstützten Archivformaten gehören beispielsweise .tar, .gz., .zip.
Maximalzahl verschachtelter Archive	Definiert, bis in welche Ebene in verschachtelten Archiven gescannt wird. Es wird davon abgeraten, diesen Wert zu hoch einzustellen, da das Produkt damit anfälliger für DoS-Angriffe (Denial of Service) wird. Wenn die Zahl verschachtelter Archive in einem Archiv über diesem Wert liegt, wird ein Scanfehler generiert.
Passwortgeschützte Archive als sicher behandeln.	Definiert die Vorgehensweise für passwortgeschützte Archive. Mit der Einstellung "Ja" gelten passwortgeschützte Archive als sicher und der Zugriff wird zugelassen. Andernfalls wird der Zugriff nicht zugelassen.
Bei erster Infektion in einem Archiv anhalten.	Definiert die Vorgehensweise nachdem die erste Infektion in einem Archiv gefunden wurde. Mit der Einstellung "Ja" hält der Scan bei der ersten Infektion an. Andernfalls wird das gesamte Archiv gescannt.

Element	Beschreibung
Auf Riskware scannen	Wenn Sie diese Option aktivieren, wird Riskware gemeldet und bearbeitet. Riskware ist potenzielle Spyware.
Primäre Riskware-Aktion	Geben Sie die primäre Aktion an, die ausgeführt wird, wenn Riskware entdeckt wird. Nichts unternehmen = Es wird nichts unternommen. (Dem Benutzer wird nur die Entdeckung gemeldet.) Nur Bericht = Es wird nur ein Alarm gesendet. Umbenennen = Die infizierte Datei erhält die Erweiterung .riskware. Löschen = Die infizierte Datei wird gelöscht. Wenn die primäre Aktion fehlschlägt, wird die sekundäre Aktion ausgeführt. Wenn auch die sekundären Aktionen fehlschlägen, wird ein Alarm gesendet, der die fehlgeschlagenen Aktionen beschreibt.
Sekundäre Riskware-Aktion	Geben Sie die sekundäre Aktion an, die ausgeführt wird, wenn Riskware entdeckt wird und die primäre Aktion fehlgeschlagen ist. Nichts unternehmen = Es wird nichts unternommen. (Dem Benutzer wird nur die Entdeckung gemeldet.) Nur Bericht = Es wird nur ein Alarm gesendet. Umbenennen = Die infizierte Datei erhält die Erweiterung .riskware. Löschen = Die infizierte Datei wird gelöscht. Wenn die primäre Aktion fehlschlägt, wird die sekundäre Aktion ausgeführt. Wenn auch die sekundäre Aktion fehlschlägt, wird ein Alarm gesendet, der die fehlgeschlagenen Aktionen beschreibt.
Ausgeschlossene Riskware	Typ der Riskware, die nicht entdeckt werden soll.
Zugriffszeiten beibehalten	Wenn diese Einstellung aktiviert ist, werden die Zugriffszeiten beim Scannen nicht geändert. Wenn eine Datei aufgrund einer Desinfektion geändert wird, ändern sich die Zugriffs- und Änderungszeiten.

Firewall

In den folgenden Tabellen werden die Firewall-Einstellungen dargestellt.

Allgemeine Einstellungen

Auf der Seite **Erweiterte Benutzeroberfläche** > **Firewall** > **Allgemeine Einstellungen** werden die folgenden Benutzeroberflächen-Steuerelemente angezeigt.

Element	Beschreibung
Firewall aktivieren	Gibt an, ob die Firewall aktiviert oder deaktiviert ist. Wenn sie aktiviert ist, werden die Firewall-Regeln der ausgewählten Sicherheitsstufe auf ein- und ausgehende Pakete angewandt. Wenn sie deaktiviert ist, wird der gesamte Datenverkehr zugelassen. Zum vollständigen Deaktivieren der Firewall-Komponente verwenden Sie das Programm fschooser.
Alle unbehandelten Netzwerkpakete protokollieren	Wenn diese Option aktiviert ist, erstellt die Firewall eine Regel, die in syslog alle Pakete aufzeichnet, die keiner der Firewall-Regeln in der aktuellen Sicherheitsstufe entsprechen. Wird sie aktiviert,

Element	Beschreibung
	werden unter Umständen zahlreiche Protokolleinträge erstellt (abhängig von den Firewall-Regeln und dem Typ des Netzwerkdatenverkehrs).
Vertrauenswürdige Netzwerkschnittstellen (durch Trennzeichen getrennte Liste)	Hier können die Namen vertrauenswürdiger Netzwerkschnittstellen angegeben werden. Mehrere Namen werden mit einem Komma getrennt. Der gesamte Datenverkehr zu und von diesen Schnittstellen wird zugelassen.

Regeln

Auf der Seite **Erweiterte Benutzeroberfläche** > **Firewall** > **Firewall-Regeln** werden die folgenden Benutzeroberflächen-Steuerelemente angezeigt.

Element	Beschreibung
Zu bearbeitendes Profil	Diese Tabelle enthält die Namen und Beschreibungen der Sicherheitsstufen. Einige Sicherheitsstufen wurden vorab definiert, um Administratoren beim Erstellen ihrer eigenen verwalteten Umgebung zu unterstützen. Standardmäßig sind einige dieser Sicherheitsstufen aktiviert, andere sind deaktiviert.
Firewall-Regeln	Diese Tabelle enthält die Firewall-Regeln. Firewall-Regeln filtern IP-Pakete auf Basis von IP-Adressen, Portnummern usw. Beachten Sie, dass normalerweise mehr als eine Sicherheitsstufe definiert ist und Sie zu einem Zeitpunkt nur die Regeln für jeweils eine Sicherheitsstufe definieren können.

Netzwerkdienste

Auf der Seite **Erweiterte Benutzeroberfläche** > **Firewall** > **Netzwerkdienste** werden die folgenden Benutzeroberflächen-Steuerelemente angezeigt.

Element	Beschreibung
Netzwerkdienste	Diese Tabelle enthält die Definitionen der Dienste, mit denen Firewall-Regeln konfiguriert werden können. Die Protokolle finden Sie bei IANA oder unter "grep IPPROTO.*= /usr/include/netinet/in.h" (vorausgesetzt, Sie haben enthaltene Elemente installiert) Offiziell zugewiesene Ports sind erhältlich unter: ftp://ftp.iana.org/assignments/port-numbers

Integritätsprüfung

In den folgenden Tabellen werden die Einstellungen der Integritätsprüfung dargestellt.

Bekannte Dateien

Auf der Seite **Erweiterte Benutzeroberfläche** > **Integritätsprüfung** > **Bekannte Dateien** werden die folgenden Benutzeroberflächen-Steuerelemente angezeigt.

Element	Beschreibung
Bekannte Dateien	Diese Tabelle enthält Dateien, die zur Integritätsprüfung hinzugefügt wurden.

Allgemeine Einstellungen

In den folgenden Tabellen werden die allgemeinen Einstellungen dargestellt.

Kommunikation

Auf der Seite **Erweiterte Benutzeroberfläche** > **Allgemein** > **Kommunikation** werden die folgenden Benutzeroberfläche-Steuerelemente angezeigt.

Element	Beschreibung
Serveradresse	URL von F-Secure Management Server. Der Inhalt des Kommunikationsverzeichnis-Alias und das dienstspezifische Verzeichnis und der Dateiname werden mit dieser Adresse verknüpft, wenn HTTP-GET-Vorgänge ausgeführt werden. Der URL-Tail wird mit dieser Adresse verknüpft, wenn auf die anderen Serverfunktionen zugegriffen wird.
Policy Manager Server-Zertifikat heraufladen	Der Administrator kann mit dieser Einstellung den Managementschlüssel ändern.
Alarmweiterleitung	Gibt an, wohin die Alarme auf Basis ihrer Schweregardeinstufung gesendet werden.
Server	Die Adresse des SMTP-Servers in der Form <Host>[:<Port>], wobei "Host" der DNS-Name oder die IP-Adresse des SMTP-Servers und "Port" die SMTP-Serverportnummer ist. Weitere Informationen finden Sie in der RFC 2821-Spezifikation.
Von	Die E-Mail-Adresse des Absenders, die in das Feld "Von:" der E-Mail-Nachricht eingefügt wird, die den Alarm enthält.
Betreff	Betreff der SMTP-Alarmmeldung. Außer dem Text können die folgenden Symbole verwendet werden: - %SEVERITY% (Information, Warnung, Fehler, schwerwiegender Fehler, Sicherheitsalarm) - %HOST_DNS% (DNS-Adresse des Hosts, der den Alarm gesendet hat) - %HOST_IP% (IP-Adresse des Hosts, der den Alarm gesendet hat) - %USER% (Anmeldename des aktiven Benutzers) - %PRODUCT_NAME% (Name des Produkts, das den Alarm generiert hat) - %PRODUCT_OID% (OID des Produkts, das den Alarm generiert hat) - %DESCRIPTION% (Alarmbeschreibung) - %DATE% (Datum, an dem ein Alarm gesendet wird, im Format JJJJ-MM-TT) - %TIME% (Uhrzeit, zu der ein Alarm gesendet wird, im Format SS:MM:SS+GMT) - %ALERT_NUMBER% (Alarmnummer während der Sitzung)

Automatische Updates

Auf der Seite **Erweiterte Benutzeroberfläche** > **Allgemein** > **Automatische Updates** werden die folgenden Benutzeroberfläche-Steuerelemente angezeigt.

Element	Beschreibung
Updates aktiviert	Aktivieren bzw. Deaktivieren der Prüfung auf Verfügbarkeit neuer Updates. Wenn die Option "Deaktiviert" gewählt wird, prüft der Automatic Update Agent nicht automatisch, ob neue Updates verfügbar sind. Vom Benutzer ausgeführte Updates werden jedoch nicht verhindert (Schaltfläche "Jetzt prüfen"). Beachten Sie, dass diese Einstellung nur für Workstation-Produkte verfügbar ist.
F-Secure Anti-Virus-Proxys	Diese Tabelle enthält die Liste der Policy Manger-Proxys in Reihenfolge ihrer Priorität. Ein Policy Manager-Proxy wird verwendet, um die Serverauslastung durch Zwischenspeichern des Policy Manager-Inhalts im Proxy zu verringern. F-Secure Automatic Update Agent stellt zunächst über die konfigurierten Policy Manager-Proxys eine Verbindung zum Policy Manager Update-Server her. Anschließend stellt er eine direkte Verbindung zum Policy Manager Update-Server her. Darauf folgt eine Verbindung zum F-Secure Update Server über die konfigurierten Policy Manager-Proxys. Anschließend stellt er eine direkte Verbindung zum F-Secure Update-Server her.
HTTP-Proxy verwenden	Zum Kontigurieren wird das HTTP-Proxy verwendet. Beachten Sie, dass in Windows NT, 2000, XP und 2003 die Proxy-Einstellungen der Browsereinstellungen jeweils für ein Benutzerkonto gelten und in den meisten Fällen nicht entdeckt werden können, wenn kein Benutzer angemeldet ist. Alle Verbindungen zwischen dem Automatic Update Agent und einem Update-Server oder PM-Proxy verlaufen über ein HTTP-Proxy. Wenn ein HTTP-Proxy nicht erreicht werden kann, wechselt der Automatic Update Agent zurück zu einer direkten Verbindung.
HTTP-Proxy-Adresse	Benutzerdefinierte HTTP-Proxy-Adresse. Diese Option wird verwendet, wenn "HTTP-Proxy verwenden" auf "Benutzerdefiniert" eingestellt ist. Dies kann als http://[Benutzer[:Passwort]@]Host:port definiert werden, z. B.: http://meinproxy.com http://meinproxy.com:8080 http://thomasmustermann@meinproxy.com http://thomasmustermann:geheimespasswort@meinproxy.com Benutzername und Passwort sind optionale Felder. Die Authentifizierung kann auch in der Benutzeroberfläche der Anwendung konfiguriert werden.
Failoverzeit des Zwischenservers (Min.)	Gibt den Zeitraum an, in dem F-Secure Automatic Update Agent versuchen soll, eine Verbindung zum Zwischenserver herzustellen, bevor er zum F-Secure Update-Server wechselt.

Element	Beschreibung
Abrufen von Updates vom F-Secure Update Server zulassen	Legt fest, ob es dem Automatic Update Agent erlaubt wird, eine Verbindung zum F-Secure Update-Server herzustellen. Wenn für diese Einstellung "Nein" festgelegt wird, stellt der Automatic Update-Server niemals eine direkte Verbindung zum F-Secure Update-Server her.
Scan-Vorgang nach Updates starten	Gibt an, ob alle lokalen Festplatten gescannt werden, nachdem neue Datenbanken in Betrieb genommen wurden.
Erinnerungen senden	Definiert, ob Benutzer daran erinnert werden, die Virusdefinitionsdatenbanken manuell zu aktualisieren, wenn das Alter der Datenbanken das definierte Zeitlimit überschreiten.
Datenbanken altern in Tagen, bevor die Erinnerungen versendet werden.	Definiert, wie viele Tage seit der Veröffentlichung der aktuell verwendeten Virusdefinitionen verstrichen sein müssen, bevor der Benutzer daran erinnert wird, sie zu aktualisieren.

Anhang

D

Liste von Traps

Trap-Nummer, Schweregrad und Trab-Beschreibungen.

Integritätsprüfung

Liste der FSIC- Traps:

Trap-Nummer	Schweregrad	Beschreibung
710	Sicherheitsalarm	Integritätsprüfungs-Baseline bei Host generiert
711	Sicherheitsalarm	Gültigkeitsprüfung der Integritätsprüfungs-Baseline fehlgeschlagen. Baseline wurde beeinträchtigt oder die Passphrase, die zur Verfizierung der Baseline verwendet wurde, ist falsch
730	Sicherheitsalarm	Integritätsprüfung für Datei fehlgeschlagen
799	Fehler	Baseline-Einträge konnten nicht in Richtlinie gespeichert werden

Policy Manager

Die Liste der FSAVPMD-Traps. Alle anderen Alarmmeldungen, die von einem Perl-Script gesendet wurden, weisen die Stufe "FEHLER" auf.

Trap-Nummer	Schweregrad	Beschreibung
50	Information	Scan gestartet
51	Information	Scan beendet
60	Information	Datenbankaktualisierung gestartet
61	Information	Datenbankaktualisierung beendet
100	Sicherheitsalarm	Virenzugriffs-Alarmmeldung
150	Information	Prozess gestartet
151	Information	Prozess gestoppt
152	Schwerwiegender Fehler	Prozess abgestürzt
153	Schwerwiegender Fehler	Prozess-Start fehlgeschlagen

Trap-Nummer	Schweregrad	Beschreibung
158	Information	F-Secure Anti-Virus Linux Security gestartet
159	Information	F-Secure Anti-Virus Linux Security gestoppt
170	Sicherheitsalarm	Testzeitraum abgelaufen
171	Information	Testversion
200	Sicherheitsalarm	Virusalarm
201	Sicherheitsalarm	Virusalarm: Desinfiziert
202	Sicherheitsalarm	Virusalarm: Datei gelöscht
203	Sicherheitsalarm	Virusalarm: Datei umbenannt
204	Sicherheitsalarm	Virusalarm: Nicht desinfiziert
205	Sicherheitsalarm	Virusalarm: Maßnahme fehlgeschlagen
206	Sicherheitsalarm	Virusalarm: Benutzerdefinierte Maßnahme ausgeführt
207	Sicherheitsalarm	Virusalarm: Scan abgebrochen
322	Information	Datenbankaktualisierungs-Dateien erhalten
500	Information	Integrität der Virusdefinitionsdantenbank erfolgreich überprüft
999	Information	Debug-Ausgabe

Gültigkeitsprüfung der Virendefinitionsdatenbank

Die Liste der DAAS- Traps.

Trap-Nummer	Schweregrad	Beschreibung
506	Warnung	Zusätzliche Dateien im Datenbankaktualisierungspaket gefunden
512	Warnung	Das Paket wurde verändert
513	Warnung	Ungültige oder fehlende Manifestdatei
514	Warnung	Ungültiges oder fehlendes Manifestdateizertifikat
515	Warnung	Die Aktualisierung der Virendefinitionsdatenbank ist älter als die zuvor aktzeptierte
516	Warnung	Die Manifestdatei weist kein entsprechendes Zertifikat auf
518	Warnung	Ungültiges oder fehlender F-Secure Corporation-Zertifikat

Trap-Nummer	Schweregrad	Beschreibung
519	Warnung	Ungültiges oder fehlender Zertifikat vom Verleger der Virendefinitionsdatenbank
520	Warnung	Kein Zertifikat des Verlegers entspricht dem Manifestdateizertifikat
521	Warnung	Das Zertifikat in dem Paket wurde nicht von F-Secure Corporation ausgegeben
522	Warnung	Das Zertifikat des Verlegers war nicht gültig, als die Datenbankaktualisierung veröffentlicht wurde
523	Warnung	Das Zertifikat des Verlegers im Paket gewährt kein Recht zur Veröffentlichung von Datenbankaktualisierungen
530	Warnung	Das Verlegerzertifikat im Paket wurde aufgehoben, als die Datenbankaktualisierung veröffentlicht wurde
531	Warnung	Das Verlegerzertifikat in diesem Paket wurde aufgrund eines schwerwiegenden Problems zurückgezogen
535	Warnung	Ungültige oder fehlende Widerrufsdatei
550	Warnung	Nicht genügen Arbeitsspeicher, um den Vorgang abzuschließen
551	Warnung	Während des Vorgangs ist ein Datei-E/A-Fehler aufgetreten
552	Warnung	Nicht unterstützter Datenbanktyp

DBTool

Die Liste der DBTool-Traps.

Trap-Nummer	Schweregrad	Beschreibung
4	Fehler	Datei nicht gefunden
308	Fehler	Datei kann nicht geöffnet werden
309	Fehler	Datei ist verschlüsselt
310	Fehler	Scan einer Datei kann zurzeit nicht abgeschlossen werden
311	Fehler	Schreiben in Datei nicht möglich
323	Fehler	Die Virendefinitionsdatenbank-Datei ist ungültig
324	Fehler	Die Virendefintionsdatenbank-Datei ist ungültig. Die Integritätsprüfung für die Datenbankdatei ist fehlgeschlagen.

Firewall

Liste der Firewall-Daemon-Traps.

Trap-Nummer	Schweregrad	Beschreibung
153	Schwerwiegender Fehler	Prozess nicht gestartet
801	Information	Firewall aktiviert
802	Fehler	Firewall deaktiviert
803	Fehler	Firewall-Regeln konnten nicht eingestellt werden
804	Information	Firewall-Regeln aktualisiert

Anti-Virus

Die Liste der Zugriffsscanner-Traps

Trap-Nummer	Schweregrad	Beschreibung
150	Information	Prozess gestartet
153	Schwerwiegender Fehler	Prozess nicht gestartet
200	Sicherheitsalarm	Virusalarm
201	Sicherheitsalarm	Virusalarm: Desinfiziert
202	Sicherheitsalarm	Virusalarm: Datei gelöscht
203	Sicherheitsalarm	Virusalarm: Datei umbenannt
205	Sicherheitsalarm	Virusalarm: Maßnahme fehlgeschlagen
220	Sicherheitsalarm	Riskware-Alarm
221	Sicherheitsalarm	Riskware-Alarm: Desinfiziert
222	Sicherheitsalarm	Riskware-Alarm: Datei gelöscht
223	Sicherheitsalarm	Riskware-Alarm: Datei umbenannt
225	Sicherheitsalarm	Riskware-Alarm: Maßnahme fehlgeschlagen
301	Fehler	Scan-Fehler
309	Fehler	Datei verschlüsselt
318	Fehler	Scan abgebrochen
600	Sicherheitsalarm	Schwerwiegender Fehler bei Echtzeitschutz
700	Sicherheitsalarm	Schwerwiegender Fehler bei Integritätsprüfung
720	Sicherheitsalarm	Hash-Berechnung für Integritätsprüfung fehlgeschlagen

Trap-Nummer	Schweregrad	Beschreibung
721	Sicherheitsalarm	Attributsprüfung für Datei bei Integritätsprüfung fehlgeschlagen
730	Sicherheitsalarm	Von Integritätsprüfung überprüfte Datei beschädigt
731	Sicherheitsalarm	Integritätsprüfung hat einen Änderungsversuch verhindert, um eine Datei zu schützen
733	Sicherheitsalarm	Nicht verwendbar mit Produktversion 9.10 und höher
734	Sicherheitsalarm	Nicht verwendbar mit Produktversion 9.10 und höher
735	Sicherheitsalarm	Nicht verwendbar mit Produktversion 9.10 und höher
736	Sicherheitsalarm	Kernel vor Veränderung geschützt
741	Sicherheitsalarm	Kernel verändert

Anhang

E

Weitere Hilfe

Wenn Sie keine Antwort auf Ihre Fragen finden, können Sie im Internet nach weiteren Informationen suchen oder mit einem Experten sprechen.

Der `fsdiag`-Bericht, der vom Diagnosetool von F-Secure generiert wird, enthalt wichtige Daten von Ihrem System. Die Informationen sind für unsere Support-Mitarbeiter erforderlich, damit diese Ihr Problem lösen können. Nach der Ausführung von `fsdiag`, wird der `fsdiag.tar.gz`-Bericht im aktuellen Verzeichnis erstellt.

Der Bericht enthält Informationen zu F-Secure-Produkten sowie Betriebssystemprotokolle und Systemeinstellungen. Die erfassten Daten sind für die Lösung des Problems und zur Problembehandlung unerlässlich. In einigen Fällen können die Informationen als vertraulich eingestuft werden. Beachten Sie, dass die erfassten Daten lokal gespeichert werden.

Wechseln Sie zu *http://support.f-secure.com*, um weitere Informationen zur Fehlerbehandlung und zur Kontaktaufnahme mit unserem technischen Support zu erhalten.