F-Secure Client Security

Administratorhandbuch

Inhalt

Kapitel 1: Einführung.....9

Systemanforderungen.....10
Policy Manager Server.....10
Policy Manager Console.....10
Hauptkomponenten.....11
Funktionen.....12
Produktregistrierung.....13
Anwendungsverwaltung.....13
Grundlegende Terminologie.....14

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

Installationsschritte.....16
Herunterladen und Ausführen des Installationspakets.....16
Auswählen der zu installierenden Komponenten.....16
Abschließen des Migrationsassistenten.....17
Abschließen der Produktinstallation.....17
Ändern des Pfads für den Webbrowser.....18
das Produkt deinstallieren.....18

Kapitel 3: Benutzeroberfläche für Anti-Virus-Modus.....19

Anmelden.....20
Verbindungseigenschaften.....20
Neue Benutzer hinzufügen.....20
Ändern des Kennworts.....20
Registerkarte "Richtliniendomänen".....21
Registerkarten für Verwaltungsaufgaben.....21
Registerkarte "Zusammenfassung".....21
Registerkarte "Einstellungen".....24
Registerkarte "Status".....33
Registerkarte "Alarme".....35
Registerkarte "Scan-Berichte".....36
Registerkarte "Installation".....36
Registerkarte "Operationen".....37
Die Symbolleiste.....37
Menübefehle.....38
Vererbung von Einstellungen.....40
Anzeige der Vererbung von Einstellungen auf der Benutzeroberfläche.....40
Alle Einstellungen auf einer Seite gleichzeitig sperren oder Sperre aufheben.....41

Vererbung von Einstellungen in Tabellen....41

Kapitel 4: Einrichten eines verwalteten Netzwerks....43

Verwalten von Domänen und Hosts....44
Hinzufügen von Richtliniendomänen....44
Hinzufügen von Hosts....44
Importieren von Hosts aus einer Active Directory-Struktur....44
Hinzufügen von Hosts in Windows-Domänen....45
Importieren neuer Hosts....45
Push-Installationen....48
Installation auf Richtlinienbasis....50
Lokale Installation und Updates mit vorkonfigurierten Paketen....52
Lokale Installation und Policy Manager....53
Systemanforderungen....54
Deinstallieren anderer Virenschutzprogramme....54
Installationsschritte....54
Installation auf einem infizierten Host....55
Überprüfen der Management-Verbindungen....56

Kapitel 5: Konfigurieren von Viren- und Spyware-Schutz....57

Konfigurieren automatischer Updates....58
So funktionieren automatische Updates....58
Einstellungen für automatische Updates....58
Konfigurieren der automatischen Updates von Policy Manager Server....58
Konfigurieren von Policy Manager Proxy....59
Konfigurieren von Clients zum Herunterladen von Updates von anderen Clients....60
Konfigurieren des Echtzeit-Scanning....60
Einstellungen für das Echtzeit-Scanning....60
Aktivieren des Echtzeit-Scannings für die gesamte Domäne....62
Erzwingen der Verwendung des Echtzeit-Scannings auf allen Hosts....62
Ausschließen von Microsoft Outlook PST-Dateien vom Echtzeit-Scanning....63
Konfigurieren von DeepGuard....63
DeepGuard-Einstellungen....64
DeepGuard-Serverabfragen....64
Konfigurieren des Rootkit-Scannings (Blacklight)....65
Einstellungen für das Rootkit-Scanning....65
Starten eines Rootkit-Scannings für die gesamte Domäne....65
Konfigurieren des E-Mail-Scannings....66
Einstellungen für das E-Mail-Scanning....66
Aktivieren des E-Mail-Scannings für eingehende und ausgehende E-Mails....67
Konfigurieren von Web Traffic (HTTP) Scanning....68
Einstellungen für das Web Traffic Scanning....68
Aktivieren von Web Traffic Scanning für die gesamte Domäne....68

Ausschließen einer Website vom Web Traffic Scanning....68
Konfigurieren des Spyware-Scannings....69
Einstellungen der Spyware-Steuerung....70
Einrichten der Spyware-Steuerung für die gesamte Domäne....71
Ausführen des Spyware-Scannings in der gesamten Domäne....71
Zulassen eines Spyware- oder Riskware-Elements....72
Verwalten unter Quarantäne gestellter Objekte....72
Löschen von Objekten, die unter Quarantäne stehen....72
Wiederherstellen von Objekten aus der Quarantäne....73
Verhindern, dass Benutzer Einstellungen eigenmächtig ändern....73
Alle Virenschutz-Einstellungen als endgültig definieren....74
Konfigurieren der Alarmmeldungen....74
Einrichten der Weiterleitung von Client Security-Virenbenachrichtigungen an eine E-Mail-Adresse.74
Deaktivieren der Alarm-Popups von Client Security....75
Überwachen der Virenvorfälle im Netzwerk....75
Überprüfen der Virenschutzfunktionen....75

Kapitel 6: Konfigurieren von Internet Shield....77

Globale Firewall-Sicherheitsstufen....78
Designgrundlagen für die Sicherheitsstufe....79
Konfigurieren von Sicherheitsstufen und Regeln....79
Wählen Sie einer aktive Sicherheitsstufe für eine Workstation....80
Konfigurieren einer Standard-Sicherheitsstufe für die verwalteten Hosts....80
Hinzufügen einer neuen Sicherheitsstufe für eine bestimmte Domäne....80
Konfigurieren der Netzwerk-Quarantäne....82
Einstellungen der Netzwerk-Quarantäne....82
Aktivieren der Netzwerk-Quarantäne für die gesamte Domäne....83
Anpassen der Netzwerk-Quarantäne....83
Konfigurieren von Warnmeldungen nach Regelverletzungen....83
Hinzufügen einer neuen Regel mit Alarmausgabe....83
Konfigurieren der Anwendungssteuerung....86
Einstellungen für die Anwendungssteuerung....87
Erstmaliges Einrichten der Anwendungssteuerung....88
Erstellen einer Regel für eine unbekannte Anwendung auf Root-Ebene....88
Bearbeiten einer vorhandenen Regel für die Anwendungsteuerung....89
Deaktivieren des Popup-Fensters der Anwendungssteuerung....90
Verwenden von Alarmen zum Prüfen der Funktionsweise von Internet Shield....90
Konfigurieren der Intrusion Prevention....91
Einstellungen für Intrusion Prevention....91
Konfigurieren von IPS für Desktops und Laptops....92

Kapitel 7: So prüfen Sie, ob die Netzwerkumgebung geschützt ist.93

Überprüfen, ob alle Hosts über die neueste Richtlinie verfügen....94

Überprüfen, ob sich die neuesten Virendefinitionen auf dem Server befinden.....94
Überprüfen, ob die Hosts über die neuesten Virendefinitionen verfügen.....94
Überprüfen, ob alle Hosts verbunden sind.....95
Anzeigen von Scan-Berichten.....95
Anzeigen von Alarmen.....95
Erstellen eines wöchentlichen Infektionsberichts.....96
Überwachen eines möglichen Netzwerkangriffs.....96

Kapitel 8: Aktualisieren der Software.....97

Verwenden von richtlinienbasierter Installation.....98

Kapitel 9: Arbeitsvorgänge auf lokalen Hosts.....101

Manuell scannen.....102
Art des manuellen Scans auswählen 102
Malware automatisch bereinigen.....103
Ergebnisse manueller Scans anzeigen.....104
Zu festgelegten Zeiten scannen.....105
Planen von Scans.....105
Geplanten Scan abbrechen 105
Ergebnisse geplanter Scans anzeigen.....106
Wo finde ich die Alarmmeldungen und Protokolldateien der Firewall?.....106
Firewall-Alarme anzeigen.....106
Aktionsprotokoll anzeigen.....108
Datenverkehr im Netzwerk mit Paketprotokollierung überwachen.....108
Manuelles Herstellen einer Verbindung mit Policy Manager und Importieren einer Richtliniendatei.110
Aussetzen von Downloads und Updates.....110
Benutzern erlauben, F-Secure-Produkte aus dem Speicher zu entfernen.....111

Kapitel 10: Vireninformationen.....113

Malware-Informationen und Tools auf den F-Secure-Webseiten.....114
Richtlinien für den Versand von Virenproben an F-Secure.....114
Versandrichtlinien für Virenproben.....114
Benötigte Dateien.....114
Versandrichtlinien für Virenproben.....116
Vorgehensweise bei einem Virusausbruch.....116

Kapitel 11: Einrichten des Cisco NAC-Plugins.....119

Installieren des Cisco NAC-Plugins.....120
Importieren der Posture Validation-Attributdefinitionen.....120
Verwenden von Attributen für Posture Token der Anwendung.....120

Kapitel 12: Erweiterte Funktionen: Viren- und Spyware-Schutz..123

Konfigurieren geplanter Scan-Vorgänge....124
Erweiterte Einstellungen von DeepGuard....125
Administratoren die Zulassung oder Ablehnung von Ereignissen von Programmen anderer Benutzer gestatten. 125
Von einer bestimmten Anwendung angeforderte Ereignisse automatisch zulassen oder ablehnen. 125
Konfigurieren von Policy Manager Proxy....126
Konfigurieren automatischer Updates der Hosts vom Policy Manager Proxy....126
Ausschließen von Anwendungen für den Web Traffic Scanner....127

Kapitel 13: Erweiterte Funktionen: Internet Shield....129

Remote-Verwaltung der Eigenschaften von Internet Shield....130
Einsatz der Paketprotokollierung....130
Verwenden der vertrauenswürdigen Schnittstelle....130
Einsatz der Paketfilterung....131
Konfigurieren der automatischen Auswahl der Sicherheitsstufe....131
Fehlerbehebung bei Verbindungsproblemen....132
Hinzufügen neuer Dienste....133
Erstellen eines neuen Internet-Dienstes auf Grundlage von Standard-HTTP....133
Einrichten der Verbindungskontrolle....135
Zulassen und Sperren von Telefonnummern....135
Einsatz der Anrufprotokollierung....136

Kapitel 14: Ändern von prodsett.ini....137

Konfigurierbare prodsett.ini-Einstellungen....138

Kapitel 15: Alarm- und Fehlermeldungen beim E-Mail-Scanning.147

Warn- und Fehlermeldungen....148

Kapitel

1

Einführung

Themen:

- *Systemanforderungen*
- *Hauptkomponenten*
- *Funktionen*
- *Produktregistrierung*
- *Anwendungsverwaltung*
- *Grundlegende Terminologie*

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

Mit Policy Manager können folgende Aufgaben ausgeführt werden:

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

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

Systemanforderungen

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

Policy Manager Server

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

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

Policy Manager Console

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

Betriebssystem:	Microsoft Windows: • Windows XP Professional (SP2 oder höher) • Windows Vista (32-Bit oder 64-Bit) mit oder ohne SP1; Business, Enterprise oder Ultimate Editionen • Windows 7 (32-Bit oder 64-Bit) mit oder ohne SP1; Professional, Enterprise oder Ultimate Editions • Microsoft Windows Server 2003 SP1 oder höher (32-Bit); Standard, Enterprise, Web Edition oder Small Business Server Editionen

	• Windows Server 2003 SP1 oder höher (64-Bit); Standard oder Enterprise Editionen • Windows Server 2008 SP1 (32-Bit); Standard, Enterprise oder Web Server Editionen • Windows Server 2008 SP1 (64-Bit); Standard, Enterprise, Web Server, Small Business Server oder Essential Business Server Editionen • Windows Server 2008 R2 mit oder ohne SP1; Standard, Enterprise oder Web Server Edition
Prozessor:	P4-2-GHz-Prozessor
Arbeitsspeicher:	512 MB - 1 GB RAM, abhängig vom Betriebssystem und der Größe der verwalteten Umgebung.
Speicherplatz:	200 MB freier Festplattenspeicher.
Anzeige:	16-Bit-Grafik mit einer Auflösung von 1024 x 768 (32-Bit-Farbe bei einer Auflösung von 1280 x 1024 oder höher wird empfohlen).
Netzwerk:	100-Mbit-Netzwerk.

Hauptkomponenten

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

Policy Manager Console

Policy Manager Console stellt eine zentrale Verwaltungskonsole bereit, mit der alle Sicherheitsaspekte der verwalteten Hosts kontrolliert und gesteuert werden können. Mit dieser Komponente kann der Administrator das Netzwerk in logische Einheiten für übergreifende Richtlinien strukturieren. Diese Richtlinien werden auf Policy Manager Console definiert und danach über den Policy Manager Server an die Arbeitsstationen verteilt. Policy Manager Console ist eine *Java*-basierte Anwendung, die auf verschiedenen Plattformen installiert werden kann. Hiermit können Sie Management Agent von einem entfernten Standort ohne jegliche Eingriffe durch den Endbenutzer, Anmeldeskripts oder Neustarts auf anderen Arbeitsstationen installieren.

Policy Manager Console verfügt über zwei Benutzeroberflächen:

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

Policy Manager Server

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

Management Agent

Management Agent implementiert die Sicherheitsrichtlinien, die vom Administrator für die verwalteten Hosts festgelegt werden, und stellt für die Endbenutzer eine Benutzeroberfläche

und weitere Dienste bereit. Er steuert alle Verwaltungsfunktionen auf einer lokalen Arbeitsstation, bietet eine gemeinsame Schnittstelle für alle F-Secure-Anwendungen und arbeitet innerhalb der Verwaltungsinfrastruktur auf Richtlinienbasis.

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

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

Funktionen

Hier werden einige der Hauptfunktionen von Policy Manager beschrieben.

Software-Verteilung

- Installation von F-Secure-Produkten auf den Hosts von einem zentralen Standort aus und Aktualisierung der Programm- und Datendateien inkl. der Virendefinitions-Updates.
- Updates können unter Zuhilfenahme mehrerer Methoden bereitgestellt werden:
  - Von einer F-Secure-CD.
  - Von der F-Secure-Website zum Kunden. Diese Updates können automatisch vom Automatic Update Agent installiert (Push-Installation) oder manuell von der F-Secure-Website abgerufen werden.
- Mit Policy Manager Console können vorkonfigurierte Installationspakete exportiert werden, die auch über Fremdanbietersoftware, wie SMS oder ähnliche Tools, bereitgestellt werden können.

Konfiguration und Richtlinienverwaltung

- Zentrale Konfiguration von Sicherheitsrichtlinien. Die Richtlinien werden vom Administrator über den Policy Manager Server an die Arbeitsstationen der Benutzer verteilt. Die Integrität der Richtlinien wird mithilfe digitaler Signaturen gewährleistet.

Ereignisverwaltung

- Berichterstattung an Event Viewer (lokale Protokolle und Remote-Protokolle), SNMP-Agent, E-Mail, Berichtdateien und die Erstellung von Ereignisstatistiken.

Leistungsmanagement

- Verarbeitung und Berichterstellung für Statistiken und Leistungsdaten.

Aufgabenverwaltung

- Verwaltung der Aufgaben zur Virenüberprüfung und anderer Vorgänge.

Produktregistrierung

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

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

Warum erfasst F-Secure Daten?

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

Welche Informationen werden gesendet?

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

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

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

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

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

Anwendungsverwaltung

Policy Manager umfasst verschiedene Komponenten zur Verwaltung der Anwendungen innerhalb eines Netzwerks.

Management Agent

Der Management Agent setzt die vom Administrator festgelegten Sicherheitsrichtlinien auf den verwalteten Hosts um. Auf den Hosts dient das Programm als zentrale Konfigurationskomponente und wertet beispielsweise die Richtliniendateien aus, sendet Anforderungen zur automatischen Registrierung und Host-Statusinformationen an Policy Manager und führt richtlinienbasierte Installationen durch.

Unterstützung für Cisco Network Admission Control (NAC)

F-Secure Corporation ist Teilnehmer der von Cisco Systems® geleiteten *Network Admission Control*-Initiative (*NAC*). Cisco NAC schränkt den Netzwerkzugriff für Hosts mit veralteten Virendefinitionsdatenbanken bzw. mit deaktivierter Anti-Virus-Software oder Firewall ein.

Grundlegende Terminologie

Hier finden Sie eine Beschreibung der am häufigsten verwendeten Begriffe in diesem Handbuch.

Host

Ein Host ist ein Computer, der mit Policy Manager zentral verwaltet wird.

Richtlinie

Eine Sicherheitsrichtlinie besteht aus einer Anzahl genau festgelegter Regeln, die bestimmen, wie vertrauliche Daten und andere Ressourcen verwaltet, geschützt und verteilt werden sollen. Die Verwaltungsarchitektur von F-Secure verwendet Richtlinien, die vom Administrator zentral konfiguriert werden, um eine optimale Sicherheitskontrolle in einer Unternehmensumgebung zu gewährleisten.

Der Informationsfluss zwischen Policy Manager Console und den Hosts erfolgt durch die Übertragung von Richtliniendateien.

Richtliniendomäne

Richtliniendomänen sind Host- oder Unterdomänen-Gruppen mit einer ähnlichen Sicherheitsrichtlinie.

Richtlinienvererbung

Durch das Vererben von Richtlinien wird die Definition einer gemeinsamen Richtlinie vereinfacht. In Policy Manager Console erbt jede Richtliniendomäne automatisch die Einstellungen der übergeordneten Domäne. Auf diese Weise lassen sich große Netzwerke bequem und effizient verwalten. Die vererbten Einstellungen können auf einzelnen Hosts oder Domänen geändert werden. Wenn die vererbten Einstellungen einer Domäne geändert werden, werden diese Änderungen von allen Hosts und untergeordneten Domänen der jeweiligen Domäne übernommen.

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

Kapitel

2

Installieren von das Produkt.

Themen:

- *Installationsschritte*
- *Ändern des Pfads für den Webbrowser*
- *das Produkt deinstallieren.*

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

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

Installationsschritte

Führen Sie die Schritte in der angegebenen Reihenfolge aus, um Policy Manager Server und Policy Manager Console auf demselben Computer zu installieren.

Herunterladen und Ausführen des Installationspakets

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

So beginnen Sie mit der Installation des Produkts:

1. Laden Sie das Installationspaket unter *www.f-secure.com/webclub* herunter.

   Sie finden die Datei im Abschnitt **Download** der Seite **Policy Manager**.
2. Doppelklicken Sie auf die ausführbare Datei, um mit der Installation zu beginnen.
   Das Installationsprogramm wird gestartet.
3. Wählen Sie die Installationssprache und klicken auf **Weiter**, um fortzufahren.
4. Lesen Sie die Lizenzvereinbarung, wählen Sie dann **Lizenz annehmen** und klicken Sie auf **Weiter**, um fortzufahren.

Auswählen der zu installierenden Komponenten

Als Nächstes müssen Sie die zu installierenden Produktkomponenten auswählen.

So fahren Sie mit der Installation des Produkts fort:

1. Wählen Sie die Komponenten, die installiert werden sollen, und klicken Sie auf **Weiter**, um fortzufahren.
   - Wählen SePolicy Manager Server und Policy Manager Console, um beide Komponenten auf demselben Computer zu installieren.
   - Wählen Sie Policy Manager Server, wenn Sie Policy Manager Console auf einem anderen Computer installieren möchten.
2. Wählen Sie den Zielordner, und klicken Sie dann auf **Weiter**.

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

   Hinweis: Wenn Sie Management Agent auf demselben Computer installiert haben, wird dieses Fenster nicht angezeigt.
3. Geben Sie Ihre Kundennummer ein, und klicken Sie auf **Weiter**.

   Ihre Kundennummer finden Sie im Lizenzvertrag, der dem Produkt beigefügt ist.
4. Geben Sie ein Kennwort für Ihr admin-Benutzerkonto ein und bestätigen Sie dieses. Klicken Sie auf **Weiter**.

   Nutzen Sie dieses Kennwort für die Anmeldung bei Policy Manager Console mit dem Benutzernamen `admin`.
5. Wählen Sie die Policy Manager Server-Module, die aktiviert werden sollen:
   - Das **Host**-Modul wird für die Kommunikation mit den Hosts benötigt. Der Standard-Port ist Port 80.
   - Das **Verwaltungs-Modul** wird für die Kommunikation mit Policy Manager Console verwendet. Der Standard-HTTP-Port ist 8080.

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

Standardmäßig ist der Zugriff auf das **Verwaltungs-Modul** auf den lokalen Computer beschränkt. Dies gewährleistet die größte Sicherheit für die Verwendung des Produkts. Wenn jedoch eine Verbindung über das Netzwerk verwendet wird, empfiehlt es sich, die Datenkommunikation mit F-Secure SSH zu sichern.

- Das Modul für die **Web-Berichterstellung** wird für die Kommunikation mit Web Reporting verwendet. Geben Sie an, ob das Modul aktiviert werden soll. Bei der Web-Berichterstellung werden Serverdaten über eine lokale Socket-Verbindung zum **Verwaltungs-Modul** abgerufen. Der Standard-Port ist Port 8081.

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

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

Abschließen des Migrationsassistenten

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

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

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

1. Geben Sie die Pfade zum Kommunikationsverzeichnis und Schlüsselpaar der älteren Version ein und klicken Sie auf **Weiter**.
2. Lesen Sie sich die unten angegebenen Informationen über Richtliniendomänen durch und klicken Sie auf **Start**.
3. Warten Sie, bis der Datenimport abgeschlossen ist, und klicken Sie auf **Schließen**, um den Assistenten zu beenden.

Der Migrationsassistent wird geschlossen und der Installationsassistent wird wieder angezeigt.

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

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

Abschließen der Produktinstallation

Als nächster Schritt muss die Installation des Produkts abgeschlossen werden.

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

Ändern des Pfads für den Webbrowser

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

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

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

das Produkt deinstallieren.

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

So deinstallieren Sie Policy Manager-Komponenten:

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

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

Kapitel

3

Benutzeroberfläche für Anti-Virus-Modus

Themen:

- *Anmelden*
- *Registerkarte "Richtliniendomänen"*
- *Registerkarten für Verwaltungsaufgaben*
- *Die Symbolleiste*
- *Menübefehle*
- *Vererbung von Einstellungen*

Dieser Abschnitt enthält eine Einführung in die Benutzeroberfläche des **Anti-Virus-Modus** von Policy Manager.

In diesem Abschnitt werden die verfügbaren Einstellmöglichkeiten auf den diversen Bildschirmseiten der Benutzeroberfläche des **Anti-Virus-Modus** aufgeführt.

Hinweis: Policy Manager beinhaltet auch eine Benutzeroberfläche für den **erweiterten Modus**. Diese dient zur Verwaltung anderer Programme als Client Security und Anti-virus for Workstations. Außerdem wird sie zur Änderung erweiterter Client Security Einstellungen verwendet. Sie können zwischen den Modi wechseln, indem Sie **erweiterter Modus** bzw. **Anti-Virus-Modus** im Menü **Ansicht** wählen.

Die Benutzeroberfläche des **Anti-Virus-Modus** besteht aus den folgenden Hauptkomponenten:

- Der Registerkarte **Richtliniendomänen**, auf der die Struktur der verwalteten Richtliniendomänen dargestellt wird.
- Die Registerkarten für die Verwaltung: **Zusammenfassung**, **Einstellungen**, **Status**, **Warnungen**, **Scan-Berichte**, **Installation** und **Aktionen**, die zur Konfiguration und Überwachung von dem auf Hosts installierten Client Securityund für die Ausführung von Aktionen verwendet werden können.
- Die Ansicht **Meldung** unten im Programmfenster. Dort erscheinen Systemmeldungen von Policy Manager, z. B. wenn die Virendefinitionen vom Server aktualisiert wurden.

Anmelden

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

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

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

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

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

Verbindungseigenschaften

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

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

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

Neue Benutzer hinzufügen

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

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

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

Ändern des Kennworts

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

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

Ihr Kennwort wurde nun geändert.

Registerkarte "Richtliniendomänen"

Sie können Vorgänge für Richtliniendomänen und Hosts auf der Registerkarte **Richtliniendomänen** durchführen.

Auf der Registerkarte **Richtliniendomänen** können Sie die folgenden Vorgänge durchführen:

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

Nach Auswahl einer Domäne oder eines Hosts können Sie auf obige Optionen zugreifen, indem Sie auf das Menü **Bearbeiten** oder mit der rechten Maustaste auf den ausgewählten Host oder die Domäne klicken. Die Vorgänge **Automatische Erkennung** und **Neue Hosts importieren** stehen ebenfalls auf der Registerkarte **Installation** zur Verfügung.

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

Registerkarten für Verwaltungsaufgaben

In diesem Abschnitt werden die Registerkarten für die Verwaltung (**Zusammenfassung**, **Einstellungen**, **Status**, **Warnungen**, **Scan-Berichte**, **Installation** und **Vorgänge**) und die unterschiedlichen Seiten auf diesen Registerkarten beschrieben.

Alle Änderungen, die Sie an Richtlinienvariablen vornehmen, werden automatisch in Ihrem Benutzerkonto gespeichert, daher müssen Sie die Richtlinienänderungen nicht speichern, wenn Sie Policy Manager Console schließen. Ihre Änderungen werden anderen Benutzern nicht verfügbar gemacht und sie haben keine Auswirkungen auf verwaltete Hosts, solange Sie die Richtlinienänderungen nicht verteilen.

Registerkarte "Zusammenfassung"

Auf der Registerkarte **Zusammenfassung** werden die wichtigsten Informationen zu den ausgewählten Domänen oder Hosts in einer übersichtlichen Form angezeigt.

Wenn Sie eine Domäne ausgewählt haben, werden auf der Registerkarte **Zusammenfassung** Informationen zur gesamten Domäne angezeigt. Wenn Sie einen einzelnen Host auswählen, werden ausführlichere Informationen zum Host angezeigt.

Wenn einige der Einstellungen, die auf der Registerkarte **Zusammenfassung** angezeigt werden, einen Benutzereingriff erfordern, wird ein Symbol neben der Einstellung angezeigt. Die Symbole können wie folgt interpretiert werden:

	Warnmeldung über einen Fehlerzustand, der einen Benutzereingriff erfordert. Der Fehler kann nicht automatisch behoben werden. Das Symbol wird z. B. angezeigt, wenn die neuesten Richtlinien nicht verteilt wurden oder wenn die Virendefinitionen auf dem Host abgelaufen sind.
	Warnmeldung über einen Fehlerzustand, der einen Benutzereingriff erfordert. In diesem Fall ist noch kein Sicherheitsproblem aufgetreten. Wird der Fehler jedoch jetzt nicht behoben, kann es später zu Sicherheitsproblemen kommen. Das Symbol wird z. B. angezeigt, wenn die Verbindungen zu Hosts unterbrochen wurden.

Welche Informationen auf der Registerkarte **Zusammenfassung** angezeigt werden, hängt davon ab, was auf der Registerkarte **Richtliniendomänen** gewählt wurde:

- Wenn Sie eine Domäne ausgewählt haben, sind die auf der Registerkarte **Zusammenfassung** angezeigten Informationen in folgende Abschnitte unterteilt: **Policy Manager**, **Domäne**, **Virenschutz für Arbeitsstationen** und **Internet Shield**.
- Wenn Sie einen Host ausgewählt haben, werden folgende Abschnitte angezeigt: **Policy Manager**, **Host**, **Virenschutz** und **Internet Shield**.

Registerkarte "Zusammenfassung" bei Auswahl einer Domäne

Die hier beschriebenen Informationen werden auf der Registerkarte **Zusammenfassung** angezeigt, wenn auf der Registerkarte **Richtliniendomänen** eine Domäne gewählt wurde.

Policy Manager

Im Abschnitt **Policy Manager** können Sie:

- den aktuellen Status der **Richtlinienverteilung** (**gespeichert/nicht gespeichert, verteilt/nicht verteilt**) prüfen und gegebenenfalls die Richtliniendaten speichern und die neuen Richtlinien an die Hosts verteilen.
- den Status der Virendefinitionen auf dem Server anzeigen.
- den Status der Spyware-Definitionen auf dem Server anzeigen.
- den Status der **DeepGuard**-Updates auf dem Server anzeigen.
- die Anzahl der neuen automatisch registrierten Hosts anzeigen. Wenn neue Hosts gefunden werden, können Sie diese zur Domäne hinzufügen. Klicken Sie dazu auf **Diese Hosts einer Domäne hinzufügen...**.
- Hosts aus einer Windows-Domäne automatisch erkennen. Klicken Sie dazu auf **Windows-Hosts automatisch feststellen...**.

Domäne

Im Abschnitt **Domäne** können Sie:

- die Anzahl der Hosts anzeigen, die die neueste Richtlinie erhalten haben, und auf eine Zusammenfassung des letzten Updates der Sicherheitsrichtlinie zugreifen. Klicken Sie dazu auf **Neueste Richtlinien-Updates der Hosts anzeigen...**. Damit gelangen Sie zur Registerkarte **Status** und zur Seite **Zentrale Verwaltung**.
- die Anzahl der nicht verbundenen Hosts anzeigen. Sie können außerdem auf eine detaillierte Liste mit Angaben zum Verbindungsstatus der Hosts zugreifen. Klicken Sie dazu auf **Getrennte Hosts anzeigen**. Daraufhin werden die Registerkarte **Status** und die Seite **Zentrale Verwaltung** geöffnet.
- eine Zusammenfassung neuer Warnmeldungen anzeigen. Um detaillierte Informationen zu Warnmeldungen anzuzeigen, klicken Sie auf den Link **Alarme nach Schweregrad anzeigen**, um die Registerkarte **Alarme** zu öffnen.

  Der Schweregrad der Warnmeldungen wird durch folgende Symbole gekennzeichnet:

Symbol	Bezug	Beschreibung
	Info	Normale Informationen eines Hosts über einen Arbeitsvorgang.
	Warnung	Eine Warnung vom Host.
	Fehler	Behebbarer Fehler auf dem Host.
	Schwerwiegender Fehler	Unbehebbarer Fehler auf dem Host.
	Sicherheitsalarm	Sicherheitsrisiko auf dem Host.

Virenschutz für Arbeitsstationen

Im Abschnitt **Virenschutz für Arbeitsstationen** können Sie:

- feststellen, auf wie vielen Hosts in der Domäne **Virenschutz** installiert wurde.
- feststellen, auf wie vielen Hosts in der Domäne **Echtzeit-Scanning** aktiviert wurde. Wenn Sie feststellen möchten, auf welchen Hosts dieser Schutz aktiviert ist, klicken Sie auf **Gesamtschutz der Hosts anzeigen...**. Sie erhalten daraufhin Zugriff auf ausführlichere Informationen auf der Registerkarte **Status** und auf der Seite **Allgemeiner Schutz**.
- feststellen, wie viele Infektionen in der Domäne gefunden wurden. Wenn Sie spezifische Informationen zu Infektionen auf einzelnen Hosts anzeigen möchten, klicken Sie auf **Infektionsstatus der Hosts anzeigen...**. Sie erhalten daraufhin Zugriff auf detaillierte Informationen auf der Registerkarte **Status** und der Seite **Allgemeiner Schutz**.
- Feststellen, auf wie vielen der Hosts die letzten Virendefinitionen installiert wurden und ob die Virendefinitionen auf einigen Hosts noch aktuell oder abgelaufen sind.
  - **Aktuell** bedeutet, dass die Virendefinitionen nicht auf dem neuesten Stand sind.
  - **Veraltet** bedeutet, dass die Virendefinitionen älter als das konfigurierte Zeitlimit sind.

    Hinweis: Wenn auf einigen HostsF-Secure Anti-Virus 5.40 installiert ist, werden die Versionen der Virendefinitionen auf diesen Hosts als **Unbekannt** gekennzeichnet.

  Wenn Sie die Virendefinitionen auf einigen Hosts aktualisieren müssen, klicken Sie auf **Virusdefinitionen aktualisieren...**. Daraufhin wird die Registerkarte **Operationen** geöffnet.

Internet Shield

Im Abschnitt **Internet Shield** können Sie:

- feststellen, auf wie vielen Hosts in der Domäne Internet Shield installiert wurde.
- feststellen, welche Angriffe in der letzten Zeit am häufigsten vorgekommen sind und wie viel Prozent der Domäne davon betroffen waren. Um detaillierte Informationen zu den letzten Angriffen anzuzeigen, klicken Sie auf **Status von Internet Shield anzeigen...**. Daraufhin werden die Registerkarte **Status** und die Seite **Internet Shield** geöffnet.

Registerkarte "Zusammenfassung" bei Auswahl eines Hosts

Wenn Sie auf der Registerkarte **Richtliniendomänen** einen Host ausgewählt haben, werden auf der Registerkarte **Zusammenfassung** im Abschnitt **Host** ausführliche Informationen angezeigt:

Host

Im Abschnitt **Host** können Sie:

- den Namen des ausgewählten Hosts sehen, der neben der **Computer-Identität** angezeigt wird. Sie können auch auf detaillierte Informationen zum Host zugreifen. Klicken Sie dazu auf **Host-Eigenschaften anzeigen...**. Daraufhin werden die Registerkarte **Status** und die Seite **Host-Eigenschaften** geöffnet.
- feststellen, welches Protokoll (HTTP oder gemeinsamer Dateizugriff) aktiviert ist, sowie die Adresse des Policy Manager Server, mit dem der Host verbunden ist, und Datum und Uhrzeit der letzten Verbindung anzeigen.
- feststellen, ob die momentan vom Host verwendete Richtliniendatei aktuell ist.
- feststellen, ob die Verbindung zum Host unterbrochen wurde.
- eine Zusammenfassung neuer Warnmeldungen anzeigen. Um detaillierte Informationen zu Warnmeldungen anzuzeigen, klicken Sie auf **Alarme nach Schweregrad anzeigen...**. Daraufhin wird die Registerkarte **Alarme** geöffnet.

Virenschutz für Arbeitsstationen

Neben den Informationen, die bei Auswahl einer Domäne angezeigt werden, wird im Abschnitt **Virenschutz für Arbeitsstationen** auch die Versionsnummer der Virendefinitionen angezeigt.

Internet Shield

Neben den Informationen, die bei Auswahl einer Domäne angezeigt werden, wird im Abschnitt **Internet Shield** auch die momentan auf dem Host eingestellte Sicherheitsstufe angezeigt.

Registerkarte "Einstellungen"

Die Registerkarte **Einstellungen** ist in 12 Seiten unterteilt, auf denen die Komponenten von Client Security konfiguriert werden. Diese Seiten werden in diesem Abschnitt kurz beschrieben.

Kontextmenü auf den Seiten "Einstellungen"

Sie können auf einer Seite **Einstellungen** mit der rechten Maustaste auf eine beliebige Option klicken. Daraufhin wird ein Kontextmenü mit folgenden Optionen geöffnet:

Bereinigen	Mit dieser Option löschen Sie eine Einstellung, die für die aktuelle Stufe neu definiert wurde.
Wert erzwingen	Der Menübefehl **Wert erzwingen** ist nur verfügbar, wenn zuvor eine Richtliniendomäne ausgewählt wurde. Sie können vorgeben, dass die aktuelle Domäneneinstellung auch in allen Subdomänen und auf allen Hosts aktiv ist. In der Praxis werden bei diesem Vorgang alle entsprechenden Einstellungen in allen Subdomänen und Hosts unter der aktuellen Domäne gelöscht. Dadurch ist eine Vererbung des aktuellen Werts in alle Subdomänen und auf allen Hosts möglich. Setzen Sie diesen Befehl mit Bedacht ein: Alle Werte, die in den Subdomänen oder auf den Hosts unter der ausgewählten Domäne definiert wurden, werden gelöscht. Dieser Befehl lässt sich nicht rückgängig machen.
Domänenwerte anzeigen	Der Menübefehl **Domänenwerte anzeigen** ist nur verfügbar, wenn zuvor eine Richtliniendomäne ausgewählt wurde. Sie können eine Liste aller Richtliniendomänen und Hosts unterhalb der ausgewählten Richtliniendomäne zusammen mit dem Wert des ausgewählten Felds anzeigen. Klicken Sie auf eine beliebige Domäne oder einen beliebigen Host-Namen, um die Domäne oder den Host schnell

	auf der Registerkarte **Richtliniendomänen** auszuwählen. Es ist möglich, gleichzeitig mehrere Dialogfelder vom Typ **Domänenwert** zu öffnen.
In den erweiterten Modus wechseln	Diese Option ist für erfahrene Benutzer gedacht. Nach der Auswahl wird die Benutzeroberfläche für den **erweiterten Modus** geöffnet. Hier können Sie anschließend die Einstellungen festlegen.

Gehen Sie zu Automatische Updates.

Die Seite **Automatische Updates** ist in zwei Abschnitte unterteilt: **Automatische Updates** und **NeighborCast**.

Automatische Updates

Im Abschnitt **Automatic Updates** haben Sie folgende Möglichkeiten:

- Automatische Updates aktivieren oder deaktivieren. Wenn diese Einstellung deaktiviert ist, kann der Host keine automatischen Updates erhalten.
- Das Intervall festlegen, in dem Updates von Policy Manager Server abgerufen werden.
- Eine Liste der Policy Manager Proxy Server anzeigen. Darüber hinaus können Sie neue Server zur Liste hinzufügen, Server von der Liste löschen und die Adressen und Prioritätseinstellungen der Server bearbeiten.
- Festlegen, ob ein HTTP-Proxy-Server verwendet werden kann und gegebenenfalls die Adresse des HTTP-Proxy angeben.
- Festlegen, ob die Clients Updates nicht nur von Servern oder Proxy-Servern, sondern auch voneinander herunterladen sollen.

NeighborCast

NeighborCast ermöglicht es den Clients, Updates nicht nur von den verfügbaren Servern oder Proxy-Servern, sondern auch voneinander herunterzuladen. In diesem Abschnitt haben Sie folgende Möglichkeiten:

- Einen Client zur Bereitstellung von Updates auf anderen Clients konfigurieren
- Einen Client zum Herunterladen von Updates von anderen Clients, die Updates bereitstellen, konfigurieren
- Den zu verwendenden Port auswählen

Echtzeit-Scanning

Die Einstellungen auf dieser Bildschirmseite betreffen das Echtzeit-Scanning von Hosts in der gewählten Domäne.

Wenn nichts anderes angegeben ist, gelten die Einstellungen auf dieser Seite für alle Client Security Versionen. Zur Anzeige und Konfiguration der Einstellungen, die nicht mehr für Client Security 9 oder höher und Anti-virus for Windows Servers 9 oder höher gelten, aber noch für ältere Programmversionen, klicken Sie auf **Einstellungen für ältere Clients (7.x, 8.x)...**.

Allgemein

In diesem Abschnitt können Sie das Echtzeit-Scanning ein- oder ausschalten.

Datei-Überprüfung

In diesem Abschnitt haben Sie folgende Möglichkeiten:

- Festlegen, welche Dateien überprüft werden sollen, und die eingeschlossenen Erweiterungen definieren.
- Festlegen, ob bestimmte Erweiterungen nicht überprüft werden sollen und diese Ausnahmen definieren.
- Festlegen, ob der Benutzer Objekte vom Echtzeit-Scanning ausschließen kann.

- Festlegen, ob auch Netzwerklaufwerke mit Echtzeit-Scanning gescannt werden sollen.
- Festlegen, welche Maßnahme bei der Erkennung einer infizierten Datei automatisch getroffen wird Client Security 9 oder höher und Anti-virus for Windows Servers 9 oder höher).
- Ein- oder Ausschalten des Schutzes der "Hosts"-Datei.
- Festlegen, ob Tracking Cookies in den Scan eingeschlossen werden sollen.

DeepGuard

In diesem Abschnitt haben Sie folgende Möglichkeiten:

- Ein- oder Ausschalten von DeepGuard.
- Festlegen, welche Maßnahme getroffen wird, wenn ein Versuch zur Systemmodifikation erkannt wird.
- Festlegen, ob ein Remote-Server abgefragt werden soll, um die Erkennungsgenauigkeit zu verbessern.
- Ein- oder Ausschalten der erweiterten Prozessüberwachung.

Manuelles Scanning

Die Einstellungen auf dieser Seite wirken sich auf die Scans aus, die von den Host-Benutzern manuell durchgeführt werden.

Manuelles Scanning von Dateien

In diesem Abschnitt legen Sie mithilfe der folgenden Optionen fest, was gescannt werden soll:

- Festlegen, welche Dateien überprüft werden sollen, und die eingeschlossenen Erweiterungen definieren.
  - **Alle Dateien**: Alle Dateien werden unabhängig von der Dateierweiterung gescannt. Die Vorgabe dieser Option ist nicht empfehlenswert, da sie unter Umständen dazu führt, dass das System erheblich langsamer arbeitet.
  - **Zu scannende Dateien**: Dateien mit bestimmten Dateierweiterungen werden gescannt. Geben Sie einen Punkt (`.`) ein, um Dateien ohne Erweiterung festzulegen. Der Platzhalter `?` steht für einen beliebigen Buchstaben. Geben Sie alle Dateierweiterungen ein, und trennen Sie sie durch ein Leerzeichen.
- Festlegen, ob der Scan komprimierte Dateien umfassen soll. Aktivieren Sie dieses Kontrollkästchen, um komprimierte Dateien wie `ZIP`-, `ARJ`-, `LZH`-, `RAR`-, `CAB`-, `TAR`-, `BZ2`-, `GZ`-, `JAR`- und `TGZ`-Dateien zu scannen. Das Scannen umfangreicher komprimierter Dateien kann unter Umständen viele Systemressourcen in Anspruch nehmen und das System verlangsamen.
- Festlegen, ob bestimmte Erweiterungen nicht überprüft werden sollen und diese Ausnahmen definieren. Sie können außerdem angeben, ob einige Dateien von der Überprüfung ausgenommen werden sollen. Dazu geben Sie die Erweiterungen der ausgeschlossenen Dateien in das Feld **Ausgeschlossene Erweiterungen** ein.
- Festlegen, ob der Benutzer Objekte vom Echtzeit-Scanning ausschließen kann. Wenn Sie **Ausgeschlossene Objekte aktivieren** auswählen, können Sie einzelne Dateien von der Überprüfung ausschließen.
- Über die Dropdown-Liste **Maßnahme bei Infektion** können Sie die Maßnahme auswählen, die Client Security bei einer infizierten Datei durchführt. Wählen Sie eine der folgenden Aktionen aus:

Aktion	Definition
Nach Scannen fragen	Startet den **Desinfektions-Assistenten**, wenn eine infizierte Datei gefunden wird.
Automatisch desinfizieren	Die Datei wird automatisch desinfiziert, wenn ein Virus festgestellt wird.

Aktion	Definition
Automatisch umbenennen	Die Datei wird automatisch umbenannt, wenn ein Virus gefunden wird.
Automatisch löschen	Die Datei wird automatisch gelöscht, wenn ein Virus gefunden wird. Diese Option ist nicht empfehlenswert, da dadurch das Objekt, an das der Virus angehängt ist, ebenfalls gelöscht wird.
Nur Bericht	Gibt an, dass ein Virus festgestellt wurde, und verhindert, dass das infizierte Objekt geöffnet wird. Bei Auswahl dieser Option werden Viren nur gemeldet, es wird aber keine Maßnahme durchgeführt.

Rootkit-Scanning

In diesem Abschnitt haben Sie folgende Möglichkeiten:

- Rootkit-Scanning ein- oder ausschalten.
- Rootkit-Scanning bei der vollständigen Überprüfung des Computers einschließen oder ausschließen.
- Angeben, ob ermittelte verdächtige Elemente im Desinfektions-Assistenten und im Scan-Bericht nach einer vollständigen Überprüfung des Computers angezeigt werden.

Geplantes Scanning

Über den Link **Geplantes Scanning im erweiterten Modus konfigurieren...** gelangen Sie zur Benutzeroberfläche des **erweiterten Modus**. Dort kann das geplante Scanning konfiguriert werden.

Manuelles Scanning des Boot-Sektors

In diesem Abschnitt haben Sie folgende Möglichkeiten:

- Die manuelle Überprüfung der Boot-Sektoren von Disketten ein- oder ausschalten.
- Festlegen, welche Maßnahme getroffen wird, wenn eine Infektion gefunden wird.

Spyware-Steuerung

Die Einstellungen auf dieser Seite sind spyware-spezifisch und stellen zusätzliche Optionen für Echtzeit-Scanning und manuelles Scanning dar.

Vom Spyware-Scanning ausgeschlossene Anwendungen

Diese Tabelle enthält eine Liste der Spyware- und Riskware-Anwendungen, die von den Administratoren auf den Hosts zugelassen sind.

Von Hosts gemeldete Spyware und Riskware

Diese Tabelle enthält eine Liste mit den von den Hosts gemeldeten bzw. auf den Hosts unter Quarantäne gestellten Spyware- und Riskware-Anwendungen. Alle Spyware- oder Riskware-Anwendungen mit dem Status **Potenziell aktiv** wurden vom Administrator auf den Hosts zugelassen.

Wenn Sie den Benutzern ermöglichen möchten, zu entscheiden, welche Spyware- und Riskware-Elemente zulässig sind, können Sie dazu die Dropdown-Liste **Benutzer dürfen zulässige Spyware-Elemente definieren** verwenden.

Quarantänenverwaltung

Diese Seite dient der Verwaltung von Malware, die auf verwalteten Hosts in Quarantäne gestellt wurde.

Elemente in Quarantäne

In dieser Tabelle werden die Elemente aufgelistet, die auf den Hosts in Quarantäne sind. In den einzelnen Tabellenzeilen werden Objekttyp, Name, Dateipfad und die Anzahl der Hosts angezeigt, auf denen sich das Objekt in Quarantäne befindet.

Durchzuführende Maßnahmen mit Objekten in Quarantäne

In dieser Tabelle werden die Objekte in Quarantäne aufgelistet, die verarbeitet wurden. Die Objekte in Quarantäne wurden entweder freigegeben (zugelassen) oder gelöscht. Die hier angegebene Maßnahme wird auf die verwalteten Hosts verteilt, sodass bei einer Erkennung der betreffenden Malware die gewählte Maßnahme angewendet wird. Wenn die Maßnahme auf **Freigabe** gesetzt ist, muss eine entsprechende Ausschlussregel je nach Objekttyp entweder auf der Seite **Spyware-Steuerung** oder **Echtzeit-Scanning** vorliegen, damit das Objekt in Zukunft nicht in Quarantäne gestellt wird.

Die angewendeten Maßnahmen werden automatisch aus der Tabelle entfernt, wenn keine Maßnahmen mehr für die jeweiligen Hosts anstehen (keine Hosts melden dieses Objekt in Quarantäne).

E-Mail-Scanning

Auf dieser Seite befinden sich jeweils separate Einstellungen für die Überprüfung eingehender und ausgehender E-Mails. Die Einstellungen im Abschnitt **Allgemein** gelten für beide Varianten.

Überprüfung eingehender E-Mails

In diesem Abschnitt haben Sie folgende Möglichkeiten:

- Ein- oder Ausschalten der Überprüfung eingehender E-Mails
- Festlegen, welche Maßnahme bei der Erkennung eines eingehenden infizierten Anhangs ausgeführt wird
- Festlegen, welche Maßnahme ausgeführt wird, wenn die Virenüberprüfung fehlschlägt
- Festlegen, welche Maßnahme bei der Erkennung eines "malformed" Nachrichtenteils ausgeführt wird

Überprüfung ausgehender E-Mails

In diesem Abschnitt haben Sie folgende Möglichkeiten:

- Ein- oder Ausschalten der Überprüfung ausgehender E-Mails
- Festlegen, welche Maßnahme bei der Erkennung eines ausgehenden infizierten Anhangs ausgeführt wird
- Festlegen, welche Maßnahme ausgeführt wird, wenn die Virenüberprüfung fehlschlägt
- Festlegen, welche Maßnahme bei der Erkennung eines "malformed" Nachrichtenteils ausgeführt wird
- Aktivieren Sie das Kontrollkästchen, wenn blockierte Nachrichten im Postausgang des Endbenutzers gespeichert werden sollen.

Allgemein

In diesem Abschnitt haben Sie folgende Möglichkeiten:

- Festlegen, ob bei der Überprüfung von E-Mails auch in komprimierten Anhängen nach Viren gesucht wird.
- Festlegen, ob und nach welchem Zeitraum der Verlauf der Überprüfung grafisch dargestellt wird.
- Festlegen, ob ein Scan-Bericht angezeigt wird, wenn eine infizierte Datei gefunden wird oder die Überprüfung fehlschlägt.

Web Traffic Scanning

Die Einstellungen, die auf dieser Seite angezeigt werden, beziehen sich auf die Überprüfung des Web-Datenverkehrs, zum Beispiel heruntergeladene Dateien.

Allgemein

In diesem Abschnitt können Sie HTTP-Scanning ein- oder ausschalten.

HTTP-Scanning

- Wählen Sie die Aktion aus, die für infizierte Dateien durchgeführt werden soll.
- Legen Sie fest, welche Maßnahme ausgeführt wird, wenn die Virenüberprüfung fehlschlägt.
- Festlegen, ob auch komprimierte Dateien gescannt werden.

Vertrauenswürdige HTTP-Sites

In dieser Tabelle werden die HTTP-Sites aufgelistet, die als vertrauenswürdig definiert sind. Downloads von diesen Sites werden nicht auf Viren geprüft.

Firewall-Sicherheitsstufen

Die Einstellungen auf dieser Seite dienen zur Festlegung der gesamten Firewall-Sicherheitsstufe auf dem gewählten Host oder in der gewählten Domäne.

Allgemein

In diesem Abschnitt haben Sie folgende Möglichkeiten:

- Die vordefinierte Sicherheitsstufe für den Host wählen.
- Die automatische Auswahl der Sicherheitsstufe konfigurieren. Dazu klicken Sie auf **Automatische Auswahl der Sicherheitsstufe im erweiterten Modus konfigurieren**. Daraufhin wird die Benutzerschnittstelle für den **erweiterten Modus** geöffnet.
- Die Firewall-Regeln der aktuellen Sicherheitsstufe auf eingehende und ausgehende Datenpakete anwenden, indem Sie die Option **Firewall-Modul aktivieren** wählen.
- Die Verwendung der vertrauenswürdigen Schnittstelle aktivieren.
- Die Anwendungssteuerung ein- oder ausschalten.

Globale Tabelle "Firewall-Sicherheitsstufen"

In dieser Tabelle werden die Sicherheitsstufen angezeigt, die global im System verfügbar sind. Die Tabelle mit den Sicherheitsstufen ist für alle Richtliniendomänen identisch. Allerdings können für einzelne Richtliniendomänen unterschiedliche Sicherheitsstufen aktiviert bzw. deaktiviert werden.

Netzwerk-Quarantäne

In diesem Abschnitt haben Sie folgende Möglichkeiten:

- Die Netzwerk-Quarantäne ein- oder ausschalten.
- Das Alter der Virendefinitionen festlegen, ab dem die **Netzwerk-Quarantäne** aktiviert wird.
- Festlegen, ob durch die Deaktivierung von Echtzeit-Scanning auf dem Host die **Netzwerk-Quarantäne** aktiviert wird.

Intrusion Prevention

In diesem Abschnitt haben Sie folgende Möglichkeiten:

- Intrusion Prevention ein- oder ausschalten.

- Die Aktion wählen, die bei Erkennung eines schädlichen Pakets auszuführen ist. Folgende Optionen stehen zur Verfügung:
  - Protokollieren und löschen
  - Protokollieren, aber nicht löschen
- Die Schweregrade für die zentrale Alarmierung definieren.
- Die Alarm- und Leistungsstufen aktivieren.

Firewallregeln

Diese Seite dient der Definition der Regeln, die für die unterschiedlichen Firewall-Sicherheitsstufen gelten sollen.

Tabelle der Firewall-Regeln

In dieser Tabelle sind die Regeln aufgelistet, die für die unterschiedlichen Sicherheitsstufen festgelegt wurden. Sie können die Stufe aus dem Dropdown-Menü **Sicherheitsstufe für Internet-Schutzschild in Bearbeitung** auswählen. Wenn die ausgewählte Sicherheitsstufe geändert wird, werden die mit der neuen Sicherheitsstufe verknüpften Regeln in der Tabelle angezeigt.

Während der Verwendung der Firewall werden die Firewall-Regeln in der Reihenfolge überprüft, in der sie in der Tabelle vorkommen (von oben nach unten). Für Sicherheitsstufen mit dem Filtermodus **Normal** ist es möglich, domänen- oder host-spezifische Regeln zu definieren. Wenn **Benutzer dürfen neue Regeln definieren** aktiviert ist, haben Endbenutzer die Möglichkeit, neue Regeln für diese Sicherheitsstufe zu definieren. In der Tabelle wird auch der Speicherort für diese Regeln angezeigt.

In der Tabelle **Firewall-Regeln** werden folgende Informationen für jede Regel angezeigt:

- Ob die Regel aktiviert oder deaktiviert ist
- Der Name und eine Beschreibung der Regel
- Der Regeltyp (Zulassen/Ablehnen)
- Der dazugehörige Dienst und die Richtung: **<=** für einen eingehenden Dienst, **=>** für einen ausgehenden Dienst und **<=>** für einen Dienst in beide Richtungen.
- Die betroffenen Remote-Hosts
- Ob das Versenden von Alarmmeldungen aktiviert oder deaktiviert ist
- Ob die Regel nur bei Einsatz einer DFÜ-Verbindung angewendet wird

Um den Ort zu verschieben, an dem neue Regeln in der Tabelle angeordnet werden, klicken Sie auf **Benutzerdefinierte Regeln hier einfügen**. Anschließend können Sie mithilfe der Schaltflächen **Nach oben** und **Nach unten** zum entsprechenden Ort in der Tabelle navigieren.

Darüber hinaus werden durch die **Anwendungssteuerung** auf den Hosts automatisch Regeln für zugelassene Anwendungen festgelegt. Die Regeln werden in der Regeltabelle unmittelbar vor der ersten Regel namens **Alles andere sperren** eingefügt. Dies ist die erste Sperrregel mit der Festlegung **Gesamter Datenverkehr** und **Beliebiger Remote-Host**. Die Regeln lassen eingehende Pakete für Server-Anwendungen zu. Die Firewall lässt die von den Server-Anwendungen ausgehenden Antwortpakete ebenfalls zu. Ausgehende Pakete von normalen Anwendungen müssen durch die Regeln der Firewall-Regeltabelle ausdrücklich zugelassen sein.

Firewalldienste

Bei einem Netzwerkdienst, kurz Dienst, handelt es sich um einen Dienst, der über das Netzwerk verfügbar ist, z. B. gemeinsamer Dateizugriff, Remote-Konsolen-Zugriff oder Webbrowsing. In den meisten Fällen wird ein Dienst durch das verwendete Protokoll und den Port beschrieben.

Tabelle der Firewall-Dienste (Global)

Diese Tabelle listet die Dienste auf, die für die Firewall definiert wurden. Sie können neue Dienste für die Firewall erstellen oder festlegen, ob Endbenutzer neue Dienste für die Firewall anlegen können.

Wenn Sie verhindern möchten, dass Benutzer neue Dienste erstellen, klicken Sie auf **Eingeschränkt**, und wählen Sie anschließend im sich öffnenden Dialogfeld die Option **Feste Größe**. Wenn diese Option aktiviert ist, können Endbenutzer keine Zeilen aus der Tabelle löschen oder in die Tabelle einfügen.

Anwendungssteuerung

Die Einstellungen auf dieser Seite dienen zur Steuerung von Anwendungen, die eingehende und abgehende Netzwerkverbindungen nutzen.

Anwendungsregeln für bekannte Anwendungen

In diesem Abschnitt wird eine Liste aller bekannten Anwendungen und der für eingehende und abgehende Verbindungsversuche definierten Regeln angezeigt.

Unbekannte Anwendungen, die von den Hosts gemeldet wurden

In dieser Liste werden Anwendungen aufgeführt, die von den Hosts gemeldet wurden und für die noch keine Regeln vorhanden sind.

In diesem Abschnitt haben Sie außerdem folgende Möglichkeiten:

- Die Standardmaßnahme für Client-Anwendungen auswählen.
- Die Standardmaßnahme für Server-Anwendungen auswählen.
- Festlegen, ob neue Anwendungen an Sie gemeldet werden, indem Sie das Kontrollkästchen "Neue unbekannte Anwendungen melden" aktivieren.

Automatische Entscheidungen

In diesem Abschnitt können Sie wählen, ob der Benutzer nach einer Entscheidung gefragt wird, wenn die Anwendung von DeepGuard oder dem Echtzeitschutz-Netzwerk erkannt wurde.

Meldung für Benutzer

Dieser Abschnitt enthält die folgenden Optionen:

- Festlegen, ob bei einem Verbindungsversuch einer unbekannten Anwendung die Standardmeldung angezeigt wird.
- Über **Standardmeldungen definieren** wird das Fenster **Meldungen definieren** geöffnet. Dort können Sie Meldungen für bekannte und unbekannte Anwendungen erstellen, z. B. um Anwendungen zuzulassen, zu sperren oder eine Benutzereingabe anzufordern.

Surfschutz

Mit den Optionen auf dieser Seite werden die Surfschutzeinstellungen für Hosts festgelegt, auf denen Client Security9 oder höher installiert ist.

Exploit Shield

In diesem Abschnitt können Sie wählen, ob der Surfschutz Exploit Shields nutzt, um den Zugriff auf Websites zu blockieren, die Exploits enthalten.

Exploit Shields erkennen schädliche Websites und hindern sie daran, solche Sicherheitslücken auszunutzen, zum Beispiel, um einen nicht autorisierten Download zu erzwingen, mit dem Malware heruntergeladen wird. Exploit Shields schützen Sie nicht vor Dateien, die Sie absichtlich herunterladen und die Malware enthalten können. Eine derartige Bedrohung wird über die Viren- und Spyware-Überprüfung abgedeckt.

Reputationsbasierter Schutz

Mit den Einstellungen in diesem Abschnitt wird festgelegt, wie Einstufungen für Websites angezeigt werden, und ob als schädlich eingestufte Websites für Benutzer gesperrt werden. Diese Sicherheitseinstufungen

basieren auf Informationen von mehreren Quellen, zum Beispiel F-Secure Malware-Analytikern und F-Secure Partnern, sowie auf Einstufungen, die von anderen Benutzern des Surfschutzes angegeben wurden.

Vertrauenswürdige Sites

Wenn der Surfschutz den Zugang zu einer Website, der Sie vertrauen und auf die Sie zugreifen möchten, blockiert, können Sie diese Site als vertrauenswürdig definieren. Alle vertrauenswürdigen Sites werden hier aufgelistet.

Erweiterte Einstellungen

Klicken Sie auf **Erweiterte Einstellungen konfigurieren**, um zu den Surfschutzeinstellungen in der Ansicht **Erweiterter Modus** zu gelangen.

Versenden von Alarmmeldungen

Mit den Einstellungen auf dieser Seite wird festgelegt, wie Alarme angezeigt und an Administratoren weitergeleitet werden.

Allgemein

In diesem Abschnitt können Sie die Sprache für die Alarmmeldungen auswählen.

Senden von Alarmen per E-Mail

- Legen Sie eine E-Mail-Server-Adresse (SMTP) fest.
- Legen Sie die Absenderadresse für E-Mails und die Betreffzeile fest, die zum Weiterleiten von Alarmmeldungen per E-Mail verwendet werden sollen.

Weiterleitung von Warnmeldungen

Anhand dieser Tabelle kann konfiguriert werden, an welche Adresse Alarmmeldungen eines bestimmten Schweregrads weiterzuleiten sind.

Zentrale Verwaltung

Diese Seite enthält Optionen zur Steuerung der Art und Weise, wie Client Security Einstellungen innerhalb des Netzwerks angewendet werden.

Allgemein

Dieser Abschnitt enthält die folgenden Optionen:

- **Benutzer dürfen alle Einstellungen auf dieser Seite ändern**

  Wenn Sie diese Option aktivieren, sind alle Einstellungen, die Sie über die Benutzeroberfläche im **Anti-Virus**-Modus und im **erweiterten Modus** vorgenommen haben, nicht endgültig, d. h., Benutzer können diese Einstellungen nach Belieben ändern.
- **Benutzer dürfen keine Einstellungen ändern**

  Wenn Sie diese Option aktivieren, sind alle Einstellungen, die Sie über die Benutzeroberfläche im **Anti-Virus**-Modus und im **erweiterten Modus** vorgenommen haben, endgültig, d. h., Benutzer dürfen diese Einstellungen nicht ändern.
- **Alle Einstellungen löschen**

  Mit dieser Option werden die Standardeinstellungen für alle Client Security Komponenten wiederhergestellt.
- **Benutzer dürfen Downloads und Updates vorübergehend aussetzen**

Über diese Option wird festgelegt, ob ein Benutzer die Netzwerkkommunikation, z. B. den automatischen Abruf von Richtlinien, den Versand von statistischen Daten und die automatische Update-Funktion, vorübergehend aussetzen darf.

Die Option ist für solche Hosts nützlich, die gelegentlich eine langsame DFÜ-Verbindung nutzen.

- **Benutzer dürfen F-Secure Programme deinstallieren**

  Wenn Sie diese Option deaktivieren, können Endbenutzer die auf ihren Computern installierte F-Secure-Software nicht deinstallieren. Unabhängig von dieser Einstellung können Programme nur deinstalliert werden, wenn der Benutzer über Administratorrechte verfügt. Dies gilt für alle Windows-Betriebssysteme, auch für Windows NT/2000/XP, bei denen auch Endbenutzer Administratorrechte haben können.

  Damit die Software lokal deinstalliert werden kann, müssen Sie entweder diese Option aktivieren oder zunächst den Dienst Management Agent herunterfahren und die Deinstallation dann fortsetzen.

- **Benutzer dürfen Programme aus dem Speicher entfernen**

  Folgende Werte sind möglich: **Immer**; **Nur bei einer Einzelplatzinstallation**; **Nicht zugelassen**.

  Über diese Option wird festgelegt, ob der Benutzer alle F-Secure-Programme vorübergehend aus dem Speicher entfernen darf, z. B. um Arbeitsspeicher für speicherintensive Programme, wie Spiele oder ähnliche Anwendungen, freizugeben. Beachten Sie, dass die Hauptfunktionen der Programme deaktiviert sind, solange die Programme nicht geladen sind und dass der Computer während dieser Zeit nicht vor Viren oder Angriffen geschützt ist.

- **Langsame Verbindungsdefinition**

  Diese Variable definiert, welche Netzwerkverbindungen als langsam eingestuft werden. Als Einheit wird kBit/s (Kilobit pro Sekunde) verwendet. Die nominale Geschwindigkeit der Verbindung ist nicht relevant. Vielmehr wird die tatsächliche Geschwindigkeit der Verbindung gemessen. Der Standardwert `0` bedeutet, dass alle Verbindungen als schnell eingestuft werden.

Einstellungen für Policy Manager Server

- **Policy Manager Server**

  URL-Adresse von Policy Manager Server

- **Abfrageintervall für eingehende Pakete**

  Mit dieser Option wird festgelegt, wie oft der Host versucht, eingehende Datenpakete von Policy Manager Server abzurufen, z. B. Basisrichtliniendateien. Der Standardwert ist 10 Minuten.

- **Aktualisierungsintervall für ausgehende Pakete**

  Mit dieser Option wird festgelegt, wie oft der Host versucht, neue Versionen regelmäßig gesendeter Informationen, z. B. statistische Daten, an Policy Manager Server zu senden. Der Standardwert ist 10 Minuten.

Registerkarte "Status"

Die einzelnen Seiten der Registerkarte **Status** enthalten ausführliche Informationen über den Status bestimmter Komponenten der zentral verwalteten Client Security Anwendungen.

Wenn Sie auf der Registerkarte **Richtliniendomänen** eine Domäne ausgewählt haben, werden auf der Registerkarte **Status** die Statusangaben aller Hosts innerhalb dieser Domäne angezeigt. Wurde stattdessen ein einzelner Host ausgewählt, werden auf der Registerkarte **Status** detaillierte Angaben zum Status dieses Hosts angezeigt.

Hinweis: Indem Sie mit der rechten Maustaste auf den entsprechenden Spaltenkopf auf den **Status**-Seiten klicken, können Sie festlegen, welche Spalten auf dieser Seite angezeigt werden.

Kontextmenü auf der Registerkarte "Status"

Sie können auf einer Seite der Registerkarte **Status** mit der rechten Maustaste auf eine beliebige Reihe klicken. Daraufhin wird ein Kontextmenü mit folgenden Optionen geöffnet:

- **Als Text kopieren** kopiert die derzeit ausgewählte(n) Zeile(n) und Spaltenüberschriften als Text aus der Tabelle.
- **Alle auswählen** markiert alle Zeilen in der Tabelle.
- **Hosts in der Domänenstruktur auswählen** eignet sich zur Auswahl von Hosts und zur Anzeige ihrer Position in der Domänenstruktur.

Allgemeiner Schutz

Auf der Seite **Allgemeiner Schutz** wird eine Zusammenfassung des Schutzstatus der einzelnen Hosts angezeigt.

- Ob Echtzeit-Scanning aktiviert oder deaktiviert ist
- Die momentan verwendete Sicherheitsstufe für Internet Shield
- Ob die Überprüfung eingehender und ausgehender E-Mails aktiviert oder deaktiviert ist
- Ob der reputationsbasierte Schutz verwendet wird
- Ob Exploit Shields verwendet werden

Gehen Sie zu Automatische Updates.

Auf dieser Seite wird eine Zusammenfassung der Virendefinitions-Datenbanken für auf den Hosts installierte Programme angezeigt.

- Datum und Uhrzeit der letzten Aktualisierung der Virendefinitionen
- Version der Virendefinitionen
- Datum und Uhrzeit der letzten Aktualisierung der Virendefinitionen in F-SecureGateway-Programmen
- Update Delta ist der Zeitraum zwischen der letzten Aktualisierung der Virendefinitionen auf dem Host und der letzten Übertragung von Statistiken zwischen dem Host und Policy Manager.
- Version der Virendefinitionen in Gateway-Programmen
- Datum und Uhrzeit der letzten Aktualisierung der Spyware-Definitionen
- Version der Spyware-Definitionen
- Datum und Uhrzeit der letzten Aktualisierung der Spam-Definitionen in Gateway-Programmen
- Version der Spam-Definitionen in Gateway-Programmen

Datum und Version der Virendefinitionen werden auch für Hosts angezeigt, auf denen Anti-virus for Citrix Servers, Anti-virus for Windows Servers,Internet Gatekeeper oder Anti-virus for Microsoft Exchange installiert ist.

Virenschutz

Auf der Seite **Virenschutz** werden die folgenden Informationen angezeigt:

- Datum der letzten Infektion
- Name der letzten Infektion
- Letztes infiziertes Objekt
- Maßnahme bei letzter Infektion
- Gesamtzahl der Infektionen

Internet Shield

Auf der Seite **Internet Shield** werden die folgenden Informationen angezeigt:

- Datum und Uhrzeit des letzten Angriffs in der Spalte **Zeitstempel des letzten Angriffs**
- Betroffener Dienst beim letzten Angriff

- Quelle des letzten Angriffs
- Aktuelle Angriffe (Sie können den Inhalt dieser Spalte sortieren, indem Sie auf die Kopfzeile der Spalte klicken)
- Wert für aktuelle Angriffe zuletzt zurückgesetzt um (Uhrzeit, zu der der Wert für die aktuellen Angriffe zum letzten Mal zurückgesetzt wurde)

Installierte Software

Auf der Seite **Installierte Software** wird eine Zusammenfassung der auf dem oder den Hosts installierten Software angezeigt.

- Client Security Softwareversion (einschließlich Build-Nummer und evtl. Hotfixes)
- Liste der Anti-Spyware-Hotfixes
- Ob Internet Shield installiert ist
- Ob das Modul zur E-Mail-Überprüfung installiert ist
- Ob Web Traffic Scanning installiert ist
- Ob der Surfschutz installiert ist
- Ob DeepGuard installiert ist
- Policy Manager Proxy Version

Zentrale Verwaltung

Auf der Seite **Zentrale Verwaltung** wird eine Zusammenfassung der Informationen bezüglich der zentralen Verwaltung angezeigt.

- Richtliniendatei-Zeitstempel
- Richtliniendatei-Zähler; dabei handelt es sich um die Nummer der Richtliniendatei, die zurzeit auf dem Host genutzt wird.
- Datum der letzten Statistikübertragung an Policy Manager
- Ob die Verbindung des Hosts getrennt ist (Sie können die Tabelle nach dieser Spalte sortieren, indem Sie auf den Spaltenkopf klicken)
- Die Anzahl der neuen Sicherheitswarnungen und -alarme
- Die Anzahl der neuen schwerwiegenden Fehler

Host-Eigenschaften

Auf der Seite **Host-Eigenschaften** werden die folgenden Informationen für jeden Host angezeigt:

- Der WINS-Name des Hosts
- Die IP-Adresse des Hosts
- Der DNS-Name des Hosts
- Das Betriebssystem des Hosts

Registerkarte "Alarme"

Auf der Registerkarte **Alarme** werden Alarmmeldungen von den gewählten Hosts und Domänen angezeigt. Sie kann auch zur Verwaltung der Alarmberichte genutzt werden.

Auf der Registerkarte **Alarme** werden für jede Alarmmeldung die folgenden Informationen angezeigt:

- Schweregrad,
- date and time,
- Beschreibung,
- Host und Benutzer und
- das Programm, auf das sich der Alarm bezieht.

Wenn Sie einen Alarm in der Alarmliste auswählen, werden in der unteren Hälfte der Seite spezifische Informationen über den Alarm angezeigt: Programm, Schweregrad, Ursprungs-Host usw. Alarme, die während der Überprüfung durch Client Security aufgetreten sind, verfügen eventuell über einen angehängten Bericht. Dieser Bericht wird in der unteren Hälfte der Seite angezeigt.

Klicken Sie auf **Alarm-Weiterleitung konfigurieren**, um die Registerkarte **Einstellungen** und die Seite **Alarme** zu öffnen. Dort können Sie die Weiterleitung von Alarmen konfigurieren.

Registerkarte "Scan-Berichte"

Auf der Registerkarte **Scan-Berichte** werden Viren-Scan-Berichte von den ausgewählten Hosts und Domänen angezeigt. Darüber hinaus können hierüber die Scan-Berichte verwaltet werden.

Auf der Registerkarte **Scan-Berichte** werden über jeden Bericht die folgenden Informationen angezeigt:

- Schweregrad,
- date and time,
- Beschreibung
- Host und Benutzer und
- das Programm, auf das sich der Bericht bezieht

Wenn Sie eine Zeile in der Berichtsliste auswählen, wird der entsprechende Scan-Bericht in der unteren Hälfte der Seite angezeigt.

Registerkarte "Installation"

Die Registerkarte **Installation** ist die erste Registerkarte, die sich bei der Installation von Policy Manager Console öffnet.

Die Registerkarte **Installation** enthält Verknüpfungen zu allen installationsbezogenen Funktionen. Darüber hinaus werden hier eine Liste der installierten Produkte und der Status der aktuellen Installationsvorgänge angezeigt.

Active Directory-Struktur importieren...	Hierüber wird der Importassistent von Active Directory gestartet. Hierüber können Sie eine vorhandene Struktur direkt in die Richtliniendomäne importieren und die der Struktur zugewiesenen Importregeln einrichten.
Windows-Hosts automatisch feststellen	Die automatische Erkennungsfunktion findet Windows-Hosts und -Domänen automatisch, führt eine Push-Installation der Software aus und importiert neue Hosts in die Richtliniendomänenstruktur.
Installationspakete auf Windows-Hosts übertragen	Diese Option ermöglicht die direkte Installation auf bestimmten Windows-Hosts anhand der IP-Adressen oder Host-Namen. Wenn diese Option aktiviert ist, können Sie Software auch auf solchen Hosts installieren, die in der Ansicht **Automatisch feststellen** nicht in der Liste der Domänen angezeigt werden.
Neue Hosts importieren...	Hosts senden Registrierungsanfragen an Policy Manager, wenn das erste Produkt auf den Hosts installiert wird. Diese neuen Hosts werden der Richtlinienverwaltung unterzogen, indem sie in den Richtliniendomänenbaum importiert werden.
Installationspakete	In der Ansicht **Installationspakete** werden die verfügbaren Installationspakete sowie detaillierte Informationen zu ihrem Inhalt angezeigt.

Hinweis: Aufgrund von Änderungen der automatischen Updates können die Virendefinitionen auf dem Server nicht mehr manuell über Policy Manager Console aktualisiert werden. Die manuelle Aktualisierung ist nur noch mittels eines speziellen Tools über Policy Manager Server möglich.

Registerkarte "Operationen"

Wir empfehlen die Nutzung der auf dieser Registerkarte verfügbaren Operationen, wenn es im LAN zu einem Virenausbruch gekommen ist.

Die Registerkarte **Operationen** enthält zwei Operationen:

Operation Virusdefinitionen aktualisieren	Über diesen Vorgang können Sie ausgewählte Hosts oder alle Hosts innerhalb der ausgewählten Domäne anweisen, die neuen Virendefinitionen sofort abzurufen.
Operation Viren- und Spyware-Scan	Über diesen Vorgang können Sie ausgewählte Hosts oder alle Hosts innerhalb der ausgewählten Domäne anweisen, sofort eine Überprüfung nach Viren und Spyware durchzuführen.

Es ist empfehlenswert, beide Vorgänge auszuführen, wenn es im LAN zu einem Virenausbruch gekommen ist.

Die Symbolleiste

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

	Verteilt die Richtlinie.
	Wechselt zur vorherigen Domäne oder zum vorherigen Host in der Auswahlhistorie der Domänenstruktur.
	Wechselt zur nächsten Domäne oder zum nächsten Host in der Auswahlhistorie der Domänenstruktur.
	Wechselt in die übergeordnete Domäne.
	Schneidet einen Host oder eine Domäne aus.
	Fügt einen Host oder eine Domäne ein.
	Fügt der derzeit ausgewählten Domäne eine Domäne hinzu.
	Fügt der derzeit ausgewählten Domäne einen Host hinzu.
	Zeigt das Feld **Eigenschaften** eines Hosts oder einer Domäne an.
	Startet das Dienstprogramm **Windows-Hosts automatisch feststellen**. Neue Hosts werden zu der momentan ausgewählten Richtliniendomäne hinzugefügt.
	Beginnt damit, eine Installation an die Windows-Hosts zu übertragen.

	Hierüber erfolgt der Import neuer Hosts zur aktuell ausgewählten Domäne. Die grüne Farbe weist darauf hin, dass der Host eine Anfrage auf automatische Registrierung gesendet hat.
	Zeigt die zur Verfügung stehenden Installationspakete an.
oder	Zeigt alle Alarme an. Wenn neue Alarme vorliegen, wird das Symbol hervorgehoben. Wenn Policy Manager Console gestartet ist, ist das Symbol generell hervorgehoben.

Menübefehle

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

Menü	Befehl	Aktion
Datei	Richtlinien verteilen	Hierüber erfolgt die Verteilung der Richtlinien.
	Richtlinienänderungen verwerfen	Hierüber werden nicht verteilte Änderungen an der Richtlinie verworfen, die seit der letzten Verteilung der Richtlinie vorgenommen wurden.
	Host-Richtliniendatei exportieren	Exportiert die Richtliniendateien.
	Beenden	Beendet Policy Manager Console.
Bearbeiten	Ausschneiden	Schneidet die ausgewählten Elemente aus.
	Einfügen	Fügt ein oder mehrere zuvor kopierte oder ausgeschnittene Elemente an der ausgewählten Position ein.
	Löschen	Löscht die ausgewählten Elemente.
	Neue Richtliniendomäne	Fügt eine neue Domäne hinzu.
	Neuer Host	Fügt einen neuen Host hinzu.
	Active Directory-Struktur importieren	Hierüber wird der Active Directory-Importassistent geöffnet.
	Neue Hosts importieren	Hierüber werden neue Hosts importiert, die eine Anfrage auf Hinzufügen zur Richtliniendomäne gesendet haben.
	Windows-Hosts automatisch erkennen	Importiert Hosts aus der Windows-Domänenstruktur.
	Installationspakete auf Windows-Hosts übertragen	Führt eine Remote-Installation der Software durch und importiert die durch ihre IP-Adresse oder WINS-Namen festgelegten Hosts.
	Suchen	Sucht in den Host-Eigenschaften nach einer Zeichenfolge. Es werden alle Hosts in der ausgewählten Domäne durchsucht.
	Eigenschaften von Domäne/Host	Zeigt die Seite **Eigenschaften** des ausgewählten Hosts oder der ausgewählten Domäne an.
Ansicht	Fensterbereich "Meldung"	Zeigt den Fensterbereich **Meldung** im unteren Teil des Bildschirms an oder blendet ihn aus.

Menü	Befehl	Aktion
	Neue Meldung automatisch öffnen	Wenn diese Option ausgewählt ist, wird der Fensterbereich **Meldung** automatisch geöffnet, wenn eine neue Meldung empfangen wird.
	Zurück	Wechselt zur vorherigen Domäne oder zum vorherigen Host in der Auswahlhistorie der Domänenstruktur.
	Weiter	Wechselt zur nächsten Domäne oder zum nächsten Host in der Auswahlhistorie der Domänenstruktur.
	Übergeordnete Domäne	Wechselt zur übergeordneten Domäne.
	Alle Alarme	Öffnet die Seite **Alarme**, auf der alle Alarme angezeigt werden.
	Erweiterter Modus	Zeigt die Benutzeroberfläche **Erweiterter Modus** an.
	Anti-Virus-Modus	Zeigt die Benutzeroberfläche des **Anti-Virus-Modus** an, der für die zentrale Verwaltung von Client Security optimiert ist.
	<Element> aktualisieren	Aktualisiert die Ansicht für den Status, Alarme oder Berichte manuell. Dieser Menübefehl ändert sich entsprechend der ausgewählten Seite.
	Alle aktualisieren	Aktualisiert alle Daten, die momentan auf der Benutzeroberfläche angezeigt werden: Richtlinien, Status, Alarme, Berichte, Installationspakete und Anfragen zur automatischen Registrierung.
Tools	Installationspakete	Hierüber werden Informationen über Installationspakete in einem Dialogfenster angezeigt.
	Berichterstellung	Erlaubt die Auswahl von Berichterstellungsmethoden sowie der Domänen/Hosts und Programme, die in den Berichten enthalten sein sollen.
	Benutzer	Hierüber wird das Dialogfenster **Benutzer** geöffnet. Hier können Policy Manager-Benutzer hinzugefügt und gelöscht werden.
	Kennwort ändern	Hierüber wird das Dialogfenster **Kennwort ändern** geöffnet, in dem Sie das Kennwort für Ihr Benutzerkonto ändern können.
	Serverkonfiguration	Hierüber wird das Dialogfenster **Serverkonfiguration** geöffnet, in dem Sie Signaturschlüssel exportieren/importieren, die Zeitdauer für die Aufhebung der Verbindung des Hosts einrichten und nicht verbundene Hosts entfernen können.
	Voreinstellungen	Legt die lokalen Voreinstellungen für Policy Manager Console fest. Diese Eigenschaften gelten nur für die lokale Installation von Policy Manager Console.
Hilfe	Inhalt	Zeigt den Index für die **Hilfe** an.
	Registrieren	Öffnet einen Dialog, in dem Sie das Programm registrieren können.
	Kontaktinformationen	Zeigt Kontaktinformationen für F-Secure an.
	Info über F-Secure Policy Manager Console	Zeigt Informationen zur Version an.

Vererbung von Einstellungen

In diesem Abschnitt wird die Vererbung von Einstellungen erläutert. Außerdem erfahren Sie, wie vererbte Einstellungen, die auf der aktuellen Ebene neu definiert wurden, auf der Benutzeroberfläche angezeigt werden.

Die Einstellungen von Policy Manager Console können entweder von einer übergeordneten Ebene in der Domänenstruktur geerbt (d. h. übernommen) oder auf der aktuellen Ebene geändert werden. Wenn Sie eine Einstellung, die lokal neu definiert wurde, löschen (indem Sie auf den Link **Löschen** neben der Einstellung klicken), wird der Wert aus der übergeordneten Domänenebene oder der Standardwert für die Einstellung neu geerbt.

Wenn notwendig können Einstellungsänderungen nicht zugelassen werden, das bedeutet, dass die Benutzer keine Änderungen an diesen vornehmen dürfen. Benutzeränderungen nicht zuzulassen, erzwingt immer die Richtlinie: Die Richtlinienvariable überschreibt alle lokalen Host-Werte und der Endbenutzer kann den Wert nicht ändern, solange die Einschränkung **Benutzeränderungen nicht zulassen** aktiv ist. Wurden die Einstellungen nicht beschränkt, können Benutzer Änderungen vornehmen.

Anzeige der Vererbung von Einstellungen auf der Benutzeroberfläche

Die vererbten und auf der aktuellen Ebene neu definierten Einstellungen werden auf der Benutzeroberfläche von Policy Manager unterschiedlich dargestellt.

Nicht vererbt	Vererbt	Beschreibung
		Ein geschlossenes Vorhängeschloss weist darauf hin, dass die Benutzer die Einstellungen nicht ändern können, da Benutzeränderungen nicht zugelassen wurden. Ein blaues Schlosssymbol zeigt an, dass die Einstellung auf der aktuellen Ebene neu definiert wurde. Ein graues Schlosssymbol dagegen bedeutet, dass die Einstellung vererbt wurde.
		Ein geöffnetes Vorhängeschloss weist darauf hin, dass Benutzer die Einstellungen auf der aktuellen Ebene ändern können. Ein blaues Schlosssymbol zeigt an, dass die Einstellung auf der aktuellen Ebene neu definiert wurde. Ein graues Schlosssymbol dagegen bedeutet, dass die Einstellung vererbt wurde.
Bereinigen		Wenn neben einer Einstellung **Löschen** angezeigt wird, wurde die Einstellung auf der aktuellen Ebene neu definiert und kann gelöscht werden. Beim Löschen dieser Einstellung wird der Standardwert

Nicht vererbt	Vererbt	Beschreibung
		oder geerbte Wert wiederhergestellt. Wenn neben einer Einstellung nichts angezeigt wird, wurde die Einstellung von einer übergeordneten Ebene geerbt.
Textfelder		Vererbte Einstellungen werden abgeblendet (mit grauer Schrift) angezeigt. Die Textfarbe von nicht geerbten Einstellungen ist dagegen schwarz auf weißem Hintergrund.
Kontrollkästchen		Vererbte Einstellungen werden abgeblendet auf einem grauen Hintergrund dargestellt. Werte, die nicht geerbt wurden, werden dagegen auf weißem Hintergrund angezeigt.

Alle Einstellungen auf einer Seite gleichzeitig sperren oder Sperre aufheben

Sie können festlegen, ob alle Einstellungen auf einer Seite gesperrt oder freigegeben werden.

Über die folgenden Links können Sie alle Einstellungen auf einer Seite sperren oder die Sperre aufheben:

Änderungen durch Benutzer zulassen	Hebt die Sperre aller Einstellungen mit einem geschlossenen Schlosssymbol auf der aktuellen Seite auf. Anschließend können Benutzer Änderungen an diesen Einstellungen vornehmen.
Änderungen durch Benutzer nicht zulassen	Sperrt alle Einstellungen mit einem geöffneten Schlosssymbol auf der aktuellen Seite. Anschließend können Benutzer Änderungen an diesen Einstellungen vornehmen.
Alles löschen	Löscht die Werte aller Einstellungen, die auf der aktuellen Seite neu definiert wurden, und stellt die Standardwerte oder die von einer übergeordneten Ebene geerbten Werte wieder her.

Vererbung von Einstellungen in Tabellen

Die Vererbung von Einstellungen wird auch in Tabellen auf den Einstellungs-Bildschirmseiten angezeigt.

Bei den Tabellen **Sicherheitsstufen** der Firewall und **Firewall-Dienste** handelt es sich um so genannte globale Tabellen, d. h., für alle Computer in einer Domäne gelten dieselben Werte. Es ist jedoch möglich, dass auf verschiedenen Subdomänen oder Hosts unterschiedliche Sicherheitsstufen aktiv sind.

Die Standardwerte in den Tabellen werden von MIBs abgeleitet und grau angezeigt. Werte, die auf der aktuellen Stufe bearbeitet wurden, werden schwarz angezeigt.

Kapitel

4

Einrichten eines verwalteten Netzwerks

Themen:

- *Verwalten von Domänen und Hosts*
- *Hinzufügen von Hosts*
- *Lokale Installation und Policy Manager*
- *Installation auf einem infizierten Host*
- *Überprüfen der Management-Verbindungen*

In diesem Kapitel wird die Planung eines verwalteten Netzwerks erläutert. Außerdem werden die besten Methoden zur Bereitstellung von Client Security in unterschiedlichen Umgebungen beschrieben.

Policy Manager bietet verschiedene Möglichkeiten, Client Security in Ihrem Unternehmen bereitzustellen:

- In einer Windows-Domäne können Sie die Funktionen **Automatische Erkennung** und **Neue Hosts importieren** nutzen, um die Erstellung der verwalteten Domäne zu automatisieren.
- Wenn auf vielen Computern Unix oder Linux ausgeführt wird oder wenn auch Server verwaltet werden müssen, können trotzdem alle Computer mit Policy Manager verbunden werden und ihre Sicherheitsanwendungen lassen sich von einem zentralen Ort aus verwalten.

Sie sollten jedoch einige Aspekte beachten, damit Sie später den optimalen Nutzen aus der zentralen Verwaltung Ihrer Sicherheitsanwendungen ziehen können. Dazu gehört unter anderem die sorgfältige Strukturplanung der verwalteten Domäne im Vorfeld der Installation.

Bei der Strukturplanung einer verwalteten Domäne sollten Sie Endbenutzer mit ähnlichen Sicherheitsanforderungen in derselben Subdomäne gruppieren. Außerdem sollten Sie eigene Subdomänen für Laptops und Desktop-PCs einrichten. So können Sie die optimalen Sicherheitseinstellungen für Computer definieren, die mit verschiedenen LANs verbunden werden können oder DFÜ-Verbindungen einsetzen, sowie für Computer, die ständig mit dem Unternehmensnetzwerk verbunden sind.

Verwalten von Domänen und Hosts

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

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

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

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

Hinzufügen von Richtliniendomänen

In diesem Thema wird das Hinzufügen neuer Richtliniendomänen beschrieben.

So fügen Sie eine neue Richtliniendomäne hinzu:

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

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

Hinzufügen von Hosts

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

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

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

Importieren von Hosts aus einer Active Directory-Struktur

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

1. Wählen Sie **Bearbeiten** > **Active Directory-Struktur importieren** aus dem Menü aus.
   Der Assistent für den **Import der Active Directory-Struktur** wird geöffnet.

2. Geben Sie den Speicherort Ihres Active Directory-Servers und den Benutzernamen und das Kennwort ein, über die Sie zumindest Lese-Zugriff erhalten, und klicken Sie auf **Weiter**.
3. Wählen Sie die Active Directory-Domäne, die Container, die Sie importieren möchten, und die Zielrichtliniendomäne aus, die Sie darin importieren möchten, und klicken Sie auf **Weiter**.

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

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

Hinzufügen von Hosts in Windows-Domänen

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

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

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

Importieren neuer Hosts

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

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

So importieren Sie neue Hosts:

1. Klicken Sie auf der Symbolleiste auf .

   Alternativ:

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

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

   - Sie können Meldungen gemäß den Werten der Spalte sortieren, indem Sie auf die entsprechende Tabellenüberschrift klicken.
   - Sie können auch die Reihenfolge der Spalten ändern. Ziehen Sie dazu die Spalten an die entsprechende Position. Die Spaltenbreite kann nach Belieben eingestellt werden.

- Sie können das Kontextmenü der Tabelle (rechter Mausklick auf die Leiste der Tabellüberschrift) verwenden, um festzulegen, welche Eigenschaften in der Tabelle sichtbar sind.

Einsatz von Importregeln

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

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

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

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

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

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

   Ein Beispiel für den Einsatz benutzerdefinierter Eigenschaften ist die Erstellung von separaten Installationspaketen für unterschiedliche Abteilungen in einem Unternehmen, die unter abteilungsspezifischen Richtliniendomänen gruppiert wurden. In diesem Fall könnten Sie den Gerätenamen als benutzerdefinierte Eigenschaft verwenden und anschließend Regeln für den Import definieren, die Gerätenamen als Importkriterien verwenden. Beachten Sie, dass Namen von ausgeblendeten benutzerdefinierten Eigenschaften verloren gehen, sobald Policy Manager Console geschlossen wird. So fügen Sie eine neue benutzerdefinierte Eigenschaft hinzu:

   a) Klicken Sie mit der rechten Maustaste auf einen Spaltenkopf, und wählen Sie **Benutzerdefinierte Eigenschaft hinzufügen**.
      Das Dialogfeld **Neue benutzerdefinierte Eigenschaft** wird geöffnet.
   b) Geben Sie einen Namen für die benutzerdefinierte Eigenschaft ein, z. B. den Abteilungsnamen, und klicken Sie dann auf **OK**.
      Die neue benutzerdefinierte Eigenschaft wird nun in der Tabelle angezeigt und Sie können neue Importregeln erstellen, in denen diese als Importkriterium verwendet wird.
3. Erstellen Sie eine neue Importregel

   a) Klicken Sie auf der Registerkarte **Regeln für den Import** auf **Hinzufügen**.
      Das Dialogfeld **Ziel-Richtliniendomäne für die Regel auswählen** wird mit einer Liste der vorhandenen Domänen und Subdomänen angezeigt.
   b) Wählen Sie die Domäne aus, für die Sie die Regel erstellen möchten, und klicken Sie auf **OK**.
   c) Wählen Sie die neu erstellte Zeile aus und klicken Sie auf die Zelle, der der Wert hinzugefügt werden soll.
   d) Geben Sie den Wert in die Zelle ein.

Die Importkriterien sind definiert.

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

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

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

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

   Die definierten Importregeln werden validiert, bevor der Import beginnt.

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

Manuelle Definition von Hosts

In diesem Thema wir die manuelle Definition von Hosts beschrieben.

So definieren Sie einen Host manuell:

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

   Alternativ:

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

   Dieser Vorgang ist in den folgenden Fällen nützlich:

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

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

Push-Installationen

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

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

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

Windows-Hosts automatisch erkennen

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

Wählen von Ziel-Hosts:

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

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

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

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

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

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

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

   - **Aktivieren** - versieht die ausgewählten Hosts mit Häkchen (entspricht dem Drücken der Leertaste).
   - **Deaktivieren** - entfernt die Häkchen von den ausgewählten Hosts (entspricht dem Drücken der Leertaste).
   - **Alle aktivieren** - versieht alle Hosts in der ausgewählten Windows-Domäne mit Häkchen.

- **Alle deaktivieren** - entfernt die Häkchen von allen Hosts, die in der ausgewählten Windows-Domäne markiert waren.

5. Klicken Sie auf **Installieren**, um fortzufahren.

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

Installationspakete auf Windows-Hosts übertragen

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

Wählen von Ziel-Hosts:

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

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

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

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

Push-Installation nach Auswahl des Ziel-Hosts

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

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

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

   Sie können auf dieser Seite neue Installationspakete importieren, wenn dies notwendig ist.`Erzwungene NeuinstallationDie` Option ist in allen Installationspaketen immer aktiv. Daher wird die Anwendung erneut installiert, wenn der Host bereits über die gleiche Versionsnummer der installierten Anwendung verfügt.
2. Übernehmen Sie die Standardrichtlinie, oder geben Sie an, welche Host- bzw. Domänenrichtlinie als anonyme Richtlinie verwendet werden soll. Klicken Sie dann auf **Weite**, um fortzufahren
3. Wählen Sie Benutzerkonto und Passwort für die Push-Installation, indem Sie entweder **Dieses Konto** (das aktuelle Konto) oder **Anderer Benutzer** wählen.

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

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

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

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

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

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

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

   Der **Assistent für die Remote-Installation** führt Sie durch die einzelnen Installationsschritte und zeigt mehrere Dialogfelder mit Fragen an. Abhängig von Ihren Antworten legt der Assistent die Einstellungen für die Installation fest. Klicken Sie im letzten Dialogfeld auf **Fertig stellen**, und fahren Sie mit dem nächsten Schritt fort.

   Policy Manager installiert Management Agent und die ausgewählten Programme auf den Hosts. Während dieses Vorgangs wird auf der **Statusleiste** der Fortschritt der Installation angezeigt. Sie können jederzeit auf **Abbrechen** klicken, um die Installation zu stoppen.
6. Wenn die **Statuszeile** vollständig ist, ist der Prozess abgeschlossen, und Sie können über die Einstellungen für den Import die Domäne für die neuen Hosts auswählen.
7. Klicken Sie auf **Fertig stellen**.

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

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

Installation auf Richtlinienbasis

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

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

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

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

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

Verwenden von richtlinienbasierter Installation

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

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

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

So verwenden Sie richtlinienbasierte Installation:

1. Öffnen Sie die Registerkarte **Installation**.
   Auf der Registerkarte **Installation** wird in der Tabelle **Richtlinienbasierte Installationen** der Status der aktuellen Installationsvorgänge angezeigt. In der Tabelle **Zusammenfassung installierter Produkte** werden die Produkte aufgelistet, die aktuell auf verwalteten Hosts installiert sind.
2. Klicken Sie auf **Installieren** unter der Tabelle **Richtlinienbasierte Installationen**, um den Assistenten für die Remote-Installation zu starten.
3. Führen Sie die Anweisungen des Assistenten für die Remote-Installation aus, indem Sie die notwendigen Details angeben.

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

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

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

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

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

Beim Deinstallieren von Management Agent werden keine statistischen Informationen gesendet, mit denen angegeben wird, dass die Deinstallation erfolgreich ausgeführt wurde, da Management Agententfernt wurde

und keine Informationen mehr senden kann. Beispiel: Deinstallieren von F-Secure Anti-Virus und Management Agent:

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

Lokale Installation und Updates mit vorkonfigurierten Paketen

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

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

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

Verwendung des angepassten Remote-Installationspakets

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

So verwenden Sie ein benutzerdefiniertes Installationspaket:

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

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

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

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

Ein Beispiel für die Art der Nutzung benutzerdefinierter Eigenschaften ist die Erstellung eines separaten Installationspakets für unterschiedliche organisatorische Einheiten, die unter der Einheit spezifischen Richtliniendomänen gruppiert werden sollten. Der Name der Eigenschaft könnte `Einheit` lauten und der Wert ist für jedes Installationspaket anders. Nun können Hosts aus jeder Einheit in der neuen Host-Ansicht unterschieden werden. Darüber hinaus können über die Spaltensortierung und eine Mehrfachauswahl alle Hosts aus einer Einheit zu ihrer Zieldomäne importiert werden. Beachten Sie, dass die Zieldomäne direkt über die Ansicht **Neue Hots** geändert werden kann. Danach können die Hosts aus einer anderen Einheit in ihre Zieldomäne importiert werden.

10. Wenn Sie die letzte Seite des Assistenten erreichen, klicken Sie auf **Fertig stellen**, um fortzufahren.
11. Darüber hinaus können Sie eine exportierte JAR-Datei auf den Hosts installieren, indem Sie die Datei `ilaunchr.exe` ausführen.

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

    a) Kopieren Sie die Datei `ilaunchr.exe` und das exportierte JAR-Paket in ein Verzeichnis, in dem das Anmeldeskript auf die Dateien zugreifen kann.

    b) Geben Sie folgenden Befehl ein:`ilaunchr <paketname>.jar` wobei Sie anstelle von `paketname` den Namen des zu installierenden JAR-Pakets eingeben.

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

    Für **ILAUNCHR** gelten die folgenden Befehlszeilenparameter:

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

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

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

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

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

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

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

Lokale Installation und Policy Manager

Die lokale Installation wird empfohlen, wenn Sie Client Security lokal auf einer Arbeitsstation installieren müssen, die ansonsten von Policy Manager zentral verwaltet wird.

Policy Manager muss bereits installiert sein, bevor Sie mit der Installation fortfahren können.

Hinweis: Bei der Installation von Client Security zur Verwaltung durch Policy Manager wählen Sie **Zentrale Verwaltung über F-Secure Policy Manager** aus, wenn der Schritt zur Verwaltungsauswahl

während der Einrichtung angezeigt wird. Darüber hinaus erhalten Sie eine Abfrage zur Angabe des Speicherortes des öffentlichen Schlüssels von Policy Manager (`admin.pub`) und der Netzwerkadresse des eingesetzten Policy Manager Server. Diese Informationen sind für die sichere Kommunikation mit Policy Manager notwendig. Sie können den öffentlichen Schlüssel von der Begrüßungsseite von Policy Manager Server herunterladen.

Systemanforderungen

Lesen Sie die folgenden Informationen, bevor Sie mit der Verwendung des Produkts beginnen.

Für die Installation und Verwendung des Produkts auf Ihrem Computer werden folgende Voraussetzungen empfohlen:

Systemanforderungen

Prozessor:	• Unter Windows Vista und Windows 7: Intel Pentium 4,2 GHz oder höher • Unter Windows XP: Intel Pentium III 1 GHz oder höher
Betriebssystem:	• Windows 7 32-Bit und 64-Bit • Windows Vista 32-Bit und 64-Bit • Windows XP SP2 oder neuer
Arbeitsspeicher:	• Unter Windows Vista und Windows 7: 1 GB RAM oder mehr • Unter Windows XP: 512 MB RAM oder mehr
Speicherplatz:	800 MB freier Speicher auf Festplatte
Anzeige:	• Unter Windows Vista und Windows 7: 16 Bits oder mehr (65000 Farben) • Unter Windows XP: 16 Bits, 65000 Farben oder mehr
Internetverbindung:	Erforderlich zur Validierung Ihres Abonnements und zum Empfang von Updates

Deinstallieren anderer Virenschutzprogramme

Vor der Installation von Client Security sollten Sie jegliche anderen Virenschutzprogramme entfernen, die momentan auf den Arbeitsstationen installiert sind.

So deinstallieren Sie andere Virenschutzprogramme:

1. Wählen Sie im Dialogfeld **Start** > **Einstellungen** > **Systemsteuerung** > **Software** die derzeit installierten Programme aus.
2. Entfernen Sie alle zugehörigen Komponenten.

   Manchen Programmen können mehrere Komponenten zugeordnet sein, die unter Umständen separat deinstalliert werden müssen. Bei Problemen siehe die Benutzerdokumentation für das derzeit installierte Virenschutzprogramm.
3. Starten Sie Ihren Computer neu.

Installationsschritte

Sie benötigen die Installations-CD, einen gültigen Abonnementschlüssel und eine Internetverbindung. Wenn mehrere Benutzer auf den Computer zugreifen und ihn verwenden, melden Sie sich mit Administratorrechten an, um das Produkt zu installieren.

So installieren Sie die Software:

1. Legen Sie die Installations-CD ein.

   Die Installation sollte automatisch starten. Falls nicht, rufen Sie den Windows Explorer auf, doppelklicken Sie auf das CD-ROM-Symbol und anschließend auf die Datei`setup.exe`, um die Installation zu starten.

   Der erste Installationsdialog erscheint.
2. Wählen Sie die Installationssprache und klicken auf **Weiter**, um fortzufahren.
3. Lesen Sie die Lizenzvereinbarung. Um die Vereinbarung anzunehmen und fortzufahren, klicken Sie auf **Akzeptieren**.
4. Geben Sie Ihren Abonnementschlüssel ein und klicken Sie auf **Weiter**, um fortzufahren.

   Hinweis: Wenn Sie das Produkt testen möchten, lassen Sie das Feld **Mein Abonnementschlüssel ist** frei und klicken auf **Weiter**. Wählen Sie dann im Dialogfeld **Testoptionen** den zu testenden Dienst.

   - Wenn Sie das Produkt auf CD erworben haben, finden Sie den Abonnementschlüssel auf dem Deckblatt der Schnellinstallationsanleitung.
   - Wenn Sie das Produkt vom F-Secure eStore heruntergeladen haben, wurde Ihnen der Abonnementschlüssel in der Bestätigungs-E-Mail der Bestellung mitgeteilt.

   Hinweis: Verwenden Sie nur den Abonnementschlüssel, der mit dem Produkt übermittelt wurde. Sie können den Abonnementschlüssel für die Anzahl der Installationen verwenden, für die Ihre Lizenz gültig ist (siehe Hinweis "F-Secure-Lizenz" in dieser Anleitung). Wenn Sie Probleme mit der Registrierung haben, wenden Sie sich bitte an den technischen F-Secure-Support.
5. Wählen Sie den Installationstyp:

   - Automatische Installation: Das Produkt wird automatisch installiert. Vorhandene Sicherheitsprodukte werden möglicherweise automatisch ersetzt. Das Produkt wird im Standardverzeichnis installiert.
   - Schrittweise Installation: Sie können während der Installation Optionen auswählen. So können Sie zum Beispiel das Installationsverzeichnis ändern. Wir empfehlen jedoch die Verwendung des Standardverzeichnisses.
6. Klicken Sie auf **Weiter**.
7. Entnehmen Sie nach Abschluss der Installation die Installations-CD.
8. Der Computer wird automatisch neu gestartet. Für einen sofortigen Neustart wählen Sie **Jetzt neu starten**.
9. Nach dem Neustart versucht das Produkt, eine Internetverbindung aufzubauen, um Ihr Abonnement zu validieren und Updates herunterzuladen. Achten Sie darauf, dass eine Internetverbindung besteht. Der Download dieser größeren Updates kann einige Zeit in Anspruch nehmen. Wenn die Updates heruntergeladen wurden, ist der Schutzstatus aktuell. Mit den neuesten Updates wird der optimale Schutz sichergestellt.

   Tipp: Um mehr über das Produkt zu erfahren, können Sie durch Klicken auf die Schaltfläche **Hilfe** im Produkt auf die Online-Hilfe zugreifen. Die Online-Hilfe finden Sie zudem auf der Installations-CD.

Installation auf einem infizierten Host

Wenn der Host, auf dem Sie Client Security installieren möchten, mit einer Variante des Klez-Virus infiziert ist, sollten Sie zunächst das Dienstprogramm zum Entfernen des Klez-Virus ausführen, bevor Sie mit der Installation beginnen.

Das Installationsprogramm `Ilaunchr.exe` kann nicht auf einem Computer ausgeführt werden, der mit dem Klez-Virus infiziert ist.

Sie können das Dienstprogramm zum Entfernen von Klez von folgender Adresse herunterladen: ftp://ftp.europe.f-secure.com/anti-virus/tools/kleztool.zip.

Im Archiv `kleztool.zip` befindet sich unter anderem die Datei `kleztool.txt` mit Anweisungen zur Ausführung von Kleztool auf einem infizierten Computer. Lesen Sie diese Anweisungen sorgfältig durch, bevor Sie fortfahren.

Überprüfen der Management-Verbindungen

Die Funktion der Management-Verbindungen lässt sich anhand der nachstehend angegebenen Schritte überprüfen.

1. Kontrollieren Sie den **Status der Richtlinienverteilung**auf der Registerkarte **Zusammenfassung**.
2. Speichern und verteilen Sie die Richtlinien, falls notwendig.
3. Wechseln Sie zur Registerkarte **Status** und wählen die Seite **Zentrale Verwaltung**.
4. Überprüfen Sie den Zeitstempel und den Zähler der momentan verwendeten Richtliniendatei.

Kapitel

5

Konfigurieren von Viren- und Spyware-Schutz

Themen:

- *Konfigurieren automatischer Updates*
- *Konfigurieren des Echtzeit-Scanning*
- *Konfigurieren von DeepGuard*
- *Konfigurieren des Rootkit-Scannings (Blacklight)*
- *Konfigurieren des E-Mail-Scannings*
- *Konfigurieren von Web Traffic (HTTP) Scanning*
- *Konfigurieren des Spyware-Scannings*
- *Verwalten unter Quarantäne gestellter Objekte*
- *Verhindern, dass Benutzer Einstellungen eigenmächtig ändern*
- *Konfigurieren der Alarmmeldungen*
- *Überwachen der Virenvorfälle im Netzwerk*
- *Überprüfen der Virenschutzfunktionen*

Der Viren- und Spyware-Schutz von Client Security umfasst automatische Updates, manuelles Scanning, geplantes Scanning, Echtzeit-Scanning, Spyware-Scanning, DeepGuard, Rootkit-Scanning, E-Mail-Scanning und Browser-Schutz.

Der Viren- und Spyware-Schutz sorgt dafür, dass der Computer vor Dateiviren, Spyware, Riskware, Rootkits und Viren, die als E-Mail-Anhänge und über das Internet verbreitet werden, geschützt ist.

Automatische Updates gewährleisten, dass der Viren- und Spyware-Schutz immer aktuell ist. Wenn Sie den Viren- und Spyware-Schutz und die automatischen Updates eingerichtet und die Einstellungen als Sicherheitsrichtlinie verteilt haben, können Sie sich darauf verlassen, dass das verwaltete Netzwerk vor Viren und Spyware geschützt ist. Darüber hinaus können Sie die Scan-Ergebnisse und andere Informationen überwachen, die von den verwalteten Hosts an Policy Manager Console zurückgesendet werden.

Wird ein Virus auf einem Computer gefunden, kann eine der folgenden Maßnahmen ausgeführt werden:

- die infizierte Datei wird desinfiziert,
- die infizierte Datei wird umbenannt,
- die infizierte Datei wird gelöscht,
- die infizierte Datei wird unter Quarantäne gestellt,
- der Benutzer wird aufgefordert zu entscheiden, welche Maßnahme mit der infizierten Datei ausgeführt wird,
- die infizierte Datei oder Anlage (beim E-Mail-Scanning) wird nur gemeldet oder
- die infizierte Anlage (beim E-Mail-Scanning) wird desinfiziert, entfernt oder blockiert.

Konfigurieren automatischer Updates

In diesem Abschnitt werden die verschiedenen Konfigurationseinstellungen von Policy Manager für automatische Updates erläutert. Außerdem finden Sie hier einige praktische Konfigurationsbeispiele für Hosts mit unterschiedlichen Schutzanforderungen.

Wenn Sie die folgenden Anweisungen beachten, sorgen Sie dafür, dass die Viren- und Spyware-Definitionen auf den Hosts immer aktuell sind, und Sie können anhand der Benutzeranforderungen die beste Aktualisierungsquelle auswählen.

So funktionieren automatische Updates

Der mit Client Security installierte Automatic Update Agent lädt die automatischen Updates von den konfigurierten Update-Quellen herunter.

Der Automatic Update Agent versucht, Updates in der folgenden Reihenfolge herunterzuladen:

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

Hinweis: Wenn Client Security für das Herunterladen von NeighborCast-Updates konfiguriert ist, werden möglicherweise auch Updates von anderen Client Security-Installationen heruntergeladen, auf denen NeighborCast aktiviert ist.

Einstellungen für automatische Updates

Auf der Seite **Automatische Updates** können Sie auf der Registerkarte **Einstellungen** festlegen, ob Client Security Updates für Viren- und Spyware-Definitionen automatisch abrufen soll.

Um automatische Updates zuzulassen, aktivieren Sie das Kontrollkästchen **Automatische Updates aktivieren**. Die automatischen Updates sollten immer aktiviert sein.

Geben Sie in das Feld **Abfrageintervall für Updates vom F-Secure Policy Manager Server** das Abfrageintervall für die automatischen Updates ein.

Policy Manager Proxy enthält eine Liste der verfügbaren **Policy Manager Proxy**-Server. Der mit Client Security installierte Automatic Update Agent versucht in der Reihenfolge, in der die Proxy-Server in dieser Liste aufgeführt sind, eine Verbindung mit diesen Servern herzustellen.

Wenn Sie einen HTTP-Proxy-Server verwenden möchten, wählen Sie aus der Dropdown-Liste **HTTP-Proxy verwenden** die Option **Wie Browser-Einstellungen** oder **Benutzerdefiniert**. Geben Sie dann die **HTTP-Proxy-Adresse** ein.

Konfigurieren der automatischen Updates von Policy Manager Server

Wenn die Domäne zentral verwaltet wird, können alle Hosts die Viren- und Spyware-Definitions-Updates von Policy Manager Server abrufen.

Gehen Sie bei der Konfiguration folgendermaßen vor:

1. Wählen Sie auf der Registerkarte **Richtliniendomänen** den Eintrag **Stamm**.
2. Öffnen Sie die Registerkarte **Einstellungen**, und wählen Sie die Seite **Automatische Updates**.
3. Vergewissern Sie sich, dass die Option **Automatische Updates aktivieren** aktiviert ist.
4. Stellen Sie im Feld **Abfrageintervall für Updates vom F-Secure Policy Manager** ein für Ihre Umgebung geeignetes Abfrageintervall ein.
5. Wenn Sie HTTP-Proxy-Server verwenden möchten, überprüfen Sie die Einstellungen unter **HTTP-Proxy verwenden** und **HTTP-Proxy-Adresse**.
6. Wenn das System auf Policy Manager Server oder den F-Secure-Update-Server zurückgreifen soll, wenn auf keinen Policy Manager Proxy zugegriffen werden kann, wählen Sie die Option **Rückgriff auf Policy Manager Server zulassen, wenn keine Policy Manager Proxy-Server verfügbar sind** bzw. **Rückgriff auf F-Secure-Update-Server zulassen, wenn keine Policy Manager Proxy-Server verfügbar sind**.
7. Wenn Sie verhindern möchten, dass Benutzer die Einstellungen ändern können, klicken Sie auf das Schlosssymbol, das neben den Einstellungen angezeigt wird.
8. Klicken Sie auf , um die Richtlinie zu verteilen.

Konfigurieren von Policy Manager Proxy

Wenn die Niederlassungen eines Unternehmens über eigene Policy Manager Proxy-Server verfügen, empfiehlt es sich in vielen Fällen, die Laptops der Benutzer, die in mehreren Niederlassungen eingesetzt werden, so zu konfigurieren, dass ein Policy Manager Proxy-Server als Update-Quelle eingesetzt wird.

Hinweis: Policy Manager Proxy ist ein neues Produkt und nicht mit dem F-Secure Anti-Virus Proxy-Server zu verwechseln.

In diesem Konfigurationsbeispiel gehen wir davon aus, dass die Laptops bereits auf der Registerkarte **Richtliniendomänen** in eine Subdomäne importiert wurden und dass die verschiedenen Niederlassungen des Unternehmens über eigene Policy Manager Proxy-Server verfügen, die alle in der Liste der Policy Manager Proxy-Server enthalten sind.

1. Wählen Sie auf der Registerkarte **Richtliniendomänen** die Subdomäne aus, in der der Policy Manager Proxy-Server eingesetzt werden soll.
2. Öffnen Sie die Registerkarte **Einstellungen**, und wählen Sie die Seite **Automatische Updates**.
3. Vergewissern Sie sich, dass die Option **Automatische Updates aktivieren** aktiviert ist.
4. Klicken Sie auf **Hinzufügen**, um neue Server zur Liste der verfügbaren Proxy-Server hinzuzufügen. Daraufhin wird das Fenster **Eigenschaften des F-Secure Policy Manager Proxy-Servers** geöffnet.
5. Geben Sie in das Feld **Priorität** einen Wert für den Policy Manager Proxy-Server ein.

   Der eingegebene Wert bestimmt die Reihenfolge, in der die Hosts versuchen, eine Verbindung mit dem Policy Manager Proxy-Server herzustellen. Geben Sie z.B. für den Policy Manager Proxy-Server in der Niederlassung, in der sich der Host normalerweise befindet, den Wert `10` ein, für die anderen Proxy-Server den Wert `20`, `30` usw.
6. Geben Sie in das Feld **Adresse** die URL des Policy Manager Proxy-Servers ein, und klicken Sie auf **OK**.
7. Wiederholen Sie die oben beschriebenen Schritte, um die anderen Server zur Liste hinzuzufügen.
8. Nachdem Sie alle Proxy-Server zur Liste hinzufügt haben, überprüfen Sie, ob sie in der richtigen Reihenfolge aufgeführt werden.

   Bei Bedarf können Sie die Reihenfolge der Server ändern, indem Sie deren Priorität ändern.
9. Wenn Sie verhindern möchten, dass Benutzer die Einstellungen ändern können, klicken Sie auf das Schlosssymbol, das neben den Einstellungen angezeigt wird.
10. Klicken Sie auf , um die Richtlinie zu verteilen.

Hinweis: Über die lokale Benutzeroberfläche können auch Endbenutzer Policy Manager Proxy-Server aus der Liste hinzufügen. Beim Herunterladen von Viren- und Spyware-Definitions-Updates verwendet der Host eine Kombination aus beiden Listen. Ein von einem Endbenutzer hinzugefügter Policy Manager Proxy-Server wird vor den vom Administrator hinzugefügten Proxy-Servern abgefragt.

Konfigurieren von Clients zum Herunterladen von Updates von anderen Clients

Sie können Automatic Update Agent so konfigurieren, dass die Clients Updates nicht nur von vorhandenen Servern oder Proxy-Servern, sondern auch voneinander herunterladen.

Diese Funktion wird als NeighborCast bezeichnet. Updates können von den folgenden Quellen heruntergeladen werden:

- Von einem Policy Manager Server
- Von einem Policy Manager Proxy
- Von einem HTTP-Proxy-Server
- Von einem F-Secure-Update-Server
- Von einem anderen Automatic Update Agent(beispielsweise Client Security), auf dem NeighborCast aktiviert ist.

So aktivieren Sie NeighborCast

1. Wählen Sie die Zieldomäne.
2. Öffnen Sie auf der Registerkarte **Einstellungen** die Seite **Automatische Updates**.
   a) Um die Clients in der ausgewählten Domäne zum Herunterladen von Updates von anderen Clients zu konfigurieren, wählen Sie **NeighborCast-Client** aus.
   b) Um die Clients in der ausgewählten Domäne zum Bereitstellen von Updates für andere Clients zu konfigurieren, wählen Sie **NeighborCast-Server** aus.
3. Um den für NeighborCast verwendeten Port zu ändern, geben Sie unter **NeighborCast-Port** eine neue Port-Nummer ein.

Konfigurieren des Echtzeit-Scanning

Das Echtzeit-Scanning sorgt dafür, dass der Computer jederzeit geschützt ist, da die Dateien beim Zugreifen, Öffnen oder Schließen gescannt werden.

Das Echtzeit-Scanning wird im Hintergrund ausgeführt. Das bedeutet, dass diese Funktion nach der Einrichtung für den Benutzer praktisch unsichtbar ist.

Einstellungen für das Echtzeit-Scanning

Hier werden die auf der Seite **Einstellungen** > **Echtzeit-Scanning** verfügbaren Einstellungen beschrieben.

Um das Echtzeit-Scanning zu aktivieren, aktivieren Sie das Kontrollkästchen **Echtzeit-Scanning aktiviert**. Um das Echtzeit-Scanning zu deaktivieren, deaktivieren Sie das Kontrollkästchen **Echtzeit-Scanning aktiviert**.

Mithilfe der folgenden Optionen legen Sie fest, was gescannt werden soll:

- **Alle Dateien**

  Alle Dateien werden unabhängig von der Dateierweiterung gescannt. Diese Option ist für den allgemeinen Einsatz nicht empfehlenswert, da sie unter Umständen dazu führt, dass das System erheblich langsamer arbeitet.

- **Dateien mit diesen Erweiterungen**

Dateien mit bestimmten Dateierweiterungen werden gescannt. Geben Sie einen Punkt (.) ein, um Dateien ohne Erweiterung festzulegen. Der Platzhalter ? kann für einen beliebigen Buchstaben eingegeben werden. Geben Sie alle Dateierweiterungen ein, und trennen Sie sie durch ein Leerzeichen. Diese Option wird für den Echtzeitschutz empfohlen. Bei der Aktualisierung der Virendefinitionsdatenbank werden automatisch neue Datenerweiterungen zu der Liste hinzugefügt.

- **Ausgeschlossene Erweiterungen aktivieren**

  Sie können außerdem angeben, ob einige Dateien von der Überprüfung ausgenommen werden sollen. Dazu geben Sie die Erweiterungen der ausgeschlossenen Dateien in das Feld **Ausgeschlossene Erweiterungen** ein. Diese Einstellung ist besonders nützlich, wenn Sie zuvor für das Scanning **Alle Dateien** festgelegt haben.

- **Ausgeschlossene Objekte aktivieren**

  Bei ausgeschlossenen Objekten handelt es sich um einzelne Dateien oder Ordner, die in der Regel lokal festgelegt werden. Die Festlegung kann aber auch über Policy Manager Console erfolgen. Klicken Sie hierzu mit der rechten Maustaste auf das Kontrollkästchen **Ausgeschlossene Objekte aktivieren**, und wählen Sie **In den erweiterten Modus wechseln**.

- **Netzwerklaufwerke scannen**

  Aktivieren Sie dieses Kontrollkästchen, um alle Dateien zu scannen, die sich auf einem Netzwerklaufwerk befinden.

  Wichtig: In Client Security ist die Einstellung **Netzwerklaufwerke scannen** standardmäßig deaktiviert.

- **Nach Erstellung oder Änderung scannen**

  Normalerweise werden Dateien gescannt, wenn ein Benutzer die Datei öffnet, um sie zu lesen oder auszuführen. Wenn eine Datei zum Schreiben geöffnet oder eine neue Datei erstellt wird und diese Einstellung aktiv ist, wird die Datei auch beim Schließen gescannt. Wenn diese Einstellung aktiviert ist, werden Änderungen in neuen oder bearbeiteten Dateien beim Schließen sofort erkannt. Diese Einstellung ist standardmäßig aktiviert, und es wird empfohlen, dies nicht zu ändern.

- **Maßnahme bei Infektion automatisch auswählen**

  In Client Security9 oder höher und Anti-virus for Windows Servers 9 oder höher können Sie diese Option auswählen, um das Programm automatisch entscheiden zu lassen, welche Maßnahme ergriffen werden soll, wenn beim Scanning eine Infektion erkannt wird.

- **Benutzerdefinierte Maßnahme bei Infektion**

  Wenn die automatische Auswahl deaktiviert ist, können Sie die Standardmaßnahme, die das Programm ausführt, wenn eine infizierte Datei erkannt wird, aus diesem Dropdown-Menü auswählen. Wählen Sie eine der folgenden Maßnahmen aus:

Aktion	Definition
Nach Scannen fragen	Startet den **Desinfektions-Assistenten**, wenn eine infizierte Datei gefunden wird.
Automatisch desinfizieren	Die Datei wird automatisch desinfiziert, wenn ein Virus festgestellt wird.
Automatisch umbenennen	Die Datei wird automatisch umbenannt, wenn ein Virus gefunden wird.
Automatisch löschen	Die Datei wird automatisch gelöscht, wenn ein Virus gefunden wird. Diese Option ist nicht empfehlenswert, da dadurch die Datei, an die der Virus angehängt wurde, ebenfalls gelöscht wird.

Aktion	Definition
Nur Bericht	Es wird darauf hingewiesen, dass ein Virus festgestellt wurde, und verhindert, dass das infizierte Objekt geöffnet wird. Bei Auswahl dieser Option werden Viren nur gemeldet, es wird aber keine Maßnahme durchgeführt.
Automatisch in Quarantäne stellen	Die infizierte Datei wird automatisch in das Quarantäne-Repository verschoben.

- **"Host"-Datei schützen**

  Wenn diese Option aktiviert ist, wird die "Host"-Datei vor Änderungen durch Spyware geschützt. Manche Malware-Anwendungen können versuchen, mithilfe dieser Datei die IP-Adresse eines bekannten DNS-Namens durch die IP-Adresse einer bösartigen Website zu ersetzen.

- **Auf Tracking Cookies prüfen**

  Wenn diese Einstellung aktiviert ist, werden Tracking Cookies erkannt. Beim Echtzeit-Scanning werden nur Tracking Cookies erkannt, die auf Festplatte gespeichert sind. Cookies, die sich nur im Cache des Webbrowsers befinden, werden hingegen nicht erkannt. Beim manuellen Scanning werden sowohl auf der Festplatte als auch im Cache des Webbrowsers gespeicherte Cookies erkannt.

Handhabung von Dateierweiterungen

Die Richtlinie von Client Security legt eine Liste der eingeschlossenen Dateierweiterungen fest (dies können auch "Alle Dateien" sein). Die Liste der **Eingeschlossenen Erweiterungen** kann auch Bestandteil eines Virendefinitions-Updates sein. Diese eingeschlossenen Erweiterungen werden zunächst von Client Security zusammengestellt. Anschließend werden alle ausgeschlossenen Erweiterungen aus dieser Liste entfernt, um die tatsächliche Liste der Dateien zu bestimmen, die überprüft werden sollen. Dies betrifft das Echtzeit-Scanning, das manuelle Scanning und das E-Mail-Scanning.

Aktivieren des Echtzeit-Scannings für die gesamte Domäne

In diesem Beispiel wird das Echtzeit-Scanning für die gesamte Domäne aktiviert.

1. Wählen Sie auf der Registerkarte **Richtliniendomänen** den Eintrag **Stamm**.
2. Öffnen Sie die Registerkarte **Einstellungen**, und wählen Sie die Seite **Echtzeit-Scanning**.
3. Aktivieren Sie das Kontrollkästchen **Echtzeit-Scanning aktiviert**.
4. Wählen Sie aus der Dropdown-Liste **Zu scannende Dateien** die Option **Dateien mit diesen Erweiterungen**.
5. Wählen Sie aus der Dropdown-Liste **Scanning von Dateien: Maßnahme bei Infektion** die Maßnahme aus, die ausgeführt werden soll, wenn eine infizierte Datei gefunden wird.
6. Überprüfen Sie, ob alle anderen Einstellungen auf dieser Seite für Ihr System geeignet sind. Nehmen Sie bei Bedarf Änderungen vor.
7. Klicken Sie auf , um die Richtlinie zu verteilen.

Erzwingen der Verwendung des Echtzeit-Scannings auf allen Hosts

In diesem Beispiel wird das Echtzeit-Scanning so konfiguriert, dass es vom Endbenutzer nicht deaktiviert werden kann. Dadurch ist gewährleistet, dass alle Hosts unter allen Umständen geschützt sind.

1. Wählen Sie auf der Registerkarte **Richtliniendomänen** den Eintrag **Stamm**.
2. Öffnen Sie die Registerkarte **Einstellungen**, und wählen Sie die Seite **Echtzeit-Scanning**.

3. Aktivieren Sie das Kontrollkästchen **Echtzeit-Scanning aktiviert**.
4. Wählen Sie aus der Dropdown-Liste **Zu scannende Dateien** die Option **Dateien mit diesen Erweiterungen**.
5. Wählen Sie aus der Dropdown-Liste **Benutzerdefinierte Maßnahme bei Infektion** die Maßnahme aus, die ausgeführt werden soll, wenn eine infizierte Datei gefunden wird.

   Alternatively, select **Maßnahme bei Infektion automatisch auswählen** to let the product automatically decide what action to take.
6. Überprüfen Sie, ob alle anderen Einstellungen auf dieser Seite für Ihr System geeignet sind. Nehmen Sie bei Bedarf Änderungen vor.
7. Klicken Sie auf **Änderungen durch Benutzer nicht zulassen**, um zu verhindern, dass Benutzer das Echtzeit-Scanning auf ihren Computern deaktivieren.
   Daraufhin wird neben allen Einstellungen dieser Seite ein Schlosssymbol angezeigt.
8. Klicken Sie auf , um die Richtlinie zu verteilen.

Ausschließen von Microsoft Outlook PST-Dateien vom Echtzeit-Scanning

Wenn Sie das Echtzeit-Scanning so konfiguriert haben, dass alle Dateien gescannt werden, ist es unter Umständen empfehlenswert, die PST-Dateien von Microsoft Outlook von der Überprüfung auszuschließen. Diese Dateien sind im Normalfall sehr groß und benötigen entsprechend viel Zeit für die Überprüfung. Dadurch kann das System belastet und verlangsamt werden.

Gehen Sie folgendermaßen vor, um die Überprüfung der PST-Dateien für die gesamte Domäne auszuschließen:

1. Wählen Sie auf der Registerkarte **Richtliniendomänen** den Eintrag **Stamm**.
2. Öffnen Sie die Registerkarte **Einstellungen**, und wählen Sie die Seite **Echtzeit-Scanning**.
3. Aktivieren Sie das Kontrollkästchen **Ausgeschlossene Erweiterungen aktivieren**.
4. Geben Sie die Erweiterung PST in das Feld **Ausgeschlossene Erweiterungen** ein.

   Beachten Sie, dass die Erweiterung ohne den voranstehenden Punkt (".") eingegeben werden muss.
5. Wenn Sie verhindern möchten, dass Benutzer die Einstellungen ändern können, klicken Sie auf das Schlosssymbol, das neben den Einstellungen angezeigt wird.
6. Klicken Sie auf , um die Richtlinie zu verteilen.

Konfigurieren von DeepGuard

DeepGuard ist ein hostbasiertes Intrusion Prevention-System, das das Verhalten von Dateien und Programmen analysiert.

Mithilfe von DeepGuard können aufdringliche Werbe-Popups blockiert und wichtige Systemeinstellungen geschützt werden. Zudem lassen sich Einstellungen von Internet Explorer gegen unerwünschte Änderungen schützen.

Wenn eine Anwendung versucht, eine potenziell gefährliche Aktion aufzuführen, wird überprüft, ob die Anwendung vertrauenswürdig ist. Sichere Anwendungen können ausgeführt werden, Aktionen von unsicheren Anwendungen werden hingegen blockiert.

Wenn DeepGuard aktiviert ist, können Sie die Anwendungssteuerung so konfigurieren, dass Benutzer nur dann gefragt werden, wie vorgegangen werden soll, wenn DeepGuard die Anwendung als nicht vertrauenswürdig einschätzt.

DeepGuard-Einstellungen

Hier werden die Einstellungen für DeepGuard beschrieben, die auf der Seite **Einstellungen** > **Echtzeit-Scanning** angezeigt werden.

Aktivieren Sie das entsprechende Kontrollkästchen, um DeepGuard zu aktivieren.

Sie können die Maßnahmen bestimmen, die ausgeführt werden sollen, wenn ein Systemänderungsversuch erkannt wird. Folgende Maßnahmen stehen zur Auswahl:

Aktion	Definition
Immer Genehmigung einholen	DeepGuard fragt den Benutzer, ob er alle überwachten Aktionen zulassen oder blockieren möchten, selbst wenn DeepGuard die Anwendung als sicher eingestuft hat.
In nicht eindeutigen Fällen fragen	Nur wenn die Anwendung nicht als sicher oder unsicher eingestuft werden kann, fragt DeepGuard den Benutzer, ob überwachte Aktionen zugelassen oder blockiert werden sollen (Standardoption).
Automatisch: Keine Abfrage	DeepGuard blockiert unsichere Anwendungen und lässt sichere Anwendungen automatisch zu, ohne den Benutzer zu fragen.

Falls berechtigte Programme von DeepGuard blockiert werden, können Sie versuchen, die Option **Erweiterte Prozessüberwachung** zu deaktivieren. Zum maximalen Schutz werden laufende Programme von DeepGuard vorübergehend geändert. Aufgrund dieser erweiterten Prozessüberwachung werden manche Programme möglicherweise nicht richtig ausgeführt. Dies betrifft Programme, die ihre eigene Integrität überprüfen.

DeepGuard-Serverabfragen

DeepGuard-Serverabfragen stellen aktuelle Informationen zur Erkennung bösartiger Programme bereit und verringern die Anzahl der Fehlalarme.

Aktivieren Sie die Option **Serverabfragen zur Verbesserung der Erkennungsgenauigkeit verwenden**, um die F-Secure-Server zu überprüfen, wenn DeepGuard eine unbekannte Anwendung erkennt. Wir empfehlen, Serverabfragen aus zwei Gründen zu aktivieren:

- Ein Computer mit aktivierten Serverabfragen verfügt über einen höheren Schutz. Der Zeitraum zwischen der Entdeckung einer neuen Sicherheitsbedrohung und dem Schutz gegen diese Bedrohung wird verkürzt.
- Ein Computer mit aktivierten Serverabfragen erzeugt erheblich weniger Meldungen, ob ein unbekannter Prozess ausgeführt werden soll oder nicht. Der Benutzer hat weniger Möglichkeiten, Entscheidungen zu treffen, die die Sicherheit des Computers beeinträchtigen könnten. Der Benutzer wird außerdem weniger von seiner Arbeit abgehalten.

Was sollte ich über Serverabfragen wissen?

Serverabfragen erfordern eine funktionierende Verbindung mit dem Internet. Wenn Ihr Netzwerk den Zugang nur über einen HTTP-Proxy zulässt, geben Sie für den Automatic Update Agent-HTTP-Proxy die Adresse Ihres Proxyservers ein, um sicherzustellen, dass Serverabfragen durchgeführt werden.

Konfigurieren des Rootkit-Scannings (Blacklight)

Rootkit-Scanning kann verwendet werden, um ein Scanning nach Dateien und Laufwerken auszuführen, die durch Rootkits verborgen sind.

Mit Rootkits wird in der Regel schädliche Software (z.B. Spyware) vor den Benutzern, den Systemtools und den herkömmlichen Virenscannern verborgen. Die mithilfe von Rootkits verborgenen Elemente sind häufig mit Viren, Würmern oder Trojanern infiziert.

Einstellungen für das Rootkit-Scanning

Die Einstellungen für das Rootkit-Scanning werden auf der Seite **Manuelles Scanning** der Registerkarte **Einstellungen** angezeigt.

Das Rootkit-Scanning kann als manueller Vorgang oder als Teil einer vollständigen Überprüfung des Computers ausgeführt werden.

Wählen Sie **Rootkit-Scanning aktivieren** aus, um ein Scanning nach Dateien und Laufwerken auszuführen, die durch Rootkits versteckt sind. Mit dieser Option können Benutzer außerdem lokale Schnell-Scans ausführen, um nach Rootkits und anderen verborgenen Elementen zu suchen.

Wählen Sie **Rootkit-Scanning bei der vollständigen Überprüfung des Computers einschließen** aus, um nach Elementen zu suchen, die durch Rootkits versteckt werden, wenn eine vollständige Überprüfung des Computers vom lokalen Host gestartet wird oder ein manueller Scan-Vorgang über Policy Manager Console gestartet wird.

Wählen Sie **Verdächtige Elemente nach der vollständigen Überprüfung des Computers anzeigen**aus, um erkannte verdächtige Elemente nach der vollständigen Überprüfung des Computers im Desinfektions-Assistenten und im Scan-Bericht anzuzeigen. Wenn Sie diese Option aktivieren, können Sie anhand der Scan-Berichte sehen, ob für die verwalteten Hosts Elemente erkannt wurden, die mithilfe von Rootkits verborgen wurden.

Starten eines Rootkit-Scannings für die gesamte Domäne

Dieses Beispiel veranschaulicht, wie das Rootkit-Scanning für die gesamte Domäne gestartet wird.

1. Wählen Sie auf der Registerkarte **Richtliniendomänen** den Eintrag **Stamm**.
2. Öffnen Sie die Registerkarte **Einstellungen**, und wählen Sie die Seite **Manuelles Scanning** aus.
3. Vergewissern Sie sich, dass im Abschnitt **Rootkit-Scanning** das Kontrollkästchen **Rootkit-Scanning aktivieren** aktiviert ist.
4. Aktivieren Sie das Kontrollkästchen **Verdächtige Elemente nach der vollständigen Überprüfung des Computers anzeigen**.
5. Überprüfen Sie, ob alle anderen Einstellungen auf dieser Seite für Ihr System geeignet sind. Nehmen Sie bei Bedarf Änderungen vor.
6. Öffnen Sie die Registerkarte **Operationen**, und klicken Sie auf die Schaltfläche **Nach Viren und Spyware scannen**.

   Hinweis: Zur Ausführung des Vorgangs müssen Sie die Richtlinie verteilen.

7. Klicken Sie auf , um die Richtlinie zu verteilen.

Nachdem der Scan-Vorgang auf den lokalen Hosts abgeschlossen ist, können Sie über **Scan-Berichte** auf der Registerkarte **Scan-Berichte** überprüfen, ob Rootkits erkannt wurden.

Konfigurieren des E-Mail-Scannings

Das E-Mail-Scanning schützt sowohl eingehende als auch ausgehende E-Mails wirkungsvoll vor Viren.

Wenn Sie die Funktion auch für ausgehende E-Mails aktivieren, stellen Sie sicher, dass Sie nicht versehentlich infizierte E-Mail-Anlagen versenden. In diesem Abschnitt werden die Einstellungen des E-Mail-Scannings erläutert. Außerdem finden Sie ein praktisches Konfigurationsbeispiel.

Beim E-Mail-Scanning wird der gesamte POP-, IMAP- und SMTP-Verkehr überprüft. Wenn das SSL-Protokoll benutzt wird, werden alle Dateianlagen, die über SSL empfangen werden, beim Speichern im lokalen E-Mail-Cache überprüft. Darüber hinaus werden alle ausgehenden Dateien vom Echtzeit-Scanning gescannt.

Einstellungen für das E-Mail-Scanning

Die Einstellungen für das E-Mail-Scanning werden auf der Seite **E-Mail-Scanning** der Registerkarte **Einstellungen** angezeigt.

Um die Überprüfung eingehender E-Mails und Anlagen (POP3-Verkehr) einzuschalten, aktivieren Sie das Kontrollkästchen **Scanning eingehender E-Mails aktivieren**.

Um die Überprüfung ausgehender E-Mails und Anlagen (SMTP-Verkehr) einzuschalten, aktivieren Sie das Kontrollkästchen **Scanning ausgehender E-Mails aktivieren**.

Sie können die Maßnahmen bestimmen, die ausgeführt werden sollen, wenn eine infizierte E-Mail-Nachricht erkannt wird.

- Überprüfung eingehender E-Mails:
  1. **Aktion bei infiziertem Dateianhang (Empfang)**:
     - **Anlage desinfizieren**. Wenn ein infizierter Dateianhang gefunden wird, wird der Desinfektions-Assistent gestartet.
     - **Anlage entfernen**. Die Anlage wird gelöscht.
     - **Nur Bericht**. Die infizierte Anlage wird ignoriert, aber der Vorfall wird dem Administrator gemeldet.
  2. **Aktion, wenn Scanning fehlschlägt**:
     - **Anlage entfernen**. Die Anlage wird gelöscht.
     - **Nur Bericht**. Die fehlgeschlagene Überprüfung wird ignoriert, aber der Vorfall wird dem Administrator gemeldet.
  3. **Aktion bei "malformed" Nachrichtenteilen**:
     - **Nachrichtenteil entfernen**. Die E-Mail wird gelöscht.
     - **Nur Bericht**. Der "malformed" Nachrichtenteil wird ignoriert, aber der Vorfall wird dem Administrator gemeldet.

- Überprüfung ausgehender E-Mails:
  1. **Aktion bei infiziertem Dateianhang (Senden)**:
     - **E-Mail blockieren**. Verhindert, dass die E-Mail gesendet wird.
     - **Nur Bericht**. Die infizierte Anlage wird ignoriert, aber der Vorfall wird dem Administrator gemeldet.
  2. **Aktion, wenn Scanning fehlschlägt**:
     - **E-Mail blockieren**. Verhindert, dass die E-Mail gesendet wird.
     - **Nur Bericht**. Die fehlgeschlagene Überprüfung wird ignoriert, aber der Vorfall wird dem Administrator gemeldet.

3. **Aktion bei "malformed" Nachrichtenteilen**:
   - **Nachrichtenteil entfernen**. Die E-Mail wird gelöscht.
   - **Nur Bericht**. Der "malformed" Nachrichtenteil wird ignoriert, aber der Vorfall wird dem Administrator gemeldet.

Vorsicht: Die Option **Nur Bericht** birgt einige Risiken und sollte während des Normalbetriebs nicht verwendet werden.

Damit blockierte E-Mails im **Postausgang** des Benutzers gespeichert werden, aktivieren Sie das Kontrollkästchen **Blockierte E-Mails im Postausgang speichern**. In diesem Fall können die betroffenen Benutzer erst wieder E-Mails versenden, wenn sie die infizierten E-Mails aus dem **Postausgang** gelöscht, in einen anderen Ordner verschoben oder geändert haben.

Welche Dateitypen beim E-Mail-Scanning berücksichtigt werden, hängt von den auf der Seite **Echtzeit-Scanning** vorgenommenen Einstellungen ab.

Wenn bei der Überprüfung großer Dateien ein Dialogfeld angezeigt werden soll, aktivieren Sie das Kontrollkästchen **Beim Scannen großer Dateien Verlaufsanzeige einblenden**, und legen Sie im Feld **Verlaufsanzeige anzeigen nach** ein geeignetes Zeitlimit fest.

Wenn nach Abschluss des Scan-Vorgangs ein Scan-Bericht angezeigt werden soll, aktivieren Sie das Kontrollkästchen **Bericht anzeigen, wenn Infektionen festgestellt wurden**.

Aktivieren des E-Mail-Scannings für eingehende und ausgehende E-Mails

In diesem Beispiel wird das E-Mail-Scanning für eingehende und ausgehende E-Mails aktiviert.

1. Wählen Sie auf der Registerkarte **Richtliniendomänen** den Eintrag **Stamm**.
2. Öffnen Sie die Registerkarte **Einstellungen**, und wählen Sie die Seite **E-Mail-Scanning** aus.
3. Überprüfung eingehender E-Mails konfigurieren:
   a) Wählen Sie **Überprüfung eingehender E-Mails aktivieren** aus.
   b) Wählen Sie in der Dropdown-Liste **Aktion bei infiziertem Dateianhang (Empfang)** aus, welche Maßnahme ausgeführt werden soll.
   c) Wählen Sie in der Dropdown-Liste **Aktion bei Scan-Fehler** aus, welche Maßnahme ausgeführt werden soll.
   d) Wählen Sie in der Dropdown-Liste **Aktion bei "malformed" Nachrichtenteilen** aus, welche Maßnahme ausgeführt werden soll.
4. Überprüfung ausgehender E-Mails konfigurieren:
   a) Wählen Sie**Überprüfung ausgehender E-Mails aktivieren**.
   b) Wählen Sie in der Dropdown-Liste **Aktion bei infiziertem Dateianhang (Senden)** aus, welche Maßnahme ausgeführt werden soll.
   c) Wählen Sie in der Dropdown-Liste **Aktion bei Scan-Fehler** aus, welche Maßnahme ausgeführt werden soll.
   d) Wählen Sie in der Dropdown-Liste **Aktion bei "malformed" Nachrichtenteilen** aus, welche Maßnahme ausgeführt werden soll.
5. Prüfen Sie die **Allgemeinen Einstellungen**.

   Überprüfen Sie, ob alle anderen Einstellungen auf dieser Seite für Ihr System geeignet sind. Nehmen Sie bei Bedarf Änderungen vor.
6. Klicken Sie auf , um die Richtlinie zu verteilen.

Konfigurieren von Web Traffic (HTTP) Scanning

Web Traffic Scanning schützt den Computer vor Viren, die über HTTP-Datenverkehr übertragen werden.

Wenn Web Traffic Scanning aktiviert ist, werden HTML-Dateien, Bilddateien, heruntergeladene Anwendungen oder ausführbare Dateien und andere heruntergeladene Dateien überprüft. Die Downloads werden automatisch von Viren bereinigt. Die Endbenutzer können benachrichtigt werden, sobald Web Traffic Scanning eine infizierte Datei im HTTP-Datenverkehr bzw. bei Downloads blockiert.

In diesem Abschnitt werden die Einstellungen für Web Traffic Scanning erläutert. Außerdem finden Sie hier einige praktische Konfigurationsbeispiele.

Einstellungen für das Web Traffic Scanning

Hier werden die Einstellungen für das HTTP-Scanning beschrieben, die auf der Seite **Einstellungen** > **Web Traffic Scanning** angezeigt werden.

Wählen Sie die Option **HTTP-Scanning aktivieren** aus, um das HTTP-Scanning zu aktivieren.

In der Dropdown-Liste **Maßnahme bei Infektion** können Sie die Maßnahme festlegen, die bei einer Infektion im HTTP-Datenverkehr durchgeführt werden soll. Folgende Maßnahmen stehen zur Auswahl:

- **Blockieren**. Der Zugriff auf die infizierte Datei wird blockiert.
- **Nur Bericht**. Die Infektion wird ignoriert, aber der Vorfall wird dem Administrator gemeldet.

In der Dropdown-Liste **Aktion bei Scan-Fehler** können Sie die Maßnahme festlegen, die durchgeführt werden soll, wenn eine Datei im HTTP-Datenverkehr nicht gescannt werden kann. Diese Einstellung gilt zum Beispiel für Archive mit Passwort-Schutz. Folgende Maßnahmen stehen zur Auswahl:

- **Blockieren**. Die nicht überprüfbare Datei wird blockiert.
- **Nur Bericht**. Die Datei wird ignoriert, aber der Vorfall wird dem Administrator gemeldet.

Aktivieren Sie das Kontrollkästchen **In komprimierten Dateien scannen**, um auch komprimierte `ZIP`-, `ARJ`-, `LZH`-, `RAR`-, `CAB`-, `TAR`-, `BZ2`-, `GZ`-, `JAR`- und `TGZ`-Dateien zu scannen.

In der Tabelle **Vertrauenswürdige Sites** können Sie eine Liste vertrauenswürdiger Sites festlegen. Der Inhalt dieser Sites wird nicht auf Viren gescannt.

Aktivieren von Web Traffic Scanning für die gesamte Domäne

In diesem Beispiel wird das HTTP-Scanning für die gesamte Domäne aktiviert.

1. Wählen Sie auf der Registerkarte **Richtliniendomänen** den Eintrag **Stamm**.
2. Öffnen Sie die Registerkarte **Einstellungen**, und wählen Sie die Seite **HTTP-Scanning** aus.
3. Aktivieren Sie das Kontrollkästchen **HTTP-Scanning aktivieren**.
4. Vergewissern Sie sich, dass **Aktion bei Infektion** auf **Blockieren** eingestellt ist.
5. Vergewissern Sie sich, dass **Aktion bei Scan-Fehler** auf **Blockieren** eingestellt ist.
6. Überprüfen Sie, ob alle anderen Einstellungen auf dieser Seite für Ihr System geeignet sind. Nehmen Sie bei Bedarf Änderungen vor.
7. Klicken Sie auf , um die Richtlinie zu verteilen.

Ausschließen einer Website vom Web Traffic Scanning

Bestimmte Websites oder Webseiten können Sie in der Tabelle der **Vertrauenswürdigen Sites** vom HTTP-Scanning ausschließen.

Ein solcher Ausschluss ist ratsam, wenn eine Site nicht identifizierbare Streaming-Inhalte enthält, die zu ungewünschten Verzögerungen führen können (siehe Zeitüberschreitung beim Download).

Im folgenden Konfigurationsbeispiel werden eine vollständige Domäne (www.beispiel.com) sowie ein Unterverzeichnis einer anderen Domäne (www.beispiel2.com/news) vom HTTP-Scanning ausgeschlossen.

1. Wählen Sie auf der Registerkarte **Richtliniendomänen** den Eintrag **Stamm**.
2. Öffnen Sie die Registerkarte **Einstellungen**, und wählen Sie die Seite **Web Traffic Scanning** aus.
3. Ausschließen einer Domäne vom HTTP-Scanning:

   Wenn Sie eine vollständige Domäne vom HTTP-Scanning ausschließen möchten, geben Sie die URL der Domäne wie folgt in die Tabelle der **Vertrauenswürdigen Sites** ein:

   a) Klicken Sie unter der Tabelle **Vertrauenswürdige Sites** auf **Hinzufügen**.
   Dadurch wird der Tabelle eine neue Zeile hinzugefügt.
   b) Klicken Sie auf die neu erstellte Zeile, um sie zu aktivieren, und geben Sie `http://*.beispiel.com/*` ein.
   Dadurch werden alle Unterdomänen der Domäne vom Scanning ausgeschlossen.
   c) Klicken Sie unter der Tabelle **Vertrauenswürdige Sites** auf **Hinzufügen**.
   In dieTabelle wird eine weitere neue Zeile eingefügt.
   d) Klicken Sie auf die neu erstellte Zeile, um sie zu aktivieren, und geben Sie `http://beispiel.com/*` ein.
   Dadurch wird die Unterdomäne der zweiten Ebene vom Scanning ausgeschlossen.
4. Ausschließen eines Unterverzeichnisses vom HTTP-Scanning:

   Wenn Sie ein Unterverzeichnis vom HTTP-Scanning ausschließen möchten, geben Sie in die Tabelle der **Vertrauenswürdigen Sites** die URL der Domäne mit dem Verzeichnispfad ein. Gehen Sie dazu wie folgt vor:

   a) Klicken Sie unter der Tabelle **Vertrauenswürdige Sites** auf **Hinzufügen**.
   Dadurch wird der Tabelle eine neue Zeile hinzugefügt.
   b) Klicken Sie auf die neu erstellte Zeile, um sie zu aktivieren, und geben Sie `http://www.beispiel2.com/news/*` ein.
5. Klicken Sie auf , um die Richtlinie zu verteilen.

Konfigurieren des Spyware-Scannings

Spyware-Scanning schützt die Hosts vor verschiedenen Spyware-Typen wie Data Miner, Überwachungstools und Dialer.

Im zentral verwalteten Modus kann Spyware-Scanning z.B. so konfiguriert werden, dass alle auf den Hosts festgestellten Spyware-Elemente dem Administrator gemeldet oder automatisch unter Quarantäne gestellt werden. Bestimmte Spyware-Anwendungen können auch auf der Seite **Spyware-Steuerung** zugelassen werden.

Hinweis zum Säubern von Spyware und Riskware

Spyware befindet sich im Graubereich zwischen legitimer Anwendung und einem Virus oder Trojaner. Einige Spyware-Anwendungen werden sogar von regulären Anwendungen benötigt. Beim größten Teil der Spyware handelt es sich allerdings um Malware, die keinesfalls ausgeführt werden sollte. In der Standardeinstellung lässt das Spyware-Scanning die Ausführung jeder Spyware zu. Bevor Sie die Sicherheitsregeln enger definieren und jegliche neue Spyware an der Ausführung hindern, sollten Sie überprüfen, ob Sie die Ausführung bestimmter Spyware-Anwendungen in Ihrem Netzwerk zulassen sollten.

Beim Spyware-Scanning wird auch Riskware erkannt und gemeldet. Riskware ist jedes Programm, das zwar nicht absichtlich Schäden verursacht, jedoch bei falscher Anwendung, insbesondere bei nicht korrekter

Einrichtung, gefährlich sein kann. Beispiele für solche Programme sind Chat-Programme (IRC) oder Programme zur Übertragung von Dateien zwischen Computern.

Einstellungen der Spyware-Steuerung

Hier werden die Einstellungen für das Spyware-Scanning beschrieben.

Das Spyware-Scanning wird als Teil des Echtzeit-Scannings und des manuellen Scannings ausgeführt. Wenn auf der Seite **Echtzeit-Scanning** die Option **Echtzeit-Scanning aktiviert** ausgewählt wird, wird das Spyware-Scanning ebenfalls aktiviert. Gleichermaßen wird Spyware automatisch berücksichtigt, wenn ein manuelles Scanning ausgeführt wird. Welche Maßnahme ausgeführt werden soll, wenn Spyware erkannt wird, wird durch die Einstellung auf den Seiten **Echtzeit-Scanning** und **Manuelles Scanning** bestimmt.

In der Tabelle **Vom Spyware-Scanning ausgeschlossene Anwendungen** sind die Spyware- und Riskware-Elemente aufgeführt, die vom Administrator zugelassen wurden.

Die Tabelle **Von Hosts gemeldete Spyware und Riskware** enthält folgende Informationen:

Von Hosts gemeldete Spyware und Riskware	
Spyware- oder Riskware-Name	Der Name des Spyware- oder Riskware-Objekts.
Typ	Der Typ des Spyware-Elements. Bei Spyware kann es sich um Adware, Data Miner, Dialer, Malware, Überwachungstools, Dialer für pornografisches Material, Riskware, Sicherheitslücken, Würmer, Cookies (Tracking Cookies) oder Sonstiges handeln.
Schweregrad	Der Schweregrad des Spyware-Elements – ein Wert zwischen 3 und 10.
Host	Der Name des Hosts, auf dem die Spyware festgestellt wurde.
Spyware-Status	Der aktuelle Status des Spyware-Elements wie folgt: **Potenziell aktiv** – Möglicherweise ist das Spyware-Element noch auf dem Host aktiv. Auf dem Host wurden keine Maßnahmen gegen diese Spyware ergriffen. **Entfernt** – Das Spyware-Element wurde vom Host entfernt. **In Quarantäne** – Das Spyware-Element wurde auf dem Host unter Quarantäne gestellt. **Derzeit unter Quarantäne gestellt** – Das Spyware-Element befindet sich auf dem Host zurzeit unter Quarantäne.
Zeitstempel	Das Datum und die Uhrzeit, zu der das Spyware-Element auf dem Host festgestellt wurde.

Die von den Hosts gemeldete Spyware wird bei einem manuellen Scan-Vorgang wie auch bei der regelmäßigen Entfernung der unter Quarantäne gestellten Spyware automatisch gelöscht.

Einrichten der Spyware-Steuerung für die gesamte Domäne

Dieses Beispiel veranschaulicht, wie eine für die Endbenutzer transparente Spyware-Steuerung eingerichtet wird, die die Benutzer vor Spyware und Tracking Cookies schützt.

Wenn Sie noch wenig Erfahrung mit der Spyware-Steuerung haben, sollten Sie sie zunächst in einer kleinen Testumgebung einrichten. Diese Umgebung sollte aus Hosts bestehen, auf denen die in Ihrem Unternehmen üblichen Anwendungen installiert sind. In dieser Testphase können Sie bei Bedarf auch bestimmte Spyware-Anwendungen zulassen. Nach einer erfolgreichen Durchführung der Testphase können Sie die Richtlinie an die gesamte verwaltete Domäne verteilen.

Mithilfe der Spyware-Steuerung wird auch Riskware erkannt. Riskware ist jedes Programm, das zwar nicht absichtlich Schäden verursacht, jedoch bei falscher Anwendung, insbesondere bei nicht korrekter Einrichtung, gefährlich sein kann. Beispiele für solche Programme sind Chat-Programme (IRC) oder Programme zur Übertragung von Dateien zwischen Computern. Wenn Sie die Verwendung dieser Programme in einer verwalteten Domäne zulassen möchten, sollten Sie diese in die Testumgebung integrieren und ihre Verwendung zulassen, wenn Sie Regeln für die Anwendungen in der Tabelle **Von Hosts gemeldete Spyware und Riskware** überprüfen und konfigurieren.

1. Erstellen einer Testdomäne und Aktivieren des Spyware-Scannings:
   a) Erstellen Sie eine Testumgebung mit nur wenigen Computern, auf denen die normalerweise im Unternehmen eingesetzten Programme installiert sind.
   b) Importieren Sie diese Hosts in die zentral verwaltete Domäne.
   c) Öffnen Sie die Registerkarte **Einstellungen**, und wählen Sie die Seite **Real-time scanning**.
   d) Stellen Sie sicher, dass das Kontrollkästchen **Echtzeit-Scanning aktiviert** aktiviert ist.

      Alternativ können Sie die Hosts auch manuell nach Spyware scannen.

   e) Klicken Sie auf , um die Richtline zu speichern und zu verteilen.
2. Überprüfen der gemeldeten Spyware und Riskware:

   In der Tabelle **Von Hosts gemeldete Spyware und Riskware** werden die während des Scan-Vorgangs festgestellten Spyware- und Riskware-Anwendungen aufgeführt. Diese Tabelle wird auf der Seite **Spyware-Steuerung** angezeigt.
   a) Überprüfen Sie die Liste der gemeldeten Spyware und Riskware.
   b) Falls die Liste Anwendungen aufführt, die in Ihrem Unternehmen benötigt werden, wählen Sie die betreffende Anwendung aus, und klicken Sie auf **Anwendung ausschließen**.
      Ein Bestätigungsdialogfeld wird geöffnet.
   c) Lesen Sie die Informationen in diesem Dialogfeld und klicken Sie auf **OK**, wenn Sie sicher sind, dass Sie die Spyware oder Riskware auf dem Host oder in der Domäne zulassen möchten..
      Die ausgewählte Anwendung wird in die Tabelle **Vom Spyware-Scanning ausgeschlossene Anwendungen** verschoben.
3. Wenn Sie auf jeden Fall verhindern möchten, dass Benutzer Spyware oder Riskware auf ihren Computern selbst zulassen, wählen Sie unter **Zulassen von Spyware durch Benutzer ermöglichen** die Option **Nicht zugelassen** aus.
4. Überprüfen Sie, ob die Einstellungen für das manuelle Scanning für die verwaltete Domäne korrekt sind.
5. Klicken Sie auf , um die Richtlinie zu verteilen.

Ausführen des Spyware-Scannings in der gesamten Domäne

In diesem Beispiel wird veranschaulicht, wie ein manueller Scan-Vorgang für die gesamte Domäne ausgeführt wird.

Hierbei wird die Tabelle **Von Hosts gemeldete Spyware und Riskware** zum Teil entfernt.

1. Wählen Sie auf der Registerkarte **Richtliniendomänen** den Eintrag **Stamm**.

2. Da beim manuellen Scanning auch Viren gesucht werden, sollten Sie die Einstellungen auf der Seite **Manuelles Scanning** überprüfen und bei Bedarf anpassen.
3. Öffnen Sie die Registerkarte **Operationen**, und klicken Sie auf die Schaltfläche **Nach Viren und Spyware scannen**.

   Hinweis: Zur Ausführung des Vorgangs müssen Sie die Richtlinie verteilen.

4. Klicken Sie auf , um die Richtlinie zu verteilen.

Zulassen eines Spyware- oder Riskware-Elements

In diesem Beispiel wird die Verwendung eines Spyware- oder Riskware-Elements, das beim Spyware-Scanning erkannt wurde, für einen Host zugelassen.

1. Wählen Sie auf der Registerkarte **Richtliniendomänen** den Host aus, für den die Verwendung von Spyware oder Riskware zugelassen werden soll.
2. Öffnen Sie die Registerkarte **Einstellungen**, und wählen Sie die Seite **Spyware-Steuerung** aus.
3. Wählen Sie in der Tabelle **Von Hosts gemeldete Spyware und Riskware** das Spyware-Element aus, das zugelassen werden soll, und klicken Sie auf **Anwendung ausschließen**.
   Es wird ein Dialogfeld geöffnet, in dem Sie dazu aufgefordert werden, den Vorgang zu bestätigen.
4. Lesen Sie die Informationen in diesem Dialogfeld, und klicken Sie auf **OK**, wenn Sie sicher sind, dass Sie die Ausführung der Anwendung auf dem Host oder in der Domäne zulassen möchten.
   Die ausgewählte Anwendung wird in die Tabelle **Vom Spyware-Scanning ausgeschlossene Anwendungen** verschoben.
5. Klicken Sie auf , um die Richtlinie zu verteilen.

Verwalten unter Quarantäne gestellter Objekte

Mithilfe der Quarantäne-Verwaltung können Sie Objekte zentral verarbeiten, die auf Hostcomputern unter Quarantäne gestellt wurden.

Alle infizierten Dateien sowie Spyware oder Riskware, die auf Hostcomputern unter Quarantäne gestellt wurden, werden auf der Seite **Einstellungen** > **Quarantäne-Verwaltung** angezeigt. Hier können Sie entweder die Quarantäne für diese Objekte aufheben oder die Objekte löschen.

Hinweis: Die Quarantäne-Verwaltung sollte vor allem zur Problembehandlung eingesetzt werden. Wird zum Beispiel eine geschäftskritische Anwendung als Riskware eingestuft, die noch nicht in der Virendefinitionsdatenbank enthalten ist, können Sie mithilfe der Quarantäne-Verwaltung die Verwendung der Anwendung zulassen. Solche Fälle sind verhältnismäßig selten, und sobald neue Virendefinitions-Updates verfügbar sind, in denen die Anwendung als normal eingestuft wird, sollte das Problem automatisch behoben werden.

Löschen von Objekten, die unter Quarantäne stehen

Infizierte Dateien, Spyware oder Riskware, die auf Hosts unter Quarantäne gestellt wurden, können aus der Quarantäne entfernt werden. Dadurch werden sie vom Hostcomputer gelöscht.

1. Wählen Sie die Zieldomäne.
2. Öffnen Sie die Registerkarte **Einstellungen**, und wählen Sie die Seite **Quarantäne-Verwaltung**.
3. Wählen Sie in der Tabelle **Unter Quarantäne stehende Objekte** das zu löschende Objekt aus, und klicken Sie auf **Löschen**.
   Das Objekt wird in die Tabelle **Maßnahmen für unter Quarantäne stehende Objekte** verschoben, wobei **Löschen** als **Maßnahme** angegeben ist.

4. Klicken Sie auf , um die Richtlinie zu verteilen.

Wiederherstellen von Objekten aus der Quarantäne

Infizierte Dateien, Spyware oder Riskware, die auf Hosts unter Quarantäne gestellt wurden, können aus der Quarantäne wiederhergestellt werden. Sie werden dann auf den Hostcomputern zugelassen, sodass sie wie gewohnt ausgeführt werden können.

1. Wählen Sie die Zieldomäne.
2. Erstellen Sie eine Ausnahmeregel für das Objekt.

   Mithilfe von Ausnahmeregeln wird sichergestellt, dass das Objekt künftig nicht wieder unter Quarantäne gestellt wird. Wenn das Objekt als Virus oder infizierte Datei aufgelistet wird, gehen Sie wie folgt vor:

   a) Öffnen Sie die Seite **Einstellungen** > **Quarantäne-Verwaltung**, und kopieren Sie den Dateipfad des Objekts.
   b) Öffnen Sie die Seite **Einstellungen** > **Echtzeit-Scanning**.
   c) Klicken Sie mit der rechten Maustaste auf **Ausgeschlossene Objekte aktivieren**, und wählen Sie im Kontextmenü die Option **In den erweiterten Modus wechseln** aus.
   Daraufhin wird die Benutzeroberfläche des **Erweiterten Modus** angezeigt.
   d) Wählen Sie auf der Registerkarte **Richtlinie** die Option **Ausgeschlossene Objekte** aus.
   e) Klicken Sie auf **Hinzufügen**, und geben Sie den Dateipfad des unter Quarantäne stehenden Objekts ein.
   f) Wählen Sie die Menüoption **Ansicht** > **Anti-Virus-Modus** aus, um zur Benutzeroberfläche des **Anti-Virus-Modus** zurückzukehren. Stellen Sie sicher, dass auf der Seite **Einstellungen** > **Echtzeit-Scanning** das Kontrollkästchen **Ausgeschlossene Objekte aktivieren** aktiviert ist.

   Gehen Sie wie folgt vor, falls das Objekt als Spyware oder Riskware eingestuft wurde:

   a) Öffnen Sie die Seite **Einstellungen** > **Spyware-Steuerung**.
   b) Wählen Sie in der Tabelle **Von Hosts gemeldete Spyware und Riskware** das Objekt aus, das zugelassen werden soll, und klicken Sie auf **Anwendung ausschließen**.
   Es wird ein Dialogfeld geöffnet, in dem Sie dazu aufgefordert werden, den Vorgang zu bestätigen. Anschließend wird die ausgewählte Anwendung in die Tabelle **Vom Spyware-Scanning ausgeschlossene Anwendungen** verschoben.
3. Öffnen Sie die Registerkarte **Einstellungen**, und wählen Sie die Seite **Quarantäne-Verwaltung**.
4. Wählen Sie in der Tabelle **Objekte unter Quarantäne** das unter Quarantäne stehende Objekt aus, das zugelassen werden soll, und klicken Sie auf **Freigeben**.
   Das Objekt wird in die Tabelle **Maßnahmen für unter Quarantäne stehende Objekte** verschoben, wobei **Freigeben** als **Maßnahme** für das Objekt angegeben ist.
5. Klicken Sie auf , um die Richtlinie zu verteilen.

Verhindern, dass Benutzer Einstellungen eigenmächtig ändern

Wenn Sie sichergehen möchten, dass die Benutzer einige oder alle Virenschutzeinstellungen nicht ändern können, legen Sie die entsprechenden Einstellungen als endgültig fest.

Dabei können Sie folgendermaßen vorgehen:

- Wenn Sie verhindern möchten, dass Benutzer eine bestimmte Einstellung ändern können, klicken Sie auf das Schlosssymbol neben der betreffenden Einstellung.
- Wenn Sie sich auf einer der Seiten auf der Registerkarte **Einstellungen** befinden, können Sie alle Einstellungen gleichzeitig als endgültig definieren. Klicken Sie dazu auf **Änderungen durch Benutzer nicht zulassen**. Diese seitenspezifische Verknüpfung betrifft nur die Einstellungen mit einem Schlosssymbol. Es werden alle Schlosssymbole auf der Seite gleichzeitig aktiviert oder deaktiviert.

- Wenn Sie alle Einstellungen für den Virenschutz und für Internet Shield als endgültig definieren möchten, öffnen Sie die Seite **Zentrale Verwaltung** der Registerkarte **Einstellungen**, und klicken Sie auf **Benutzer dürfen keine Einstellungen ändern**. Hierdurch werden auch die Einstellungen des **Erweiterten Modus** als endgültig definiert.

Alle Virenschutz-Einstellungen als endgültig definieren

In diesem Beispiel wird veranschaulicht, wie alle Virenschutz-Einstellungen als endgülstig definiert werden.

1. Wählen Sie auf der Registerkarte **Richtliniendomänen** den Eintrag **Stamm**.
2. Öffnen Sie die Registerkarte **Einstellungen**, und wählen Sie die Seite **Automatische Updates**.
3. Überprüfen Sie, ob alle Einstellungen auf dieser Seite Ihren Vorstellungen entsprechen.
4. Klicken Sie auf **Änderungen durch Benutzer nicht zulassen**.
   Alle Einstellungen auf dieser Seite sind nun als "endgültig" markiert.
5. Wählen Sie die Seite **Echtzeit-Scanning** aus.
6. Überprüfen Sie, ob alle Einstellungen auf dieser Seite Ihren Vorstellungen entsprechen.
7. Klicken Sie auf **Änderungen durch Benutzer nicht zulassen**.
8. Wählen Sie die Seite **Manuelles Scanning** aus.
9. Überprüfen Sie, ob alle Einstellungen auf dieser Seite Ihren Vorstellungen entsprechen.
10. Klicken Sie auf **Änderungen durch Benutzer nicht zulassen**.
11. Wählen Sie die Seite **E-Mail-Scanning** aus.
12. Überprüfen Sie, ob alle Einstellungen auf dieser Seite Ihren Vorstellungen entsprechen.
13. Klicken Sie auf **Änderungen durch Benutzer nicht zulassen**.
14. Klicken Sie auf , um die Richtlinie zu verteilen.

Konfigurieren der Alarmmeldungen

In diesem Abschnitt wird beschrieben, wie das Produkt konfiguriert werden muss, um Client Security-Virenbenachrichtigungen an eine E-Mail-Adresse zu senden, und wie Alarm-Popups deaktiviert werden können.

Es wird empfohlen, alle Virenbenachrichtigungen per E-Mail an die Administratoren zu senden, um sicherzustellen, dass sie so schnell wie möglich über potenzielle Virenausbrüche informiert werden.

Einrichten der Weiterleitung von Client Security-Virenbenachrichtigungen an eine E-Mail-Adresse

In diesem Beispiel werden alle Sicherheitswarnungen, die von den verwalteten Client Security-Clients generiert werden, an eine E-Mail-Adresse weitergeleitet.

1. Wählen Sie auf der Registerkarte **Richtliniendomänen** den Eintrag **Stamm**.
2. Öffnen Sie die Registerkarte **Einstellungen**, und wählen Sie die Seite **Versendung von Alarmen**.
3. Einrichten der **Sendeoptionen für Alarmmeldungen**:
   Wenn Sie die Versendung von Alarmmeldungen per E-Mail zum ersten Mal einrichten, gehen Sie wie folgt vor:
   a) Geben Sie in das Feld **Adresse des E-Mail-Servers (SMTP)** die Adresse des SMTP-Servers ein.
      Verwenden Sie dabei das folgende Format:
      `<Host>[:<Port>]`. Dabei steht `Host` für den DNS-Namen oder die IP-Adresse des SMTP-Servers und `Port` für die Port-Nummer auf dem SMTP-Server.

b) Geben Sie in das Feld **Adresse des E-Mail-Absenders (Von)** die Absenderadresse für die Alarmmeldung ein.
c) Geben Sie in das Feld **E-Mail-Betreffzeile** den Betreff der Alarmmeldung ein.

   Eine Liste der möglichen Parameter, die im Betreff verwendet werden können, finden Sie in der Online-Hilfe zu MIB.

4. Einrichten der **Alarm-Weiterleitung**:

   Mithilfe der Tabelle **Alarm-Weiterleitung** können Sie festlegen, an welche Adresse die verschiedenen Alarmmeldungen weitergeleitet werden.

   a) Aktivieren Sie in der Zeile **Sicherheitsalarm** das Kontrollkästchen **E-Mail**.
   Daraufhin wird das Dialogfeld **Adressen der E-Mail-Empfänger (An)** geöffnet.
   b) Aktivieren Sie das Kontrollkästchen **Dieselbe Adresse für alle Produkte verwenden**, und geben Sie die E-Mail-Adresse in das daraufhin aktivierte Textfeld ein.

   Wenn die Alarmmeldungen an mehrere E-Mail-Adressen gesendet werden sollen, trennen Sie diese durch Kommata.

   c) Klicken Sie abschließend auf **OK**.

5. Klicken Sie auf , um die Richtlinie zu verteilen.

Deaktivieren der Alarm-Popups von Client Security

In diesem Beispiel wird die Alarmausgabe von Client Security so konfiguriert, dass bei einem Vorfall keine Alarm-Popups auf den Computern der Benutzer angezeigt werden

1. Wählen Sie auf der Registerkarte **Richtliniendomänen** den Eintrag **Stamm**.
2. Öffnen Sie die Registerkarte **Einstellungen**, und wählen Sie die Seite **Versendung von Alarmen**.
3. Deaktivieren Sie in der Spalte **Lokale Benutzeroberfläche** die Kontrollkästchen für alle Produkte.
4. Klicken Sie auf , um die Richtlinie zu verteilen.

Überwachen der Virenvorfälle im Netzwerk

Policy Manager bietet verschiedene Methoden und Detailstufen für die Überwachung von Infektionen in Ihrem Netzwerk.

Wenn Sie überwachen möchten, ob sich Viren im Netzwerk befinden, überprüfen Sie am besten den Abschnitt **Virenschutz** auf der Registerkarte **Zusammenfassung**. Dort werden alle neuen Infektionen angezeigt. Wenn Sie ausführlichere Informationen zu diesen Viren anzeigen möchten, klicken Sie auf **Infektionsstatus der Hosts anzeigen**. Daraufhin wird die Registerkarte **Status** mit der Seite **Virenschutz** geöffnet, auf der Details zur Infektion auf den Hosts angezeigt werden.

Darüber hinaus können Sie die Registerkarten **Warnungen** und **Scan-Berichte** prüfen, um die Scan-Berichte der unterschiedlichen Hosts einzusehen.

Überprüfen der Virenschutzfunktionen

Zur Überprüfung der Funktion von Client Security können Sie eine spezielle Testdatei verwenden, die von Client Security als Virus identifiziert und behandelt wird.

Diese Datei, die als Standard-Anti-Virus-Testdatei EICAR bekannt ist, wird auch von einigen anderen Anti-Virus-Programmen erkannt. Die EICAR-Testdatei eignet sich auch zum Testen des E-Mail-Scannings. EICAR ist die Abkürzung für das Europäische Institut für Computer-Anti-Virus-Forschung (European Institute

of Computer Anti-Virus Research). Sie finden die EICAR-Infoseite unter *http://www.europe.f-secure.com/virus-info/eicar_test_file.shtml*.

Gehen Sie folgendermaßen vor, um die Virenschutzfunktionen zu testen:

1. Sie können die `EICAR`-Testdatei unter folgender Adresse herunterladen: *http://www.europe.f-secure.com/virus-info/eicar_test_file.shtml*.

   Wahlweise können Sie die Datei mit einem beliebigen Texteditor selbst erstellen. Die Datei enthält lediglich folgende Zeile:

   `X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*`

2. Speichern Sie die Datei unter einem beliebigen Namen mit einer `COM`-Erweiterung, zum Beispiel `EICAR.COM`.

   Verwenden Sie dabei das ASCII-Format, das Standardformat für MS-DOS. Achten Sie auch darauf, dass das dritte Zeichen der Erweiterung ein großes O ist und keine Null (0).

3. Jetzt können Sie anhand dieser Datei testen, was geschieht, wenn Client Security einen Virus erkennt.

   Normalerweise ist die Datei kein Virus. Erfolgt eine Ausführung ohne Virenschutz, zeigt `EICAR.COM` den Text an`EICAR-STANDARD-ANTIVIRUS-TEST-FILE!`und wird beendet.

Kapitel

6

Konfigurieren von Internet Shield

Themen:

- *Globale Firewall-Sicherheitsstufen*
- *Designgrundlagen für die Sicherheitsstufe*
- *Konfigurieren von Sicherheitsstufen und Regeln*
- *Konfigurieren der Netzwerk-Quarantäne*
- *Konfigurieren von Warnmeldungen nach Regelverletzungen*
- *Konfigurieren der Anwendungssteuerung*
- *Verwenden von Alarmen zum Prüfen der Funktionsweise von Internet Shield*
- *Konfigurieren der Intrusion Prevention*

In diesem Abschnitt erhalten Sie einen Überblick über Internet Shield sowie Informationen, wie Sie das Programm für Ihr spezifisches Netzwerk konfigurieren können.

Internet Shield schützt die Computer vor unbefugten Zugriffen aus dem Internet und vor Angriffen, die ihren Ursprung innerhalb des LANs haben.

Internet Shield bietet Schutz gegen Informationsdiebstahl, da unbefugte Zugriffsversuche verhindert und rechtzeitig erkannt werden. Das Programm schützt Benutzer außerdem vor böswilligen Anwendungen. Es stellt Möglichkeiten zur Kontrolle der Netzwerknutzung bereit und verhindert den Einsatz von Anwendungen, die zu viel Bandbreite belegen.

Internet-Schutzschild enthält auch eine Firewall-Komponente, die es möglich macht, den Datenverkehr anhand der verwendeten Protokolle einzuschränken. Die Anwendungssteuerung verhindert, dass böswillige Programme Informationen aus dem Computer an Dritte senden. Sie bietet Möglichkeiten, um den Datenverkehr basierend auf den verwendeten Anwendungen, IP-Adressen und Ports weiter einzuschränken. Das Intrusion Prevention-System stoppt böswillige Datenpakete, die Ports auf dem Host öffnen sollen.

Internet Shield enthält sieben vordefinierte Sicherheitsstufen. Jede Stufe ist mit einem Satz vordefinierter Firewall-Regeln ausgestattet. Es ist möglich, verschiedenen Benutzern unterschiedliche Sicherheitsstufen zuzuordnen. Als Grundlage können dabei die Sicherheitsrichtlinie des Unternehmens, die Mobilität des Benutzers sowie der Standort und die Erfahrung des Benutzers herangezogen werden.

Globale Firewall-Sicherheitsstufen

Sollte keine Anpassung der Firewall-Einstellungen für Ihr Netzwerk erforderlich sein, stehen Ihnen mehrere vorkonfigurierte Sicherheitsstufen zur Auswahl.

Folgende Sicherheitsstufen in Internet Shield sind global:

Netzwerk-Quarantäne	Wenn die Netzwerk-Quarantäne aktiviert ist und die Kriterien für die Netzwerk-Quarantäne auf dem Host erfüllt sind, wird diese Sicherheitsstufe automatisch ausgewählt. Diese Sicherheitsstufe ermöglicht das Herunterladen automatischer Updates sowie Verbindungen mit Policy Manager Server.
Alle blockieren	Bei Aktivierung dieser Sicherheitsstufe wird der gesamte Netzwerkdatenverkehr blockiert.
Mobil	Bei dieser Sicherheitsstufe sind normales Web-Browsing, Dateiübertragung (HTTP, HTTPS, FTP) sowie E-Mail- und Usenet-Datenverkehr möglich. Verschlüsselungsprogramme, wie VPN und SSH, sind ebenfalls erlaubt. Alle anderen Einsatzbereiche sind gesperrt, und bei eingehendem TCP-Datenverkehr wird eine Warnmeldung erzeugt. Nach dem Erkennen von schädlichen Datenpaketen können lokale Regeln hinzugefügt werden.
Start	Diese Sicherheitsstufe lässt den gesamten ausgehenden TCP-Datenverkehr und das Herunterladen von Dateien über FTP zu. Alle anderen Einsatzbereiche sind gesperrt, und bei eingehendem TCP-Datenverkehr wird eine Warnmeldung erzeugt. Um eine weitere Netzwerkfunktionalität zu aktivieren, können lokale Regeln hinzugefügt werden.
Büro	Diese Sicherheitsstufe lässt den gesamten ausgehenden TCP-Datenverkehr und das Herunterladen von Dateien über FTP zu. Alles andere wird standardmäßig gesperrt, und nur bei böswilligen Verbindungsversuche werden Warnmeldungen erzeugt. Um eine weitere Netzwerkfunktionalität zu aktivieren, können lokale Regeln hinzugefügt werden.
Streng	Diese Sicherheitsstufe lässt ausgehendes Web-Browsing, E-Mail- und Usenet-Verkehr, die verschlüsselte Datenkommunikation, FTP-Dateiübertragungen und Updates von einem entfernten Standort zu. Alles andere wird standardmäßig gesperrt, und bei eingehenden schädlichen Datenpakete sowie TCP-Verbindungsversuchen werden Warnmeldungen erzeugt.

Normal	Diese Sicherheitsstufe lässt den gesamten ausgehenden Datenverkehr zu, sperrt jedoch spezielle eingehende Dienste. Auch in diesem Fall können mithilfe der Anwendungssteuerung Regeln hinzugefügt werden, sodass die meisten Netzwerkanwendungen ordnungsgemäß funktionieren, sofern sie zugelassen sind.
Deaktiviert	Bei dieser Sicherheitsstufe ist der gesamte eingehende und ausgehende Datenverkehr zugelassen. Es werden keine Warnmeldungen erzeugt. Lokale Regeln können nicht erstellt werden.

Designgrundlagen für die Sicherheitsstufe

Hier werden die hinter den Sicherheitsstufen stehenden Designgrundlagen erläutert.

Jede Sicherheitsstufe hat mehrere vorkonfigurierte Firewall-Regeln. Darüber hinaus können Sie für alle Sicherheitsstufen, für die in der Tabelle **Firewall-Sicherheitsstufen** als **Filtermodus** > **Normal** erscheint, neue Regeln erstellen. Die Regeln in der **Firewall-Sicherheitsstufen-Tabelle** werden von oben nach unten gelesen.

Wenn Sie neue Sicherheitsstufen erstellen, sollten Sie den folgenden wesentlichen Grundsatz für die Definition von Firewall-Regeln beachten:

- Lassen Sie nur die benötigten Dienste zu und lehnen Sie alles andere ab. Auf diese Weise lässt sich das Sicherheitsrisiko auf ein Minimum beschränken. Der Nachteil besteht darin, dass die Firewall immer dann neu konfiguriert werden muss, wenn ein neuer Dienst benötigt wird. Das ist jedoch ein geringer Preis für die erhöhte Sicherheit.

Das entgegengesetzte Konzept, gefährliche Dienste ablehnen und alle anderen Dienste zulassen, ist nicht annehmbar, da niemand mit Gewissheit sagen kann, welche Dienste gefährlich sind oder in Zukunft eine Gefahr darstellen könnten, wenn ein neues Sicherheitsproblem erkannt wird.

Eine gute Sicherheitsstufe könnte wie folgt aussehen:

1. Regeln zum Ablehnen der gefährlichsten Dienste oder Hosts, wahlweise mit Alarmausgabe.
2. Regeln zum Zulassen häufig verwendeter, allgemeiner Dienste und Hosts.
3. Regeln zum Ablehnen bestimmter Dienste mit Alarmausgabe (z. B. Port-Abfragen durch Trojaner).
4. Allgemeine Regeln zum Zulassen von Diensten.
5. Alle anderen Dienste sperren.

Konfigurieren von Sicherheitsstufen und Regeln

In diesem Abschnitt erfahren Sie, wie Sie Sicherheitsstufen anhand der Benutzeranforderungen festlegen und auswählen können.

In den praktischen Konfigurationsbeispielen gehen wir davon aus, dass die verwalteten Hosts in eine Domänenstruktur importiert wurden, wo sich Laptops und Desktop-PCs in ihren eigenen Subdomänen befinden.

Wenn Sie eine bestimmte Sicherheitsstufe für eine Domäne aktivieren, sollten Sie überprüfen, ob sich die Sicherheitsstufe für diese Domäne eignet. Für verschiedene Domänen können unterschiedliche Sicherheitsstufen aktiviert werden.

Wichtig: Wenn Sie die Sicherheitsstufe auf einem Host ändern, klicken Sie anschließend auf das Schlosssymbol neben der Einstellung, um sicherzustellen, dass die neue Sicherheitsstufe übernommen wird.

Wählen Sie einer aktive Sicherheitsstufe für eine Workstation

In diesem Beispiel wird die Sicherheitsstufe **Büro** als aktive Sicherheitsstufe für die Arbeitsstationen in der Subdomäne `Desktops/Eng.` festgelegt.

Gehen Sie wie folgt vor, um die Sicherheitsstufe für Internet Shield für die Subdomäne `Desktops/Eng.` zu ändern:

1. Wählen Sie auf der Registerkarte **Richtliniendomänen**die Subdomäne **Desktops/Eng.**.
2. Öffnen Sie die Registerkarte **Einstellungen** und wählen Sie dort die Seite **Sicherheitsstufen für die Firewall**.
   In der Dropdown-Liste **Sicherheitsstufe für Internet Shield auf dem Host** wird die zurzeit in der Richtlinie enthaltene Standard-Sicherheitsstufe angezeigt.
3. Wählen Sie aus der Dropdown-Liste **Sicherheitsstufe für Internet Shield auf dem Host** die Sicherheitsstufe **Büro**.
4. Wenn Benutzer nicht in der Lage sein sollen, die Einstellungen zu ändern, klicken Sie auf das daneben stehende Schlosssymbol.
5. Klicken Sie auf , um die Richtlinie zu verteilen.

Sie können überprüfen, ob die ausgewählte Sicherheitsstufe aktiviert wurde. Öffnen Sie dazu die Registerkarte **Status** und wählen Sie die Seite **Allgemeiner Schutz**.

Hinweis: Wenn die ausgewählte Sicherheitsstufe aus irgendeinem Grund nicht verwendet werden kann, wird stattdessen die Standard-Sicherheitsstufe aktiviert. Angaben zur aktuellen Standard-Sicherheitsstufe finden Sie in der Tabelle **Global security levels** auf der Seite **Firewall-Sicherheitsstufen**.

Konfigurieren einer Standard-Sicherheitsstufe für die verwalteten Hosts

Bei der Standard-Sicherheitsstufe handelt es sich um eine globale Einstellung, die nur dann zum Einsatz kommt, wenn die ausgewählte Sicherheitsstufe deaktiviert ist.

In diesem Beispiel wird die Sicherheitsstufe **Büro** als Standard für alle Hosts in der Domäne konfiguriert.

1. Wählen Sie auf der Registerkarte **Richtliniendomänen** die Subdomäne **Laptops/Eng.**.
2. Öffnen Sie die Registerkarte **Einstellungen** und wählen Sie dort die Seite **Sicherheitsstufen für die Firewall**.
3. Klicken Sie in der Tabelle **Firewall-Sicherheitsstufen** auf das Optionsfeld **Standard** in der Zeile **Büro**.
   Policy Manager fordert Sie auf, die Änderung der Sicherheitsstufe für alle verwalteten Hosts zu bestätigen.
4. Klicken Sie auf **OK**.
5. Klicken Sie auf , um die Richtlinie zu verteilen.

Hinzufügen einer neuen Sicherheitsstufe für eine bestimmte Domäne

In diesem Beispiel erstellen Sie eine neue Sicherheitsstufe mit zwei Regeln.

Die neue Sicherheitsstufe wird nur für eine Subdomäne hinzugefügt und die Hosts müssen die neue Sicherheitsstufe verwenden. In der Subdomäne befinden sich Computer, die nur zum Internet-Browsen verwendet werden und nicht mit dem Unternehmens-LAN verbunden sind.

Wenn Sie eine neue Sicherheitsstufe für eine bestimmte Domäne hinzufügen, müssen Sie diese Sicherheitsstufe zunächst auf Root-Ebene deaktivieren und anschließend auf der entsprechend tieferen Ebene erneut aktivieren.

Definieren der neuen Sicherheitsstufe

Wenn Sie eine neue Sicherheitsstufe hinzufügen möchten, müssen Sie diese zunächst definieren.

Gehen Sie dazu folgendermaßen vor:

1. Wählen Sie auf der Registerkarte **Richtliniendomänen** den Eintrag **Stamm**.
2. Öffnen Sie die Registerkarte **Einstellungen** und wählen Sie dort die Seite **Sicherheitsstufen für die Firewall**.
3. Klicken Sie auf **Hinzufügen**, um die neue Sicherheitsstufe hinzuzufügen.
   Daraufhin wird das Dialogfeld **Sicherheitsstufe - Beschreibung** geöffnet.
4. Geben Sie einen Namen für die neue Sicherheitsstufe ein, z. B. `BrowserSicherheit`.

   Sie können außerdem eine Beschreibung in das Textfeld **Beschreibung** eingeben.
5. Klicken Sie auf **Fertig stellen**.
6. Klicken Sie auf , um die Richtlinie zu verteilen.

Definieren von Regeln für die neue Sicherheitsstufe

Der nächste Schritt besteht im Definieren der Regeln für die neue Sicherheitsstufe.

Die Regeln für die neue Sicherheitsstufe werden folgendermaßen definiert:

1. Öffnen Sie die Seite **Firewall-Regeln**.
2. Wählen Sie die gerade erstellte Sicherheitsstufe **BrowserSicherheit** aus.

   Wenn Sie die Sicherheitsstufe auswählen, wird in der Tabelle **Firewall-Regeln** nichts angezeigt, weil Sie noch keine Regeln definiert haben.
3. Klicken Sie auf **Hinzufügen vor**, um als erste Regel in der Liste eine Regel hinzuzufügen, die den gesamten ausgehenden HTTP-Datenverkehr zulässt.
   Daraufhin wird der **Firewall-Regel**-Assistent gestartet.
4. Führen Sie den **Firewall-Regel**-Assistenten aus:
   a) Wählen Sie auf der Seite **Regeltyp** als Regeltyp **Zulassen**.
   b) Wählen Sie auf der Seite **Remote-Hosts** die Option **Beliebiger Remote-Host**, um die Regel auf alle Internet-Verbindungen anzuwenden.
   c) Wählen Sie auf der Seite **Dienste** in der Spalte **Dienst** die Option **HTTP**, um die Regel auf den HTTP-Datenverkehr anzuwenden.
   d) Wählen Sie auf der Seite **Dienste** in der Spalte **Richtung** die Option **=>**, um die Regel nur auf ausgehende Verbindungen anzuwenden.
   e) Auf der Seite **Erweiterte Einstellungen** können Sie die Standardwerte übernehmen.
   f) Überprüfen Sie die Einstellungen für die neue Regel auf der Seite **Zusammenfassung**.

      Sie können für die Regel eine Beschreibung hinzufügen, z. B. `Ausgehenden HTTP-Datenverkehr zum Browsen zulassen.`.
   g) Klicken Sie auf **Fertig stellen**.
5. Klicken Sie auf **Hinzufügen nach**, um als letzte Regel in der Liste eine Regel hinzuzufügen, die den gesamten anderen Datenverkehr in beide Richtungen sperrt.
6. Führen Sie den **Firewall-Regel**-Assistenten aus:

a) Wählen Sie auf der Seite **Regeltyp** als Regeltyp **Ablehnen**.
b) Wählen Sie auf der Seite **Remote-Hosts** die Option **Beliebiger Remote-Host**, um die Regel auf alle Verbindungen anzuwenden.
c) Wählen Sie auf der Seite **Dienste** in der Spalte **Dienst** die Option **Gesamter Datenverkehr**, um die Regel auf den gesamten Datenverkehr anzuwenden.
d) Wählen Sie auf der Seite **Dienste** in der Spalte **Richtung**die Option **Beide**, um die Regel auf eingehende und ausgehende Verbindungen anzuwenden.
e) Auf der Seite **Erweiterte Einstellungen** können Sie die Standardwerte übernehmen.
f) Überprüfen Sie die Einstellungen für die neue Regel auf der Seite **Zusammenfassung**.

   Sie können für die Regel eine Beschreibung hinzufügen, z. B. `Alles andere sperren`.

g) Klicken Sie auf **Fertig stellen**.

Aktivieren der neuen Sicherheitsstufe

Als Nächstes müssen Sie die neue Sicherheitsstufe aktivieren.

Damit die neue Sicherheitsstufe nur in der oder den ausgewählten Subdomänen eingesetzt wird, müssen Sie sie zunächst auf der Root-Ebene deaktivieren und anschließend auf einer tieferen Ebene in der Richtliniendomänenhierarchie aktivieren. Gehen Sie dazu folgendermaßen vor:

1. Wählen Sie auf der Registerkarte **Richtliniendomänen** den Eintrag **Stamm**.
2. Öffnen Sie die Seite **Firewall-Sicherheitsstufen**.
3. Deaktivieren Sie die Sicherheitsstufe **BrowserSecurity**, indem Sie das Kontrollkästchen **Aktiviert** neben der Tabelle **Firewall-Sicherheitsstufen** deaktivieren.
4. Wählen Sie auf der Registerkarte **Richtliniendomänen** die Subdomäne aus, in der die Sicherheitsstufe eingesetzt werden soll.
5. Aktivieren Sie die Sicherheitsstufe **BrowserSecurity**, indem Sie das Kontrollkästchen **Aktiviert** neben der Tabelle **Firewall-Sicherheitsstufen** aktivieren.
6. Legen Sie die neue Sicherheitsstufe als aktive Sicherheitsstufe fest, indem Sie sie aus der Dropdown-Liste **Sicherheitsstufe für Internet Shield auf dem Host** auswählen.
7. Klicken Sie auf , um die Richtlinie zu verteilen.

Konfigurieren der Netzwerk-Quarantäne

Die Netzwerk-Quarantäne ist eine Funktion von Internet Shield, mit der sich der Netzwerkzugriff von Hosts mit sehr alten Virendefinitionen bzw. mit deaktiviertem Echtzeit-Scanning eingeschränkt werden kannt.

Die normalen Zugriffsrechte werden automatisch wiederhergestellt, sobald die Virendefinitionen auf diesen Hosts aktualisiert bzw. das Echtzeit-Scanning aktiviert wurde.

In diesem Abschnitt werden die Einstellungen der Netzwerk-Quarantäne beschrieben und anhand eines Beispiels zur Aktivierung der Netzwerk-Quarantäne in einer verwalteten Domäne veranschaulicht. Außerdem wird in diesem Abschnitt kurz auf die Konfiguration der Sicherheitsstufe der Netzwerk-Quarantäne durch Hinzufügen neuer Firewall-Regeln eingegangen.

Einstellungen der Netzwerk-Quarantäne

Die Netzwerk-Quarantäne wird auf der Seite **Firewall-Sicherheitsstufen** konfiguriert.

Im Abschnitt **Netzwerk-Quarantäne** können Sie:

- Die Netzwerk-Quarantäne aktivieren oder deaktivieren.
- Das Alter der Virendefinitionen festlegen, ab dem die Netzwerk-Quarantäne aktiviert wird.

- Festlegen, ob durch die Deaktivierung von Echtzeit-Scanning auf einem Host automatisch die Netzwerk-Quarantäne aktiviert wird..

Aktivieren der Netzwerk-Quarantäne für die gesamte Domäne

Führen Sie die folgenden Schritte aus, um die Netzwerk-Quarantäne für die gesamte Domäne zu aktivieren.

1. Wählen Sie auf der Registerkarte **Richtliniendomänen** den Eintrag **Stamm**.
2. Öffnen Sie die Registerkarte **Einstellungen** und wählen Sie dort die Seite **Sicherheitsstufen für die Firewall**.
3. Wählen Sie die Option **Netzwerk-Quarantäne aktivieren**.
4. Geben Sie das **Alter der Virusdefinitionen zur Aktivierung der Netzwerk-Quarantäne** an.
5. Wenn der Netzwerkzugriff von Hosts mit deaktiviertem Echtzeit-Scanning eingeschränkt sein soll, wählen Sie die Option **Netzwerk-Quarantäne auf Host bei deaktiviertem Echtzeit-Scanning aktivieren**.
6. Klicken Sie auf , um die Richtlinie zu verteilen.

Anpassen der Netzwerk-Quarantäne

Die Netzwerk-Quarantäne aktiviert auf den Hosts die Sicherheitsstufe **Netzwerk-Quarantäne**. Es handelt sich hier um einen restriktiven Satz an Firewall-Regeln.

Den Firewall-Regeln der Sicherheitsstufe **Netzwerk-Quarantäne** können Sie neue Regeln hinzufügen, die den Netzwerkzugriff der Hosts bei aktivierter Netzwerk-Quarantäne unter bestimmten Umständen **zulassen**. Sie sollten den Netzwerkzugriff allerdings nicht weiter einschränken, da die Netzwerk-Konnektivität auf den Hosts dann womöglich völlig zum Erliegen kommt.

Konfigurieren von Warnmeldungen nach Regelverletzungen

Mit Alarmen und Warnmeldungen, die Internet Shield aufgrund von Regelverletzungen ausgibt, können Administratoren oder Benutzer benachrichtigt werden, wenn bestimmte Arten von Malware versuchen, auf den Computer zuzugreifen.

Es ist auch möglich, Warnmeldungen immer dann auszugeben, wenn eine Regel ausgelöst oder ein illegales Datagramm empfangen wird. Auf diese Weise lässt sich die Art des Datenverkehrs auf Ihrem System mühelos feststellen.

Eine geeignete Alarmausgabe lässt sich nur durch eine geeignete Granularität in der Sicherheitsstufe erreichen: Es sollte jeweils eine Regel für jeden gewünschten Alarmtyp geben. Wenn Sie die Alarmgebung anhand weit gefasster Regeln definieren, werden viele Warnmeldungen erzeugt. In der hohen Anzahl der Meldungen gehen aber die wirklich wichtigen Informationen verloren.

Hinzufügen einer neuen Regel mit Alarmausgabe

In diesem Beispiel erstellen Sie eine Regel, die den eingehenden ICMP-Verkehr für eine bestimmte Subdomäne **sperrt**, sodass ein Alarm ausgegeben wird, wenn ein Dritter versucht, den Computer anzupingen.

Am Ende dieses Beispiels wird die Regel getestet, indem ein Computer aus der Subdomäne angepingt wird. Dieses Beispiel beschreibt auch die unterschiedlichen Auswahlmöglichkeiten, die Sie beim Erstellen neuer Regeln mit dem **Firewall-Regel**-Assistenten haben.

Auswählen des Regeltyps und des abgelehnten Dienstes

In einem ersten Schritt wird der Regeltyp ausgewählt und der abgelehnte Dienst definiert.

Gehen Sie wie folgt vor:

1. Wählen Sie auf der Registerkarte **Richtliniendomänen** die Subdomäne aus, für die die neue Regel erstellt werden soll.
2. Öffnen Sie die Registerkarte **Einstellungen** und wählen Sie dort die Seite **Firewall-Regeln**.
3. Wählen Sie aus dem Dropdown-Menü **Bearbeitete Sicherheitsstufe für Internet-Schutzschild** die Sicherheitsstufe aus, für die die neue Regel hinzugefügt werden soll.
   Jetzt werden alle Regeln, die für diese Sicherheitsstufe für Internet Shield definiert wurden, in der Tabelle angezeigt.
4. Klicken Sie auf **Hinzufügen vor**, um die neue Regel als erste Regel in der Liste hinzuzufügen.
   Daraufhin wird der **Firewall-Regel**-Assistent gestartet.
5. Wählen Sie **Ablehnen**, um die eingehenden ICMP-Verbindungen zu sperren.
6. Betroffene Hosts festlegen.

   Wählen Sie aus, ob Sie diese Regel auf alle Verbindungen oder nur auf bestimmte Verbindungen anwenden möchten. Sie können folgende Möglichkeiten auswählen:

   - Aktivieren Sie die Option **Beliebiger Remote-Host** , um die Regel auf alle Internet-Verbindungen anzuwenden.
   - Aktivieren Sie die Option **Alle Hosts aus lokal verbundenen Netzwerken**, um die Regel auf alle Verbindungen vom lokalen Netzwerk anzuwenden.
   - Aktivieren Sie die Option **Angegebene Remote-Hosts** , um die Regel auf eine IP-Adresse, einen Bereich von IP-Adressen oder auf DNS-Adressen anzuwenden. Wenn Sie diese Option aktivieren, können Sie die Adressen im weiter unten angezeigten Textfeld eingeben. Wenn Sie mehrere Adressen oder Adressbereiche in das Feld eingeben möchten, verwenden Sie Leerzeichen als Trennzeichen.

   Für diese Regel wählen Sie **Beliebiger Remote-Host**.

7. Gesperrten Dienst und Richtung für die Regel auswählen.

   Wählen Sie aus der Liste der verfügbaren Dienste den Dienst aus, für den diese Regel angewendet werden soll. Wenn die Regel auf alle Dienste angewendet werden soll, wählen Sie oben aus der Liste die Option **Alle** aus. Sie können in diesem Fenster beliebig viele Einzeldienste auswählen.

   Wählen Sie für die ausgewählten Dienste die Richtung aus, in der die Regel angewendet wird, indem Sie auf den Pfeil in der Spalte **Richtung** klicken. Durch wiederholtes Klicken wechseln Sie zwischen den verfügbaren Optionen. In der unten stehenden Tabelle finden Sie einige Beispiele dazu.

Richtung	Erklärung
<=>	Der Dienst wird von Ihrem Computer aus in beide Richtungen zugelassen/abgelehnt.
<=	Der Dienst wird zugelassen/gesperrt, wenn er von den definierten Remote-Hosts oder Netzwerken kommt.
=>	Der Dienst wird zugelassen/gesperrt, wenn er von Ihrem Computer zu den Remote-Hosts oder Netzwerken geht.

   Wählen Sie für diese Regel Folgendes aus:

   - **ICMP** aus der Dropdown-Liste **Dienst**
   - **<=** aus der Spalte **Richtung**.

Definieren der erweiterten Optionen

Als Nächstes werden die erweiterten Optionen für die Regel definiert.

Gehen Sie wie folgt vor:

1. Definieren Sie, ob die Regel nur angewendet wird, wenn durch Aktivieren oder Deaktivieren eines Kontrollkästchens ein DFÜ-Link geöffnet wird.
   a) Definieren Sie, ob die Regel nur angewendet wird, wenn durch Aktivieren oder Deaktivieren eines Kontrollkästchens ein DFÜ-Link geöffnet wird.
   b) Wählen Sie aus der Dropdown-Liste **Alarm senden** die Art der Alarmierung.

      Wählen Sie für diese Regel **Sicherheitsalarm**.
   c) Wählen Sie aus der Dropdown-Liste **Alarm-Trap** den Alarm-Auslöser.
   d) Geben Sie eine Beschreibung für den Alarm in das Feld **Alarmkommentar** ein.
   e) Für die restlichen Felder in diesem Fenster können Sie die Standardwerte übernehmen.
2. Wählen Sie aus der Dropdown-Liste **Alarm senden** die Art der Alarmierung.
3. Wählen Sie aus der Dropdown-Liste **Alarm-Trap** den Alarm-Auslöser.

   Wählen Sie für diese Regel **Netzwerkereignis: Eingehender Dienst abgelehnt**.
4. Geben Sie eine Beschreibung für den Alarm in das Feld **Alarmkommentar** ein.

   Dieser Kommentar wird auf der lokalen Benutzeroberfläche von Client Security angezeigt.
5. Für die restlichen Felder in diesem Fenster können Sie die Standardwerte übernehmen.
6. Überprüfen und akzeptieren Sie die Regel.

   Sie können Ihre Regel jetzt überprüfen. Außerdem können Sie eine Beschreibung für die Regel eingeben, damit Sie die Regel besser verstehen, wenn sie in der Tabelle **Firewall-Regeln** angezeigt wird. Wenn Sie Änderungen an der Regel vornehmen möchten, klicken Sie auf **Zurück**.
7. Wenn Sie mit Ihrer neuen Regel zufrieden sind, klicken Sie auf **Fertig stellen**.
   Die neue Regel wird im aktiven Regelsatz auf der Seite **Firewall-Regeln** n oberster Position hinzugefügt.

Alarmweiterleitung konfigurieren

Als Nächstes wird die Alarm-Weiterleitung für die Rege konfiguriert.

Gehen Sie wie folgt vor:

1. Öffnen Sie die Registerkarte **Einstellungen** und wählen Sie dort das Fenster **Versendung von Alarmen**.
2. Vergewissern Sie sich im Abschnitt **Alarmweiterleitung**, dass Sicherheitsalarme an Policy Manager Console weitergeleitet werden .
3. Aktivieren Sie - falls nötig - das Kontrollkästchen**Sicherheitsalarm** in der Spalte **Policy Manager-Konsole**.

Anwenden und Testen der neuen Regel

In einem letzten Schritt wird die neue Regel aktiviert und getestet.

Gehen Sie wie folgt vor:

1. Vergewissern Sie sich, dass auf der Registerkarte **Richtliniendomänen** die richtige Subdomäne ausgewählt wurde.
2. Öffnen Sie auf der Registerkarte **Einstellungen** die Seite **Firewall-Sicherheitsstufen**.
3. Legen Sie die Sicherheitsstufe, für die Sie die Regel erstellt haben, als aktive Sicherheitsstufe fest, indem Sie diese aus der Dropdown-Liste **Sicherheitsstufe für Internet Shield auf dem Host** auswählen.
4. Klicken Sie auf , um die Richtlinie zu verteilen.
5. Testen Sie die gerade erstellte Regel.

   Sie können die gerade erstellte Regel testen. Dazu pingen Sie einen der verwalteten Hosts in der Subdomäne von einem Computer an, der sich außerhalb der Domäne befindet. Anschließend können Sie folgendermaßen prüfen, ob die Regel funktioniert:
   a) Wählen Sie auf der Registerkarte **Richtliniendomänen** die Subdomäne aus, für die Sie die Regel erstellt haben.

b) Öffnen Sie die Registerkarte **Zusammenfassung** und prüfen Sie, ob neue Sicherheitswarnungen für die Domäne angezeigt werden.
c) Um Details zu den Warnungen anzuzeigen, klicken Sie auf **Alarme nach Schweregrad anzeigen**. Daraufhin wird die Registerkarte **Alarme** mit einer ausführlichen Liste der Sicherheitsalarme angezeigt.

Konfigurieren der Anwendungssteuerung

Die Anwendungssteuerung gewährleistet sicheres Web-Browsing und ist eine hervorragende Verteidigung gegen schädliche Programme.

Darüber hinaus eignet sich die Anwendungssteuerung ideal zur Bekämpfung von Trojanern und anderer Schädlinge im Netzwerk, da sie verhindert, dass diese Programme Informationen an das Netzwerk senden.

Über die Regeln der Anwendungssteuerung können Sie spezifische Einschränkungen des Netzwerkverkehrs definieren, die ergänzend zu den Beschränkungen der Firewall-Regeln wirken. Über diese Anwendungsberechtigungen ist es nicht möglich, Datenverkehr zuzulassen, der durch die statischen Firewall-Regeln gesperrt wurde. Wenn Sie jedoch bestimmte Arten von Netzwerkdatenverkehr über die statischen Regeln zugelassen haben, können Sie über die Anwendungssteuerung festlegen, ob die Zulassung durch die Regeln für die Anwendung gilt. Anders ausgedrückt: Sie können eine Regel erstellen, die Datenverkehr zulässt, und die Wirkung dieser Regel über die Anwendungssteuerung begrenzen.

Bei einer zentralen Verwaltung der Anwendungssteuerung kann der Administrator entscheiden, welche Programme, die auf das Netzwerk zugreifen, auf den Arbeitsstationen verwendet werden können. Dadurch kann der Einsatz von Programmen verhindert werden, die der Sicherheitsrichtlinie des Unternehmens widersprechen. Außerdem kann überwacht werden, mit welchen Programmen die Endbenutzer tatsächlich arbeiten.

Beachten Sie bei der Konfiguration der Anwendungssteuerung, dass Sie alle notwendigen Anwendungen zulassen und den Rest sperren sollten.

Wie Anwendungssteuerung und DeepGuard zusammenarbeiten

Wenn die Anwendungssteuerung einen abgehenden Verbindungsversuch erkennt und so konfiguriert ist, dass der Benutzer angeben muss, ob die Verbindung zugelassen oder abgelehnt werden soll, können Sie die Anwendungssteuerung so einrichten, dass über DeepGuard geprüft wird, ob eine Verbindung zugelassen werden kann. Dadurch wird die Anzahl der Anwendungssteuerungs-Popups reduziert, die dem Benutzer angezeigt werden.

Beispiel:

1. Wenn in der Tabelle **Anwendungsregeln für bekannte Anwendungen** eine Regel für die Anwendung verfügbar ist, die versucht, eine abgehende Verbindung herzustellen, lässt die Anwendungssteuerung den Verbindungsversuch auf Grundlage dieser Regel zu oder blockiert ihn.
2. Wenn in der Tabelle **Anwendungsregeln für bekannte Anwendungen** keine Regel für die Anwendung verfügbar ist, lässt die Anwendungssteuerung den Verbindungsversuch auf Grundlage der aktuell definierten **Standardmaßnahme für Client-Anwendungen** zu oder blockiert ihn.
3. Wenn die aktuell definierte Standardmaßnahme **Benutzereingabe anfordern** lautet und die Einstellung **Keine Benutzereingabe für Anwendungen, die von DeepGuard identifiziert werden** aktiviert ist, überprüft die Anwendungssteuerung über DeepGuard, ob die ausgehende Verbindung zugelassen werden kann. Wenn die Anwendung nun von DeepGuard identifiziert wird, erfolgt keine Benutzereingabe und die ausgehende Verbindung wird zugelassen.
4. Wenn die Anwendung nicht von DeepGuard identifiziert wird, kann der Benutzer festlegen, ob die Verbindung zugelassen oder blockiert wird.

Einstellungen für die Anwendungssteuerung

Im Folgenden werden die Einstellungsmöglichkeiten auf der Seite **Einstellungen** > **Anwendungssteuerung** beschrieben.

Auf der Seite **Anwendungssteuerung** werden folgende Informationen angezeigt:

Anwendungsregeln für bekannte Anwendungen	
Anwendung	Zeigt den Namen der Programmdatei (.exe) an.
Als Client (ausgehend)	Folgende Aktionen stehen zur Auswahl: **Ablehnen**, **Zulassen**, **Entscheidung des Benutzers**.
Als Server (eingehend)	Folgende Aktionen stehen zur Auswahl: **Ablehnen**, **Zulassen**, **Entscheidung des Benutzers**.
Beschreibung	Zeigt die interne Beschreibung der ausführbaren Datei (.exe) an. Normalerweise handelt es sich dabei um den Namen der Anwendung. Sie können die Beschreibung ändern.
Nachricht	Zeigt eine Meldung (falls vorhanden) an, die gemeinsam mit der Regel erstellt wurde.
Verleger	Zeigt den Verleger der Anwendung an.
Version	Zeigt die interne Versionsbeschreibung der ausführbaren Datei (.exe) an.

Unbekannte Anwendungen, die von den Hosts gemeldet wurden

Für unbekannte Anwendungen werden dieselben Informationen wie für bekannte Anwendungen angezeigt. Die einzige Ausnahme besteht darin, dass für unbekannte Anwendungen weder Regeln noch dazugehörige Meldungen existieren

Mithilfe der Optionen **Standardmaßnahme für Client-Anwendungen** und **Standardmaßnahme für Server-Anwendungen** können Sie festlegen, welche Aktionen ausgeführt werden sollen, wenn eine Anwendung versucht, eine Verbindung zum Netzwerk aufzubauen. Folgende Aktionen sind möglich:

Aktion	Beschreibung
Ablehnen	Lehnt alle Verbindungsversuche der Anwendung mit dem Netzwerk ab.
Zulassen	Lässt alle Verbindungsversuche der Anwendung mit dem Netzwerk zu.
Entscheidung des Benutzers	Bei jedem Versuch der Anwendung, eine Verbindung zum Netzwerk herzustellen, wird ein Dialogfeld eingeblendet, in dem der Benutzer entscheidet, ob die Verbindung zulässig ist.

Wenn der Benutzer die Vorgehensweise für abgehende Verbindungsversuche selbst festlegen soll, können Sie die Anzahl der angezeigten Popups reduzieren, indem Sie die Option **Keine Benutzereingabe für Anwendungen, die von DeepGuard identifiziert werden** aktivieren.

Die Anwendungssteuerung begrenzt nicht die Verwendung von Plugins in Browsern, wie Netscape oder Microsoft Internet Explorer. Alle Plugins müssen dieselben Eigenschaften wie der Browser haben. Sie sollten jedoch den Endbenutzern mitteilen, dass nur vertrauenswürdige Plugins installiert werden dürfen.

Erstmaliges Einrichten der Anwendungssteuerung

Wenn Sie die Anwendungssteuerung zum ersten Mal einrichten, sollten Sie mithilfe einer kleinen Testumgebung eine Liste zulässiger Anwendungen erstellen. Diese Liste sollte die Standardanwendungen enthalten, die im Unternehmen eingesetzt werden.

Die Liste zulässiger Anwendungen wird in einer Richtlinie an die gesamte verwaltete Domäne verteilt. Gehen Sie dazu folgendermaßen vor:

1. Erstellen Sie die Liste aller bekannten Anwendungen:
   a) Erstellen Sie eine Testumgebung mit beispielsweise zwei Computern, auf denen die normalerweise im Unternehmen eingesetzten Programme installiert sind.
   b) Importieren Sie diese Hosts in die zentral verwaltete Domäne.
   c) Wählen Sie aus der Dropdown-Liste **Benachrichtigungen für neue Anwendungen senden** die Option **Bericht**, sodass die neuen Anwendungen in der Liste **Unbekannte Anwendungen, die von den Hosts gemeldet wurden** vermerkt werden.
   d) Legen Sie die Regeln zum Zulassen für diese Anwendungen fest.
   e) Wenn für alle notwendigen Anwendungen Regeln definiert wurden, kann diese Regelsammlung als Richtlinie an die gesamte verwaltete Domäne übertragen werden.
2. Konfigurieren Sie die Grundeinstellungen für die Anwendungssteuerung, die angewendet werden, wenn die Anwendungssteuerung läuft:
   a) Wählen Sie aus der Dropdown-Liste **Standardmaßnahme für Client-Anwendungen** die Maßnahme aus, die ausgeführt werden soll, wenn eine unbekannte Anwendung versucht, eine ausgehende Verbindung aufzubauen.
   b) Wählen Sie aus der Dropdown-Liste **Standardmaßnahme für Server-Anwendungen** die Maßnahme aus, die ausgeführt werden soll, wenn eine unbekannte Anwendung versucht, eine eingehende Verbindung aufzubauen.
   c) Legen Sie fest, dass neue Anwendungen an den Administrator gemeldet werden. Aktivieren Sie dazu das Kontrollkästchen **Neue unbekannte Anwendungen melden**.
   Auf diese Weise können Sie feststellen, welche Art von Anwendungen von Endbenutzern gestartet wird, und können gegebenenfalls neue Regeln für diese Anwendungen definieren.
   d) Legen Sie fest, ob Standardmeldungen für Benutzer angezeigt werden sollen, wenn eine unbekannte Anwendung versucht, eine eingehende oder ausgehende Verbindung aufzubauen. Aktivieren oder deaktivieren Sie dazu das Kontrollkästchen **Standardmeldungen für unbekannte Anwendungen anzeigen**.
3. Prüfen und übernehmen Sie die Einstellungen.
   Gehen Sie folgendermaßen vor, um die Anwendungssteuerung für die gesamten Domäne zu aktivieren:
   a) Wählen Sie auf der Registerkarte **Richtliniendomänen**den Eintrag **Stamm**.
   b) Öffnen Sie auf der Registerkarte **Einstellungen** die Seite **Firewall-Sicherheitsstufen** und vergewissern Sie sich, dass das Kontrollkästchen **Anwendungssteuerung aktivieren** aktiviert ist.
   c) Klicken Sie auf , um die Richtlinie zu verteilen.

Erstellen einer Regel für eine unbekannte Anwendung auf Root-Ebene

In diesem Beispiel wird eine Regel erstellt, welche die Verwendung von Internet Explorer 4 sperrt.

In diesem Fall wird angenommen, dass sich diese Anwendung bereits auf der Liste **Unbekannte Anwendungen, die von den Hosts gemeldet wurden** befindet.

1. Wählen Sie die Anwendung(en) für die Regel aus:

a) Öffnen Sie die Registerkarte **Einstellungen** und wählen Sie dort die Seite **Anwendungssteuerung** .
b) Wählen Sie aus der Tabelle **Unbekannte Anwendungen, die von den Hosts gemeldet wurden** den Eintrag **Internet Explorer 4.01** aus.
c) Klicken Sie auf **Regel(n) erstellen**, um den Regelassistenten für die Anwendungssteuerung zu starten.

2. Wählen Sie die Art der Anwendungsregel aus:
   a) Wählen Sie als Maßnahme **Ablehnen**. Diese Maßnahme wird ausgeführt, wenn die Anwendung als Client agiert und versucht, eine ausgehende Verbindung aufzubauen.
   b) Wählen Sie die Maßnahme **Ablehnen**. Diese Maßnahme wird ausgeführt, wenn die Anwendung als Server agiert und versucht, eine eingehende Verbindung aufzubauen.
3. Wählen Sie die Meldung, die dem Benutzer angezeigt wird:
   a) Wählen Sie aus, ob der Benutzer bei einem Verbindungsversuch eine Meldung erhalten soll.

      Sie können unter folgenden Optionen wählen: **Keine Meldung**, **Standardmeldung** oder **Benutzerdefinierte Meldung**.

      Wenn Sie **Standardmeldung** ausgewählt haben, können Sie auf **Standardmeldungen definieren** klicken, um die momentan definierte Standardmeldung zu überprüfen.
   b) Wenn Sie **Benutzerdefinierte Meldung** ausgewählt haben, wird ein Textfeld zur Eingabe einer eigenen Meldung aktiviert.

      In diesem Fall können Sie eine eigene Meldung verwenden, wie z. B.: `Die Verwendung von Internet Explorer 4 wird durch die Sicherheitsrichtlinie des Unternehmens untersagt. Verwenden Sie stattdessen bitte einen anderen Browser.`
4. Wählen Sie das Ziel für die Regel aus:
   a) Wählen Sie aus den in diesem Fenster aufgeführten Domänen und Hosts diejenigen aus, die von der Regel betroffen sind.

      Wenn für den Ziel-Host oder die Ziel-Domäne bereits eine Regel für eine der von der Regel betroffenen Anwendungen definiert wurde, erscheint ein Dialogfeld, in dem Sie festlegen, ob Sie fortfahren und die auf dem Host vorhandene Regel überschreiben möchten.

      Wählen Sie in diesem Beispiel **Stamm**.
   b) Klicken Sie auf **Fertig stellen**, wenn die Regel Ihren Vorstellungen entspricht.
      Die neue Regel wird daraufhin in der Tabelle **Anwendungsregeln für bekannte Anwendungen** angezeigt. Die Tabelle **Unbekannte Anwendungen, die von den Hosts gemeldet wurden** wurde aktualisiert.
5. Klicken Sie auf , um die Richtlinie zu verteilen.

Bearbeiten einer vorhandenen Regel für die Anwendungsteuerung

In diesem Beispiel wird die zuvor erstellte Regel bearbeitet, und die Verwendung von Internet Explorer 4 wird vorübergehend zu Testzwecken in der Subdomäne `Technik/Prüfung` zugelassen.

1. Wählen Sie die zu bearbeitende Regel:
   a) Öffnen Sie die Registerkarte **Einstellungen** und wählen Sie dort die Seite **Anwendungssteuerung**.
   b) Wählen Sie aus der Liste **Anwendungsregeln für bekannte Anwendungen** die Regel, die bearbeitet werden soll.
   c) Klicken Sie auf **Bearbeiten**, um den Regelassistenten für die Anwendungssteuerung zu starten.
2. Bearbeiten Sie den Anwendungsregeltyp:
   a) Wählen Sie die Maßnahme, die ausgeführt werden soll, wenn die Anwendung als Client agiert und versucht, eine ausgehende Verbindung aufzubauen.

      Wählen Sie in diesem Fall **Zulassen** für **Als Client (ausgehend)**.

b) Wählen Sie die Maßnahme, die ausgeführt werden soll, wenn die Anwendung als Server agiert und versucht, eine eingehende Verbindung aufzubauen.

3. Wählen Sie die Benutzermeldung.

   Wählen Sie aus, ob der Benutzer bei einem Verbindungsversuch eine Meldung erhalten soll.

4. Wählen Sie das neue Ziel für die Regel:

   a) Wählen Sie die Domänen oder Hosts, die von der Regel betroffen sind.

      Wählen Sie in diesem Fall **Technik/Prüfung**.

      Wenn für den Ziel-Host oder die Ziel-Domäne bereits eine Regel für eine der von der Regel betroffenen Anwendungen definiert wurde, erscheint ein Dialogfeld, in dem Sie festlegen, ob Sie fortfahren und die auf dem Host vorhandene Regel überschreiben möchten.

   b) Klicken Sie auf **Fertig stellen**, wenn die Regel Ihren Vorstellungen entspricht.
      Die geänderte Regel wird daraufhin in der Tabelle **Anwendungsregeln für bekannte Anwendungen** angezeigt. Dabei handelt es sich um eine Kopie der ursprünglichen Regel mit den gerade vorgenommenen Änderungen.

5. Klicken Sie auf , um die Richtlinie zu verteilen.

Deaktivieren des Popup-Fensters der Anwendungssteuerung

Wenn die Anwendungssteuerung so konfiguriert werden soll, dass sie für den Endbenutzer völlig transparent ist, müssen alle Popups deaktiviert werden.

1. Wählen Sie auf der Registerkarte **Richtliniendomänen** den Eintrag **Stamm**.
2. Öffnen Sie die Registerkarte **Einstellungen** und wählen Sie dort die Seite **Anwendungssteuerung**.

   Wählen Sie auf dieser Seite Folgendes aus:

   - **Zulassen** aus der Dropdown-Liste **Standardmaßnahme für Server-Anwendungen**.
   - **Zulassen** aus der Dropdown-Liste **Standardmaßnahme für Client-Anwendungen**.

3. Wenn Sie Regeln mit dem Assistenten für **Anwendungssteuerungsregeln** erstellen, wählen Sie Folgendes aus:

   - Entweder **Zulassen** oder **Ablehnen** im Dialogfeld **Anwendungsregeltyp** als Maßnahme bei eingehenden oder ausgehenden Verbindungsversuchen.
   - **Keine Meldung** im Dialogfeld **Benutzermeldung**.

4. Klicken Sie auf , um die Richtlinie zu verteilen.

Verwenden von Alarmen zum Prüfen der Funktionsweise von Internet Shield

Während des Normalbetriebs sollten Sie keine Alarme von Internet-Schutzschild erhalten; wenn Sie plötzlich viele Alarme erhalten, kann dies entweder auf einen Fehler in der Konfiguration oder ein ernstes Problem hindeuten.

Bei der Konfiguration der Alarmausgabe sollten Sie für jeden gewünschten Alarmtyp eine Regel definieren. Wenn Sie die Alarmgebung anhand weit gefasster Regeln definieren, werden viele Warnmeldungen erzeugt. In der hohen Anzahl der Meldungen gehen aber die wirklich wichtigen Informationen verloren.

Sie können auch spezielle Regeln erstellen, um die Funktionsweise von Internet Shield zu testen. In diesem Beispiel wird eine Regel definiert, die die Verwendung von Ping zulässt. Wenn diese Regel eine Alarmausgabe beinhaltet, kann man sie zur Überprüfung der Funktionsfähigkeit der Alarmausgabe heranziehen.

1. Öffnen Sie die Registerkarte **Einstellungen** und wählen Sie dort die Seite **Firewall-Regeln** aus.
2. Wählen Sie die für Testzwecke gewünschte Sicherheitsstufe.
3. Um eine neue Regel zu definieren, klicken Sie auf **Hinzufügen vor**.
   Daraufhin wird der **Firewall-Regel**-Assistent gestartet.
4. Wählen Sie auf der Seite **Regeltyp** die Option **Zulassen**.
5. Wählen Sie auf der Seite **Remote-Hosts** die Option **Beliebiger Remote-Host**.
6. Wählen Sie auf der Seite **Dienste** aus der Dropdown-Liste **Dienst** die Option **Ping** und aus der Dropdown-Liste **Richtungen** die Einstellung **Beide**.
7. Wählen Sie auf der Seite **Erweiterte Optionen** die folgenden Optionen:
   - **Sicherheitsalarm** aus der Dropdown-Liste **Alarm senden**
   - **Potenziell gefährlicher Dienst zugelassen** aus der Dropdown-Liste **Alarm-Trap**
   - Sie können eine Beschreibung des Alarms in das Feld **Alarmkommentar** eingeben.
8. Auf der Seite **Zusammenfassung** können Sie überprüfen, ob die Regel korrekt ist, und eine Beschreibung für die Regel eingeben.
9. Klicken Sie auf , um die Richtlinie zu verteilen.
10. Nun können Sie die Regel testen. Pingen Sie dazu einen der verwalteten Hosts an und überprüfen Sie, ob ein Alarm erzeugt und auf der Registerkarte **Alarme** angezeigt wird.

Konfigurieren der Intrusion Prevention

Intrusion Prevention überwacht den eingehenden Datenverkehr und versucht, Eindringversuche zu erkennen.

Intrusion Prevention (IPS) eignet sich außerdem zum Überwachen von Viren, die versuchen, Computer in einem LAN anzugreifen. Intrusion Prevention analysiert die Nutzdaten (den Inhalt) und die Informationen aus der Kopfzeile eines IP-Pakets und vergleicht diese Informationen mit bekannten Angriffsmustern. Wenn die Informationen einem bekannten Angriffsmuster ähneln oder diesem entsprechen, erzeugt Intrusion Prevention einen Alarm und führt die in der Konfiguration festgelegte Maßnahme durch.

Einstellungen für Intrusion Prevention

Die Einstellungen für Intrusion Prevention befinden sich im Abschnitt **Intrusion Prevention** der Seite **Firewall-Sicherheitsstufen**.

- **Intrusion Prevention aktivieren**

  Im aktivierten Zustand überwacht Intrusion Prevention den eingehenden Datenverkehr, um Eindringversuche aufzudecken. Im deaktivierten Zustand wird der Datenverkehr nicht überwacht.

- **Maßnahme bei bösartigem Paket**

  Folgende Optionen sind verfügbar:

  - **Paket(e) protokollieren und löschen** bedeutet, dass das Paket mit den Headerinformationen (IPs, Ports und Protokoll) im Alarmprotokoll aufgezeichnet und von Intrusion Prevention blockiert wird..
  - **Paket(e) protokollieren, aber nicht löschen** bedeutet, dass das Paket mit den Headerinformationen (IPs, Ports und Protokoll) im Alarmprotokoll aufgezeichnet, jedoch von Intrusion Prevention durchgelassen wird.

- **Alarmschweregrad**

  Folgende Optionen sind verfügbar: **Kein Alarm**, **Informativ**, **Warnung**, **Sicherheitsalarm**. Es ist möglich, Eindringversuche nach unterschiedlichen Schweregraden zu klassifizieren. Diese Einstellung hängt davon ab, welche Vorlieben der Administrator oder lokale Benutzer im Hinblick auf die Meldungen haben.

- Erkennungsempfindlichkeit

  Dieser Parameter hat zwei Aufgaben: Er soll die Anzahl der Alarme verringern und wirkt sich darüber hinaus auf die Leistung des lokalen Rechners aus. Wenn Sie einen niedrigeren Wert eingeben, werden weniger Fehlalarme erzeugt.

  - 10 = maximale Netzwerkleistung, minimale Alarmanzahl
  - 50 = nur 50 % (die wichtigsten und böswilligsten) IPS-Muster werden ausgewertet und im Fall einer Übereinstimmung gemeldet.
  - 100 = alle programmierten Muster werden ausgewertet und bei einer Übereinstimmung gemeldet.
  - Je kleiner der eingegebene Wert, desto weniger Muster werden ausgewertet.
  - Der empfohlene Wert für Privatbenutzer lautet 100 %
  - Der empfohlene Wert für Desktops lautet 25 %

Definition eines Fehlalarms

Bei einem Fehlalarm handelt es sich um einen Alarm, der ein Ereignis, wie eine Schutzverletzung, fälschlicherweise meldet. Bei Internet Shield wird dies im Alarmtext häufig anhand bestimmter Begriffe wie "wahrscheinlich" oder "möglich" angedeutet. Diese Art von Alarm sollte ganz ausgeschlossen oder auf ein Minimum begrenzt werden.

Konfigurieren von IPS für Desktops und Laptops

In diesem Beispiel wird IPS für alle Desktops und Laptops in zwei Subdomänen aktiviert.

Dabei wird angenommen, dass sich Desktop und Laptops in ihren jeweiligen Subdomänen, nämlich `Desktops/Eng` und `Laptops/Eng`, befinden. Es wird ferner angenommen, dass die Desktops auch durch die Unternehmens-Firewall geschützt sind und aus diesem Grund das für sie ausgewählte Leistungsniveau für Warnungen eine niedrigere Priorität hat. Die Laptops sind regelmäßig mit Netzwerken verbunden, die man schwerlich als sicher bezeichnen kann. Aus diesem Grund muss hier für das Leistungsniveau für Warnungen eine höhere Priorität ausgewählt werden.

1. Konfigurieren von IPS für Desktops:
   a) Wählen Sie auf der Registerkarte **Richtliniendomänen** die Subdomäne **Desktops/Eng**.
   b) Öffnen Sie die Registerkarte **Einstellungen** und wählen Sie dort die Seite **Sicherheitsstufen für die Firewall**.
   c) Aktivieren Sie das Kontrollkästchen **Intrusion Prevention aktivieren**.
   d) Wählen Sie aus der Dropdown-Liste **Maßnahme bei bösartigem Paket** die Option **Paket(e) protokollieren, aber nicht löschen**.
   e) Wählen Sie aus der Dropdown-Liste **Alarmschweregrad** die Option **Warnung**.
   f) Wählen Sie aus der Dropdown-Liste **Erkennungsempfindlichkeit** die Option **25%**.
2. Konfigurieren von IPS für Laptops:
   a) Wählen Sie auf der Registerkarte **Richtliniendomänen** die Subdomäne **Laptops/Eng**.
   b) Öffnen Sie die Registerkarte **Einstellungen** und wählen Sie dort die Seite **Firewall-Sicherheitsstufen**.
   c) Aktivieren Sie das Kontrollkästchen **Intrusion Prevention aktivieren**.
   d) Wählen Sie aus der Dropdown-Liste **Maßnahme bei bösartigem Paket** die Option **Paket(e) protokollieren, aber nicht löschen**.
   e) Wählen Sie aus der Dropdown-Liste **Warnung** die Option **Schweregrad zentraler Alarme**.
   f) Wählen Sie aus der Dropdown-Liste **Alarm- und Leistungsniveau** die Option **100%**.
3. Klicken Sie auf , um die Richtlinie zu verteilen.

Kapitel

7

So prüfen Sie, ob die Netzwerkumgebung geschützt ist

Themen:

- *Überprüfen, ob alle Hosts über die neueste Richtlinie verfügen*
- *Überprüfen, ob sich die neuesten Virendefinitionen auf dem Server befinden*
- *Überprüfen, ob die Hosts über die neuesten Virendefinitionen verfügen*
- *Überprüfen, ob alle Hosts verbunden sind*
- *Anzeigen von Scan-Berichten*
- *Anzeigen von Alarmen*
- *Erstellen eines wöchentlichen Infektionsberichts*
- *Überwachen eines möglichen Netzwerkangriffs*

Dieser Abschnitt enthält eine Checkliste, mit der Sie überprüfen können, ob die Netzwerkumgebung geschützt ist.

Im Rahmen der Überwachung und Systemverwaltung können Sie die hier aufgeführten Aufgaben regelmäßig ausführen, um den Schutz der Netzwerkumgebung sicherzustellen.

Überprüfen, ob alle Hosts über die neueste Richtlinie verfügen

Sie können sicherstellen, dass die Einstellungen aller Hosts korrekt sind, indem Sie überprüfen, ob sie über die neuste Richtlinie verfügen.

1. Wählen Sie auf der Registerkarte **Richtliniendomänen** den Eintrag **Stamm**.
2. Öffnen Sie die Registerkarte **Zusammenfassung**, und prüfen Sie, wie viele Hosts in der gesamten Domäne über die neueste Richtlinie verfügen.
3. Wenn die neueste Richtlinie noch nicht auf allen Hosts implementiert ist, klicken Sie auf **Neueste Richtlinien-Updates der Hosts anzeigen**.
   Daraufhin wird die Registerkarte **Status** mit der Seite **Zentrale Verwaltung** angezeigt.
4. Überprüfen Sie auf der Seite **Zentrale Verwaltung**, welche Hosts noch nicht über die neueste Sicherheitsrichtlinie verfügen.

   Sie können auch die möglichen Gründe hierfür anzeigen. So ist möglicherweise die Verbindung zum Host getrennt, oder auf dem Host ist ein schwerwiegender Fehler aufgetreten.

Überprüfen, ob sich die neuesten Virendefinitionen auf dem Server befinden

Sie sollten überprüfen, ob die Virendefinitionen auf dem Server aktuell sind.

1. Wählen Sie auf der Registerkarte **Richtliniendomänen** den Eintrag **Stamm**.
2. Öffnen Sie die Registerkarte **Zusammenfassung**, und prüfen Sie, ob die neuesten verfügbaren Virendefinitionen auf dem Server installiert sind.

Überprüfen, ob die Hosts über die neuesten Virendefinitionen verfügen

Sie sollten regelmäßig überprüfen, ob die Virendefinitionen auf allen Hosts in der Domäne auf dem neuesten Stand sind.

1. Wählen Sie auf der Registerkarte **Richtliniendomänen** den Eintrag **Stamm**.
2. Öffnen Sie die Registerkarte **Zusammenfassung**, und überprüfen Sie die Angaben im Abschnitt **Virenschutz für Arbeitsstationen** neben **Virendefinitionen**.
3. Wenn die Virendefinitionen auf einigen Hosts veraltet sind, gibt es für die weitere Vorgehensweise zwei Alternativen:

   - Auf der Seite **Allgemeiner Schutz** der Registerkarte **Status** können Sie feststellen, welche Hosts noch nicht über die neuesten Virendefinitionen verfügen. Wählen Sie diese Hosts anschließend auf der Registerkarte **Richtliniendomänen** aus, öffnen Sie die Registerkarte **Operationen**, und klicken Sie auf **Virusdefinitionen aktualisieren**. Daraufhin rufen die ausgewählten Hosts sofort die neuen Virendefinitionen ab.
   - Wahlweise können Sie auch auf die Verknüpfung **Virusdefinitionen aktualisieren** klicken. Daraufhin wird die Registerkarte **Operationen** geöffnet. Klicken Sie auf der Registerkarte **Operationen** auf **Virusdefinitionen aktualisieren**. Daraufhin rufen alle Hosts sofort die neuen Virendefinitionen ab.

Überprüfen, ob alle Hosts verbunden sind

Sie können sicherstellen, dass alle Hosts die neuesten Updates erhalten, indem Sie überprüfen, ob alle Hosts verbunden sind.

1. Wählen Sie auf der Registerkarte **Richtliniendomänen** den Eintrag **Stamm**.
2. Öffnen Sie die Registerkarte **Zusammenfassung**, und überprüfen Sie die Angaben im Abschnitt **Domäne** neben **Getrennte Hosts**.
3. Falls getrennte Hosts vorhanden sind, klicken Sie auf **Getrennte Hosts anzeigen**.
   Daraufhin wird die Registerkarte **Status** mit der Seite **Zentrale Verwaltung** angezeigt.
4. Überprüfen Sie, welche Hosts keine Verbindung haben und welche Gründe dafür vorliegen.

   Hinweis: Sie können die Dauer angeben, nach der die Verbindung des Hosts als aufgehoben angesehen wird. Wählen Sie **Tools** > **Serverkonfiguration** aus dem Menü aus und wählen Sie dann die Registerkarte **Hosts** aus. Nun sehen Sie die aktuell eingerichtete Dauer, nach der die Verbindung von Hosts als aufgehoben angesehen wird.

Anzeigen von Scan-Berichten

Sie können die Scan-Berichte von Hosts anzeigen, um zu überprüfen, ob Probleme aufgetreten sind.

Gehen Sie folgendermaßen vor, um einen Scan-Bericht von einem bestimmten Host abzurufen:

1. Wählen Sie die entsprechenden Hosts auf der Registerkarte **Richtliniendomänen** aus.
2. Wechseln Sie zur Registerkarte **Scan-Berichte**.
   Die Scan-Informationen von den ausgewählten Hosts werden in der Tabelle **Scan-Berichte** angezeigt.
3. Wählen Sie einen einzelnen Host aus, indem Sie auf die entsprechende Tabellenzeile klicken.
   Der entsprechende Scan-Bericht von diesem Host wird in der Berichtansicht im unteren Fensterbereich angezeigt.

Anzeigen von Alarmen

Bei Problemen mit einem Programm oder einem Arbeitsvorgang können die betroffenen Hosts Alarme und Berichte zum Vorfall senden.

Sie sollten regelmäßig prüfen, ob neue Alarme vorliegen, und Alarme quittieren und löschen, deren Ursache behoben wurde.

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

1. Klicken Sie auf geändert.
   Wahlweise können Sie auch auf der Registerkarte **Zusammenfassung** auf **Alarm-Zusammenfassung anzeigen** klicken.
   Die Registerkarte **Alarme** wird geöffnet. Die empfangenen Alarme werden in folgendem Format angezeigt:

Quittieren	Klicken Sie auf die Schaltfläche **Quittieren**, um einen Alarm zu quittieren. Wenn alle Alarme quittiert wurden, wird die Schaltfläche **Quittieren** grau angezeigt. Das bedeutet, dass die Schaltfläche deaktiviert ist.

Schweregrad	Der Schweregrad des Problems. Für jeden Schweregrad gibt es ein eigenes Symbol:		
		Info	Normale Informationen eines Hosts über einen Arbeitsvorgang.
		Warnung	Eine Warnung vom Host.
		Fehler	Behebbarer Fehler auf dem Host.
		Schwerwiegender Fehler	Unbehebbarer Fehler auf dem Host.
		Sicherheitsalarm	Sicherheitsrisiko auf dem Host.
Datum/Uhrzeit	Datum und Uhrzeit des Alarms.		
Beschreibung	Beschreibung des Problems.		
Host/Benutzer	Name des Hosts bzw. des Benutzers.		
Programm	Das F-Secure-Programm, das den Alarm gesendet hat.		

Bei Auswahl eines Alarms aus der Liste werden im Fensterbereich **Alarmansicht** unter der Alarmtabelle detaillierte Informationen zu dem Alarm angezeigt.

2. Mithilfe der Schaltfläche **Quittieren** können Sie die Alarme quittieren, die Sie bereits überprüft haben und deren Ursache Sie beheben möchten.
3. Die zusammenfassenden Informationen zu den Alarmen auf der Registerkarte **Zusammenfassung** werden nicht automatisch aktualisiert. Klicken Sie auf **Alarm-Zusammenfassung aktualisieren**, um die Anzeige zu aktualisieren.

Erstellen eines wöchentlichen Infektionsberichts

Wenn Sie einen wöchentlichen Bericht zu Infektionen (oder einen anderen Bericht, der in regelmäßigen Abständen erstellt werden soll) erstellen möchten, haben Sie zwei Möglichkeiten.

- Mit dem Browser-basierten Dienstprogramm Web Reporting können Sie viele verschiedene grafische Berichte zu den von Client Security erzeugten Alarmmeldungen und Statusdaten erstellen.

Überwachen eines möglichen Netzwerkangriffs

Wenn Sie einen Netzwerkangriff im LAN vermuten, können Sie diesen überwachen, indem Sie folgende Schritte ausführen.

1. Wählen Sie auf der Registerkarte **Richtliniendomänen** den Eintrag **Stamm**.
2. Öffnen Sie die Registerkarte **Zusammenfassung**.
3. Prüfen Sie die Angaben neben **Häufigster Wert bei letzter Angriff**.
4. Bei einem Angriff können Sie detaillierte Informationen abrufen, indem Sie auf **Status von Internet Shield anzeigen** klicken.
   Daraufhin wird die Registerkarte **Status** mit der Seite **Internet Shield** geöffnet. Dort werden ausführliche Informationen zu den letzten Virenangriffen auf die einzelnen Hosts angezeigt.

Kapitel

8

Aktualisieren der Software

Themen:

- *Verwenden von richtlinienbasierter Installation*

In diesem Abschnitt wird die Aktualisierung der Software mit dem Installationseditor beschrieben.

Mithilfe des **Installationseditors** können Sie eine vorhandene Installation der F-Secure Anti-Virus-Software über ein Remote-Upgrade aktualisieren. Dabei definiert der Editor richtlinienbasierte Installationsaufgaben, die jeder Host in der Ziel-Domäne nach der nächsten Richtlinienaktualisierung ausführt.

Hinweis: Sie können ein Client Security-Upgrade auch mit jedem anderen Installationsverfahren durchführen.

Verwenden von richtlinienbasierter Installation

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

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

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

So verwenden Sie richtlinienbasierte Installation:

1. Öffnen Sie die Registerkarte **Installation**.
   Auf der Registerkarte **Installation** wird in der Tabelle **Richtlinienbasierte Installationen** der Status der aktuellen Installationsvorgänge angezeigt. In der Tabelle **Zusammenfassung installierter Produkte** werden die Produkte aufgelistet, die aktuell auf verwalteten Hosts installiert sind.
2. Klicken Sie auf **Installieren** unter der Tabelle **Richtlinienbasierte Installationen**, um den Assistenten für die Remote-Installation zu starten.
3. Führen Sie die Anweisungen des Assistenten für die Remote-Installation aus, indem Sie die notwendigen Details angeben.

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

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

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

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

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

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

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

Kapitel

9

Arbeitsvorgänge auf lokalen Hosts

Themen:

- *Manuell scannen*
- *Zu festgelegten Zeiten scannen*
- *Wo finde ich die Alarmmeldungen und Protokolldateien der Firewall?*
- *Manuelles Herstellen einer Verbindung mit Policy Manager und Importieren einer Richtliniendatei*
- *Aussetzen von Downloads und Updates*
- *Benutzern erlauben, F-Secure-Produkte aus dem Speicher zu entfernen*

Dieser Abschnitt enthält Anweisungen zur Durchführung von Arbeitsvorgängen und zur lokalen Fehlerbehebung auf den Hosts.

Sie müssen die in diesem Abschnitt aufgeführten Vorgänge unter Umständen ausführen, wenn Sie einen Virus auf dem lokalen Host vermuten oder andere administrative Aufgaben lokal ausführen müssen.

Manuell scannen

Sie können Ihren Computer manuell scannen, wenn Sie den Verdacht haben, dass sich *Malware* auf Ihrem Computer befindet.

Art des manuellen Scans auswählen

Sie können Ihren gesamten Computer scannen oder nach einem bestimmten Typ von *Malware* oder einen bestimmten Bereich scannen.

Wenn Sie einen bestimmten Typ von *Malware* befürchten, können Sie nur nach diesem Typ scannen. Wenn Sie im Bezug auf einen bestimmten Bereich Ihres Computers einen Verdacht haben, dann scannen Sie nur diesen Bereich. Diese Scans verlaufen viel schneller als ein vollständiger Scan des gesamten Computers.

So starten Sie das Scannen Ihres Computers manuell:

1. Klicken Sie auf der Hauptseite auf den Pfeil unter **Scannen**.
   Die Scan-Optionen werden angezeigt.
2. Wählen Sie **Server-Schutz** > **Manuelles Scanning**.
3. Wählen Sie den Scan-Typ.
   Wenn Sie die Scan-Einstellungen ändern möchten, wählen Sie **Scan-Einstellungen ändern...**
4. Wählen Sie unter **Neuer Scan-Vorgang** die Art des Scan-Vorgangs aus.
   Wenn Sie die Einstellungen für das Scanning ändern möchten, öffnen Sie die Registerkarte **Einstellungen**.
5. Bei Auswahl von **Elemente für Scan wählen** wird ein Fenster geöffnet, in dem Sie das zu prüfende Verzeichnis oder Objekt angeben können.
   Der **Scan-Assistent** wird geöffnet.
6. Wenn Sie **Zu scannende Elemente auswählen** ausgewählt haben, klicken Sie auf **Auswählen**.
   Es wird ein Fenster geöffnet, in dem Sie auswählen können, welcher Speicherort gescannt werden soll.
7. Klicken Sie auf **Start**, um den Scan-Vorgang zu starten.
   Wurde keine Malware erkannt, wird in der Statuszeile im oberen Teil der Seite "Abgeschlossen" angezeigt.
   Wurde Malware erkannt, wird der Scan-Assistent geöffnet.

Hinweis: Sie können den Server auch manuell scannen, indem Sie in der Taskleiste mit der rechten Maustaste auf das Produktsymbol klicken.

Scantypen

Sie können Ihren gesamten Computer scannen oder nach einem bestimmten Typ von Malware oder einen bestimmten Bereich scannen.

Dies sind die verschiedenen Scantypen:

Scantyp	Was wird gescannt?	Wann dieser Typ verwendet werden sollte
Vollständiger Scan des Computers	Ihr gesamter Computer (interne und externe Festplatten) auf Viren, Spyware und Riskware	Wenn Sie absolut sicher sein wollen, dass keine Malware oder Riskware auf Ihrem Computer ist.Diese Art des Scannens dauert am längsten.Sie kombiniert den schnellen Malware-Scan und den Festplattenscan. Außerdem sucht sie nach Elementen, die unter Umständen durch ein Rootkit verborgen sind.
Auswahl für Scan...	Eine spezielle Datei, ein spezieller Ordner oder ein spezielles Laufwerk für	Wenn Sie den Verdacht haben, dass sich an einem bestimmten Speicherort Ihres Computers Malware befindet, weil sich dort Downloads von potenziell gefährlichen

Scantyp	Was wird gescannt?	Wann dieser Typ verwendet werden sollte
	Viren, Spyware und Riskware	Quellen, wie Peer-to-Peer File Sharing-Netzwerken, befinden.Wie lange der Scan dauert, hängt von der Größte des zu scannenden Ziels ab.Der Scan wird beispielsweise schnell abgeschlossen, wenn Sie einen Ordner mit nur ein paar kleinen Dateien scannen.
Festplatten scannen	Alle internen Festplatten auf Ihrem Computer auf Viren, Spyware und Riskware	Dabei werden alle Festplatten des Computers gescannt.Im Gegensatz zum schnellen Malware-Scan werden bei diesem Scantyp nicht nur gezielt die Teile Ihres Systems mit installierten Programmdateien durchsucht, sondern auch alle Datendateien wie Dokumente, Musik, Bilder und Videos. Diese Art des Scannens ist langsam und wird nur dann empfohlen, wenn der schnelle Malware-Scan keine Malware entdeckt hat, Sie aber sicher gehen möchten, dass die übrigen Teile Ihres Computer keine schädlichen Dateien enthalten.
Festplatten scannen	Alle internen Festplatten auf Ihrem Computer auf Viren, Spyware und Riskware	Dabei werden alle Festplatten des Computers gescannt.Im Gegensatz zum schnellen Malware-Scan werden bei diesem Scantyp nicht nur gezielt die Teile Ihres Systems mit installierten Programmdateien durchsucht, sondern auch alle Datendateien wie Dokumente, Musik, Bilder und Videos. Diese Art des Scannens ist langsam und wird nur dann empfohlen, wenn der schnelle Malware-Scan keine Malware entdeckt hat, Sie aber sicher gehen möchten, dass die übrigen Teile Ihres Computer keine schädlichen Dateien enthalten.
Viren- und Spyware-Scanning	Teile Ihres Computers auf Viren, Spyware und Riskware	Diese Art des Scannens ist weitaus schneller als ein vollständiger Scan.Es werden nur die Teile Ihres Systems durchsucht, die installierte Programmdateien enthalten. Dieser Scantyp wird empfohlen, wenn Sie rasch überprüfen möchten, ob Ihr Computer sauber ist, da Sie mit dieser Funktion aktive Malware auf Ihrem Computer rasch entdecken können.
Rootkit-Scan	Wichtige Sytembereiche, wo verdächtige Elemente zu einem Sicherheitsproblem werden könnenScannt nach verborgenen Dateien, Ordnern, Laufwerken oder Prozessen	Wenn Sie vermuten, dass auf Ihrem Computer ein Rootkit installiert ist.Beispielsweise, wenn vor kurzem auf Ihrem Computer Malware entdeckt wurde und Sie sichergehen möchten, dass dabei kein Rootkit installiert wurde.

Malware automatisch bereinigen

Wenn während des Scannens *Malware* gefunden wird, kann das Progamm automatisch entscheiden, wie sie von Ihrem Computer entfernt wird. Oder Sie treffen diese Entscheidung für jedes Element selbst.

1. Wählen Sie eine Option aus:

Option	Was passieren soll
Automatisches Verfahren (empfohlen)	Das Programm entscheidet, wie die jeweilige *Malware* behandelt wird, um Ihren Computer automatisch zu bereinigen.

Option	Was passieren soll
Benutzer entscheidet abhängig vom jeweiligen Element	Das Programm fragt Sie bei jedem *Malware*-Element, wie Sie verfahren möchten.

2. Klicken Sie auf **Weiter**.
   - Wenn Sie **Automatisches Verfahren (empfohlen)** ausgewählt haben, wird ein Fenster mit den Ergebnissen der automatischen Malware-Behandlung angezeigt.

     Hinweis: Manche Malware-Elemente verfügen über den Status "Nicht verarbeitet". Das bedeutet, dass sich die infizierte Datei in einem Archiv befindet (z. B. einer ZIP-Datei) und nicht automatisch behandelt werden kann. Sie können die infizierte Datei löschen, indem Sie das Archiv öffnen und die Datei manuell entfernen. Wenn der Inhalt des Archivs nicht von Bedeutung ist, können Sie das gesamte Archiv löschen.

   - Wenn Sie **Benutzer entscheidet abhängig vom jeweiligen Element** ausgewählt haben, müssen Sie für jedes erkanntes Malware-Element eine Aktion angeben.
3. Klicken Sie auf **Fertig stellen**, um Scan-Assistent zu schließen.

Ergebnisse manueller Scans anzeigen

Nachdem der Scan abgeschlossen ist, können Sie einen Bericht der Scan-Ergebnisse anzeigen.

Hinweis: Sie sollten diesen Bericht anzeigen, da es sich bei der von Ihnen ausgewählten Aktion nicht immer um die durchgeführte Aktion handelt. Wenn Sie beispielsweise eine infizierte bereinigen, der *Virus* jedoch nicht aus ihr entfernt werden konnte, kann das Produkt auch eine andere Aktion für die Datei durchgeführt haben.

So zeigen Sie den Bericht an:

1. Klicken Sie auf **Bericht anzeigen**.

   Der Bericht enthält:
   - Die Anzahl gefundener *Malware*.
   - Der Typ der gefundenen *Malware* und Links zu Beschreibungen der *Malware* im Internet.
   - Die bei den einzelnen *Malware* -Elementen durchgeführten Aktionen.
   - Alle Elemente, die vom Scannen ausgeschlossen wurden.
   - Die Scanning Engines, die für die Überprüfung auf *Malware* verwendet wurden.

     Hinweis: Die Anzahl der gescannten Dateien kann unterschiedlich sein, je nachdem, ob Dateien in Archiven in den Scanvorgang einbezogen wurden. Wurden bereits archivierte Dateien gescannt, können sich die Scan-Ergebnisse im Cachespeicher befinden.
2. Klicken Sie auf **Fertig stellen**, um **Scan-Assistent** zu schließen.
3. Wählen Sie **Server-Schutz** > **Manuelles Scanning**, und öffnen Sie die Registerkarte **Status**.
4. Klicken Sie unter **Aufgaben** auf **Scan-Bericht anzeigen**.

   Hinweis: Im zentral verwalteten Modus wird der Scan-Bericht an F-Secure Policy Manager gesendet. Sie können ihn auch in der F-Secure Policy Manager-Konsole anzeigen.

Tipp: Sie können die Ergebnisse des letzten Scans auch anzeigen, indem Sie folgende Befehlsfolge wählen: **Einstellungen** > **Computer** > **Manuelles Scanning**. Klicken Sie dann auf **Letzten Scan-Bericht anzeigen**.

Zu festgelegten Zeiten scannen

Sie können Ihren Computer in regelmäßigen Abständen auf *Malware* überprüfen lassen, etwa täglich, wöchentlich oder monatlich.

Das Scannen nach *Malware* ist ein intensiver Prozess. Er beansprucht die volle Leistung Ihres Computers und nimmt geraume Zeit in Anspruch. Aus diesem Grund können Sie festlegen, dass das Programm Ihren Computer dann scannt, wenn Sie ihn nicht benutzen.

Planen von Scans

Konfigurieren Sie das Programm so, dass Ihr Computer in regelmäßigen Abständen gescannt wird.

So planen Sie einen Scan:

1. Klicken Sie auf der Hauptseite auf **Einstellungen**.
2. Wählen Sie **Computer** > **Geplantes Scanning**.
3. Wählen Sie **Server-Schutz** > **Geplantes Scanning**.
4. Wählen Sie **Geplantes Scanning einschalten**.
5. Wählen Sie die Tage aus, an denen nach *Viren* und *Spyware* gescannt werden soll.

Option	Beschreibung
Täglich	Um jeden Tag zu scannen.
Wöchentlich	Um an ausgewählten Wochentagen zu scannen. Wählen Sie rechts in der Liste die Tage aus, an denen gescannt werden soll.
Monatlich	So scannen Sie an bis zu drei Tagen pro Monat. Wählen Sie die Tage aus: 1. Wählen Sie eine Option für **Ta** aus. 2. Wählen Sie in der Liste neben dem ausgewählten Tag den Tag des Monats aus. 3. Wiederholen Sie diesen Schritt, wenn Sie an einem anderen Tag scannen möchten.

6. Wählen Sie aus, wann Sie den Scan an den ausgewählten Tagen starten möchten.

Option	Beschreibung
Startzeit	Der Zeitpunkt, an dem das Scannen gestartet wird. Wählen Sie einen Zeitpunkt aus, zu dem Sie den Computer voraussichtlich nicht verwenden.
Nachdem der Computer nicht benutzt wurde für	Wählen Sie eine Inaktivitätszeit aus, nach der mit dem Scannen begonnen werden soll, wenn der Computer nicht verwendet wird.

7. Klicken Sie auf **Übernehmen**.

Geplanten Scan abbrechen

Sie können einen geplanten Scan-Vorgang gegebenenfalls lokal abbrechen. Der geplante Scan-Vorgang wird dann zum nächsten geplanten Zeitpunkt ausgeführt.

Hinweis: Sie können einen geplanten Scan-Vorgang nicht über die Webkonsole abbrechen.

Geplante Scans können einen sich deutlich auf die Leistung Ihres Computers auswirken. So brechen Sie den geplanten Scan ab:

Hinweis: Im zentral verwalteten Modus können Sie einen geplanten Scan-Vorgang unter Umständen nicht abbrechen.

1. Klicken Sie auf den Link **Geplanter Scan wurde gestartet** im Benachrichtigungsfenster **Viren- und Spyware-Scan**.

   Das Benachrichtigungsfenster bleibt ca. 15 Sekunden lang geöffnet und verschwindet dann wieder. Wenn Sie den Link im Benachrichtigungsfenster nicht anklicken, können Sie den geplanten Scanvorgang nicht mehr abbrechen.
2. Klicken Sie auf den Link **Abbrechen** im Fenster **Viren- und Spyware-Scan**.
3. Klicken Sie auf den Link **Schließen** aus.

Der geplante Scan wurde abgebrochen. Der nächste geplante Scan wird wie gewohnt ausgeführt.

Ergebnisse geplanter Scans anzeigen

Sobald ein geplanter Scan fertiggestellt ist, können Sie überprüfen, ob *Malware* gefunden wurde.

So überprüfen Sie die Ergebnisse eines geplanten Scans:

1. Klicken Sie auf **Geplanter Scan fertiggestellt** im Benachrichtigungsfenster **Viren- und Spyware-Scan**.
2. Klicken Sie auf **Bericht anzeigen** , um anzuzeigen, was während des Scanvorgangs passiert ist.

   Hinweis: Wenn Sie das Dialogfeld über das Dialogfeld **Historie des Fensters** öffnen, ist die Schaltfläche **Bericht anzeigen** deaktiviert. Sie können die Ergebnisse früherer geplanter Scans nicht anzeigen.
3. Klicken Sie auf **Schließen** , um das Dialogfeld zu schließen.

Tipp: Sie können die Ergebnisse des letzten Scans auch anzeigen, indem Sie folgende Befehlsfolge wählen: **Einstellungen** > **Computer** > **Geplantes Scanning**. Klicken Sie anschließend auf **Letzten Scan-Bericht anzeigen**.

Tipp: Sie können die Ergebnisse des letzten Scans auch anzeigen, indem Sie **Server-Schutz** > **Geplantes Scanning** wählen. Klicken Sie anschließend auf **Letzten Scan-Bericht anzeigen**.

Hinweis: Im zentral verwalteten Modus wird der Scan-Bericht an F-Secure Policy Manager gesendet. Sie können ihn auch über die F-Secure Policy Manager-Konsole anzeigen.

Wo finde ich die Alarmmeldungen und Protokolldateien der Firewall?

Anhand der Alarmmeldungen und Protokolldateien der Firewall können Sie feststellen, wie die Netzwerkverbindungen Ihres Computers geschützt sind.

Firewall-Alarme anzeigen

Sie können eine Liste aller erzeugten Firewall-Alarme anzeigen.

Die Liste enthält Alarme, die von der Firewall und dem Schutz gegen Eindringlinge ausgelöst wurden.

So zeigen Sie die Liste an:

1. Klicken Sie auf der Hauptseite auf **Einstellungen**.
2. Wählen Sie **Netzwerkverbindungen** > **Firewall**.
3. Klicken Sie auf die Registerkarte **Regeln**.
4. Klicken Sie auf **Alarmprotokoll anzeigen**.
   Das Dialogfeld **Firewall-Alarme** wird geöffnet und zeigt folgende Informationen an:

Feld	Beschreibung
Zeit	Zeitpunkt des Alarms.
Remote-Adresse	*IP-Adresse* des Computers, von dem Datenverkehr empfangen wurde bzw. an den Datenverkehr gesendet wurde.
Treffer	Zeigt, wie oft ein ähnlicher Alarm erzeugt wurde.
Beschreibung	Ein Alarmtext, der für die *Firewallregel* hinzugefügt wurde. Wenn der Alarm wegen eines Eindringungsversuchs ausgelöst wurde, enthält das Feld eine Information über das *Muster* des Eindringungsversuchs.

5. Um Alarmdetails anzuzeigen, wählen Sie den Alarm aus und klicken Sie auf **Details**.
6. Um zum vorherigen oder zum nächsten Alarm zu gelangen, klicken Sie auf die Schaltfläche **Zurück** oder **Weiter**.
7. Klicken Sie nach der Ansicht der Details auf **Schließen**, um das Dialogfeld mit den Details der **Firewall-Alarme** zu schließen.
8. Klicken Sie auf **Schließen**, um das Dialogfeld mit der Liste der **Firewall-Alarme** zu schließen.

Informationen in den Alarmmeldungen der Firewall

Die Alarmmeldungen der Firewall enthalten Informationen über den Datenverkehr, der die Meldung ausgelöst hat.

Eine Alarmmeldung der Firewall enthält die folgenden Informationen:

Feld	Beschreibung
Beschreibung	Ein Alarmtext, der für die *Firewallregel* hinzugefügt wurde. Wenn der Alarm durch einen Eindringungsversuch ausgelöst wurde, zeigt der Alarm Informationen über das *Muster* des Eindringungsversuchs an.
Aktion	Zeigt, was passiert ist, z. B., dass die *Firewall* den Datenverkehr blockiert oder zugelassen hat.
Zeit	Das Datum und den Zeitpunkt, zu dem der Alarm generiert wurde.
Richtung	Zeigt, ob der Datenverkehr eingehend oder ausgehend ist (von einem Remote-Computer an Ihren Computer oder umgekehrt).
Protokoll	Das verwendete *IP-Protokoll*.
Dienste	Zeigt die *Firewalldienste*, mit denen der Datenverkehr übereinstimmte.
Remote-Adresse	Die *IP-Adresse* des Remote-Computers.
Remote-Port	Der *Port* auf dem Remote-Computer.
Lokale Adresse	Die *IP-Adresse* Ihres eigenen Computers.

Feld	Beschreibung
Lokaler Port	Der *Port* auf Ihrem eigenen Computer.

Aktionsprotokoll anzeigen

Wenn ein Programm, beispielsweise ein Netzwerkspiel, nicht funktioniert, können Sie im Aktionsprotokoll prüfen, ob die Anwendungssteuerung das Programm daran gehindert hat, eine Internetverbindung herzustellen.

Das *Aktionsprotokoll* ist eine Textdatei (`action.log`) die automatisch Daten über die Netzwerkverbindungen erfasst. Die Maximalgröße der Datei beträgt 10 MB. Sobald die Datei voll ist, werden die alten Protokolleinträge gelöscht.

So zeigen Sie das *Aktionsprotokoll* an:

1. Klicken Sie auf der Hauptseite auf **Einstellungen**.
2. Wählen Sie **Netzwerkverbindung** > **Protokollfunktion**.
3. Klicken Sie auf **Aktionsprotokoll anzeigen**.

Das *Aktionsprotokoll* wird im standardmäßigen Texteditor oder in einem Anzeigeprogramm wie z. B. Notepad geöffnet.

Datenverkehr im Netzwerk mit Paketprotokollierung überwachen

Sie können bei Bedarf die Paketprotokollierung starten, um Informationen über den *IP*-Datenverkehr im Netzwerk aufzuzeichnen.

Wie funktioniert die Paketprotokollierung?

Das Paketprotokoll sammlet Informationen zum IP-Netzwerkdatenverkehr.

Standardmäßig ist die Paketprotokollierung ausgeschaltet. Die Paketprotokollierung richtet sich in erster Linie an erfahrene Benutzer, die mit Computernetzwerken vertraut sind.

Sie können die Paketprotokollierung wieder einschalten, wenn Sie Ihre eigenen *Firewallregeln* erstellt haben und überprüfen wollen, wie diese den Datenverkehr blockieren. Sie können dies auch tun, wenn Sie schädliche Netzwerkaktivitäten vermuten.

Die Informationen werden in 10 Dateien gesammelt (`packetlog.0-packetlog.9`). Jedes Mal, wenn Sie die Protokollierung einschalten, wird das *Paketprotokoll* in einer neuen Datei gespeichert. Wenn die zehnte Datei voll ist, wird das Protokoll wieder in der ersten Datei gespeichert. So können Sie sich die vorhergehenden Protokolle ansehen, während ein neues Protokoll erstellt wird.

Zusätzlich zum *IP*-Datenverkehr sammelt das *Paketprotokoll* auch Informationen über andere Typen von Netzwerkdatenverkehr, z. B. über die *Protokolle*, die Ihr *lokales Netzwerk* (LAN) benötigt. Zu diesen Informationen gehören z. B. die *Routing*-Daten.

Das *Paketprotokoll* ist im *Hexadezimal*-Format und unterstützt das *tcpdump*-Format. So können Sie die *Protokoll*dateien auch in einem Programm für die *Paketprotokoll*ierung öffnen, das nicht ihr standardmäßiger Viewer für das Paketprotokoll ist. Sie können außerdem ein Programm zur Netzwerk-Protokoll-Analyse verwenden, um die Inhalte weiter zu analysieren.

Paketprotokollierung starten

Wenn Sie den Verdacht haben, dass bösartige Netzwerkaktivitäten stattfinden, oder wenn z. B. ein Netzwerkspiel nicht mehr funktioniert, können Sie die Paketprotokollierung starten.

So starten Sie die Protokollierung:

1. Klicken Sie auf der Hauptseite auf **Einstellungen**.
2. Wählen Sie **Netzwerkverbindung** > **Protokollfunktion**.

3. Verwenden Sie die vorgeschlagenen Werte für die **Protokollzeit** und die Dateigröße der Felder Protokollzeit und **Maximalgröße der Protokolldatei** und geben Sie die Werte in die Felder Typ und Code ein. Wenn Sie möchten, können Sie die Werte auch ändern.
4. Klicken Sie auf **Protokollierung starten**. Zur Liste der Protokolldateien wird eine neue Datei hinzugefügt. Die Größe der Datei steigt an, je mehr Informationen gesammelt werden. Wenn die Liste bereits 10 Protokolldateien enthält, wird das nächste Protokoll in eine vorhandene Datei geschrieben.
5. Um die Protokollierung manuell zu stoppen, klicken Sie auf **Protokollierung starten**. Die Protokollierung wird automatisch nach Ablauf der vorgegebenen Protokollzeit beendet bzw. wenn die Maximalgröße der Protokolldatei erreicht ist.

Eine neue Protokolldatei wird erzeugt und zur Liste der Protokolldateien hinzugefügt.

Paketprotokoll anzeigen

Nachdem Sie ein *Paketprotokoll* erstellt haben, können Sie es öffnen und anzeigen.

So zeigen Sie das *Paketprotokoll* an:

1. Klicken Sie auf der Hauptseite auf **Einstellungen**.
2. Wählen Sie **Netzwerkverbindung** > **Protokollfunktion**.
3. Wählen Sie das *Paketprotokoll* aus, das Sie anzeigen möchten, und klicken Sie auf **Details**.
   Der standardmäßige *Paketprotokoll*-Viewer wird geöffnet. Im oberen Fensterbereich werden alle protokollierten Verbindungen angezeigt.

Sie können folgende Informationen anzeigen:

Feld	Beschreibung
Zeit	Zeit in Sekunden seit dem Beginn der Protokollierung. Wenn die definierte Protokollierungszeit 60 Sekunden beträgt, liegt die Startzeit für das erste *Paket* nahe bei 0 Sekunden und die Startzeit für das letzte *Paket* nahe bei 60 Sekunden.
Verwerfen (Verz.)	Zeigt, ob die *Firewall* das *Paket* durchgelassen oder verworfen hat, und zeigt die Richtung des *Pakets*: • **Nein**: hat das *Paket* zugelassen. • **Ja**: hat das *Paket* verworfen. • **Eingehend**: eingehendes *Paket*. • **Ausgehend**: ausgehendes *Paket*. Diese Informationen sind nicht verfügbar, wenn Sie die Datei in einem anderen Paketprotokollierungsprogramm anzeigen als dem standardmäßigen *Paketprotokoll*-Viewer.
Protokoll	Das verwendete *IP-Protokoll*.
Ursprung	Ursprungs- *IP-Adresse* des *Pakets*.
Ziel	Ziel- *IP-Adresse* des *Pakets*.
ID	*IPPaket*-Kopfzeileninformationen: Kennung des Pakets.
TTL	*IPPaket*-Kopfzeileninformationen: Der Wert *Lebensdauer* des *Pakets* definiert die Anzahl der Netzwerkgeräte, die das *Paket* durchlaufen kann, bevor es abgeworfen wird.

Feld	Beschreibung
Len	*IPPaket* Header-Informationen: Gesamtlänge des *Pakets*.
Beschreibung	Beschreibung des *Pakets*.

Im rechten Fensterbereich werden die Datenverkehrstypen und die zugehörigen Definitionen angezeigt.

Im unteren Fensterbereich werden die Informationen in den Formaten *Hexadezimal* und *ASCII* angezeigt.

Wenn Sie alle Arten von Netzwerkverkehr anzeigen möchten (und nicht nur *IP*-Datenverkehr), müssen Sie das Kontrollkästchen **Nicht-IP-Datenverkehr filtern** deaktivieren.

Manuelles Herstellen einer Verbindung mit Policy Manager und Importieren einer Richtliniendatei

Wenn Sie manuell eine Verbindung zwischen dem lokalen Host und Policy Manager Server herstellen müssen, können Sie wie folgt vorgehen:

1. Öffnen Sie auf dem lokalen Host die Seite **Zentrale Verwaltung**, wo Datum und Uhrzeit der letzten Verbindung mit Policy Manager Server angezeigt werden.
2. Klicken Sie auf **Jetzt prüfen**, um eine neue Verbindung herzustellen.
   Wenn Sie eine neue Richtlinie manuell auf einen Host importieren müssen, müssen Sie zunächst eine Host-spezifische Richtlinie Policy Manager Console exportieren und diese anschließend auf den Host importieren. Gehen Sie hierzu wie folgt vor:
3. In Policy Manager Console:
   a) Wählen Sie auf der Registerkarte **Richtliniendomänen** den entsprechenden Host.
   b) Klicken Sie mit der rechten Maustaste auf den ausgewählten Host, und wählen Sie im Kontextmenü den Befehl **Host-Richtliniendatei exportieren**.
   c) Speichern Sie die Richtliniendatei auf einem Übertragungsmedium, z.B. auf einer Diskette.
4. Auf der lokalen Benutzeroberfläche von Client Security:
   a) Klicken Sie auf **Richtlinie manuell importieren**.
   b) Daraufhin wird ein Fenster angezeigt, in dem Sie nach der Datei `Policy.bpf` suchen können, die auf den Host importiert werden soll.

   Der Import einer Richtliniendatei ist vor allem für die Fehlerbehebung gedacht. Im Normalbetrieb werden Richtliniendateien stets automatisch übertragen. Mit den Vorgängen zum Import und Export einer Richtliniendatei kann die Verbindung zu Policy Manager wiederhergestellt werden, wenn die Verbindung zum verwalteten Host aufgrund einer falsch konfigurierten Richtlinie unterbrochen wurde.

Aussetzen von Downloads und Updates

Sie können Benutzern erlauben, die Netzwerkkommunikation vorübergehend auszusetzen, wenn z.B. gelegentlich eine DFÜ-Verbindung verwendet wird.

Diese Option wird über Policy Manager Console konfiguriert. Sie eignet sich für Hosts, die ab und zu eine langsame DFÜ-Verbindung nutzen. Über diese Option wird festgelegt, ob ein Benutzer die Netzwerkkommunikation, z.B. den automatischen Abruf von Richtlinien, den Versand von statistischen Daten und die automatische Update-Funktion, vorübergehend aussetzen darf.

1. Wählen Sie auf der Registerkarte **Richtliniendomänen** den entsprechenden Host.
2. Öffnen Sie die Registerkarte **Einstellungen**, und wählen Sie **Zentrale Verwaltung**.
3. Wählen Sie**Benutzer dürfen Downloads und Updates vorübergehend aussetzen**.
4. Klicken Sie auf , um die Richtlinie zu verteilen.

Benutzern erlauben, F-Secure-Produkte aus dem Speicher zu entfernen

Sie können Benutzern erlauben, Produkte aus dem Speicher zu entfernen, um zum Beispiel Arbeitsspeicher freizugeben.

Diese Option wird über Policy Manager Console konfiguriert. Hiermit wird festgelegt, ob der Benutzer alle F-Secure-Produkte vorübergehend aus dem Speicher entfernen darf, um z.B. Arbeitsspeicher für speicherintensive Programme wie Spiele oder ähnliche Anwendungen freizugeben.

Hinweis: Beachten Sie, dass die Hauptfunktionen der Produkte deaktiviert sind, solange die Produkte nicht geladen sind und dass der Computer während dieser Zeit nicht vor Viren oder Angriffen geschützt ist.

1. Wählen Sie auf der Registerkarte **Richtliniendomänen** den entsprechenden Host.
2. Öffnen Sie die Registerkarte **Einstellungen**, und wählen Sie **Zentrale Verwaltung**.
3. Wählen Sie eine Option aus der Dropdown-Liste **Benutzer dürfen Produkte aus dem Speicher entfernen**.
4. Klicken Sie auf , um die Richtlinie zu verteilen.

Kapitel
10

Vireninformationen

Themen:

- *Malware-Informationen und Tools auf den F-Secure-Webseiten*
- *Richtlinien für den Versand von Virenproben an F-Secure*
- *Vorgehensweise bei einem Virusausbruch*

Dieser Abschnitt enthält allgemeine, hilfreiche Informationen über Viren und deren Handhabung.

Hier finden Sie Informationen darüber, wie Sie Viren aufspüren und mit erkannten Viren umgehen.

Malware-Informationen und Tools auf den F-Secure-Webseiten

Unter folgendem Link finden Sie eine Liste mit Informationsquellen zu Malware und hilfreiche Tools: http://www.f-secure.com/security_center/.

Informationen zu den neuesten Sicherheitsbedrohungen finden Sie in folgenden Quellen:

- F-Secure-Blog: *http://www.f-secure.com/weblog/*
- Eine Liste von Sicherheitslücken gängiger Software befindet sich unter folgendem Link: *http://www.f-secure.com/vulnerabilities/*
- Sie können sich über die neuesten Bedrohungen auch über Client Security per F-Secure-Newsletter informieren.

Bevor Sie uns eine Probe zusenden, sollten Sie **RescueCD** verwenden. Hierbei handelt es sich um ein Tool, das sein eigenes Betriebssystem startet und auf diese Weise Malware finden kann, die unter Windows nicht erkannt wird. Sie finden RescueCD im Sicherheits-Center: *http://www.f-secure.com/security_center/*.

Anweisungen zur Verwendung von **RescueCD** sind in der heruntergeladenen Datei enthalten.

Richtlinien für den Versand von Virenproben an F-Secure

Dieser Abschnitt enthält Informationen zum Senden einer Virenprobe an das F-Secure Security Lab.

Hinweis: Dieser Abschnitt richtet sich an erfahrene Benutzer.

Bitte senden Sie uns eine ausführliche Beschreibung des Problems, die Symptome und Fragen nach Möglichkeit in englischer Sprache zu.

Normalerweise antworten wir innerhalb von 24 Stunden. Bei komplizierten Fällen benötigen wir unter Umständen aufgrund des größeren Rechercheaufwands mehr Zeit. Sollten Sie nicht innerhalb weniger Werktage eine Antwort von uns erhalten, übermitteln Sie Ihre Probe erneut.

Versandrichtlinien für Virenproben

Dateien müssen im ZIP-Format eingeschickt werden.

Zum Komprimieren Ihrer Virenprobe können Sie die Demoversion von WinZip verwenden, die Sie unter *http://www.winzip.com/* herunterladen können. Ein weiteres kostenloses Dienstprogramm, InfoZIP, finden Sie unter *http://www.info-zip.org/pub/infozip/*.

Zur Benennung von ZIP-Paketen dürfen ausschließlich englische Buchstaben und/oder Zahlen verwendet werden. Lange Dateinamen sind zulässig.

Um sicherzustellen, dass wir das ZIP-Archiv erhalten, schützen Sie die ZIP-Datei mit dem Passwort `infected`. Anderenfalls werden von Ihnen an uns gesendete Malware-Proben möglicherweise als Sicherheitsmaßnahme von einem zwischengeschalteten Server entfernt. Passwortgeschützte (verschlüsselte) Archivdateien können jedoch nicht gescannt werden und sollten als sicher eingestuft werden. Weitere Anweisungen zum Versand einer Virenprobe finden Sie unter diesem Link: *http://support.f-secure.com/enu/home/virusproblem/samples/index.shtml*.

Benötigte Dateien

Hie wird erläutert, welche Dateien und Informationen Sie senden müssen. Da Viren sehr individuell sind, gibt es keine Standardversandmethode.

Nachfolgend finden Sie eine Auflistung der Dateien, die für spezielle Virentypen erforderlich sind:

1. Trojaner und andere Stand-alone-Malware (schädliche Programme):

   Wenn Sie eine Probe einer verdächtigen Stand-alone-Malware (Wurm, Backdoor, Trojaner, Dropper) versenden, geben Sie an, wo sich die Datei im infizierten System befindet und wie sie gestartet wurde (Registrierungsdatenbank, `.ini`-Dateien, `Autoexec.bat`etc.). Eine Beschreibung der Dateiquelle ist ebenfalls nützlich.

2. Fehlalarm von einem unserer Anti-Virus-Programme:

   Wenn durch Client Security ein Virus nicht erkannt oder fälschlicherweise erkannt bzw. ein Fehlalarm ausgelöst wurde, senden Sie uns möglichst folgende Informationen:

   - die betroffene Datei,
   - die Client Security-Versionsnummer,
   - das Datum des letzten Updates der Virendefinitionsdatenbank,
   - eine Beschreibung der Systemkonfiguration,
   - eine Beschreibung, wie das Problem zu reproduzieren ist, und
   - die Scan-Berichtsdatei von Client Security. Anweisungen zum Speichern der Datei finden Sie unter: *http://support.f-secure.com/enu/home/virusproblem/samples/index.shtml*.

3. Neue Viren oder Trojaner:

   Wenn Sie vermuten, dass Ihr Computer durch einen unbekannten Schädling infiziert ist, der vom Virenschutzprogramm nicht festgestellt wurde, senden Sie uns bitte Folgendes:

   - Den Bericht **msinfo32**, wenn Sie Windows XP verwenden. So erstellen Sie den Bericht.

     1. Wählen Sie **Start** > **Ausführen...**.
     2. Geben Sie `msinfo32` ein, und klicken Sie auf **OK**.
     3. Zeigen Sie den Knoten **Systemübersicht** an, und wählen Sie **Datei** > **Speichern**.

   - Einige Windows-Konfigurationsdateien (`WIN.INI`, `SYSTEM.INI`) und DOS-Konfigurationsdateien (`Autoexec.bat`, `Config.sys`)
   - Vollständigen oder teilweisen Export aus der Systemregistrierung (unter Verwendung des Dienstprogramms **Regedit**, über das alle Windows-Versionen verfügen)
   - den Inhalt des Ordners `\Start Menu\Programs\Startup\`

4. Viren, die ausführbare Dateien infizieren:

   Senden Sie uns möglichst unterschiedliche infizierte Dateien vom System. Drei bis fünf unterschiedliche Proben sind gewöhnlich ausreichend. Falls möglich, fügen Sie auch saubere Kopien derselben Dateien (die Sie z. B. Ihrer Datensicherung entnehmen) bei. Verwenden Sie dafür in der ZIP-Datei zwei Verzeichnisse. Beispiel:

   `ORIGINAL\APPEND.EXE`

   `ORIGINAL\COMMAND.COM`

   `INFECTED\APPEND.EXE`

   `INFECTED\COMMAND.COM`

5. Makroviren:

   Senden Sie neben den infizierten `DOC`-Dateien auch eine infizierte Kopie der Datei `NORMAL.DOT` (globale Vorlage). Schicken Sie im Falle von Excel-Viren neben den infizierten `XLS`-Dateien auch die Datei `PERSONAL.XLS` (falls vorhanden). Sollten aufgrund des Makrovirus auch andere Dateitypen in Mitleidenschaft gezogen worden sein, senden Sie ein Beispiel jeder Dateiart.

6. Boot-Sektor-Viren:

   Sollte die Infektion auf der Festplatte eingetreten sein, verwenden Sie das GetMBR-Dienstprogramm zum Zusammenstellen von Boot-Sektor-Proben. Wenn das Skript fertiggestellt ist, senden Sie uns die Datei

`mbr.dmp` wie in diesem Kapitel beschrieben. **GetMBR** können Sie von unserer FTP-Site herunterladen: *ftp://ftp.f-secure.com/anti-virus/tools/getmbr.zip*.

Befindet sich die Infektion auf einer Diskette, erstellen Sie ein DCF-Image der infizierten Diskette, und senden Sie uns die `DCF`-Image-Datei zu. Das DCF-Dienstprogramm können Sie von unserer FTP-Site herunterladen: *ftp://ftp.f-secure.com/anti-virus/tools/dcf53.zip*.

Sie können die infizierte Diskette auch per Post an unsere Niederlassung in Helsinki senden (Adresse siehe unten). Fügen Sie eine Beschreibung des Problems bei. Wir weisen darauf hin, dass wir keine Disketten an den Absender zurückschicken.

7. Infektion oder Fehlalarm auf einer CD:

   Ist eine Infektion oder ein Fehlalarm auf einer CD aufgetreten, können Sie die CD an unsere finnische Niederlassung schicken.

   Bitte legen Sie eine Beschreibung des Problems sowie möglichst den ausgedruckten Bericht von Client Security bei. Sollte auf der CD keine Infektion feststellbar sein, senden wir die CD an Sie zurück.

Versandrichtlinien für Virenproben

Im Folgenden werden die verschiedenen Möglichkeiten näher erläutert, wie Sie uns Virenproben senden können.

Sie haben drei Möglichkeiten, uns Proben zu senden.

- Am häufigsten wird unser Webformular zur Übermittlung von Proben verwendet. Diesem Webformular können Sie sämtliche Informationen entnehmen, die Sie uns zukommen lassen müssen, damit wir die Probe verarbeiten können. Sie finden das Webformular unter: *http://www.f-secure.com/samples*.
- Wenn die Probe größer als 5 MB ist, müssen Sie sie auf unsere FTP-Site hochladen: *ftp://ftp.f-secure.com/incoming/*.
- Befindet sich die Probe auf einem physischen Datenträger, beispielsweise einer CD, DVD oder einem USB-Laufwerk, können Sie diesen physischen Datenträger an folgende Adresse senden:

  Security Labs

  F-Secure Corporation

  Tammasaarenkatu 7

  PL 24

  00181 Helsinki

  Finnland

Vorgehensweise bei einem Virusausbruch

Sie können diese Checkliste mit Maßnahmen und Aufgaben heranziehen, die bei einem Virusausbruch im Firmennetzwerk ausgeführt werden sollten.

1. Trenen Sie den infizierten Computer sofort vom Netzwerk.

   Wenn sich die Infektion weiterverbreitet, sollten Sie ohne Verzögerung das gesamte Netzwerk herunterfahren. Der gesamte ausgehende Datenverkehr sollte blockiert werden. Die Mitarbeiter müssen angewiesen werden, verdächtige Aktivitäten auf ihren Computern sofort zu melden.

2. Versuchen Sie festzustellen, ob es sich um eine tatsächliche Infektion oder um einen möglichen Fehlalarm handelt.

   Scannen Sie den Computer mit der aktuellen Version von Client Security und den aktuellen Virendefinitionen. Wird die Infektion richtig erkannt, gehen Sie zum nächsten Schritt über. Wird die Infektion

identifiziert als`möglicher neuer Virus`,`könnte ein Image eines Bootsektorvirus sein`und so weiter. Senden Sie eine Probe mitClient SecurityScan-Bericht über**Malware-Probe einreichen**Webtool an: *http://www.f-secure.com/samples*.

3. Wenn es sich um eine bekannte Infektion handelt, öffnen Sie die Virusinformationsseiten von F-Secure, und lesen Sie eine Beschreibung des Schädlings.

   Laden Sie (falls verfügbar) ein Dienstprogramm zum Desinfizieren herunter, und drucken Sie die beiliegende Anleitung aus. Wenn Sie Hilfe bei der Beseitigung benötigen, wenden Sie sich über unsere Support-Webseite an den Support: *http://support.f-secure.com*.

   Vermerken Sie in dringenden Fällen, dass Sie sehr schnell eine Antwort benötigen.

4. Wenn es sich um ein neues Virus handelt, versuchen Sie, eine Probe ausfindig zu machen, uns senden Sie sie über das Webformular zur Übermittlung von Proben an F-Secure Security Labs: *http://www.f-secure.com/samples*.

   Geben Sie so viele problembezogene Informationen wie möglich an. Es ist wichtig zu wissen, wie viele Computer mit dem Virus infiziert wurden.

5. Wenn ein Computer mit einem Schädling infiziert ist, der sich im lokalen Netzwerk ausbreitet, sollten Sie das Netzwerk herunterfahren, bis alle infizierten Computer desinfiziert wurden.

   Erst nachdem alle Computer desinfiziert wurden, kann das Netzwerk wieder in Betrieb genommen werden. Sonst besteht die Gefahr, dass ein einzelner Rechner innerhalb von Minuten das gesamte Netzwerk erneut infiziert.

6. Warten Sie, bis Sie einen Bericht von Security Labs erhalten, und befolgen Sie die angegeben Anweisungen zur Beseitigung genau.

   Es ist empfehlenswert, vor einer Desinfizierung eine Sicherung aller wichtigen Daten anzufertigen. Diese Sicherung sollte nicht über das Netzwerk erstellt werden. Verwenden Sie stattdessen ein externes Backup-Gerät. Sichern Sie nur Datendateien, keine Programmdateien. Wenn Sie zu einem späteren Zeitpunkt die Daten aus der Sicherung wiederherstellen, sollten Sie alle wiederhergestellten Daten auf Viren überprüfen.

7. Wenn eine Desinfizierungslösung bereitgestellt wird, sollten Sie die Lösung zunächst auf einem Computer testen. Wenn das funktioniert, können Sie die Lösung auf allen infizierten Computern ausführen.

   Scannen Sie die bereinigten Computer mit Client Security und den aktuellsten Virendefinitionen, um sicherzustellen, dass keine infizierten Dateien zurückgeblieben sind.

8. Sie sollten das Netzwerk erst wieder aktivieren, nachdem alle infizierten Computer vollständig desinfiziert wurden.

   Wenn der Schädling Backdoor-Komponenten enthält oder in der Lage ist, Daten zu stehlen, sollten Sie unbedingt die Passwörter und Anmeldenamen für alle Netzwerkressourcen ändern.

9. Informieren Sie die Mitarbeiter über den Virenausbruch, und warnen Sie sie davor, unbekannte Dateianlagen zu öffnen oder verdächtige Seiten im Internet zu besuchen.

   Überprüfen Sie die Sicherheitseinstellungen der auf den Arbeitsstationen installierten Software. Vergewissern Sie sich, dass die E-Mail-Scanner und Firewalls auf den Servern ordnungsgemäß funktionieren. Client Security sollte automatisch Updates empfangen, es wird jedoch empfohlen, in regelmäßigen Abständen zu überprüfen, ob diese automatischen Updates ordnungsgemäß heruntergeladen werden.

10. Informieren Sie Ihre Geschäftspartner über den Ausbruch, und empfehlen Sie ihnen, ihre Computer mit Client Security und dem neuesten Virendefinitions-Update zu scannen, um sicherzustellen, dass sich die Infektion nicht über Ihr Netzwerk hinaus verbreitet.

Kapitel

11

Einrichten des Cisco NAC-Plugins

Themen:

- *Installieren des Cisco NAC-Plugins*
- *Importieren der Posture Validation-Attributdefinitionen*
- *Verwenden von Attributen für Posture Token der Anwendung*

In diesem Abschnitt erhalten Sie einen Überblick über das Cisco NAC-Plugin.

F-Secure ist Teilnehmer der von Cisco Systems® geleiteten Network Admission Control (NAC)-Initiative. NAC schränkt den Netzwerkzugriff für Hosts mit veralteten Virendefinitionsdatenbanken bzw. mit deaktivierter Anti-Virus-Software oder Firewall ein.

Das F-Secure NAC-Plugin kommuniziert mit Cisco® Trust Agent (CTA), einer Clientsoftware auf den Hosts, die sicherheitsrelevante Informationen vom Host abruft und an den Cisco Secure Access Control Server (ACS) weiterleitet. Auf Grundlage dieser Daten wird dem Host eine passende Zugriffsrichtlinie zugewiesen

Weitere Informationen über NAC finden Sie unter *http://www.cisco.com/go/nac/*.

Das Installationspaket für Client Security enthält eine Option zur Installation des Cisco NAC-Plugins. Wenn Sie diese Option auswählen, muss CTA bereits auf dem Host installiert sein. Außerdem muss für den ACS-Server die Überwachung der F-Secure-Sicherheitsattribute konfiguriert werden.

Installieren des Cisco NAC-Plugins

Das Cisco NAC-Plugin kann sowohl lokal als auch remote auf den Hosts installiert werden.

1. Lokale Installationen: Wenn Sie Client Security lokal installieren, wählen Sie im Dialogfeld **Zu installierende Komponenten** die Option **Cisco NAC Plugin**.
2. Remote-Installationen: Wenn Sie Client Security remote installieren, wählen Sie im Dialogfeld **Zu installierende Komponenten** die Option **Cisco NAC Plugin**.

   Hinweis: Weitere Informationen finden Sie in der Dokumentation zu Cisco NAC.

Importieren der Posture Validation-Attributdefinitionen

Der Posture Validation-Attributdefinitionsdatei von Cisco Secure ACS müssen die Posture Validation-Attributdefinitionen der F-Secure-Produkte hinzugefügt werden.

1. Verwenden Sie dazu das Programm **CSUtil** auf dem Cisco Secure ACS-Server.
2. Geben Sie den folgenden Befehl ein:

   ```
   CSUtil.exe -addAVP fsnacpva.def
   ```

   Die Datei `fsnacpva.def` befindet sich im Installationspaket des Produkts.

   Hinweis: Weitere Informationen über **CSUtil** finden Sie in der Dokumentation zu Cisco ACS.

Verwenden von Attributen für Posture Token der Anwendung

Mit folgenden Schritte konfigurieren Sie den Cisco ACS-Server so, dass er die Sicherheitsattribute des Programms überwacht.

Führen Sie die folgenden Schritte aus, um den Cisco ACS-Server so zu konfigurieren, dass er die Sicherheitsattribute von F-Secure-Produkten überwacht:

1. Klicken Sie auf der Benutzeroberfläche des Cisco ACS-Servers auf die Schaltfläche **Externe Benutzerdatenbanken**.
   Die Seite **Externe Benutzerdatenbanken** wird geöffnet.
2. Klicken Sie auf **Datenbankkonfiguration**.
   Die Seite **Externe Benutzerdatenbanken konfigurieren** wird geöffnet.
3. Klicken Sie auf **Network Admission Control**.
4. Klicken Sie auf **Konfigurieren**.
5. Wählen Sie die Option **Neue lokale Richtlinie erstellen**.
6. In den Regeln für die *Posture Tokens der Anwendung* können Sie folgende Attribute von Client Security verwenden:

   - Posture Validation-Attribute für Anti-Virus:

Attribut-Name	Typ	Beispiel
Software-Name	Zeichenfolge	`F-Secure Anti-Virus`
Software-Version	Version	`8.0.0.0`

Attribut-Name	Typ	Beispiel
Dat-Date	date	`[Datum der Datenbank]`
Schutz aktiviert	Unsignierte Ganzzahl	`1=aktiviert`, `0`=deaktiviert

- Posture Validation-Attribute für Firewall:

Attribut-Name	Typ	Beispiel
Software-Name	Zeichenfolge	`F-Secure Internet Shield`
Software-Version	Version	`8.0.0.0`
Schutz aktiviert	Unsignierte Ganzzahl	`1`=aktiviert, `0`=deaktiviert

Kapitel

12

Erweiterte Funktionen: Viren- und Spyware-Schutz

Themen:

- *Konfigurieren geplanter Scan-Vorgänge*
- *Erweiterte Einstellungen von DeepGuard*
- *Konfigurieren von Policy Manager Proxy*
- *Konfigurieren automatischer Updates der Hosts vom Policy Manager Proxy*
- *Ausschließen von Anwendungen für den Web Traffic Scanner*

Hier finden Sie Informationen über erweiterte Viren- und Spyware-Schutz-Funktionen.

Dieser Abschnitt enthält Anweisungen zu einigen erweiterten Verwaltungsaufgaben, die den Virenschutz betreffen, wie die Konfiguration geplanter Scan-Vorgänge über die Benutzeroberfläche für den **erweiterten Modus** oder das Festlegen eines Anti-Virus-Proxy-Servers.

Konfigurieren geplanter Scan-Vorgänge

Sie können mit der Benutzeroberfläche für den **erweiterten Modus** einen Zeitplan für Scan-Vorgänge hinzufügen.

In diesem Beispiel wird ein geplanter Scan-Vorgang in einer Richtlinie für die gesamte Richtliniendomäne hinzugefügt. Die Überprüfung soll ab dem 25. August 2009 wöchentlich jeden Montag um 20 Uhr ausgeführt werden.

1. Wählen Sie aus dem Menü **Ansicht** > **Erweiterter Modus**.
   Die Benutzeroberfläche für den **Erweiterten Modus** wird geöffnet.
2. Wählen Sie auf der Registerkarte **Richtliniendomänen** den Eintrag **Stamm**.
3. Wählen Sie auf der Registerkarte **Richtlinie F-Secure** > **F-Secure Anti-Virus** > **Einstellungen** > **Planer** > **Aufgabenplanung** aus.
   Die aktuell eingerichteten geplanten Aufgaben werden in der Tabelle **Aufgabenplanung** angezeigt. Sie können nun geplantes Scannen als neue Aufgabe hinzufügen.
4. Klicken Sie auf **Hinzufügen**.
   Hierdurch wird der Tabelle **Aufgabenplanung** eine neue Zeile hinzugefügt.
5. Klicken Sie in der gerade erstellten Zeile auf die Zelle **Name** und anschließend auf **Bearbeiten**.
6. Die Zelle **Name** wird daraufhin aktiviert und Sie können einen Namen für die Aufgabe eingeben.

   Beispielsweise `Scan-Zeitplan für alle Hosts`.
7. Klicken Sie als Nächstes auf die Zelle **Planungsparameter** und dann auf **Bearbeiten**.
8. Sie können jetzt die Parameter für die geplante Überprüfung eingeben.

   Eine geplante Überprüfung soll ab dem 25. August 2009 wöchentlich jeden Montag um 20 Uhr ausgeführt werden. Geben Sie dafür die folgenden Werte ein: `/t20:00 /b2009-08-25 /rweekly`

   Hinweis: Wenn Sie die Zelle **Planungsparameter** auswählen, werden die zulässigen Parameter mit den entsprechenden Formaten als Hilfetext im Fensterbereich **Meldungen** (unter der Tabelle **Aufgabenplanung**) angezeigt.
9. Klicken Sie auf die Zelle **Aufgabentyp**, um den Aufgabentyp auszuwählen, und klicken Sie anschließend auf **Bearbeiten**.
10. Daraufhin öffnet sich eine Dropdown-Liste, aus der Sie die Option **Lokale Festplatten scannen** auswählen. Damit haben Sie die Definition der Scan-Aufgabe abgeschlossen und können diese nun an die Benutzer verteilen.
11. Klicken Sie auf , um die Richtlinie zu verteilen.

Ausführen geplanter Scan-Vorgänge an definierten Wochentagen oder Tagen im Monat:

Wenn Sie eine wöchentliche geplante Überprüfung konfigurieren möchten, können Sie auch feste Wochentage angeben, an denen die Überprüfung ausgeführt wird. In gleicher Weise können Sie eine monatliche geplante Überprüfung konfigurieren und feste Tage im Monat angeben, an denen die Überprüfung ausgeführt wird. Für beide Überprüfungen können Sie den Parameter `/Snn` verwenden:

- Für wöchentliche geplante Überprüfungen können Sie `/rweekly` zusammen mit den Parametern `/s1` - `/s7` verwenden. `/s1` bedeutet "Montag" und `/s7` bedeutet "Sonntag".

  Beispielsweise bedeutet `/t18:00 /rweekly /s2 /s5` dass der Scan-Vorgang jeweils Dienstag und Freitag um 18:00 Uhr erfolgt.
- ür monatliche geplante Überprüfungen können Sie `/rmonthly` zusammen mit den Parametern `/s1` - `/s31` verwenden.

  Beispielsweise bedeutet `/t18:00 /rmonthly /s5 /s20` , dass der Scan-Vorgang jeweils am 5. und am 20. des Monats um 18:00 Uhr erfolgt.

Hinweis: Wöchentliche geplante Überprüfungen werden außerdem an jedem Montag ausgeführt. Monatliche geplante Überprüfungen werden automatisch am ersten Tag des jeweiligen Monats ausgeführt.

Erweiterte Einstellungen von DeepGuard

In diesem Abschnitt werden die erweiterten Einstellungen von DeepGuard behandelt.

Administratoren die Zulassung oder Ablehnung von Ereignissen von Programmen anderer Benutzer gestatten

Einem Benutzer mit Administratorrechten können Sie gestatten, Ereignisse, die durch eine von einem anderen Benutzer gestarteten Anwendung verursacht werden, zuzulassen oder abzulehnen.

1. Wählen Sie aus dem Menü **Ansicht** > **Erweiterter Modus**.
   Die Benutzeroberfläche für den **erweiterten Modus** wird geöffnet.
2. Wählen Sie auf der Registerkarte **Richtliniendomänen** den Eintrag **Stamm**.
3. Wählen Sie auf der Registerkarte **Richtlinie** die Option **F-Secure** > **F-Secure DeepGuard** > **Einstellungen** > **Lokale Administratorsteuerung**.
4. Wählen Sie die Option **Alle Prozesse**.
5. Klicken Sie auf , um die Richtlinie zu verteilen.

Von einer bestimmten Anwendung angeforderte Ereignisse automatisch zulassen oder ablehnen

Sie können alle Ereignisse für eine sichere Anwendung zulassen bzw. alle Ereignisse für nicht zu verwendende Anwendungen ablehnen.

1. Zunächst müssen Sie die SHA-1-Hash-Kennung für die Anwendung berechnen.

   Im Internet finden Sie kostenlose SHA-1-Rechner. Sie können beispielsweise Microsoft File Checksum Integrity Verifier verwenden. Dieses Tool finden Sie unter folgendem Link: *http://support.microsoft.com/kb/841290*.

   Hinweis: Ein SHA-1-Hash identifiziert die Reihenfolge der Anweisungen, mit denen ein Programm definiert wird, eindeutig. Wenn eine neue Version des Programms zur Verfügung gestellt wird, müssen Sie diesen Vorgang wiederholen, da das neue Programm über ein anderes SHA-1-Hash verfügt.

2. Wenn das SHA-1-Hash vorliegt, wählen Sie aus dem Menü **Ansicht** > **Erweiterter Modus**.
   Die Benutzeroberfläche für den **erweiterten Modus** wird geöffnet.
3. Wählen Sie auf der Registerkarte **Richtliniendomänen** den Eintrag **Stamm**.
4. Wählen Sie auf der Registerkarte **RichtlinieF-Secure** > **F-Secure DeepGuard** > **Einstellungen** > **Anwendungen**.
5. Klicken Sie auf **Hinzufügen**, um eine neue Regel hinzuzufügen.
6. Doppelklicken Sie für den neuen Eintrag auf die Zelle **SHA-1-Hash** und fügen Sie das SHA-1-Hash in die leere Zelle ein.
7. Doppelklicken Sie für den neuen Eintrag auf die Zelle **Hinweise** und geben Sie einen Hinweis ein.

   Dieser Hinweis sollte daran erinnern, welche Anwendung durch das SHA-1 identifiziert wird.
8. Doppelklicken Sie für den neuen Eintrag auf die Zelle **Vertrauenswürdig**:

- Wählen Sie **Ja** aus, um alle Ereignisse für die Anwendung zuzulassen.
- Wählen Sie**Nein** aus, um alle Ereignisse für die Anwendung abzulehnen.

9. Doppelklicken Sie für en neuen Eintrag auf die Zelle **Aktiviert**.
10. Wählen Sie**Ja** aus, um die Regel zu aktivieren.
11. Klicken Sie auf , um die Richtlinie zu verteilen.

Die Anwendungsregel kann nicht vom Benutzer lokal übersteuert werden.

Konfigurieren von Policy Manager Proxy

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

Policy Manager Proxy speichert automatische Updates, die vom zentralen F-Secure Update-Server oder vom Policy Manager Server des Unternehmens ankommen, im Zwischenspeicher und befindet sich dabei im selben Remote-Netzwerk wie die Hosts, die die Datenbank als Verteilungspunkt nutzen. In jedem Netzwerk mit langsamen Netzwerkleitungen sollte sich ein Policy Manager Proxy befinden.

Hosts, auf denen Client Security oder Anti-virus for Workstations ausgeführt wird, rufen Virendefinitions-Updates über Policy Manager Proxy ab. Policy Manager Proxy stellt eine Verbindung zu Policy Manager Server und bei Bedarf zum F-Secure-Verteilungsserver her.

Arbeitsstationen in dezentralen Niederlassungen tauschen ebenfalls Daten mit dem Policy Manager Server in der Zentrale aus, diese Kommunikation ist jedoch auf die Remote-Verwaltung von Richtlinien, die Statusüberwachung und Alarmierung beschränkt.Da der Datenbank-Updateverkehr über den Policy Manager Proxy im gleichen lokalen Netzwerk umgeleitet wird, verringert sich die Belastung der Netzwerkverbindung zwischen den verwalteten Arbeitsstationen und dem Policy Manager Server erheblich.

Hinweis: Weitere Informationen zur Installation und Konfiguration Policy Manager Proxy, finden Sie im Administratorhandbuch von Policy Manager Proxy.

Konfigurieren automatischer Updates der Hosts vom Policy Manager Proxy

Eine Liste der Proxy-Server, von denen die Hosts Updates herunterladen, kann auf der Registerkarte **Einstellungen** eingerichtet werden.

Wenn Sie diese Konfiguration über die lokale Benutzeroberfläche eines verwalteten Hosts vornehmen möchten, gehen Sie wie folgt vor:

1. Klicken Sie auf auf der Hauptanwendungsseite auf **Einstellungen**.
2. Wählen Sie **Weitere Einstellungen** > **Policy Manager Proxy** aus.

   Auf der Seite **Policy Manager-Proxy** können Sie die Adressen, von denen das lokal installierte Client Security automatische Updates abrufen kann, anzeigen und bearbeiten.

   Die Adressen werden von oben nach unten abgearbeitet, d. h., standardmäßig wird die oberste Adresse in der Liste verwendet.
3. Klicken Sie auf **Hinzufügen**, um der Liste den neuen Proxy-Server hinzuzufügen.
4. Geben Sie den Namen des ersten Proxy-Servers in das Feld ein und klicken Sie anschließend auf **OK**.
5. Wiederholen Sie diesen Schritt für alle weiteren Proxy-Server, die Sie hinzufügen möchten.

Sie können die Reihenfolge der Server ändern. Wählen Sie dazu den gewünschten Eintrag aus und klicken Sie rechts davon auf die nach oben bzw. unten weisenden Pfeilschaltflächen, um den Eintrag zu verschieben.

6. Klicken Sie auf **OK**, wenn Sie alle Proxy-Server hinzugefügt haben.

Ausschließen von Anwendungen für den Web Traffic Scanner

Wenn Web Traffic Scanning Probleme mit einem Programm verursacht, das in Ihrem Unternehmen häufig verwendet wird, können Sie diese Anwendung für den Web Traffic Scanner ausschließen.

1. Wählen Sie aus dem Menü **Ansicht** > **Erweiterter Modus**.
2. Wählen Sie auf der Registerkarte **Richtlinie F-Secure Client Security** > **Einstellungen** > **Protokoll-Scan auswählen** > **Vertrauenswürdige Anwendungen** > **Liste vertrauenswürdiger Prozesse** aus.
3. Geben Sie den Namen des Prozesses ein, der für den Web Traffic Scanner ausgeschlossen werden soll.

   Trennen Sie bei der Eingabe mehrerer Prozesse die einzelnen Prozessnamen durch Kommata. Geben Sie zwischen den Prozessnamen keine Leerzeichen ein.

   Tipp: Unter Windows ermitteln Sie den Prozessnamen einer Anwendung mithilfe des Windows Task-Manager.

   Um beispielsweise die Anwendungen Editor und Skype für den Web Traffic Scanner auszuschließen, geben Sie `notepad.exe,skype.exe` ein.
4. Klicken Sie auf , um die Richtlinie zu verteilen.

Kapitel

13

Erweiterte Funktionen: Internet Shield

Themen:

- *Remote-Verwaltung der Eigenschaften von Internet Shield*
- *Konfigurieren der automatischen Auswahl der Sicherheitsstufe*
- *Fehlerbehebung bei Verbindungsproblemen*
- *Hinzufügen neuer Dienste*
- *Einrichten der Verbindungskontrolle*

Hier finden Sie Informationen über die erweiterten Funktionen von Internet Shield.

In diesem Abschnitt werden einige der erweiterten Funktionen von Internet Shield beschrieben. Außerdem finden Sie hier Informationen zur Fehlerbeseitigung.

Remote-Verwaltung der Eigenschaften von Internet Shield

In diesem Abschnitt erfahren Sie, wie Sie die Eigenschaften von Internet Shield remote verwalten.

Einsatz der Paketprotokollierung

Bei der Paketprotokollierung handelt es sich um ein sehr nützliches Debugging-Tool, mit dem Sie feststellen können, was in Ihrem lokalen Netzwerk passiert.

Die Paketprotokollierung ist aber auch ein leistungsfähiges Tool, das von Endbenutzern missbraucht werden kann, um die Aktivitäten anderer Benutzer im LAN auszuspionieren. Deshalb muss der Administrator die Paketprotokollierung in einigen Unternehmensumgebungen deaktivieren.

1. Wählen Sie aus dem Menü **Ansicht** die Option **Erweiterter Modus**.
   Die Benutzeroberfläche für den **erweiterten Modus** wird geöffnet.
2. Wählen Sie auf der Registerkarte **Richtliniendomänen** den Eintrag **Stamm**.
3. Wählen Sie **F-Secure Internet Shield** > **Einstellungen** > **Paketprotokollierung** > **Aktiv** aus.
   Diese Variable zeigt den Status der Paketprotokollierung an: **Deaktiviert** bedeutet, dass keine Ausführung erfolgt und **Aktiviert**, dass Sie aktuell auf dem Host ausgeführt wird.
4. Um die Protokollierung vollständig zu deaktivieren, müssen Sie sicherstellen, dass diese auf **Deaktiviert** eingerichtet ist, und wählen Sie **Änderungen durch den Benutzer nicht zulassen** aus.
5. Klicken Sie auf , um die Richtlinie zu verteilen.

Um diese Änderung später rückgängig zu machen, wählen Sie **Änderungen durch den Benutzer zulassen** aus und verteilen die neue Richtlinie.

Hinweis: Diese Option sollte nur unter äußerster Vorsicht ausgeführt werden. Wenn Sie z. B. die Variable für die gesamte Domäne auf **Aktiviert** setzen, würde eine Protokollierungssitzung auf allen betroffenen Hosts gestartet werden.

Verwenden der vertrauenswürdigen Schnittstelle

Mit dem Mechanismus für vertrauenswürdige Schnittstellen kann ein durch eine Firewall geschützter Host als Anschluss-Server für den Dateiaustausch eingesetzt werden.

Firewall-Regeln werden nicht auf Datenverkehr angewandt, der durch die vertrauenswürdige Schnittstelle läuft. Wird diese Option falsch eingesetzt, kann der Host beliebigen Angriffen aus dem Netzwerk schutzlos ausgesetzt sein. Deshalb sollte dieser Mechanismus vorsichtshalber deaktiviert werden, wenn kein dringender Bedarf besteht.

Die vertrauenswürdige Schnittstelle wird wie folgt aktiviert:

1. Wählen Sie aus dem Menü **AnsichtErweiterter Modus**.
   Die Benutzeroberfläche für den **erweiterten Modus** wird geöffnet.
2. Wählen Sie in der **Richtliniendomänen**-Struktur die Subdomäne, in der die vertrauenswürdige Schnittstelle aktiviert werden soll.
3. Wählen Sie auf der Registerkarte **RichtlinienF-Secure Internet Shield** > **Einstellungen** > **Firewall-Modul** > **Vertrauenswürdige Schnittstelle zulassen**.
4. Wählen Sie **Aktiviert**, um die vertrauenswürdige Schnittstelle für die derzeit ausgewählte Subdomäne zu aktivieren.
   Daraufhin sind Endbenutzer innerhalb der Subdomäne in der Lage, eine Netzwerkschnittstelle als vertrauenswürdige Schnittstelle zu definieren.
5. Klicken Sie auf , um die Richtlinie zu verteilen.

Einsatz der Paketfilterung

Dabei handelt es sich um einen der grundlegenden Sicherheitsmechanismen in der Firewall, der den gesamten IP-Netzwerkverkehr anhand der Informationen in den Protokoll-Headern der jeweiligen Pakete filtert.

Sie können die Paketfilterung auf der Registerkarte **Erweitert** in den Einstellungen für den **Netzwerkschutz** aktivieren oder deaktivieren. Manchmal ist eine Deaktivierung zu Testzwecken erforderlich. Dies beeinträchtigt jedoch die Sicherheit. Deshalb sollten für die meisten Unternehmensumgebungen Vorkehrungen getroffen werden, damit die Paketfilterung immer aktiviert ist.

1. Wählen Sie aus dem Menü **Ansicht** > **Erweiterter Modus**.
   Die Benutzeroberfläche für den **Erweiterten Modus** wird geöffnet.
2. Wählen Sie auf der Registerkarte **Richtliniendomänen** den Eintrag **Stamm**.
3. Wählen Sie auf der Registerkarte **Richtlinie F-Secure Internet Shield** > **Einstellungen** > **Firewall-Modul** > **Firewall-Modul aktiviert** aus.
4. Um sicherzustellen, dass Paketfilterung immer aktiviert ist, richten Sie diese Variable auf **Ja** ein und wählen **Änderungen durch Benutzer nicht zulassen** aus.
5. Klicken Sie auf , um die Richtlinie zu verteilen.

Konfigurieren der automatischen Auswahl der Sicherheitsstufe

In diesem Beispiel wurde die automatische Auswahl der Sicherheitsstufe für eine Subdomäne konfiguriert, die ausschließlich Laptops enthält, die wie Computer in einem Unternehmens-LAN miteinander vernetzt sind. Aus diesem Grund wird die Sicherheitsstufe **Büro** verwendet; wird eine DFÜ-Verbindung verwendet, ändert sich die Sicherheitsstufe zu **Mobil**.

Bevor Sie beginnen, sollten Sie die IP-Adresse des DNS-Servers und des Standard-Gateways kennen, da diese Angaben zur Definition der Kriterien für die automatische Auswahl der Sicherheitsstufe benötigt werden. Um diese Adressen herauszufinden, geben Sie den Befehl`ipconfig -all` im Fenster der Eingabeaufforderung ein.

1. Wählen Sie aus dem Menü **Ansicht** > **Erweiterter Modus**, um zur Benutzeroberfläche für den **erweiterten Modus** zu wechseln.
   Die Benutzeroberfläche für den **Erweiterten Modus** wird geöffnet.
2. Wählen Sie die Subdomäne in der Struktur der **Richtliniendomänen**.
3. Wählen Sie auf der Registerkarte **Richtlinie F-Secure** > **F-Secure Internet Shield** > **Einstellungen** > **Sicherheitsstufe** > **Auto-Auswahl-Modus** aus.
4. Vergewissern Sie sich, dass die automatische Auswahl der Sicherheitsstufe eingeschaltet ist.

   Um die automatische Auswahl der Sicherheitsstufe zu aktivieren, wählen Sie aus der Dropdown-Liste **Auto-Auswahl-Modus** die Option **Benutzeränderungen möglich** oder **Vollständige Kontrolle durch den Administrator**.
5. Wechseln Sie zur Seite **Auto-Auswahl** und klicken Sie auf **Hinzufügen**, um die erste Sicherheitsstufe, in diesem Fall **Office**, hinzuzufügen.
6. Wählen Sie eine Zelle aus und klicken Sie auf **Bearbeiten**, um die Daten in die Zellen einzugeben.

   Zur Definition der Sicherheitsstufe **Büro** geben Sie die folgenden Daten ein:

   - **Priorität**: Die Regeln werden in der durch die Prioritätsnummern definierten Reihenfolge ausgewertet, beginnend mit der kleinsten Nummer.
   - **Sicherheitsstufe**: Geben Sie die ID (bestehend aus einer Zahl und einem Namen) der Sicherheitsstufe ein, z. B.:`40Büro`.
   - **Methode 1**: Wählen Sie aus der Dropdown-Liste die Option **IP-Adresse des DNS-Servers** aus.

- **Argument 1**: Geben Sie hier die IP-Adresse für Ihren lokalen DNS-Server ein, z. B.:`10.128.129.1`.
- **Methode 2**: Wählen Sie aus der Dropdown-Liste die Option **IP-Adresse des Standard-Gateways** aus.
- **Argument 2**: Geben Sie die IP-Adresse für Ihr Standard-Gateway ein, z. B.: `10.128.130.1`.

Hinweis: Sie können in das Feld **Argument** nur ein Argument eingeben, z. B. eine IP-Adresse. Wenn in Ihrem Unternehmen mehrere Standard-Gateways eingesetzt werden, die alle bei der automatischen Auswahl der Sicherheitsstufe verwendet werden sollen, können Sie für jedes Gateway eine separate Regel in der Tabelle festlegen.

Die Definition der ersten Sicherheitsstufe ist damit abgeschlossen.

7. Klicken Sie auf **Hinzufügen**, um die zweite Sicherheitsstufe, in unserem Beispiel **Mobil**, hinzuzufügen.
8. Wählen Sie eine Zelle aus und klicken Sie auf **Bearbeiten**, um Daten in die Zellen einzugeben.

   Zur Definition der Sicherheitsstufe **Mobil** geben Sie die folgenden Daten ein:

   - **Priorität**: Die Regeln werden in der durch die Prioritätsnummern definierten Reihenfolge ausgewertet, beginnend mit der kleinsten Nummer.
   - **Sicherheitsstufe**: Geben Sie hier die ID der Sicherheitsstufe ein, z. B.: `20mobile`.
   - **Methode 1**: Wählen Sie aus der Dropdown-Liste die Option **DFÜ** aus.
   - **Argument 1**: In dieses Feld müssen Sie keinen Wert eingeben.
   - **Methode 2**: Wählen Sie aus der Dropdown-Liste die Option **Immer** aus.
   - **Argument 2**: In dieses Feld müssen Sie keinen Wert eingeben.

   Die Konfiguration ist damit abgeschlossen.
9. Klicken Sie auf , um die Richtlinie zu verteilen.

Fehlerbehebung bei Verbindungsproblemen

If there are connection problems, for example a host cannot access the Internet, and you suspect that Internet Shield might cause these problems, you can use the steps given here as a check list.

1. Überprüfen Sie, ob der Computer ordnungsgemäß angeschlossen ist.
2. Überprüfen Sie, ob das Problem durch das Netzwerkkabel verursacht wird.
3. Überprüfen Sie, ob die Ethernet-Verbindung steht und ordnungsgemäß funktioniert.
4. Check that the DHCP address is valid.

   You can do this by giving the command `ipconfig` in the command prompt.
5. Anschließend sollten Sie versuchen, das Standard-Gateway anzupingen.

   If you do not know the address, you can find it out by issuing the command `ipconfig -all` in the command prompt. Then ping the default gateway to see if it responds.
6. If normal Internet browsing does not work, you can try to ping a DNS server:

   - Run `nslookup` to make sure that the DNS service is running.
   - You can also try to ping a known web address to make sure that the computer at the other end is not down.
7. Next you should check whether something in the centrally managed domain has been changed; is there a new policy in use and does this policy contain some settings that might cause these problems?

   - Überprüfen Sie anhand der Firewall-Regeln, ob ausgehende HTTP-Verbindungen zugelassen sind.
   - Überprüfen Sie anhand der lokalen Anwendungssteuerung, ob die IP-Adresse, zu der eine Verbindung aufgebaut werden soll, versehentlich in die Liste der abgelehnten Adressen aufgenommen wurde.

8. If nothing else helps, unload F-Secure products or set the Internet Shield to allow all mode.

If even this does not help, it is likely that the problem is in routing or in some other component in the computer the user is trying to connect to.

Hinzufügen neuer Dienste

Bei einem Netzwerkdienst, kurz Dienst, handelt es sich um einen Dienst, der über das Netzwerk verfügbar ist, z. B. gemeinsamer Dateizugriff, Remote-Konsolen-Zugriff oder Webbrowsing.

Dienste werden in den meisten Fällen durch das verwendete Protokoll und den Port beschrieben.

Erstellen eines neuen Internet-Dienstes auf Grundlage von Standard-HTTP

Dieses Beispiel geht von einem Webserver aus, der auf einem Computer läuft und für den ein Web-Port definiert wurde, der nicht dem Standard entspricht.

Normalerweise würde ein Webserver TCP/IP Port 80 verwenden, aber in diesem Beispiel wurde er für Port 8000 konfiguriert. Damit Arbeitsstationen Verbindungen zu diesem Server aufbauen können, müssen Sie einen neuen Dienst erstellen. Der Standard-HTTP-Dienst kann hier nicht verwendet werden, da der herkömmliche HTTP-Port nicht zum Einsatz kommt. Der neue Dienst hat die Bezeichnung `HTTP Port 8000` und basiert auf dem Standard-`HTTP`-Dienst.

1. Wählen Sie auf der Registerkarte **Richtliniendomänen** die Subdomäne, für die der neue Dienst erstellt werden soll.
2. Öffnen Sie die Registerkarte **Einstellungen** und dort die Seite **Firewall-Dienste**.

   Auf dieser Seite befindet sich die Tabelle **Firewall-Dienste**.
3. Klicken Sie auf die Schaltfläche **Hinzufügen**, um den Assistenten zum Konfigurieren der **Firewall-Dienste** zu starten.
4. Geben Sie einen Namen für den Dienst ein:
   a) Geben Sie in das Feld **Dienstname** einen eindeutigen Namen für den Dienst ein. Es ist nicht zulässig, dass zwei Dienste denselben Namen haben.
   Beispielsweise: `HTTP Port 8000`.
   b) Geben Sie in das Feld **Dienst-Kommentar** eine Beschreibung für den Dienst ein.

   Die Beschreibung wird in der Tabelle der **Firewall-Dienste** angezeigt.
5. Wählen Sie eine IP-Protokollnummer:
   a) Wählen Sie aus der Dropdown-Liste **Protokoll** eine Protokollnummer für diesen Dienst aus.

   Sie finden dort die gängigsten Protokolle (TCP, UDP, ICMP). Wenn Ihr Dienst ein anderes Protokoll verwendet, suchen Sie den passenden Eintrag in der Tabelle weiter unten und geben Sie die entsprechende Nummer ein.

   Wählen Sie in diesem Beispiel aus der Dropdown-Liste **IP-Protokollnummer** die Option **TCP (6)** aus.

Protokollname	Protokollnummer	Vollständiger Name
ICMP	1	Internet Control Message-Protokoll
IGMP	2	Internet Group Management-Protokoll
IPIP	4	IPIP-Tunnel (IP in IP)
TCP	6	Transmission Control-Protokoll
EGP	8	Exterior Gateway-Protokoll
PUP	12	Xerox PUP-Routing-Protokoll

Protokollname	Protokollnummer	Vollständiger Name
UDP	17	User Datagram-Protokoll
IDP	22	Xerox NS Internet Datagram-Protokoll
IPV6	41	Neue 128-Bit-Version des IP-Standards (Ipv6), abwärtskompatibel zu IPv4 (64-Bit)
RSVP	46	Resource Reservation-Protokoll
GRE	47	Generic Routing Encapsulation-Tunnel von Cisco (GRE)
ESP	50	Encapsulation Security Payload-Protokoll
AH	51	Authentication Header-Protokoll
PIM	103	Protocol Independent Multicast (protokollunabhängiges Multicast)
COMP	108	Compression Header-Protokoll
RAW	255	Unverarbeitete IP-Pakete

6. Wählen Sie die Ausgangspartei-Ports:

   Wenn Ihr Dienst das TCP- oder UDP-Protokoll verwendet, müssen Sie die Ausgangspartei-Ports festlegen, die der Dienst abdeckt. Das Format für die Eingabe der Ports und Port-Bereiche lautet wie folgt:

   - `>Port`: Alle Ports mit einer höheren Adresse als `Port`
   - `>=Port`: Alle Ports mit der gleichen oder einer höheren Adresse als `Port`
   - `<Port`: Alle Ports mit einer niedrigeren Adresse als `Port`
   - `<=Port`: Alle Ports mit der gleichen oder einer niedrigeren Adresse als `Port`
   - `Port`: Nur der `Port`
   - `Min.-Port-Max.-Port`: `Min.-Port` und `Max.-Port` sowie alle Ports dazwischen (Beachten Sie, dass sich auf beiden Seiten des Bindestriches keine Leerzeichen befinden.).

   Sie können Sie können durch Kommata getrennte Kombinationen dieser Elemente festlegen. Die Ports 10, 11, 12, 100, 101, 200 und größer als 1023 können als `10-12, 100-101, 200, >1023` definiert werden.

   In this example, define the initiator port as `>1023`.

7. Select responder ports:

   Wenn Ihr Dienst das TCP- oder das UDP-Protokoll verwendet, müssen Sie die Antwortpartei-Ports festlegen, die der Dienst abdeckt.

   In diesem Beispiel definieren Sie den Antwortpartei-Port als `8000`.

8. Wählen Sie aus der Dropdown-Liste eine Klassifizierungsnummer für den Dienst aus.

   Sie können den Standardwert übernehmen.

9. Legen Sie fest, ob der vom Dienst zugelassene Datenverkehr zusätzlich zu den normalen Prüfmethoden (Paket und Stateful Inspection) gefiltert werden soll.
   In diesem Beispiel können Sie die Standardeinstellung **Deaktiviert** übernehmen.

   Hinweis: Wenn der Dienst das TCP-Protokoll verwendet und die Anwendungssteuerung nicht aktiviert wurde, können Sie aus dem Dropdown-Menü **Extra filtering** die Option **Active-Mode-FTP** auswählen. **Active-Mode-FTP** setzt eine spezielle Handhabung der Firewall voraus, da die Informationen zu dem Port, der für die Verbindung geöffnet werden sollte, in den übertragenen Daten enthalten sind.

10. Sie können Ihre Regel jetzt überprüfen.

    Wenn Sie Änderungen an der Regel vornehmen möchten, klicken Sie auf **Zurück**.

11. Klicken Sie auf **Fertig stellen**, um den Regel-Assistent zu schließen.
    Die erstellte Regel wird in der Tabelle **Firewall-Regeln** angezeigt.

12. Neue Regel aktivieren:

    Damit der neue Dienst eingesetzt werden kann, müssen Sie eine neue Regel für Internet Shield erstellen. Diese Regel lässt den Einsatz des Firewall-Dienstes **HTTP 8000** auf der derzeitigen Sicherheitsstufe für Internet Shield zu. In diesem Fall wählen Sie auf der Seite**Regelassistent** > **Dienst** den neuen Dienst aus. Sie müssen auf der Seite **Regelassistent** > **Erweiterte Optionen** keine Warnmeldungen definieren.

Einrichten der Verbindungskontrolle

Mit der Verbindungskontrolle können Sie eine Liste von Telefonnummern erstellen, die von dem Modem des Benutzers zugelassen oder gesperrt werden.

So aktivieren Sie die Verbindungskontrolle:

1. Wählen Sie aus dem Menü **Ansicht** > **Erweiterter Modus**, um zur Benutzeroberfläche für den **erweiterten Modus** zu wechseln.
2. Wählen Sie in der Registerkarte **Richtlinie** die Option **F-Secure** > **F-Secure Internet Shield** > **Einstellungen** > **Verbindungskontrolle** > **Verbindungskontrolle**.
3. Wählen Sie **Aktiviert**, um die Verbindungskontrolle zu aktivieren.
4. Klicken Sie auf , um die Richtlinie zu verteilen.

Zulassen und Sperren von Telefonnummern

Sie können spezifische Telefonnummern für DFÜ-Verbindungen zulassen oder sperren.

So fügen Sie eine neue zugelassene oder gesperrte Nummer hinzu:

1. Wählen Sie aus dem Menü **Ansicht** > **Erweiterter Modus**, um zur Benutzeroberfläche für den **erweiterten Modus** zu wechseln.
2. Wählen Sie auf der Registerkarte **Richtlinie F-Secure** > **F-Secure Internet Shield** > **Einstellungen** > **Einwählkontrolle** > **Nummer** aus.
3. Klicken Sie auf **Hinzufügen**.
4. Doppelklicken Sie in der neuen Zeile auf die Zelle **Prioritäten**, um die Priorität der Regel festzulegen.

   Wenn zwei Regeln auf eine Telefonnummer zutreffen, wird die Regel mit der niedrigsten Priorität angewendet, d. h. eine Regel mit der Priorität `1` hat Vorrang vor einer Regel mit der Priorität `3`.

5. Doppelklicken Sie in der neuen Zeile auf die Zelle **Telefonnummer**, um die Telefonnummern hinzuzufügen, für die diese Regel gilt.

   Sie können die folgenden Zeichen verwenden, um mehreren Telefonnummern eine Regel zuzuweisen:

Zeichen	Gilt für	Beispiel
?	Entspricht allen einstelligen Ziffern	`1?3` entspricht den folgenden Zahlen: 103, 113, 123,133,143, 153,163,173,183,193.
*	Entspricht jeder Anzahl an Ziffern	`0800*` entspricht allen Telefonnummern, die mit 0800 beginnen

6. Wählen Sie die Option zum **Zulassen** oder **Ablehnen**, um einen Verbindungsaufbau des Modems mit den entsprechenden Telefonnummern zuzulassen oder zu sperren.
7. Doppelklicken Sie in der neuen Zeile auf die Zelle **Kommentar** und fügen Sie eine Beschreibung hinzu, um anderen Benutzern den Zweck dieser Regel zu verdeutlichen.
8. Wählen Sie **Ja**, um die neue Regel zu aktivieren.
9. Klicken Sie auf , um die Richtlinie zu verteilen.

Einsatz der Anrufprotokollierung

Die Anrufprotokollierung bietet Ihnen die Möglichkeit, alle gewählten Nummern zu protokollieren.

So aktivieren Sie die Protokollierung von gewählten Nummern:

1. Wählen Sie aus dem Menü **Ansicht** > **Erweiterter Modus**, um zur Benutzeroberfläche für den **erweiterten Modus** zu wechseln.
2. Wählen Sie auf der Registerkarte **Richtlinie** die Option **F-Secure** > **F-Secure Internet Shield** > **Einstellungen** > **Verbindungskontrolle** > **Nummernprotokollierung**.
3. Wählen Sie **Aktiviert**, um vom Modem gewählte Nummern zu protokollieren.
4. Klicken Sie auf , um die Richtlinie zu verteilen.

Kapitel
14

Ändern von prodsett.ini

Themen:

- *Konfigurierbare prodsett.ini-Einstellungen*

`prodsett.ini` informiert das **Installationsprogramm** über die zu installierenden Module und deren Ziel-Verzeichnis auf den Arbeitsstationen.

In diesem Abschnitt finden Sie eine Liste der Einstellungen, die in der Datei `prodsett.ini` bearbeitet werden können.

Vorsicht: Ändern Sie in der Datei `prodsett.ini` keine Einstellungen, die nicht in diesem Abschnitt aufgeführt sind.

Hinweis: Abhängigkeit zwischen `RequestInstallMode` und `InstallMode` Einstellungen:

DieRequestInstallMode Einstellung kann die Auswahl für Komponenten überschreiben, die verfügen überInstallMode=0.

Konfigurierbare prodsett.ini-Einstellungen

Sie können die hier beschriebenen Einstellungen in der Datei `prodsett.ini` bearbeiten.

[F-Secure allgemein]	Allgemeine Einstellungen
CD-Schlüssel=XXXX-XXXX-XXXX-XXXX-XXXX	Geben Sie in dieses Feld den Abonnementschlüssel ein, der sich auf der Verpackung befindet..
SetupLanguage=ENG	Die festgelegte Installationssprache. Wird für diese Einstellung nichts oder `AUTO` festgelegt, wird die Installationssprache abhängig vom standardmäßigen Systemstandort automatisch auf dem Host festgelegt. Die Auswahl ist durch den unterstützen Sprachsatz eingeschränkt (siehe "SupportedLanguages").
SetupMode=1	`1` = Netzwerk-Client (Standard). Wenn `SetupMode=1`, sollten die entsprechenden Einstellungen für die zentrale Verwaltung im Abschnitt [PMSUINST.DLL] definiert werden. `2` = Einzelplatz-Installationsmodus.
SupportedLanguages=ENG FRA DEU FIN SVE ITA	Liste der Sprachen, die von diesem Installationspaket unterstützt werden. Sie können die Anzahl der unterstützten Sprachen verringern, indem Sie einige nicht benötigte Sprachen entfernen und das Paket neu zusammenstellen. Wenn Sie die Unterstützung für eine neue Sprache zum Paket hinzufügen möchten, sollten Sie die Sprache an dieser Stelle hinzufügen.
InstallLanguages=ENG FRA DEU FIN SVE ITA	Liste der Sprachen, die auf dem Host installiert werden. Diese Liste entspricht normalerweise der Liste `SupportedLanguages`. Wenn einige nicht benötigte Sprachen nicht installiert werden sollen, können Sie diese Sprachen entfernen. Wenn Sie die Unterstützung für eine neue Sprache zum Paket hinzufügen möchten, sollten Sie die Sprache an dieser Stelle hinzufügen. Die Sprachdateien der von "SetupLanguage" festgelegten Sprache werden unabhängig von der Einstellung von "InstallLanguages" installiert.
SecurityPolicy=0 | 1 | 2	Die Dateien und Ordner, die auf einer NTFS-Partition installiert werden sollen, und der Registrierungsschlüssel für das Programm werden entsprechend der definierten `SecurityPolicy` durch NT-Sicherheitsberechtigungen geschützt:

[F-Secure allgemein]	Allgemeine Einstellungen
	`0` = Es wird keine spezielle Richtlinie angewendet; Dateien und Ordner erben die Sicherheitsberechtigungen von den Eltern. `1` = weniger strikte Richtlinie; Dateien und Ordner werden geschützt durch Berechtigungen, die den vollen Zugriff für Administratoren und den schreibgeschützten Zugriff durch andere Benutzer gewähren. `2` = strikte Richtlinie; Dateien und Ordner werden geschützt durch Berechtigungen, die den vollen Zugriff für Administratoren, den schreibgeschützten Zugriff durch andere Benutzer und keinen Zugriff durch alle gewähren. Hinweis: When `SecurityPolicy = 1` or `2`, überschreibt das Setup-Programm die Zugangskontrolllisten (Access Control Lists, ACLs) von vorhandenen Dateien, Ordnern und Registrierungsschlüsseln. Wenn Sie ACLs speziell konfiguriert haben, indem sie ihnen beispielsweise Benutzer hinzugefügt haben, müssen Sie sie nach der Installation neu konfigurieren.

[Silent Setup]	Einstellungen für die unbeaufsichtigte automatische Installation
DestinationDirUnderProgramFiles=F-Secure	Standardzielpfad. Verändern Sie diese Einstellung nicht, es sei denn, Ihr Unternehmen befolgt eine bestimmte Installationsrichtlinie.
Reboot=2	`1` = Nach Installation automatisch neu starten. **Achtung:** Wenn diese Option aktiv ist, wird der Host ohne die Aufforderung an den Benutzer, seine Arbeit zu speichern, neu gestartet. Sie sollten diese Option nur verwenden, wenn Sie absolut sicher sind, dass diese Art des Neustarts am Zielcomputer kein Risiko darstellt. `2` = Vor Neustart den Benutzer zur Bestätigung auffordern (Standard). **Hinweis:** Bei Auswahl dieser Option wird der Host normal neu gestartet, d. h., es kann bei dieser Methode passieren, dass ein Benutzer den Neustart verzögert oder vollständig verhindert. `3` = Kein Neustart nach Installation.

[FSMAINST.DLL]	Einstellungen für Management Agent
RequestInstallMode=1	Diese Komponente wird bei der Installation eines vernetzten Clients immer installiert. Sie müssen keine Bearbeitung vornehmen für`RequestInstallMode` oder `InstallMode` die Einstellungen für diese Komponente.
ManagementKey=\\server\path\admin.pub	Speicherort des öffentlichen Verwaltungsschlüssels.
ManagedStandAlone=	Diese Option ist nur bei der Installation auf einem Einzelplatzrechner von Bedeutung. `0` = Normale Installation auf Einzelplatzrechner, Richtliniendateien können nicht importiert werden (Standard). `1` = Installierte Komponenten können mithilfe manuell importierter Richtlinien verwaltet werden.
win2000renamefiles=fsrec.2k|fsrec.sys;fsfilter.2k|fsfilter.sys;fsgk.2k|fsgk.sys InstallFSPKIH=0 InstallNetworkProvider=0 InstallGINA=0 RedefineSettings=0 ServiceProviderMode=0 MibVersion= GatekeeperVersion= StatisticsFilterPattern1=	Ändern Sie diese Einstellungen nicht!
UseOnlyUID=	`0` = Management Agent verwendet nur alle verfügbaren Identitäten (DNS-Name, IP-Adresse, WINS-Name, eindeutige Identität), um sich selbst beim ersten Verbindungsaufbau mit Policy Manager Server zu identifizieren. `1` = Management Agent verwendet nur die eindeutige Identität, um sich selbst bei Policy Manager Server zu identifizieren.
Debug=1	`0` = Debugging-Informationen werden nicht erstellt (Standard). `1` = Debugging-Informationen werden während der Installation und Deinstallation in das Debugging-Protokoll geschrieben.
InstallMode=0 | 1	Diese Komponente wird bei der Installation eines vernetzten Clients immer installiert. Sie müssen keine Bearbeitung vornehmen für`RequestInstallMode` oder `InstallMode` die Einstellungen für diese Komponente.

[PMSUINST.DLL]	Einstellungen für die Policy Manager Unterstützung
RequestInstallMode=0	Diese Komponente wird bei der Installation eines vernetzten Clients immer installiert. Sie müssen keine Bearbeitung vornehmen für`RequestInstallMode` oder `InstallMode` die Einstellungen für diese Komponente.
FsmsServerUrl=http://fsmsserver	URL zu Policy Manager Server.
FsmsExtensionUri=/fsms/fsmsh.dll	Ändern Sie diese Einstellung nicht.
FsmsCommdirUri=/commdir	Ändern Sie diese Einstellung nicht.
Debug=1	`0` = Debugging-Informationen werden nicht erstellt (Standard). `1` = Debugging-Informationen werden während der Installation und Deinstallation in das Debugging-Protokoll geschrieben.
InstallMode=0 | 1	Diese Komponente wird bei der Installation eines vernetzten Clients immer installiert. Sie müssen keine Bearbeitung vornehmen für `RequestInstallMode` oder `InstallMode` die Einstellungen für diese Komponente.

[FSAVINST.DLL]	Einstellungen für Client Security - Virenschutz
RequestInstallMode=1	`0` = Diese Komponente installieren wie definiert in`InstallMode`Einstellung. `1` = Die Komponente nur installieren, falls es sich um eine neuere Version handelt oder sie bisher nicht installiert war (Standard). `2` = Die Komponente installieren, wenn sie noch nicht installiert ist oder wenn eine ältere oder gleiche Version vorhanden ist.
EnableRealTimeScanning=1	`0` = Echtzeit-Scanning deaktivieren `1` = Echtzeit-Scanning aktivieren (Standard)
Debug=1	`0` = Debugging-Informationen werden nicht erstellt (Standard). `1` = Debugging-Informationen werden während der Installation und Deinstallation in das Debugging-Protokoll geschrieben.
InstallMode=0 | 1	`0` =Die Komponente wird nicht installiert (Standard). `1` = Die Komponente wird installiert, es sei denn, eine neuere Version ist bereits vorhanden.

[FSSGSUP.DLL]	**Einstellungen für das Modul zur Erkennung und Beseitigung von Konflikten**
RequestInstallMode=1	Diese Komponente wird während der Installation immer ausgeführt. Sie müssen keine Bearbeitung vornehmen für`RequestInstallMode` oder `InstallMode`die Einstellungen für diese Komponente.
Debug=0 | 1	`0` = Debugging-Informationen werden nicht erstellt (Standard). `1` = Debugging-Informationen werden während der Installation und Deinstallation in das Debugging-Protokoll geschrieben.
InstallMode=0 | 1	Diese Komponente wird während der Installation immer ausgeführt. Sie müssen keine Bearbeitung vornehmen für`RequestInstallMode` oder `InstallMode`die Einstellungen für diese Komponente.
SidegradeAction=0	`0` = Alle gefundenen Konflikte werden automatisch entfernt (Standard). `1` = Wenn Software gefunden wird, die Konflikte verursacht, wird die Installation abgebrochen.

[ES_Setup.DLL]	**Einstellungen für die Installation der E-Mail-Überprüfung**
RequestInstallMode=1	0 = Diese Komponente installieren wie definiert in`InstallMode`Einstellung. `1` = Die Komponente nur installieren, falls es sich um eine neuere Version handelt oder sie bisher nicht installiert war (Standard). `2` = Die Komponente installieren, wenn sie noch nicht installiert ist oder wenn eine ältere oder gleiche Version vorhanden ist.
Debug=0 | 1	`0` = Debugging-Informationen werden nicht erstellt (Standard). `1` = Debugging-Informationen werden während der Installation und Deinstallation in das Debugging-Protokoll geschrieben.
InstallMode=0 | 1	`0` =Die Komponente wird nicht installiert (Standard). `1` = Die Komponente wird installiert, es sei denn, eine neuere Version ist bereits vorhanden.

[FWESINST.DLL]	**Einstellungen für die interne allgemeine Komponente FWES.**
RequestInstallMode=1	`0` = Diese Komponente installieren wie definiert in`InstallMode`Einstellung. `1` = Die Komponente nur installieren, falls es sich um eine neuere Version handelt oder sie bisher nicht installiert war (Standard). `2` = Die Komponente installieren, wenn sie noch nicht installiert ist oder wenn eine ältere oder gleiche Version vorhanden ist.
Debug=0 | 1	`0` = Debugging-Informationen werden nicht erstellt (Standard). `1` = Debugging-Informationen werden während der Installation und Deinstallation in das Debugging-Protokoll geschrieben.
InstallMode=0 | 1	`0` =Die Komponente wird nicht installiert (Standard). `1` = Die Komponente wird installiert, es sei denn, eine neuere Version ist bereits vorhanden.

[FWINST.DLL]	**Einstellungen für Client Security Internet-Schutzschild**
RequestInstallMode=1	`0` = Diese Komponente installieren wie definiert in`InstallMode`Einstellung. `1` = Die Komponente nur installieren, falls es sich um eine neuere Version handelt oder sie bisher nicht installiert war (Standard). `2` = Die Komponente installieren, wenn sie noch nicht installiert ist oder wenn eine ältere oder gleiche Version vorhanden ist.
Debug=0 | 1	`0` = Debugging-Informationen werden nicht erstellt (Standard). `1` = Debugging-Informationen werden während der Installation und Deinstallation in das Debugging-Protokoll geschrieben.
InstallMode=0 | 1	`0` =Die Komponente wird nicht installiert (Standard). `1` = Die Komponente wird installiert, es sei denn, eine neuere Version ist bereits vorhanden.
InstallDC=0 | 1	`0` = Dialerschutz nicht installieren (Standard) `1` = Dialerschutz installieren
InstallNetworkQuarantine=0 | 1	`0` = Netzwerk-Quarantäne nicht installieren (Standard) `1` = Netzwerk-Quarantäne installieren

[FWINST.DLL]	**Einstellungen für Client Security Internet-Schutzschild**
DisableWindowsFirewall=0 | 1	`0` = Windows-Firewall (unter XP SP2 oder höher) nicht deaktivieren (Standard) `1` = Windows-Firewall nach Installation von Internet Shield deaktivieren

[FSBWINST.DLL]	**Einstellungen für Automatic Update Agent**
RequestInstallMode=1	`0` = Diese Komponente installieren wie definiert in`InstallMode`Einstellung. `1` = Die Komponente nur installieren, falls es sich um eine neuere Version handelt oder sie bisher nicht installiert war (Standard). `2` = Die Komponente installieren, wenn sie noch nicht installiert ist oder wenn eine ältere oder gleiche Version vorhanden ist.
InstallMode=0 | 1	`0` =Die Komponente wird nicht installiert (Standard). `1` = Die Komponente wird installiert, es sei denn, eine neuere Version ist bereits vorhanden.

[FSPSINST.DLL]	**Einstellungen für Client Security-Netzwerk-Scanning**
RequestInstallMode=1	`0` = Diese Komponente installieren wie definiert in`InstallMode`Einstellung. `1` = Die Komponente nur installieren, falls es sich um eine neuere Version handelt oder sie bisher nicht installiert war (Standard). `2` = Die Komponente installieren, wenn sie noch nicht installiert ist oder wenn eine ältere oder gleiche Version vorhanden ist.
Debug=0 | 1	`0` = Debugging-Informationen werden nicht erstellt (Standard). `1` = Debugging-Informationen werden während der Installation und Deinstallation in das Debugging-Protokoll geschrieben.
InstallMode=0 | 1	`0` =Die Komponente wird nicht installiert (Standard). `1` = Die Komponente wird installiert, es sei denn, eine neuere Version ist bereits vorhanden.
DisableScanningForApps= Wget.exe,mplayer.exe	Deaktiviert Netzwerk Scanning bei bestimmten Programmdateien.

[FSPSINST.DLL]	Einstellungen für Client Security-Netzwerk-Scanning
	Die Einstellung besteht aus einer komma-getrennten Liste mit den Namen von Programmdateien ohne Pfadangabe. **Hinweis:** Zwischen den Einträgen dürfen sich keine Leerzeichen befinden.
EnableHTTPScanning=1	`0` = HTTP Scanning deaktivieren 0 = HTTP Scanning aktivieren
StartImmediatelyForApps= iexplore.exe,firefox.exe, netscape.exe,opera.exe, msimn.exe,outlook.exe, mozilla.exe	Diese Einstellung legt fest, bei welchen Programmdateien HTTP Scanning sofort gestartet werden soll. Bei anderen Prozessen startet der Scan-Modus erst nach dem ersten Zugriff auf einen externen Server-Port 80. Die Einstellung besteht aus einer komma-getrennten Liste mit den Namen von Programmdateien ohne Pfadangabe. **Hinweis:** Zwischen den Einträgen dürfen sich keine Leerzeichen befinden.

[FSNACINS.DLL]	Einstellungen für Cisco NAC-Plugin
RequestInstallMode=1	0 = Diese Komponente installieren wie definiert in`InstallMode`Einstellung. `1` = Die Komponente nur installieren, falls es sich um eine neuere Version handelt oder sie bisher nicht installiert war (Standard). `2` = Die Komponente installieren, wenn sie noch nicht installiert ist oder wenn eine ältere oder gleiche Version vorhanden ist.
CTAversion=1.0.55	`CTAversion` gibt die im Lieferumfang enthaltene Version von Cisco Trust Agent an. Das Installationspaket für Cisco Trust Agent kann aktualisiert werden durch den Austausch von`ctasetup.msi`der Datei, in dem Verzeichnis, in dem sich`prodsett.ini` befindet.
Debug=0 | 1	`0` = Debugging-Informationen werden nicht erstellt (Standard). `1` = Debugging-Informationen werden während der Installation und Deinstallation in das Debugging-Protokoll geschrieben.
InstallMode=0 | 1	`0` =Die Komponente wird nicht installiert (Standard). `1` = Die Komponente wird installiert, es sei denn, eine neuere Version ist bereits vorhanden.

Kapitel

15

Alarm- und Fehlermeldungen beim E-Mail-Scanning

Themen:

- *Warn- und Fehlermeldungen*

Hier finden Sie Informationen zu Alarm- und Fehlermeldungen, die beim E-Mail-Scanning ausgegeben werden können.

Dieser Abschnitt enthält eine Liste der Alarm- und Fehlermeldungen, die beim E-Mail-Scanning erzeugt werden können.

Warn- und Fehlermeldungen

Im Folgenden finden Sie eine Liste der vom E-Mail-Scanning erzeugten Meldungen.

Meldungstitel	Meldungs-ID	Definition	Meldungsinhalt
Fehler bei Sitzung zum Scannen von E-Mails: Systemfehler	602		Verbindung mit<Servername>Server wurde durch E-Mail-Scan aufgrund eines Systemfehlers beendet. E-Mail-Scan ist weiterhin funktionstüchtig.
E-Mail Scanning ist fehlerhaft: Systemfehler	603		E-Mail Scanning ist aufgrund eines schwerwiegenden Fehlers nicht mehr funktionsfähig. Wenn das Problem weiterhin auftritt, wenden Sie sich an den Systemadministrator.
Nachrichtenparser zum Scannen von E-Mails ist ausgefallen: Systemfehler	604		Wegen einer Fehlfunktion des Nachrichtenparsers konnte eine E-Mail nicht gescannt werden. Die Sitzung wurde nicht abgebrochen. Die angegebene Nachricht wurde nicht gescannt.
Fehler beim Initialisieren von E-Mail Scanning	610		Die E-Mail-Scan-Initialisierung ist fehlgeschlagen. Grund:<Beschreibung der Ursache siehe oben>
Viruswarnung in Bezug auf eine E-Mail-Anlage	620-623	Wenn ein Virus festgestellt wird, wird er gemäß den Einstellungen in der **erweiterten** Konfiguration von F-Secure Client Security. Mögliche Maßnahmen: • Infektion wurde nur gemeldet • Anlage wurde desinfiziert • Anhang wurde gelöscht	E-Mail-Virusalarm! Infektion: <Name des Virus> Anhang: <E-Mail-Nachrichtenteil; angehängte infizierte Datei> Aktion:<ergriffene Maßnahme> Nachricht<Nachrichten-ID>

Meldungstitel	Meldungs-ID	Definition	Meldungsinhalt
		• Die infizierte E-Mail wurde geblockt	von: `<E-Mail-Kopf: E-Mail-Adresse des Absenders>` an: `<E-Mail-Kopf: E-Mail-Adresse des Empfängers>` Betreff: `<E-Mail-Kopf: Der Betreff der Nachricht>`
Alarm: ""Malformed"" E-Mail	630-633	Wenn eine "malformed" Nachricht festgestellt wird, wird sie gemäß den Einstellungen in der **erweiterten** Konfiguration von F-Secure Client Security behandelt. Mögliche Maßnahmen: • Der "malformed" Nachrichtenteil wurde nur gemeldet • Der "malformed" Nachrichtenteil wurde gelöscht • Die "malformed" E-Mail wurde geblockt	Warnung: Deformierte E-Mail Beschreibung: `<Beschreibung der Fehlbildung>` Nachrichtenteil: `<fehlgebildeter Teil der Nachricht>` Aktion:`<ergriffene Maßnahme>` Nachricht`<Nachrichten-ID>` von: `<E-Mail-Kopf: E-Mail-Adresse des Absenders>` an: `<E-Mail-Kopf: E-Mail-Adresse des Empfängers>` Betreff: `<E-Mail-Kopf: Der Betreff der Nachricht>`
Fehler beim Scannen von E-Mail-Anhängen	640-643	Wenn eine Überprüfung fehlschlägt, wird die Nachricht gemäß den Einstellungen in der **erweiterten** Konfiguration behandelt. Grund für den Scan-Fehler: • Der festgelegte Timeout zur Überprüfung einer Datei wurde ausgelöst. • Der festgelegte Timeout zur Überprüfung einer E-Mail wurde ausgelöst.	Fehler beim Scannen von E-Mail-Anhängen Grund:`<Beschreibung des Scan-Fehlers>` Anhang: `<Der einen Scan-Fehler verursachende Anhang>` Aktion:`<Ergriffene Maßnahme>` Nachricht`<Nachrichten-ID>` von: `<E-Mail-Kopf: E-Mail-Adresse des Absenders>`

Meldungstitel	Meldungs-ID	Definition	Meldungsinhalt
		• Beim Dateianhang handelt es sich um eine passwortgeschützte ZIP-Datei. • Bei der Überprüfung des Anhangs ist ein Fehler aufgetreten (zu wenig Speicherplatz auf dem Datenträger, zu wenig Arbeitsspeicher usw.). Mögliche Maßnahmen • Der Scan-Fehler wurde nur gemeldet. • Anhang wurde gelöscht • Die E-Mail wurde blockiert.	an: `<E-Mail-Kopf: E-Mail-Adresse des Empfängers>` Betreff: `<E-Mail-Kopf: Der Betreff der Nachricht>`