ESET Endpoint Antivirus

Benutzerhandbuch

Klicken Sie hier um die Hilfe-Version dieses Dokuments anzuzeigen

Copyright ©2023 by ESET, spol. s r.o.

ESET Endpoint Antivirus wurde entwickelt von ESET, spol. s r.o.

Weitere Informationen finden Sie unter https://www.eset.com.

Alle Rechte vorbehalten. Kein Teil dieser Dokumentation darf ohne schriftliche Einwilligung des Verfassers reproduziert, in einem Abrufsystem gespeichert oder in irgendeiner Form oder auf irgendeine Weise weitergegeben werden, sei es elektronisch, mechanisch, durch Fotokopien, Aufnehmen, Scannen oder auf andere Art.

ESET, spol. s r.o. behält sich das Recht vor, ohne vorherige Ankündigung Änderungen an allen hier beschriebenen Software-Anwendungen vorzunehmen.

Technischer Support: https://support.eset.com

REV. 19.03.2023

1 ESET Endpoint Antivirus 7 ... 1
1.1 Neuerungen in Version 7 ... 2
1.2 Systemanforderungen ... 3
1.2 Unterstützte Sprachen ... 4
1.3 Prävention ... 5
1.4 Hilfeseiten ... 6
2 Dokumentation für remote verwaltete Endpunkte ... 8
2.1 Einführung in ESET Security Management Center ... 8
2.2 Einführung in ESET PROTECT Cloud ... 9
2.3 Passwortgeschützte Einstellungen ... 9
2.4 Was sind Policies? ... 11
2.4 Zusammenführen von Policies ... 11
2.5 Funktionsweise von Markierungen ... 12
3 ESET Endpoint Antivirus selbst benutzen ... 13
3.1 Installationsmethoden ... 13
3.1 Installation mit ESET AV Remover ... 14
3.1 ESET AV Remover ... 15
3.1 Deinstallation mit ESET AV Remover wurde mit einem Fehler beendet ... 17
3.1 Installation (.exe) ... 18
3.1 Installationsordner ändern (.exe) ... 20
3.1 Installation (.msi) ... 21
3.1 Erweiterte Installation (.msi) ... 23
3.1 Kommandozeileninstallation ... 24
3.1 Remote-Bereitstellung per GPO oder SCCM ... 29
3.1 Upgrade auf eine aktuellere Version ... 29
3.1 Bekannte Probleme bei der Installation ... 30
3.1 Fehler bei der Aktivierung ... 31
3.2 Produktaktivierung ... 31
3.3 Computer-Scan ... 31
3.4 Erste Schritte ... 32
3.4 Die Benutzeroberfläche ... 32
3.4 Einstellungen für Updates ... 36
4 Arbeiten mit ESET Endpoint Antivirus ... 37
4.1 Computer ... 40
4.1 Erkennungsroutine (7.2 und höher) ... 41
4.1 Erweiterte Einstellungen für die Erkennungsroutine ... 46
4.1 Erkennungsroutine (7.1 und niedriger) ... 46
4.1 Eingedrungene Schadsoftware wurde erkannt ... 48
4.1 Gemeinsam genutzter lokaler Cache ... 50
4.1 Echtzeit-Dateischutz ... 51
4.1 Echtzeit-Dateischutz prüfen ... 52
4.1 Wann sollten die Einstellungen für den Echtzeit-Dateischutz geändert werden? ... 52
4.1 Vorgehensweise bei fehlerhaftem Echtzeit-Dateischutz ... 53
4.1 Computerprüfung ... 53
4.1 Benutzerdefinierte Prüfung ... 55
4.1 Stand der Prüfung ... 57
4.1 Computerprüfungs-Log ... 58
4.1 Malware-Scans ... 59
4.1 Scan im Leerlaufbetrieb ... 59
4.1 Prüfprofile ... 60

4.1 Zu prüfende Objekte ... 60
4.1 Erweiterte Optionen für Scans ... 60
4.1 Medienkontrolle ... 61
4.1 Regel-Editor für die Medienkontrolle ... 62
4.1 Erkannte Geräte ... 63
4.1 Gerätegruppen ... 63
4.1 Hinzufügen von Regeln für die Medienkontrolle ... 64
4.1 Host-based Intrusion Prevention System (HIPS) ... 66
4.1 HIPS-Interaktionsfenster ... 69
4.1 Mögliches Ransomware-Verhalten erkannt ... 70
4.1 HIPS-Regelverwaltung ... 70
4.1 HIPS-Regeleinstellungen ... 71
4.1 Erweiterte HIPS-Einstellungen ... 74
4.1 Treiber dürfen immer geladen werden ... 75
4.1 Präsentationsmodus ... 75
4.1 Scan der Systemstartdateien ... 75
4.1 Prüfung Systemstartdateien ... 76
4.1 Dokumentenschutz ... 76
4.1 Ausschlussfilter ... 77
4.1 Leistungsausschlüsse ... 77
4.1 Leistungsausschluss hinzufügen oder bearbeiten ... 79
4.1 Format für ausgeschlossene Pfade ... 81
4.1 Ereignisausschlüsse ... 81
4.1 Ereignisausschluss hinzufügen oder bearbeiten ... 84
4.1 Assistent zum Erstellen von Ereignisausschlüssen ... 85
4.1 Ausschlüsse (7.1 und niedriger) ... 85
4.1 Ausgeschlossene Prozesse ... 86
4.1 Ausgeschlossene Prozesse hinzufügen oder bearbeiten ... 87
4.1 HIPS-Ausschlüsse ... 87
4.1 ThreatSense-Parameter ... 88
4.1 Säuberungsstufen ... 91
4.1 Von der Prüfung ausgeschlossene Dateiendungen ... 93
4.1 Zusätzliche ThreatSense-Parameter ... 94
4.2 Netzwerk ... 94
4.2 Netzwerkangriffsschutz ... 95
4.2 Erweiterte Filteroptionen ... 95
4.2 IDS-Ausnahmen ... 97
4.2 Verdächtige Bedrohung blockiert ... 99
4.2 Fehlerbehebung für den Netzwerkschutz ... 99
4.2 Vorübergehende Negativliste der IP-Adressen ... 100
4.2 Lösen von Problemen mit der ESET Firewall ... 100
4.2 Fehlerbehebungsassistent ... 101
4.2 Erstellen von Logs und Erstellen von Regeln oder Ausnahmen anhand des Logs ... 101
4.2 Regel aus Log erstellen ... 101
4.2 Erstellen von Ausnahmen von Firewall-Hinweisen ... 102
4.2 Erweitertes PCAP-Logging ... 102
4.2 Lösen von Problemen bei der Protokollfilterung ... 102
4.3 Web und E-Mail ... 104
4.3 Prüfen von Anwendungsprotokollen ... 104
4.3 Ausgeschlossene Anwendungen ... 105
4.3 Ausgeschlossene IP-Adressen ... 106

4.3 SSL/TLS ... 107
4.3 Zertifikate ... 108
4.3 Verschlüsselte Netzwerkverbindung ... 109
4.3 Liste bekannter Zertifikate ... 109
4.3 Liste der vom SSL/TLS-Filter betroffenen Anwendungen ... 110
4.3 E-Mail-Schutz ... 111
4.3 E-Mail-Protokolle ... 112
4.3 E-Mail-Warnungen und Hinweise ... 113
4.3 Integration mit E-Mail-Programmen ... 114
4.3 Microsoft Outlook-Symbolleiste ... 114
4.3 Symbolleisten für Outlook Express und Windows Mail ... 115
4.3 Bestätigungsfenster ... 115
4.3 E-Mails erneut prüfen ... 115
4.3 Web-Schutz ... 116
4.3 Erweiterte Einstellungen für den Web-Schutz ... 118
4.3 Webprotokolle ... 118
4.3 URL-Adressverwaltung ... 119
4.3 URL-Adressliste ... 120
4.3 Erstellen einer neuen URL-Adressliste ... 121
4.3 Hinzufügen einer URL-Maske ... 122
4.3 Phishing-Schutz ... 123
4.4 Aktualisieren des Programms ... 124
4.4 Einstellungen für Updates ... 128
4.4 Update-Rollback ... 131
4.4 Updates für Programmkomponenten ... 132
4.4 Verbindungsoptionen ... 133
4.4 Update-Mirror ... 135
4.4 HTTP-Server ... 136
4.4 Aktualisieren über Update-Mirror ... 137
4.4 Fehlerbehebung bei Problemen mit Updates über Update-Mirror ... 139
4.4 So erstellen Sie Update-Tasks ... 140
4.5 Tools ... 140
4.5 Log-Dateien ... 141
4.5 Log-Filter ... 144
4.5 Log-Dateien ... 145
4.5 Audit-Logs ... 146
4.5 Taskplaner ... 147
4.5 Schutzstatistiken ... 150
4.5 Aktivität beobachten ... 151
4.5 ESET SysInspector ... 152
4.5 Cloudbasierter Schutz ... 153
4.5 Ausschlussfilter für den cloudbasierten Schutz ... 156
4.5 Ausgeführte Prozesse ... 157
4.5 Sicherheitsbericht ... 158
4.5 ESET SysRescue Live ... 160
4.5 Proben zur Analyse einreichen ... 160
4.5 Probe für die Analyse auswählen - Verdächtige Datei ... 162
4.5 Probe für die Analyse auswählen - Verdächtige Webseite ... 162
4.5 Probe für die Analyse auswählen - Fehlalarm Datei ... 162
4.5 Probe für die Analyse auswählen - Fehlalarm Webseite ... 163
4.5 Probe für die Analyse auswählen - Sonstiges ... 163

4.5 Benachrichtigungen 163
4.5 Anwendungsbenachrichtigungen 164
4.5 Desktophinweise 165
4.5 E-Mail-Benachrichtigungen 166
4.5 Anpassen der Benachrichtigungen 168
4.5 Quarantäne 168
4.5 Einstellungen für den Proxyserver 170
4.5 Zeitfenster 171
4.5 Microsoft Windows Update 172
4.5 Lizenzintervall überprüfen 173
4.6 Benutzeroberfläche 173
4.6 Elemente der Benutzeroberfläche 174
4.6 Anzuzeigende Hinweise 175
4.6 Einstellungen für den Zugriff 176
4.6 Passwort für erweiterte Einstellungen 177
4.6 Warnungen und Hinweisfenster 178
4.6 Interaktive Warnungen 180
4.6 Bestätigungsnachrichten 181
4.6 Erweiterte Einstellungen-Konfliktfehler 182
4.6 Neustart erforderlich 182
4.6 Neustart empfohlen 184
4.6 Wechselmedien 185
4.6 Symbol im Infobereich der Taskleiste 186
4.6 Kontextmenü 188
4.6 Hilfe und Support 188
4.6 Info zu ESET Endpoint Antivirus 189
4.6 Systemkonfigurationsdaten senden 190
4.6 Profilmanager 190
4.6 Tastaturbefehle 191
4.6 Diagnose 192
4.6 Befehlszeilenscanner 193
4.6 ESET CMD 195
4.6 Leerlauferkennung 198
4.6 Import-/Export-Einstellungen 198
4.6 Alle Standardeinstellungen wiederherstellen 199
4.6 Alle Einstellungen in aktuellem Bereich zurücksetzen 199
4.6 Fehler beim Speichern der Konfiguration 200
4.6 Remoteüberwachung und -Verwaltung 200
4.6 ERMM-Kommandozeile 201
4.6 Liste der ERMM JSON-Befehle 203
4.6 Schutzstatus abrufen 204
4.6 Anwendungsinformationen abrufen 205
4.6 Lizenzinformationen abrufen 207
4.6 Logs abrufen 207
4.6 Aktivierungsstatus abrufen 209
4.6 Prüfungsinformationen abrufen 209
4.6 Konfiguration abrufen 210
4.6 Updatestatus abrufen 211
4.6 Prüfung starten 212
4.6 Aktivierung starten 213
4.6 Deaktivierung starten 214

4.6 Update starten 215
4.6 Konfiguration festlegen 216
5 Häufig gestellte Fragen 216
5.1 So aktualisieren Sie ESET Endpoint Antivirus 217
5.2 So aktivieren Sie ESET Endpoint Antivirus 218
5.2 Anmelden bei ESET Business Account 219
5.2 Aktivieren von neueren ESET-Endpunktprodukten mit veralteten Lizenzdaten 219
5.3 So entfernen Sie einen Virus von Ihrem PC 219
5.4 So erstellen Sie eine neue Aufgabe im Taskplaner 219
5.4 So planen Sie eine wöchentliche Computerprüfung 220
5.5 So verbinden Sie ESET Endpoint Antivirus mit ESET Security Management Center 221
5.5 Verwenden des Override-Modus 221
5.5 Anwenden einer empfohlenen Policy für ESET Endpoint Antivirus 223
5.6 So konfigurieren Sie einen Mirror 226
5.7 Wie aktualisiere ich auf Windows 10 mit ESET Endpoint Antivirus 226
5.8 Aktivieren der Remoteüberwachung und -verwaltung 227
5.9 Download bestimmter Dateitypen aus dem Internet blockieren 230
5.10 Minimieren der ESET Endpoint Antivirus-Benutzeroberfläche 231
6 Endbenutzer-Lizenzvereinbarung 231
7 Datenschutzrichtlinie 238

ESET Endpoint Antivirus 7

ESET Endpoint Antivirus 7 ist ein neuer Ansatz für vollständig integrierte Computersicherheit. Die neueste Version des ThreatSense®-Prüfmoduls arbeitet schnell und präzise zum Schutz Ihres Computers. Auf diese Weise ist ein intelligentes System entstanden, das permanent vor Angriffen und bösartiger Software schützt, die Ihren Computer gefährden.

ESET Endpoint Antivirus 7 ist eine umfassende Security-Lösung und das Produkt unserer langfristigen Bemühung, maximalen Schutz bei minimaler Systembelastung zu bieten. Mithilfe der auf künstlicher Intelligenz basierenden Spitzentechnologien kann das Eindringen von Viren, Spyware, Trojanern, Würmern, Adware, Rootkits und anderer durch das Internet übertragener Angriffe aktiv verhindert werden, ohne dass die Systemleistung beeinträchtigt oder Ihr Computer vom Netz getrennt würde.

ESET Endpoint Antivirus 7 wurde hauptsächlich für den Einsatz auf Workstations in kleineren Unternehmen entwickelt.

Die Hilfethemen im Abschnitt ESET Endpoint Antivirus selbst benutzen sind in verschiedene Kapitel und Unterkapitel unterteilt, um Orientierung und Kontext zu liefern, wie etwa für Download, Installation und Aktivierung.

Mit ESET Endpoint Antivirus und ESET Security Management Center in einer Firmenumgebung können Sie eine beliebige Anzahl von Client-Workstations verwalten, Policies und Regeln anwenden, Erkennungen überwachen und Clients von beliebigen Computern im Netzwerk remote konfigurieren.

Im Kapitel Häufig gestellte Fragen werden einige der häufigsten Fragen und Probleme behandelt.

Funktionen und Vorteile

Neu gestaltete Benutzeroberfläche	Die Benutzeroberfläche wurde in dieser Version zu großen Teilen umgestaltet und anhand unserer Tests zur Benutzerfreundlichkeit vereinfacht. Die Texte für Bedienelemente und Benachrichtigungen wurden sorgfältig geprüft, und die Benutzeroberfläche unterstützt jetzt Sprachen mit Schriftbild von rechts nach links, z. B. Hebräisch und Arabisch. Die Online-Hilfe ist jetzt in ESET Endpoint Antivirus integriert und enthält dynamisch aktualisierte Support-Inhalte.
Viren- und Spyware-Schutz	Erkennt und entfernt proaktiv eine Vielzahl bekannter und unbekannter Viren, Würmern, Trojanern und Rootkits. Advanced Heuristik erkennt selbst vollkommen neue Malware und schützt Ihren Computer vor unbekannten Bedrohungen, die abgewendet werden, bevor sie Schaden anrichten können. Web-Schutz und Phishing-Schutz überwachen die Kommunikation zwischen Webbrowsern und Remoteservern (einschließlich SSL-Verbindungen). Der E-Mail-Schutz dient der Überwachung eingehender E-Mails, die mit dem POP3(S)- oder dem IMAP(S)-Protokoll übertragen werden.
Reguläre Updates	Aktualisieren Sie die Erkennungsroutine (bisher auch als „Signaturdatenbank“ bezeichnet) und die Programmmodule regelmäßig, um einen optimalen Schutz Ihres Computers sicherzustellen.
ESET LiveGrid® (Cloud-basierter Reputations-Check)	Sie können die Reputation ausgeführter Prozesse und Dateien direkt mit ESET Endpoint Antivirus überprüfen.

Remote Management	Mit ESET Security Management Center können Sie ESET-Produkte auf Arbeitsstationen, Servern und Mobilgeräten in einer Netzwerkumgebung von einem zentralen Standort aus verwalten. Mit der ESET Security Management Center-Web-Konsole (ESMC-Web-Konsole) können Sie ESET-Lösungen bereitstellen, Tasks verwalten, Sicherheits-Policies umsetzen, den Systemstatus überwachen und schnell auf Probleme oder Bedrohungen auf Remotecomputern reagieren.
Netzwerkangriffsschutz	Analysiert den Inhalt von Netzwerkverkehr und schützt vor Angriffen aus dem Netzwerk. Jeglicher als schädlich erkannter Verkehr wird blockiert.
Web-Kontrolle (nur ESET Endpoint Security)	Mit der Web-Kontrolle können Sie Webseiten sperren, die potenziell Unerlaubtes enthalten könnten. Außerdem können Arbeitgeber oder Systemadministratoren mit dieser Funktion den Zugriff auf über 27 vordefinierte Webseitenkategorien und über 140 Unterkategorien unterbinden.

Neuerungen in Version 7

ESET Endpoint Antivirus 7 wurde veröffentlicht und steht zum Download bereit.

Neuigkeiten in ESET Endpoint Antivirus 7.0

- Neu gestaltete grafische Benutzeroberfläche.
- Prüfen per Ziehen und Ablegen – Sie können eine Datei oder einen Ordner in den markierten Bereich ziehen, um diese manuell zu prüfen.
- Der Netzwerkangriffsschutz ist jetzt in ESET Endpoint Antivirus verfügbar. Weitere Informationen finden Sie unter Netzwerkangriffsschutz.
- Unter Schutzstatus können Quicklinks jetzt mit einer ESET Security Management Center-Policy deaktiviert werden.
- Regeln für die Medienkontrolle können jetzt für ein bestimmtes Zeitfenster angewendet werden. Weitere Informationen finden Sie unter Zeitfenster.

Neuigkeiten in ESET Endpoint Antivirus 7.1

- Neuer Logging-Typ - Erweiterte Logging-Typen sind jetzt verfügbar. Weitere Informationen finden Sie unter Audit-Logs.

Neuigkeiten in ESET Endpoint Antivirus 7.2

- Das erweiterte Machine Learning ist als zusätzliche Schutzebene verfügbar, um die Erkennung auf Basis von Machine Learning zu verbessern. Weitere Informationen zu diesem Schutztyp finden Sie im Glossar. Der Abschnitt Erkennungsroutine einrichten enthält keine EIN-/AUS-Schalter mehr wie in Version 7.1 und niedriger. Die EIN-/AUS-Schalter wurden durch vier Schwellenwerte ersetzt: Aggressiv, Ausgewogen, Vorsichtig und Aus.
- Lettische Lokalisierung hinzugefügt.
- Änderungen an Ausschlüssen. Mit Leistungsausschlüssen können Sie Dateien und Ordner vom Scannen ausschließen. Mit Ereignisausschlüssen können Sie Objekte nach Ereignisname, Pfad oder Hash von der Säuberung ausschließen.

- Das neue HIPS-Programm-Modul verwendet eine tiefe Verhaltensinspektion, um das Verhalten aller auf dem Computer ausgeführten Programme zu analysieren und Sie vor bösartigen Verhaltensweisen zu warnen. Weitere Informationen zu HIPS finden Sie auf unseren Hilfeseiten.

- Unter Konfigurierbare interaktive Warnungen können Sie das Verhalten für konfigurierbare interaktive Warnungen anpassen, z. B. um die Warnung „Neustart empfohlen“ auf Endpunktcomputern auszublenden.

Neuigkeiten in ESET Endpoint Antivirus 7.3

- Diese Nebenversion enthält verschiedene Bugfixes und Leistungsverbesserungen.

Weitere Informationen und Screenshots zu den neuen Funktionen in ESET Endpoint Antivirus finden Sie im folgenden ESET Knowledgebase-Artikel:

- Neuigkeiten in ESET Endpoint Antivirus 7

Systemanforderungen

Für einen reibungslosen Betrieb von ESET Endpoint Antivirus sollten die folgenden Hardware- und Softwareanforderungen erfüllt sein (Produktstandardeinstellungen):

Unterstützte Prozessoren

32-Bit (x86)-Prozessor mit SSE2-Anweisungssatz oder 64-Bit (x64)-Prozessor, 1 GHz oder höher

Betriebssysteme

Microsoft® Windows® 10
Microsoft® Windows® 8.1
Microsoft® Windows® 8

Microsoft® Windows® 7 SP1 mit den neuesten Windows-Updates (mindestens KB4474419 und KB4490628)

Windows XP und Windows Vista werden für Version 7 nicht mehr unterstützt.

Sonstige

- Die Systemanforderungen des Betriebssystems und sonstiger auf dem Computer installierter Software sind erfüllt

- 0,3 GB freier Systemarbeitsspeicher (siehe Hinweis 1)

- 1 GB freier Festplattenspeicher (siehe Hinweis 2)

- Minimale Display-Auflösung 1024 x 768

- Internetverbindung oder LAN-Verbindung zu einer Quelle (siehe Hinweis 3) für Produkt-Updates

Das Produkt kann theoretisch auch auf Systemen installiert und ausgeführt werden, die diese Anforderungen

nicht erfüllen. Wir empfehlen jedoch einen Vorab-Test zur Benutzerfreundlichkeit auf Grundlage von Leistungsanforderungen.

> **Hinweis**
> (1): Das Produkt kann mehr Arbeitsspeicher belegen, wenn dieser ansonsten ungenutzt auf einem stark infizierten Computer wäre oder wenn große Datenlisten (z. B. URL-Positivlisten) in das Produkt importiert werden.
> (2): Der Speicherplatz wird zum Herunterladen des Installationsassistenten, zur Produktinstallation und zur Aufbewahrung einer Kopie des Installationsprogramms in den Programmdaten sowie für Sicherungen von Produkt-Updates zur Unterstützung der Rollback-Funktion benötigt. Das Produkt kann bei abweichenden Einstellungen mehr Speicherplatz belegen (z. B. wenn weitere Sicherungsversionen von Produkt-Updates gespeichert und Speicherabbilder oder große Mengen an Log-Einträgen aufbewahrt werden) oder bei einer Infektion des Computers (z. B. durch die Quarantänefunktion). Wir empfehlen, stets auf genügend freien Speicherplatz zu achten, damit Updates des Betriebssystems und des ESET-Produkts unterstützt werden.
> (3): Das Produkt kann auch über einen Wechseldatenträger manuell aktualisiert werden (nicht empfohlen).

Unterstützte Sprachen

Sie können ESET Endpoint Antivirus in den folgenden Sprachen installieren und herunterladen.

Sprache	Sprachcode	LCID
United States	en-US	1033
Arabisch (Ägypten)	ar-EG	3073
Bulgarisch	bg-BG	1026
Chinesisch vereinfacht	zh-CN	2052
Chinesisch traditionell	zh-TW	1028
Kroatisch	hr-HR	1050
Tschechisch	cs-CZ	1029
Estnisch	et-EE	1061
Finnisch	fi-FI	1035
Französisch (Frankreich)	fr-FR	1036
Französisch (Kanada)	fr-CA	3084
Deutsch (Deutschland)	de-DE	1031
Griechisch	el-GR	1032
*Hebräisch	he-IL	1037
Ungarisch	hu-HU	1038
*Indonesisch	id-ID	1057
Italienisch	it-IT	1040
Japanisch	ja-JP	1041
Kasachisch	kk-KZ	1087
Koreanisch	ko-KR	1042

*Lettisch	lv-LV	1062
Litauisch	lt-LT	1063
Norwegisch	nn-NO	1044
Polnisch	pl-PL	1045
Portugiesisch (Brasilien)	pt-BR	1046
Rumänisch	ro-RO	1048
Russisch	ru-RU	1049
Spanisch (Chile)	es-CL	13322
Spanisch (Spanien)	es-ES	3082
Schwedisch (Schweden)	sv-SE	1053
Slowakisch	sk-SK	1051
Slowenisch	sl-SI	1060
Thai	th-TH	1054
Türkisch	tr-TR	1055
*Vietnamesisch	vi-VN	1066

* ESET Endpoint Antivirus ist in dieser Sprache verfügbar, aber das Online-Benutzerhandbuch ist nicht verfügbar (Weiterleitung zur englischen Version).

Um die Sprache dieses Online-Benutzerhandbuchs zu ändern, verwenden Sie das Sprachauswahlfeld (in der oberen rechten Ecke).

Prävention

Bei der Arbeit am Computer und besonders beim Surfen im Internet sollten Sie sich darüber im Klaren sein, dass kein Virenschutz der Welt die mit Infiltrationen und Angriffen verbundenen Gefahren komplett eliminieren kann. Für maximalen Schutz und optimalen Komfort müssen Sie die Virenschutzsoftware richtig einsetzen und dabei einige wichtige Regeln beachten:

Führen Sie regelmäßige Updates durch

Gemäß von ESET LiveGrid® erhobenen Statistiken werden täglich tausende neuartige Schadprogramme zur Umgehung bestehender Sicherheitsmaßnahmen entwickelt, die den Entwicklern Vorteile auf Kosten anderer Benutzer verschaffen sollen. Die Experten aus dem Virenlabor von ESET analysieren diese Bedrohungen täglich und veröffentlichen Updates zur kontinuierlichen Verbesserung des Virenschutzes. Die richtige Konfiguration der Updates ist von wesentlicher Bedeutung für die Gewährleistung eines optimalen Schutzes. Weitere Informationen zur Konfiguration von Updates finden Sie im Kapitel Einstellungen für Updates.

Laden Sie Sicherheitspatches herunter

Die Entwickler von Schadsoftware nutzen oft Sicherheitslücken im System aus, um möglichst effektiv Schadcode zu verbreiten. Softwareunternehmen halten daher regelmäßig Ausschau nach neuen Sicherheitslücken in den eigenen Anwendungen und veröffentlichen Sicherheitsupdates zur Bekämpfung potenzieller Bedrohungen. Es ist wichtig, dass Sie diese Updates umgehend nach der Veröffentlichung herunterladen. Microsoft Windows und Webbrowser wie Internet Explorer sind Beispiele für Programme, für die regelmäßig Sicherheitsaktualisierungen veröffentlicht werden.

Sichern wichtiger Daten

Malware-Entwickler missachten die Interessen der Benutzer und legen mit ihrer Software oft das gesamte Betriebssystem lahm bzw. nehmen den Verlust wichtiger Daten bewusst in Kauf. Es ist wichtig, dass Sie Ihre wichtigen und vertraulichen Daten regelmäßig auf einem externen Speichermedium (z. B. einer DVD oder einer externen Festplatte) sichern. So können Sie Ihre Daten bei einem Systemfehler viel einfacher und schneller wiederherstellen.

Prüfen Sie Ihren Computer regelmäßig auf Viren

Der Echtzeit-Dateischutz erkennt eine größere Zahl bekannter und unbekannter Viren, Würmer, Trojaner und Rootkits. Jedes Mal, wenn Sie eine Datei öffnen oder auf eine Datei zugreifen, wird die Datei auf Schadcode überprüft. Sie sollten jedoch mindestens einmal im Monat eine vollständige Prüfung des Computers ausführen, da Schadcode die verschiedensten Formen annehmen kann und die Erkennungsroutine täglich aktualisiert wird.

Halten Sie grundlegende Sicherheitsregeln ein

Die nützlichste und effektivste Regel von allen ist das Prinzip ständiger Wachsamkeit. Heutzutage erfordert ein Großteil der Schadsoftware zur Ausführung und Ausbreitung ein Eingreifen des Benutzers. Wenn Sie beim Öffnen neuer Dateien achtsam sind, sparen Sie viel Zeit und Aufwand, die Sie andernfalls darauf verwenden müssten, eingedrungene Schadsoftware zu entfernen. Hier finden Sie einige nützliche Richtlinien:

- Besuchen Sie keine zweifelhaften Websites, die durch zahlreiche Popup-Fenster und bunte Werbeanzeigen auffallen.
- Seien Sie vorsichtig bei der Installation von Programmen, Codec-Paketen usw. Verwenden Sie nur sichere Programme, und besuchen Sie ausschließlich sichere Websites.
- Seien Sie vorsichtig beim Öffnen von E-Mail-Anhängen, insbesondere wenn es sich um Anhänge von Massen-E-Mails und E-Mail-Nachrichten mit unbekanntem Absender handelt.
- Verwenden Sie für die tägliche Arbeit mit dem Computer kein Administratorkonto.

Hilfeseiten

Herzlich willkommen auf den Hilfeseiten von ESET Endpoint Antivirus. Die hier bereitgestellten Informationen machen Sie mit dem Produkt vertraut und Ihren Computer sicherer.

Erste Schritte

Bevor Sie ESET Endpoint Antivirus einsetzen, sollten Sie wissen, dass das Produkt sowohl von über ESET Security Management Center verbundenen Benutzern als auch von von Benutzern selbst verwendet werden kann. Außerdem sollten Sie sich Sie sich mit den verschiedenenArten von Ereignissen und Remoteangriffen vertraut machen, die beim Arbeiten mit dem Computer auftreten können.

Unter Neue Funktionen finden Sie Informationen zu Funktionen, die in dieser Version von ESET Endpoint Antivirus neu hinzugekommen sind. Wir haben eine Anleitung vorbereitet, die Ihnen beim Einrichten und Anpassen der wichtigsten Einstellungen von ESET Endpoint Antivirus behilflich sein soll.

So finden Sie sich auf den Hilfeseiten von ESET Endpoint Antivirus zurecht

Die Hilfethemen sind in verschiedene Kapitel und Unterkapitel unterteilt, damit Sie sich besser orientieren können und den Zusammenhang zwischen den Themen erfassen. Um die passenden Informationen zu finden, navigieren Sie durch die Struktur der Hilfeseiten.

Drücken Sie **F1**, um weitere Informationen zu den einzelnen Programmfenstern zu erhalten. Die Hilfeseite zu dem aktuell angezeigten Fenster wird angezeigt.

Sie können die Hilfeseiten nach Stichwörtern oder nach Wörtern oder Sätzen durchsuchen. Der Unterschied zwischen diesen beiden Methoden ist, dass ein Stichwort logisch mit einer Hilfeseite verknüpft sein kann, ohne dass das Stichwort selbst im Text vorkommt. Bei der Suche nach Wörtern und Formulierungen wird der gesamte Inhalt aller Seiten durchsucht, und es werden nur diejenigen Seiten angezeigt, die das gesuchte Wort bzw. die gesuchte Formulierung enthalten.

Aus Konsistenzgründen und um Verwechslungen zu vermeiden, basiert die Terminologie in dieser Anleitung auf den ESET Endpoint Antivirus-Parameternamen. Außerdem verwenden wir einheitliche Symbole, um besonders wichtige Themen hervorzuheben.



HINWEIS
Notizen sind lediglich kurze Anmerkungen. Diese Notizen können zwar ausgelassen werden, enthalten jedoch wichtige Informationen wie z. B. spezielle Funktionen oder Links zu verwandten Themen.



Wichtig
Diese Abschnitte erfordern Ihre Aufmerksamkeit und sollten nicht übersprungen werden. Normalerweise handelt es sich um nicht kritische, jedoch wichtige Informationen.



Warning
Diese Informationen erfordern besondere Aufmerksamkeit und Vorsicht. Warnungen dienen dazu, Sie vor potenziell schädlichen Fehlern zu schützen. Der Text in Warnhinweisen weist auf besonders empfindliche Systemeinstellungen oder riskante Vorgänge hin und muss daher unbedingt gelesen und verstanden werden.



Beispiel
Dieses praktische Anwendungsbeispiel hilft Ihnen dabei, sich mit einer bestimmten Funktion vertraut zu machen.

Konvention	Bedeutung
Fettdruck	Namen von Elementen der Benutzeroberfläche, z. B. Schaltflächen und Optionsfelder.
Kursivdruck	Platzhalter für Informationen, die Sie eingeben. Dateiname oder Pfad bedeutet z. B, dass Sie den tatsächlichen Pfad oder den Namen einer Datei angeben.
`Courier New`	Codebeispiele oder Befehle.
Hyperlinks	Schnellzugriff auf verwandte Themen oder externe Webadressen. Hyperlinks sind in Blau hervorgehoben und normalerweise unterstrichen.
%ProgramFiles%	Das Windows-Systemverzeichnis, in dem die unter Windows installierten Programme gespeichert sind.

Die Onlinehilfe ist die primäre Quelle für Hilfeinhalte. Bei funktionierender Internetverbindung wird automatisch die neueste Version der Onlinehilfe angezeigt.

Dokumentation für remote verwaltete Endpunkte

ESET-Unternehmensprodukte und ESET Endpoint Antivirus können auf Client-Workstations, Servern und Mobilgeräten in einer Netzwerkumgebung von einem zentralen Ort aus remote verwaltet werden. Systemadministratoren mit mehr als 10 Client-Arbeitsstationen können die ESET-Remoteverwaltungstools bereitstellen, um ESET-Lösungen zu installieren, Tasks zu verwalten, Sicherheits-Policies zu erzwingen, den Systemstatus zu überwachen und von einem zentralen Ort aus schnell auf Probleme oder Bedrohungen auf Remotecomputern reagieren zu können.

ESET-Remoteverwaltungstools

ESET Endpoint Antivirus kann entweder mit ESET Security Management Center oder mit ESET PROTECT Cloud remote verwaltet werden.

- Einführung in ESET Security Management Center
- Einführung in ESET PROTECT Cloud

Externe Remoteverwaltungstools

- Remoteüberwachung und -Verwaltung (RMM)

Best Practices

- Verbinden Sie alle Endpunkte, auf denen ESET Endpoint Antivirus installiert ist, mit ESET Security Management Center
- Schützen Sie die erweiterten Einstellungen auf verbundenen Clientcomputern, um unbefugte Änderungen zu verhindern
- Wenden Sie eine empfohlene Policy an, um die verfügbaren Sicherheitsfunktionen zu nutzen
- Minimieren Sie die Benutzeroberfläche, um die Interaktion der Benutzer mit ESET Endpoint Antivirus zu reduzieren oder einzuschränken

Anleitungen

- Verwenden des Override-Modus
- Bereitstellen von ESET Endpoint Antivirus mit GPO oder SCCM

Einführung in ESET Security Management Center

Mit ESET Security Management Center können Sie ESET-Produkte auf Workstations, Servern und Mobilgeräten in einer Netzwerkumgebung von einem zentralen Ort aus verwalten.

ESET Security Management Center (ESMC) gehört zu einer neuen Generation von Remoteverwaltungssystemen und unterscheidet sich deutlich von früheren Versionen von ESET Remote Administrator (ERA). Da die Architektur komplett geändert wurde, ist ESET Security Management Center 7 nur eingeschränkt mit ERA 6 kompatibel, und

es besteht keine Abwärtskompatibilität mit ERA 5. Die Kompatibilität mit früheren Versionen von ESET-Sicherheitsprodukten bleibt jedoch erhalten.

Um das vollständige Portfolio der ESET-Sicherheitslösungen bereitzustellen, müssen die folgenden Komponenten installiert werden (Windows- und Linux-Plattformen):

- ESMC Server
- ESMC Web-Konsole
- ESET Management Agent

Die folgenden zusätzlichen Komponenten sind optional, sollten jedoch für eine optimale Ausführung der Anwendung im Netzwerk installiert werden:

- RD Sensor
- Apache HTTP Proxy
- Mobile Device Connector

Mit der ESET Security Management Center-Web-Konsole (ESMC-Web-Konsole) können Sie ESET-Lösungen bereitstellen, Tasks verwalten, Sicherheits-Policies erzwingen, den Systemstatus überwachen und schnell auf Probleme oder Bedrohungen auf Remotecomputern reagieren.



Weitere Informationen
Weitere Informationen finden Sie online im ESET Security Management Center-Benutzerhandbuch.

Einführung in ESET PROTECT Cloud

Mit ESET PROTECT Cloud können Sie ESET-Produkte auf Arbeitsstationen und Servern in einer Netzwerkumgebung von einem zentralen Standort aus verwalten, ohne physische oder virtuelle Server zu benötigen wie für ESMC. Mit der ESET PROTECT Cloud-Web-Konsole können Sie ESET-Lösungen bereitstellen, Tasks verwalten, Sicherheits-Policies umsetzen, den Systemstatus überwachen und schnell auf Probleme oder Bedrohungen auf Remotecomputern reagieren.

- Weitere Informationen finde Sie online im ESET PROTECT Cloud-Benutzerhandbuch

Passwortgeschützte Einstellungen

Um Ihr System optimal schützen zu können, muss ESET Endpoint Antivirus korrekt konfiguriert werden. Unbedachte Änderungen oder Einstellungen können die Clientsicherheit gefährden und die Schutzebene senken. Administratoren können die Einstellungen mit einem Passwort schützen, um den Benutzerzugriff auf die erweiterten Einstellungen einzuschränken.

Administratoren können eine Policy erstellen, um die erweiterten Einstellungen für ESET Endpoint Antivirus auf verbundenen Clientcomputern mit einem Passwort zu schützen. So erstellen Sie eine neue Policy:

1. Klicken Sie im linken Menü in der ESMC-Web-Konsole auf **Policies**.

2. Klicken Sie auf **Neue Policy**.

3. Benennen Sie Ihre neue Policy und geben Sie optional eine kurze Beschreibung ein. Klicken Sie auf die Schaltfläche **Weiter**.

4. Wählen Sie **ESET Endpoint für Windows** in der Liste der Produkte aus.

5. Klicken Sie auf **Benutzeroberfläche** in der Liste der **Einstellungen** und erweitern Sie den Eintrag **Einstellungen für den Zugriff**.

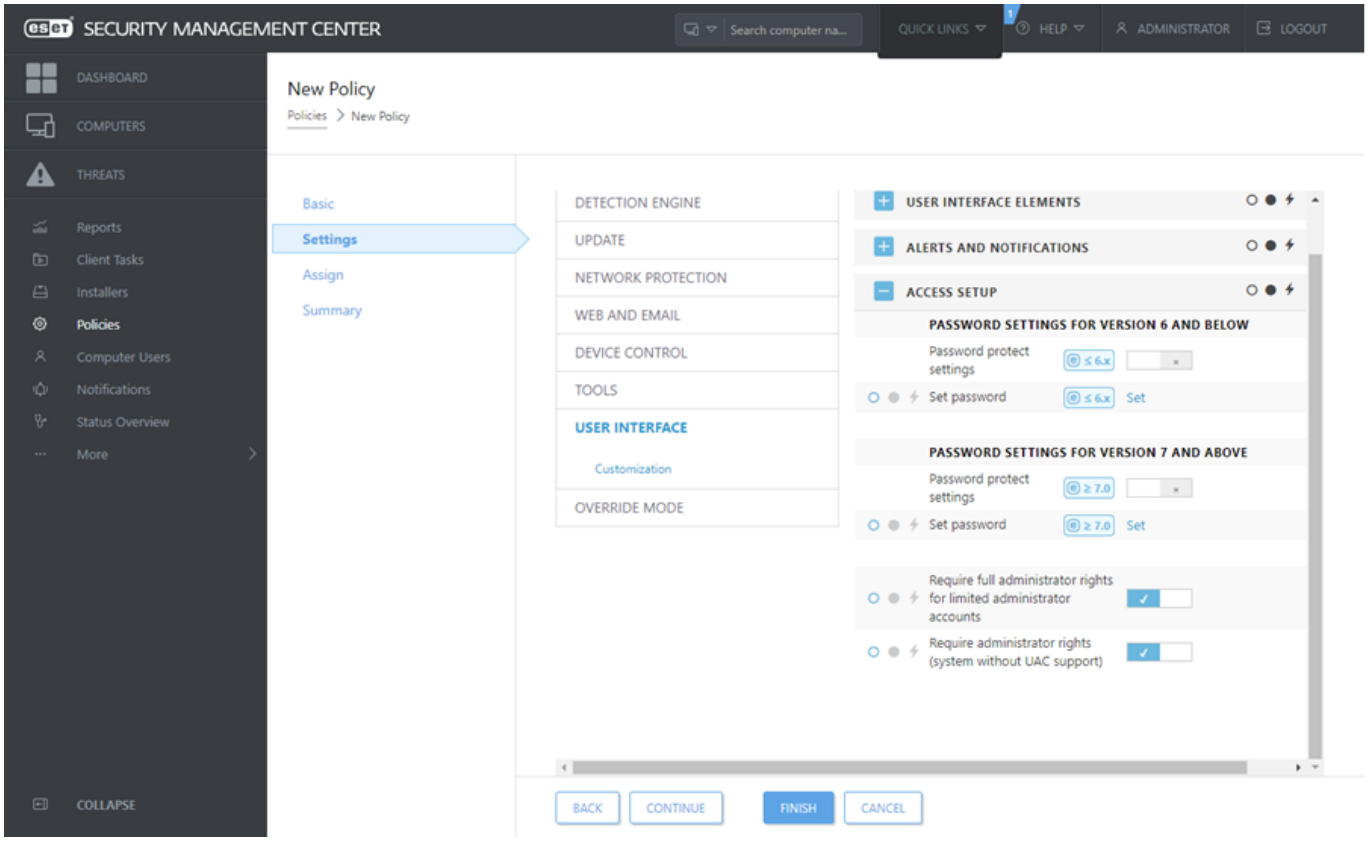
6. Klicken Sie je nach Version von ESET Endpoint Antivirus auf den Schieberegler, um den **Passwortschutz für die Einstellungen** zu aktivieren. Version 7 der ESET Endpoint-Produkte bietet mehr Sicherheit. Falls Ihr Netzwerk eine Mischung der Versionen 6 und 7 enthält, sollten Sie jeweils ein anderes Passwort festlegen. Wir raten davon ab, nur ein Passwort für Version 6 festzulegen, da ansonsten die Sicherheit der Endpoint-Produkte mit Version 7 beeinträchtigt wird.

7. Geben Sie im Popupfenster ein neues Passwort ein, bestätigen Sie es und klicken Sie auf **OK**. Klicken Sie dann auf **Weiter**.

8. Weisen Sie die Policy zu Clients zu. Klicken Sie auf **Zuweisen** und wählen Sie die Computer oder die Computergruppen aus, die Sie mit einem Passwort schützen möchten. Klicken Sie auf **OK**, um Ihre Eingaben zu bestätigen.

9. Vergewissern Sie sich, dass alle gewünschten Clientcomputer in der Liste der Ziele enthalten sind und klicken Sie auf **Weiter**.

10. Überprüfen Sie die Policy-Einstellungen in der Zusammenfassung und klicken Sie auf **Fertig stellen**, um Ihre neue Policy zu speichern.



Was sind Policies?

Mit Policies aus der ESMC-Web-Konsole können Administratoren bestimmte Konfigurationen an ESET-Produkte auf Clientcomputern verteilen. Policies können direkt auf einzelne Computer oder auf Gruppen von Computern angewendet werden. Außerdem können Sie mehrere Policies zu einem Computer oder einer Gruppe zuweisen.

Benutzer benötigen die folgenden Berechtigungen, um eine neue Policy zu erstellen: **Leseberechtigung** zum Auslesen der Liste der Policies, **Ausführungsberechtigung** zum Zuweisen von Policies zu Zielcomputern und **Schreibberechtigung**, um Policies erstellen oder bearbeiten zu können.

Policies werden in der Anordnungsreihenfolge der statischen Gruppe angewendet. Im Fall von dynamischen Gruppen werden die untergeordneten dynamischen Gruppen zuerst durchlaufen. Auf diese Weise können Sie Policies mit größeren Auswirkungen oben in der Gruppenstruktur definieren und detailliertere Policies auf Untergruppen anwenden. Mit Markierungen können ESET Endpoint Antivirus-Benutzer mit Zugriff auf Gruppen weiter oben in der Baumstruktur die Policies von untergeordneten Gruppen überschreiben. Dieser Algorithmus wird in der ESMC-Onlinehilfe ausführlich beschrieben.

Weisen Sie möglichst allgemeine Policies zu

Weisen Sie zu Gruppen weiter oben in der Baumstruktur nach Möglichkeit allgemeine Policies zu (z. B. für den Update-Server). Detailliertere Policies (z. B. Einstellungen für die Medienkontrolle) sollten weiter unten in der Gruppenstruktur angewendet werden. Die niedriger gelegene Policy überschreibt beim Zusammenführen normalerweise die Einstellungen der höheren Policies (sofern nicht mit Policy-Markierungen anderweitig definiert).

Zusammenführen von Policies

Die auf einen Client angewendete Policy ist üblicherweise das Ergebnis mehrerer Policies, die in einer endgültigen Policy zusammengeführt sind. Beim Zusammenführen von Policies ersetzt die letzte Policy normalerweise die Einstellungen der vorherigen Policy. Um dieses Verhalten zu ändern, können Sie Policy-Markierungen verwenden (für jede Einstellung verfügbar).

Beachten Sie bei der Erstellung von Policies, dass für manche Einstellungen zusätzliche Regeln (Ersetzen/Anfügen/Voranstellen) konfiguriert werden können.

- **Ersetzen** – Die gesamte Liste wird ersetzt. Neue Werte werden hinzugefügt und alle vorherigen Werte werden entfernt.

- **Anfügen** – Elemente werden an das Ende der aktuell angewendeten Liste angehängt (muss eine andere Policy sein, die lokale Liste wird immer überschrieben).

- **Voranstellen** – Elemente werden an den Anfang der Liste gesetzt (die lokale Liste wird überschrieben).

ESET Endpoint Antivirus unterstützt eine neue Methode für das Zusammenführen von lokalen Einstellungen und Remote-Policies. Wenn es sich bei der Einstellung um eine Liste handelt (z. B. eine Liste von blockierten Websites) und eine Remote-Policy mit einer lokalen Einstellung in Konflikt steht, hat die Remote-Policy Vorrang. Sie können auswählen, wie Sie lokale und Remote-Listen kombinieren möchten, indem Sie die jeweiligen Zusammenführungsregeln auswählen für:

- Zusammenführen von Einstellungen für Remote-Policies.

- Zusammenführen von Remote- und lokalen Policies – lokale Einstellungen mit der resultierenden Remote-Policy.

Weitere Informationen zum Zusammenführen von Policies finden Sie online im ESMC-Benutzerhandbuch und in unserem Beispiel.

Funktionsweise von Markierungen

Die auf einem Clientcomputer angewendete Policies ist meistens das Ergebnis der Zusammenführung mehrerer Policies zu einer endgültigen Policy. Beim Zusammenführen von Policies können Sie das erwartete Verhalten der endgültigen Policy durch die Reihenfolge der angewendeten Policies mithilfe von Policy-Markierungen anpassen. Die Markierungen legen fest, wie eine Policy eine bestimmte Einstellung verarbeitet.

Pro Einstellung können Sie eine der folgenden Markierungen auswählen:

Nicht anwenden	Einstellungen mit dieser Markierung werden nicht von der Policy festgelegt. Diese Einstellungen können daher von anderen, später angewendeten Policies geändert werden.
Anwenden	Einstellungen mit der **Anwenden**-Markierung werden auf dem Clientcomputer übernommen, können jedoch beim Zusammenführen von Policies von anderen, später angewendeten Policies überschrieben werden. Wenn ein Clientcomputer eine Policy empfängt, die Einstellungen mit dieser Markierung enthält, ändern diese Einstellungen die Konfiguration des Clientcomputers. Da die Einstellung nicht erzwungen wird, kann sie von später angewendeten Policies geändert werden.
Erzwingen	Einstellungen mit der **Erzwingen**-Markierung haben Priorität und können nicht von später angewendeten Policies überschrieben werden (selbst wenn diese auch eine **Erzwingen**-Markierung haben). Damit wird sichergestellt, dass später angewendete Policies diese Einstellung beim Zusammenführen nicht ändern können. Wenn ein Clientcomputer eine Policy empfängt, die Einstellungen mit dieser Markierung enthält, ändern diese Einstellungen die Konfiguration des Clientcomputers.

BEISPIEL: Festlegen, dass die Benutzer alle Policies sehen dürfen

Szenario: Ein *Administrator* möchte dem Benutzer *John* erlauben, Policies in seiner Stammgruppe zu erstellen und zu bearbeiten. Außerdem soll John alle vom *Administrator* erstellten Policies sehen können, inklusive Policies mit Erzwingen-Markierung. Der *Administrator* möchte, dass *John* alle Policies sehen kann, jedoch keine Änderungen an den vom *Administrator* erstellten Policies vornehmen darf. *John* kann nur Policies in seiner Stammgruppe „San Diego“ erstellen oder bearbeiten.

Lösung: Der *Administrator* führt die folgenden Schritte aus:

Benutzerdefinierte statische Gruppen und Berechtigungssätze erstellen

1. Erstellen Sie eine neue statische Gruppe mit dem Namen *San Diego*.
2. Erstellen Sie einen neuen Berechtigungssatz mit dem Namen *Policy - Alle John* mit Zugriff auf die statische Gruppe *Alle* und mit **Leseberechtigungen** für **Policies**.
3. Erstellen Sie einen neuen Berechtigungssatz mit dem Namen *Policy John* mit Zugriff auf die statische Gruppe *San Diego* und mit **Schreibberechtigungen** für **Gruppen und Computer** und **Policies**. Mit diesem Berechtigungssatz kann *John* in seiner Stammgruppe *San Diego* Policies erstellen oder bearbeiten.
4. Erstellen Sie einen neuen Benutzer *John* und wählen Sie im Abschnitt **Berechtigungssätze** sowohl *Policy - Alle John* als auch *Policy John* aus.

Policies erstellen

5. Erstellen Sie die neue Policy *Alle - Firewall aktivieren*, erweitern Sie den Bereich **Einstellungen**, wählen Sie **ESET Endpoint für Windows** aus, navigieren Sie zu **Personal Firewall** > **Einfach** und übernehmen Sie alle Einstellungen mit der **Erzwingen**-Markierung. Erweitern Sie den Bereich **Zuweisen** und wählen Sie die statische Gruppe *Alle* aus.
6. Erstellen Sie die neue Policy *John Gruppe - Firewall aktivieren*, erweitern Sie den Bereich **Einstellung** und wählen Sie **ESET Endpoint für Windows** aus. Navigieren Sie zu **Personal Firewall** > **Einfach** und übernehmen Sie alle Einstellungen mit der **Anwenden**-Markierung. Erweitern Sie den Bereich **Zuweisen** und wählen Sie die statische Gruppe *San Diego* aus.

Ergebnis

Die vom *Administrator* erstellten Policies werden zuerst angewendet, da die **Erzwingen**-Markierungen auf die Policy-Einstellungen angewendet wurden. Einstellungen mit der Erzwingen-Markierung haben Priorität und können nicht von später angewendeten Policies überschrieben werden. Die vom Benutzer *John* erstellten Policies werden nach den vom Administrator erstellten Policies angewendet.

Um die endgültige Policy-Reihenfolge anzuzeigen, navigieren Sie zu **Mehr** > **Gruppen** > **San Diego**, wählen Sie den Computer und anschließend **Details anzeigen** aus. Klicken Sie im Bereich **Konfiguration** auf **Angewendete Policies**.

ESET Endpoint Antivirus selbst benutzen

Dieser Abschnitt und das Kapitel Arbeiten mit ESET Endpoint Antivirus des Benutzerhandbuchs wenden sich an Benutzer, die ESET Endpoint Antivirus ohne ESET Security Management Center oder ESET PROTECT Cloud benutzen. Alle Funktionen und Merkmale in ESET Endpoint Antivirus sind gemäß der Kontoberechtigungen des Benutzers verfügbar.

Installationsmethoden

Sie können ESET Endpoint Antivirus Version 7 auf verschiedene Arten auf Client-Workstations installieren oder können ESET Endpoint Antivirus remote per ESET Security Management Center oder ESET PROTECT Cloud auf Client-Workstations bereitstellen.

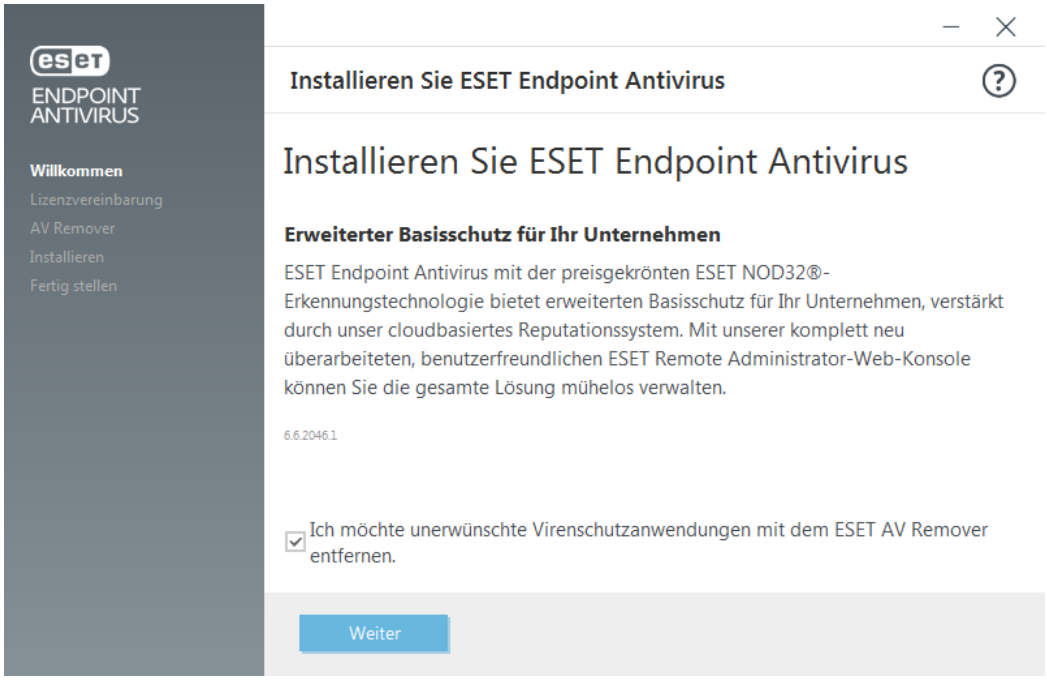
- Klicken Sie hier, falls Sie ESET Endpoint Antivirus installieren oder auf Version 6.6.x aktualisieren möchten

Methoden	Zweck	Download-Link
Installation mit ESET AV Remover	Mit dem ESET AV Remover Tool können Sie nahezu jede Virenschutz-Software entfernen, die zuvor auf Ihrem System installiert wurde, bevor Sie die Installation fortsetzen.	64-Bit herunterladen 32-Bit herunterladen
Installation (.exe)	Installationsprozedur ohne ESET AV Remover.	N/A
Installation (.msi)	Das .msi-Installationsprogramm ist die empfohlene Installationsart für Geschäftsumgebungen, hauptsächlich aufgrund von Offline- und Remote-Bereitstellungen mit verschiedenen Tools wie ESET Security Management Center.	64-Bit herunterladen 32-Bit herunterladen
Kommandozeileninstallation	Sie können ESET Endpoint Antivirus lokal mit der Kommandozeile oder remote mit einem Client-Task aus ESET Security Management Center installieren.	N/A
Bereitstellung per GPO oder SCCM	Sie können Verwaltungs-Tools wie GPO oder SCCM verwenden, um ESET Management Agent und ESET Endpoint Antivirus auf Client-Computer bereitzustellen.	N/A
Bereitstellung mit RMM-Tools	Mit den ESET DEM-Plugins für das Remote Management and Monitoring-Tool (RMM) können Sie ESET Endpoint Antivirus auf Client-Workstations bereitstellen.	N/A

ESET Endpoint Antivirus ist in mehr als 30 Sprachen verfügbar.

Installation mit ESET AV Remover

Bevor Sie den Installationsvorgang fortsetzen, sollten Sie unbedingt die auf dem Computer vorhandenen Sicherheitsanwendungen deinstallieren. Aktivieren Sie das Kontrollkästchen neben **Ich möchte unerwünschte Virenschutzanwendungen mit ESET AV Remover entfernen**, damit ESET AV Remover das System scannt und ggf. gefundene unterstützte Sicherheitsanwendungen entfernt. Lassen Sie das Kontrollkästchen deaktiviert und klicken Sie auf **Weiter**, um ESET Endpoint Antivirus ohne das Ausführen von ESET AV Remover zu installieren.

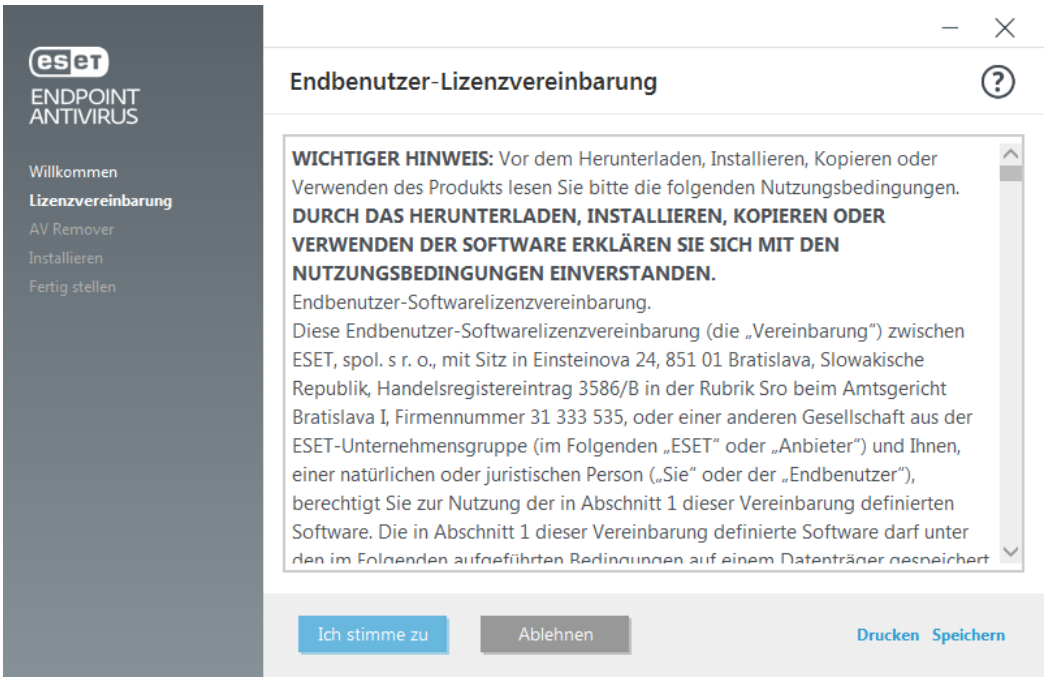


ESET AV Remover

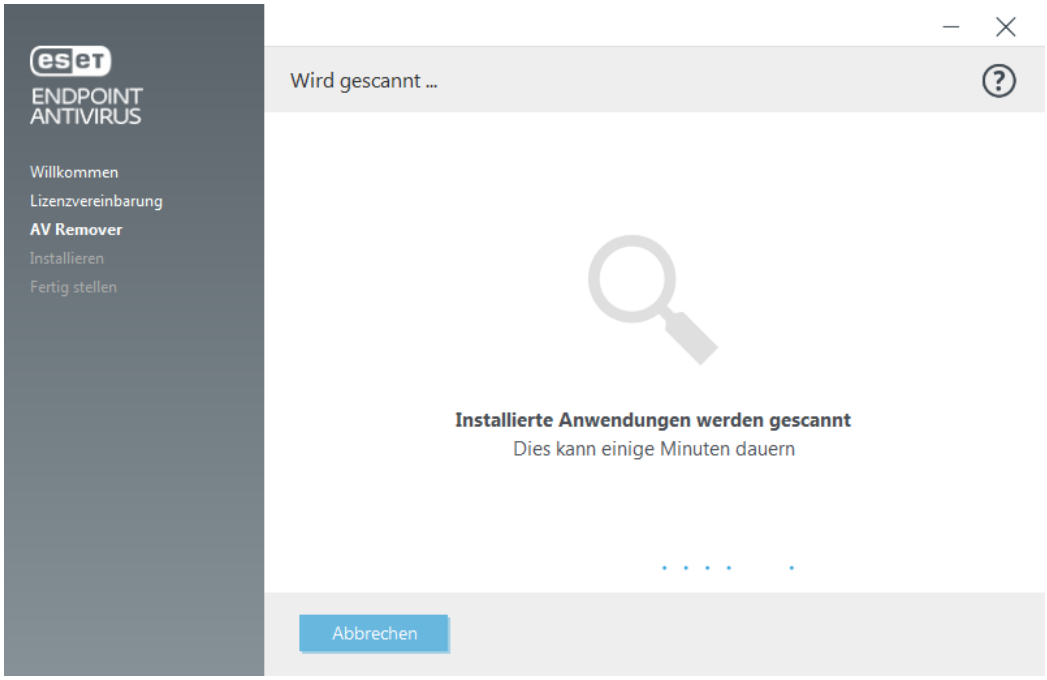
Mit dem ESET AV Remover können Sie nahezu jede Virenschutz-Software entfernen, die zuvor auf Ihrem System installiert wurde. Befolgen Sie die nachfolgenden Anweisungen, um ein vorhandenes Virenschutzprogramm mit ESET AV Remover zu entfernen:

1. Eine Liste der Virenschutzprogramme, die mit ESET AV Remover entfernt werden können, finden Sie im entsprechenden ESET-Knowledgebase-Artikel.

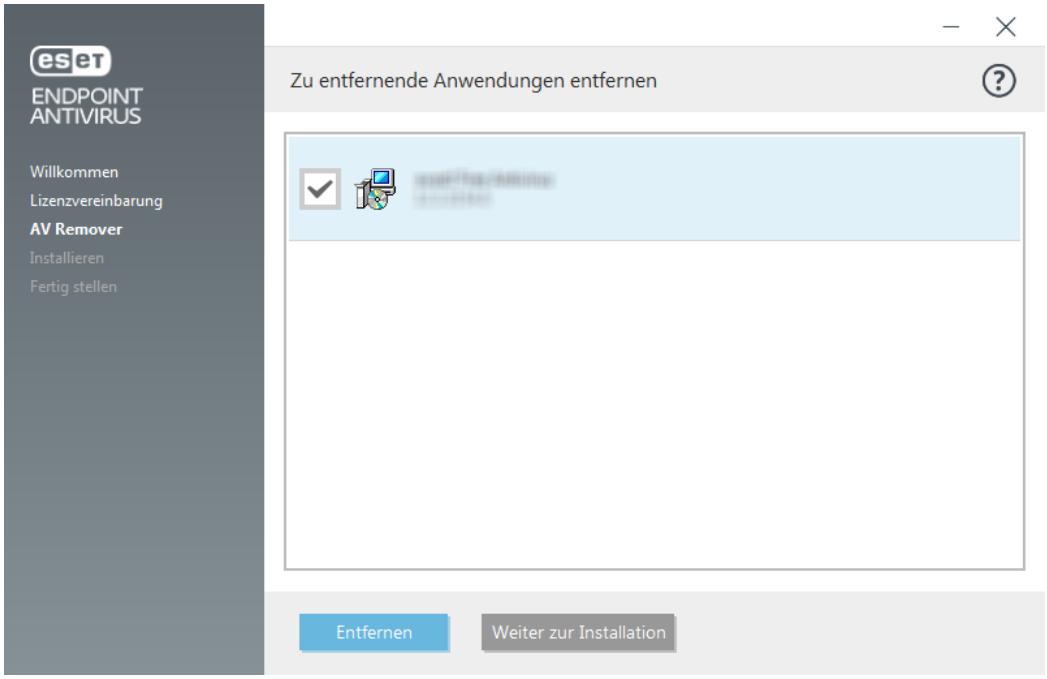
2. Lesen Sie die Endbenutzer-Lizenzvereinbarung und klicken Sie auf **Akzeptieren**, falls Sie der Vereinbarung zustimmen. Wenn Sie auf **Ablehnen** klicken, wird die Installation von ESET Endpoint Antivirus fortgesetzt, jedoch keine auf dem Computer vorhandene Sicherheitsanwendung entfernt.



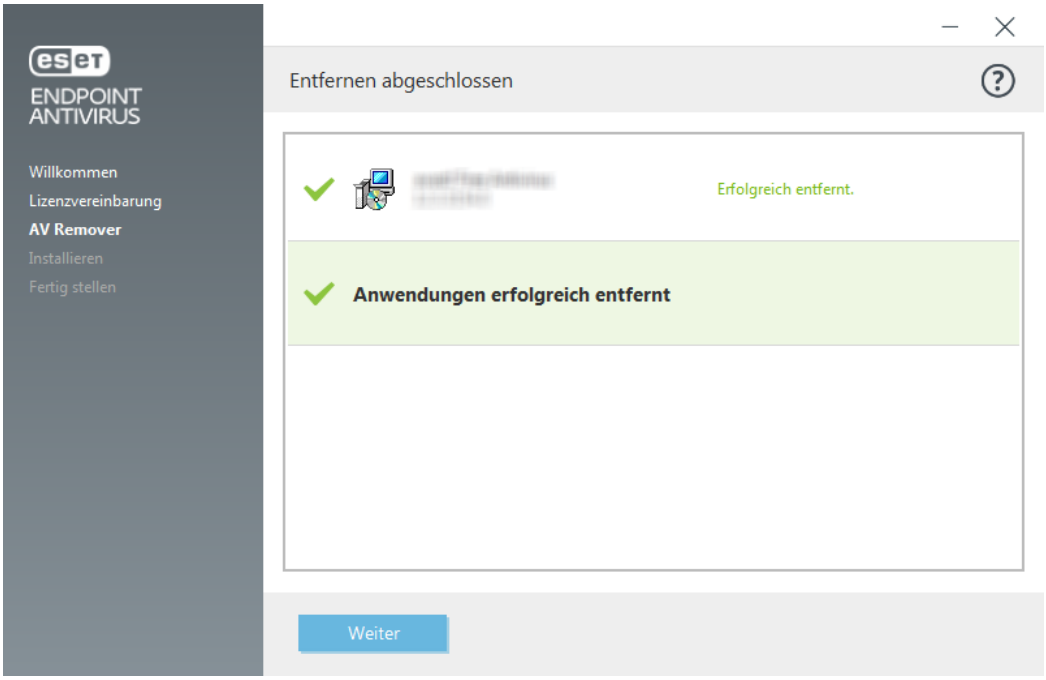
3. ESET AV Remover durchsucht das System nach Virenschutzsoftware.



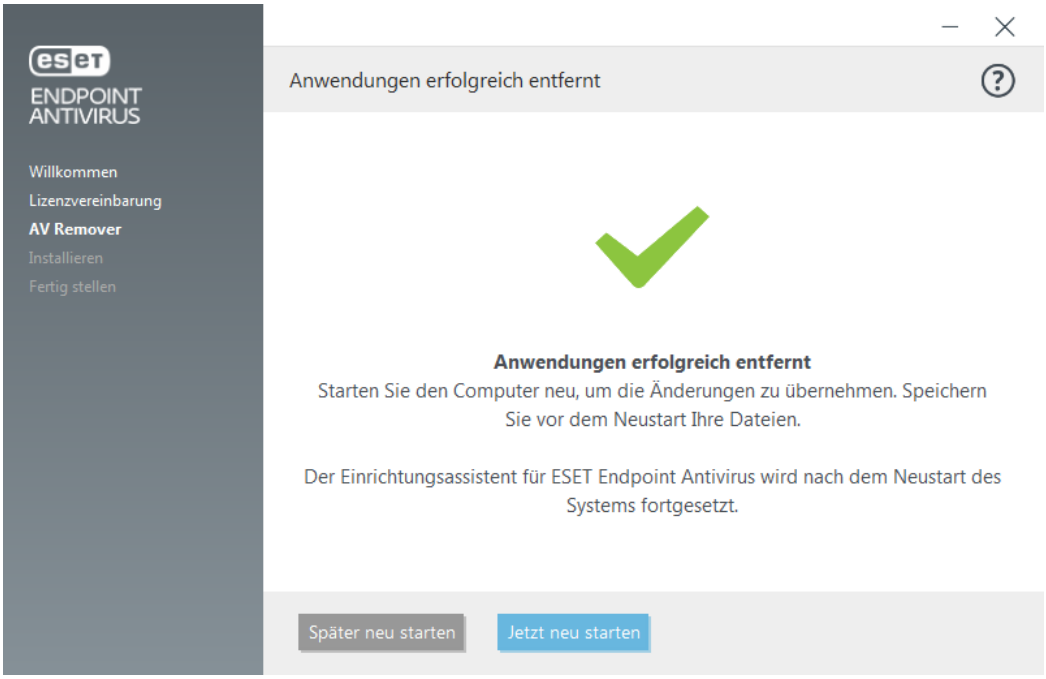
4. Wählen Sie beliebige Virenschutzprogramme aus und klicken Sie auf **Entfernen**. Dies kann eine gewisse Zeit dauern.



5. Wenn das Entfernen erfolgreich abgeschlossen wurde, klicken Sie auf **Weiter**.



6. Starten Sie den Computer neu, um die Änderungen zu übernehmen, und setzen Sie die Installation von ESET Endpoint Antivirus fort. Wenn die Deinstallation nicht erfolgreich war, beachten Sie die Hinweise unter Deinstallation mit ESET AV Remover wurde mit einem Fehler beendet in diesem Handbuch.



Deinstallation mit ESET AV Remover wurde mit einem Fehler beendet

Wenn ein Virenschutzprogramm mit ESET AV Remover nicht entfernt werden kann, wird eine Benachrichtigung angezeigt, die Sie darauf hinweist, dass die zu entfernende Anwendung möglicherweise nicht von ESET AV Remover unterstützt wird. In der ESET-Knowledgebase finden Sie eine Liste der unterstützten Produkte und Deinstallationsprogramme für übliche Windows-Virenschutz-Software, anhand derer Sie ermitteln können, ob das Programm auf diese Weise entfernt werden kann.

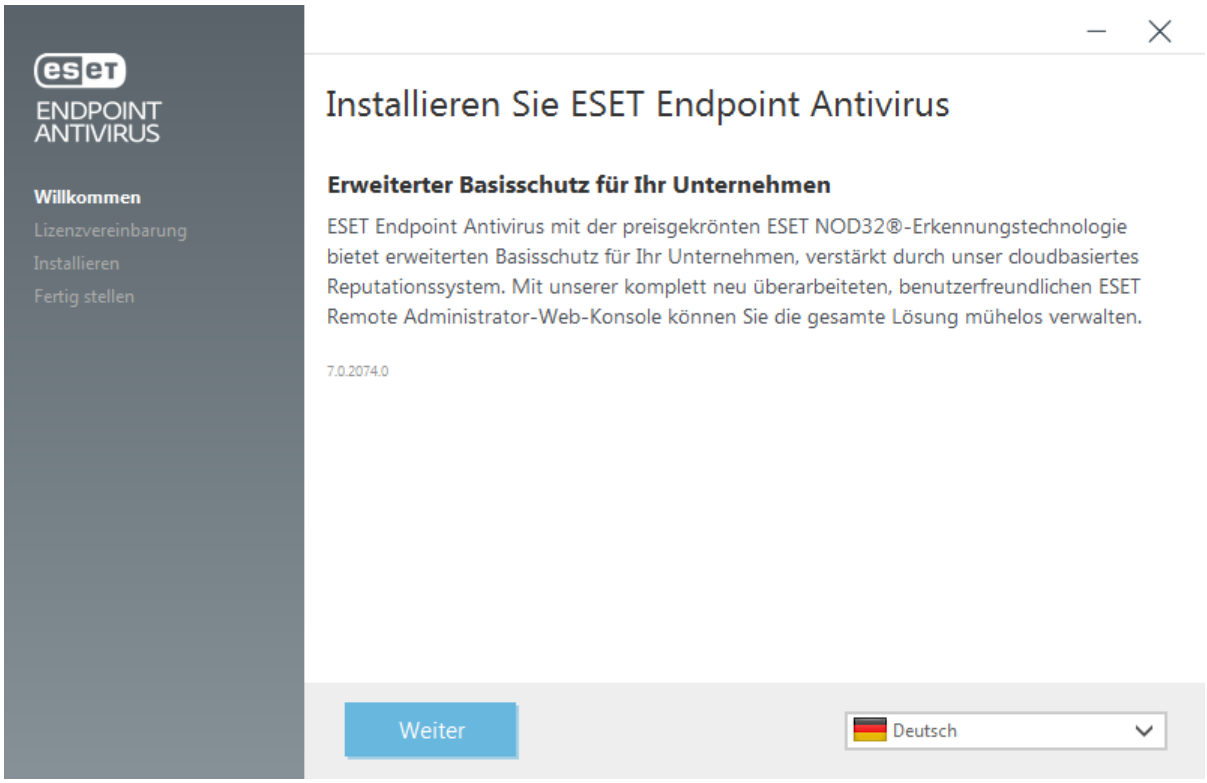
Wenn die Deinstallation des Sicherheitsprodukts nicht erfolgreich war oder ein Teil der Komponenten nur teilweise deinstalliert wurde, wird die Aufforderung **Neu starten und erneut prüfen** angezeigt. Bestätigen Sie nach dem Neustart die UAC (Benutzerkontensteuerung) und fahren Sie mit dem Scannen und dem Deinstallationsvorgang fort.

Wenden Sie sich bei Bedarf an den ESET-Support, um eine Supportanfrage einzureichen. Halten Sie dazu die Datei **AppRemover.log** bereit, die den ESET-Technikern bei der Lösung des Problems helfen kann. Die Datei **AppRemover.log** befindet sich im Ordner **eset**. Navigieren Sie im Windows Explorer zu *%TEMP%*, um zu diesem Ordner zu gelangen. Der ESET-Support nimmt umgehend Kontakt mit Ihnen auf, um Sie bei der Lösung des Problems zu unterstützen.

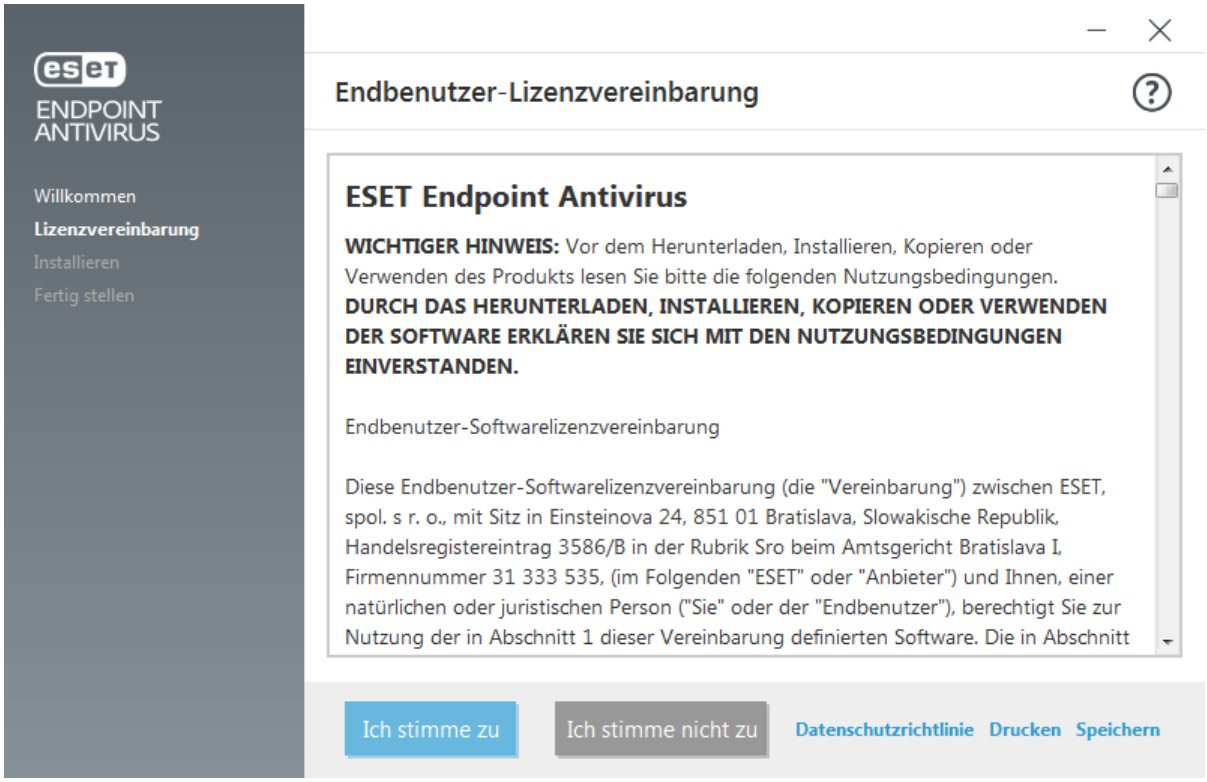
Installation (.exe)

Starten Sie das .exe-Installationsprogramm. Der Installationsassistent führt Sie durch den Installationsprozess.

Wichtig
Stellen Sie sicher, dass keine anderen Virenschutzprogramme auf Ihrem Computer installiert sind. Anderenfalls kann es zu Konflikten zwischen den Programmen kommen. Wir empfehlen Ihnen, alle anderen Virusschutzprogramme zu deinstallieren. Eine Liste von Tools zum Deinstallieren üblicher Virenschutzsoftware finden Sie in unserem Knowledgebase-Artikel (in englischer und in bestimmten weiteren Sprachen verfügbar).



1. Lesen Sie die Endbenutzer-Lizenzvereinbarung sorgfältig durch. Wenn Sie einverstanden sind, klicken Sie auf **Ich stimme zu**. Klicken Sie nach dem Akzeptieren der Bedingungen auf **Weiter**, um die Installation fortzusetzen.

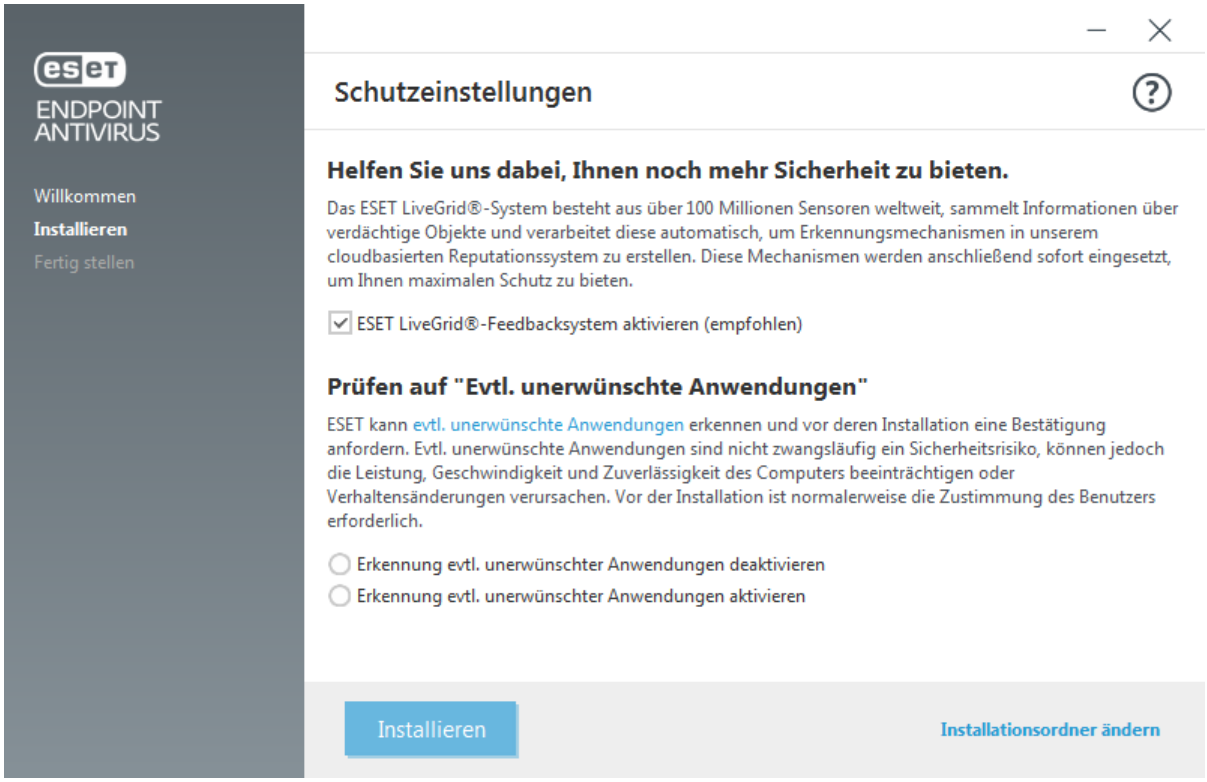


2. Wählen Sie aus, ob Sie das ESET LiveGrid®-Feedbacksystem aktivieren möchten. ESET LiveGrid® sorgt dafür, dass ESET sofort und fortlaufend über neue Schadsoftware informiert wird und wir unsere Kunden besser schützen können. Das System übermittelt neue Bedrohungen an das ESET-Virenlabor, wo die entsprechenden Dateien analysiert, bearbeitet und zur Erkennungsroutine hinzugefügt werden.

3. Im nächsten Schritt der Installation wird die die Erkennung von potenziell unerwünschten Anwendungen konfiguriert. Weitere Details finden Sie im Kapitel Potenziell unerwünschten Anwendungen.

Sie können ESET Endpoint Antivirus in einem bestimmten Ordner installieren, indem Sie auf **Installationsordner ändern** klicken.

5. Klicken Sie im letzten Schritt auf **Installieren**, um die Installation zu bestätigen. Nach Abschluss der Installation werden Sie aufgefordert, ESET Endpoint Antivirus zu aktivieren.



Installationsordner ändern (.exe)

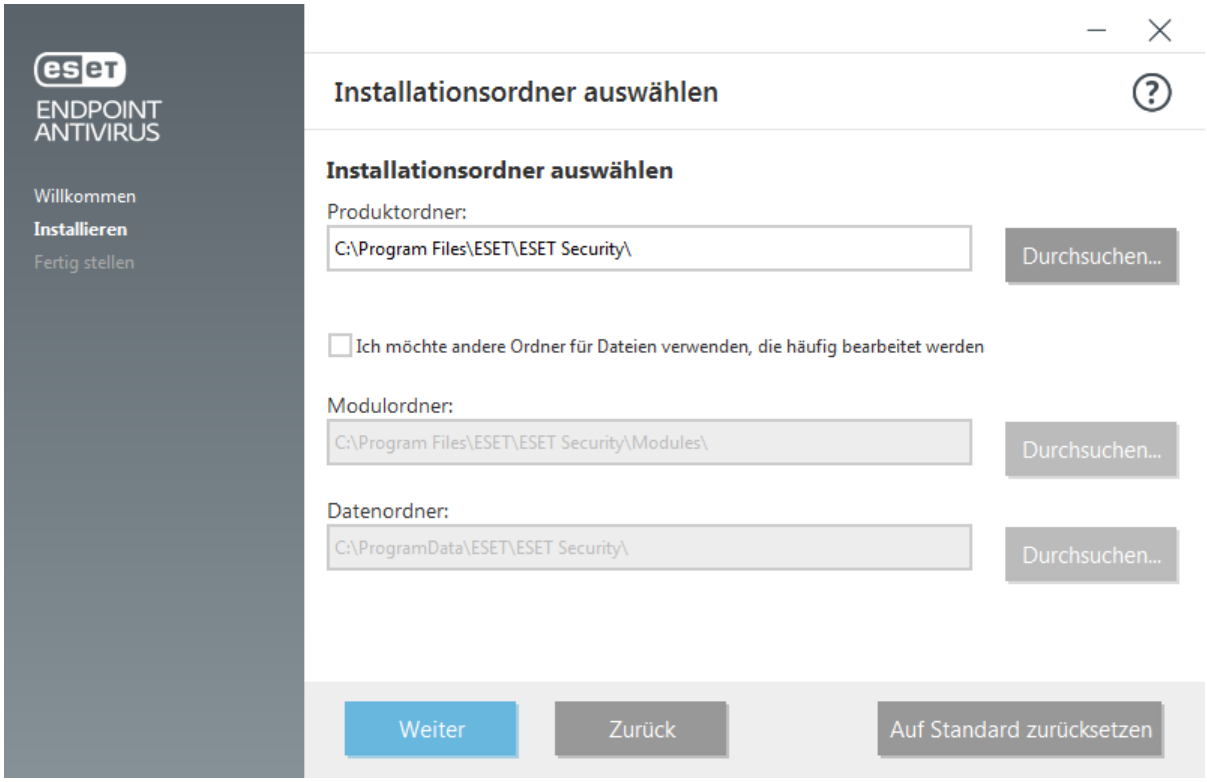
Nachdem Sie die zu erkennenden unerwünschten Anwendungen ausgewählt und auf **Installationsordner ändern** geklickt haben, werden Sie zur Auswahl eines Speicherorts für den ESET Endpoint Antivirus Installationsproduktordner aufgefordert. Standardmäßig wird das Programm in folgendes Verzeichnis installiert:

C:\Program Files\ESET\ESET Security

Sie können einen Speicherort für Programmmodule und Daten angeben. Standardmäßig werden sie in folgendes Verzeichnis installiert:

C:\Program Files\ESET\ESET Security\Modules
C:\ProgramData\ESET\ESET Security

Klicken Sie auf **Durchsuchen**, um diese Speicherorte zu ändern (nicht empfohlen).



Klicken Sie auf **Fortsetzen** und auf **Installieren**, um die Installation zu starten.

Installation (.msi)

Starten Sie das .msi-Installationsprogramm. Der Installationsassistent führt Sie durch die Einstellungen.

Zweck des .msi-Installationsprogramms

Das .msi-Installationsprogramm ist die empfohlene Installationsart für Geschäftsumgebungen, hauptsächlich aufgrund von Offline- und Remote-Bereitstellungen mit verschiedenen Tools wie ESET Security Management Center.

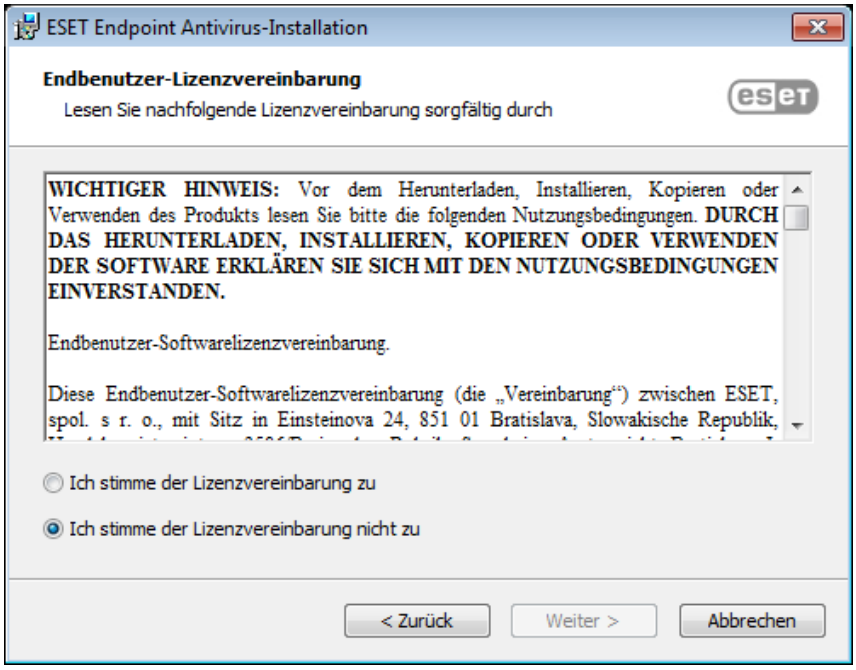
Wichtig

Stellen Sie sicher, dass keine anderen Virenschutzprogramme auf Ihrem Computer installiert sind. Anderenfalls kann es zu Konflikten zwischen den Programmen kommen. Wir empfehlen Ihnen, alle anderen Virusschutzprogramme zu deinstallieren. Eine Liste von Tools zum Deinstallieren üblicher Virenschutzsoftware finden Sie in unserem Knowledgebase-Artikel (in englischer und in bestimmten weiteren Sprachen verfügbar).

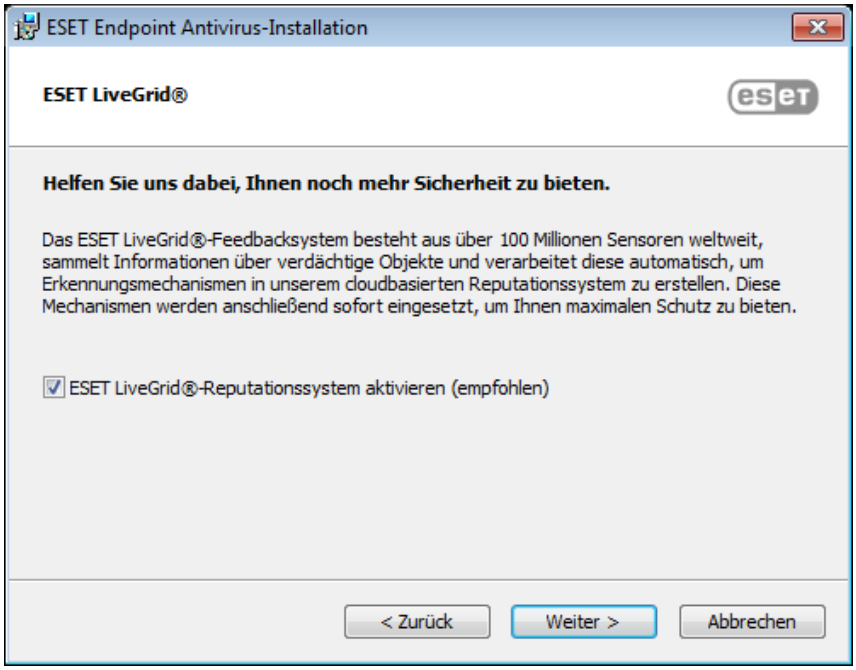
1. Wählen Sie die gewünschte Sprache aus und klicken Sie auf **Weiter**.



2. Lesen Sie die Endbenutzer-Lizenzvereinbarung sorgfältig durch. Wenn Sie einverstanden sind, klicken Sie auf **Ich akzeptiere die Bedingungen der Lizenzvereinbarung**. Klicken Sie nach dem Akzeptieren der Bedingungen auf **Weiter**, um die Installation fortzusetzen.

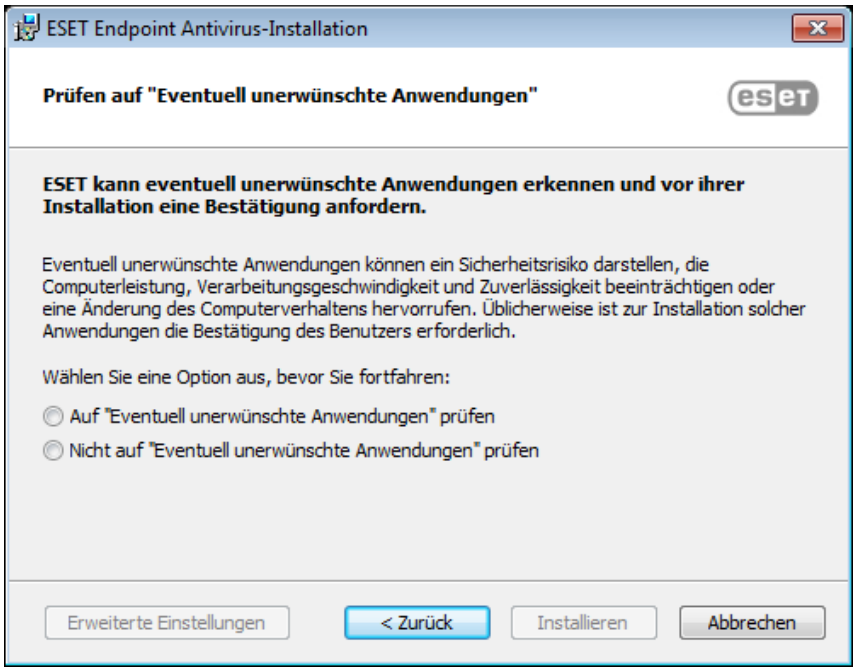


3. Wählen Sie Ihre Einstellung für das ESET LiveGrid®-Feedbacksystem aus. ESET LiveGrid® sorgt dafür, dass ESET sofort und fortlaufend über neue Schadsoftware informiert wird und wir unsere Kunden besser schützen können. Das System übermittelt neue Bedrohungen an das ESET-Virenlabor, wo die entsprechenden Dateien analysiert, bearbeitet und zur Erkennungsroutine hinzugefügt werden.



4. Im nächsten Schritt der Installation wird die Erkennung von potenziell unerwünschten Anwendungen konfiguriert. Weitere Details finden Sie im Kapitel Potenziell unerwünschte Anwendungen.

Klicken Sie auf **Erweiterte Einstellungen**, falls Sie mit der erweiterten Installation (.msi) fortfahren möchten.



5. Klicken Sie im letzten Schritt auf **Installieren**, um die Installation zu bestätigen. Nach Abschluss der Installation werden Sie aufgefordert, ESET Endpoint Antivirus zu aktivieren.

Erweiterte Installation (.msi)

Bei der erweiterten Installation können Sie zahlreiche Installationsparameter anpassen, die bei einer Standardinstallation nicht verfügbar sind.

5. Nachdem Sie die zu Potenziell unerwünschte Anwendungen ausgewählt und auf **Erweiterte Einstellungen** geklickt haben, werden Sie zur Auswahl eines Speicherorts für den Installationsproduktordner ESET Endpoint

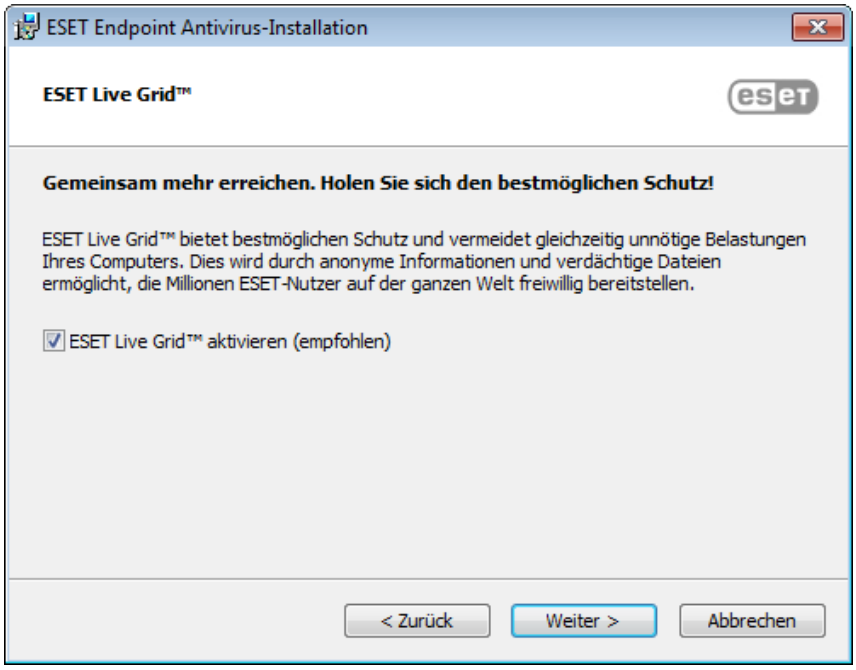
Antivirus aufgefordert. Standardmäßig wird das Programm in folgendes Verzeichnis installiert:

C:\Program Files\ESET\ESET Security

Sie können einen Speicherort für Programmmodule und Daten angeben. Standardmäßig werden sie in folgendes Verzeichnis installiert:

C:\Program Files\ESET\ESET Security\Modules
C:\ProgramData\ESET\ESET Security

Klicken Sie auf **Durchsuchen**, um diese Speicherorte zu ändern (nicht empfohlen).



7. Bestätigen Sie die Installation abschließend durch Klicken auf **Installieren**.

Kommandozeileninstallation

Sie können ESET Endpoint Antivirus lokal mit der Kommandozeile installieren oder remote mit einem Clienttask aus ESET Security Management Center.

Unterstützte Parameter

APPDIR=<Pfad>

- Pfad: gültiger Verzeichnispfad
- Installationsverzeichnis der Anwendung.

APPDATADIR=<Pfad>

- Pfad: gültiger Verzeichnispfad
- Installationsverzeichnis der Anwendungsdaten.

MODULEDIR=<Pfad>

- Pfad: gültiger Verzeichnispfad
- Installationsverzeichnis des Moduls.

ADDLOCAL=<Liste>

- Komponenteninstallation: Liste nicht obligatorischer Funktionen, die lokal installiert werden sollen.
- Verwendung mit .msi-Paketen von ESET: `ees_nt64_ENU.msi /qn ADDLOCAL=<list>`
- Weitere Informationen zur **ADDLOCAL**-Eigenschaft finden Sie unter http://msdn.microsoft.com/en-us/library/aa367536%28v=vs.85%29.aspx

ADDEXCLUDE=<Liste>

- Die ADDEXCLUDE-Liste ist eine kommagetrennte Liste mit den Namen aller Funktionen, die nicht installiert werden sollen, als Ersatz für die veraltete REMOVE-Option.
- Wenn Sie eine Funktion von der Installation ausschließen, müssen Sie den gesamten Pfad (also sämtliche Unterfunktionen) und verwandte unsichtbare Funktionen explizit in der Liste angeben.
- Verwendung mit .msi-Paketen von ESET: `ees_nt64_enu.msi /qn ADDEXCLUDE=Firewall,Network`

> **Hinweis**
> **ADDEXCLUDE** kann nicht zusammen mit **ADDLOCAL** verwendet werden.

In der Dokumentation finden Sie Hinweise zur verwendeten **msiexec**-Version für die entsprechenden Kommandozeilen-Switches.

Regeln

- Die **ADDLOCAL**-Liste ist eine kommagetrennte Liste der Namen aller zu installierenden Funktionen.
- Wenn Sie eine Funktion zur Installation auswählen, muss der gesamte Pfad (alle übergeordneten Funktionen) explizit in der Liste aufgeführt werden.
- Weitere Informationen zur richtigen Verwendung finden Sie unter „Zusätzliche Regeln“.

Komponenten und Funktionen

> **Hinweis**
> Die Komponenteninstallation mit den Parametern ADDLOCAL/ADDEXCLUDE funktioniert nicht mit ESET Endpoint Antivirus.

Die Funktionen sind in vier Kategorien unterteilt:

- **Obligatorisch** - Die Funktion wird immer installiert.

- **Optional** - Die Funktion kann deaktiviert und somit von der Installation ausgeschlossen werden.
- **Unsichtbar** - logische Funktionen, die für andere Funktionen benötigt werden
- **Platzhalter** - Funktion ohne Auswirkung auf das Produkt, die jedoch mit den untergeordneten Funktionen aufgeführt werden muss

ESET Endpoint Antivirus enthält die folgenden Funktionen:

Beschreibung	Funktionsname	Übergeordnete Funktion	Vorhandensein
Grundlegende Programmkomponenten	`Computer`		Platzhalter
Malware Scan Engine	`Antivirus`	`Computer`	Obligatorisch
Erkennungsroutine / Malware-Scans	`Scan`	`Computer`	Obligatorisch
Erkennungsroutine / Echtzeit-Dateischutz	`RealtimeProtection`	`Computer`	Obligatorisch
Erkennungsroutine / Malware-Scans / Dokumentenschutz	`DocumentProtection`	`Antivirus`	Optional
Medienkontrolle	`DeviceControl`	`Computer`	Optional
Netzwerkschutz	`Network`		Platzhalter
Netzwerkschutz / Firewall	`Firewall`	`Network`	Optional
Netzwerkschutz / Netzwerkangriffsschutz / ...	`IdsAndBotnetProtection`	`Network`	Optional
Web und E-Mail	`WebAndEmail`		Platzhalter
Web und E-Mail / Protokollprüfung	`ProtocolFiltering`	`WebAndEmail`	Unsichtbar
Web und E-Mail/Web-Schutz	`WebAccessProtection`	`WebAndEmail`	Optional
Web und E-Mail/E-Mail-Schutz	`EmailClientProtection`	`WebAndEmail`	Optional
Web und E-Mail / E-Mail-Schutz / E-Mail-Clients	`MailPlugins`	`EmailClientProtection`	Unsichtbar
Web und E-Mail/E-Mail-Schutz/Spam-Schutz	`Antispam`	`EmailClientProtection`	Optional
Web und E-Mail / Web-Kontrolle	`WebControl`	`WebAndEmail`	Optional
Tools / ESET RMM	`Rmm`		Optional
Update / Profile / Update-Mirror	`UpdateMirror`		Optional
ESET Enterprise Inspector-Plugin	`EnterpriseInspector`		Unsichtbar

Gruppenfunktionen:

Beschreibung	Funktionsname	Vorhandensein der Funktion
Alle obligatorischen Funktionen	`_Base`	Unsichtbar
Alle verfügbaren Funktionen	`ALL`	Unsichtbar

Zusätzliche Regeln

- Wenn Sie eine der **WebAndEmail**-Funktionen für die Installation auswählen, müssen Sie die unsichtbare

Funktion **ProtocolFiltering** in der Liste angeben.

• Die Namen sämtlicher Funktionen unterscheiden zwischen Groß- und Kleinschreibung. UpdateMirror ist beispielsweise nicht dasselbe wie UPDATEMIRROR.

Liste der Konfigurationseigenschaften

Eigenschaft	Wert	Funktion
CFG_POTENTIALLYUNWANTED_ENABLED=	0 - Deaktiviert 1 - Aktiviert	PUA-Erkennung
CFG_LIVEGRID_ENABLED=	Siehe unten	Siehe LiveGrid-Eigenschaft unten
FIRSTSCAN_ENABLE=	0 - Deaktiviert 1 - Aktiviert	Computer-Scan planen und nach der Installation ausführen
CFG_PROXY_ENABLED=	0 - Deaktiviert 1 - Aktiviert	Proxyserver-Einstellungen
CFG_PROXY_ADDRESS=	<ip>	IP-Adresse des Proxyservers
CFG_PROXY_PORT=	<Port>	Portnummer des Proxyservers
CFG_PROXY_USERNAME=	<Benutzername>	Benutzername für die Authentifizierung
CFG_PROXY_PASSWORD=	<Passwort>	Passwort für die Authentifizierung
ACTIVATION_DATA=	Siehe unten	Produktaktivierung, Lizenzschlüssel oder Offline-Lizenzdatei
ACTIVATION_DLG_SUPPRESS=	0 - Deaktiviert 1 - Aktiviert	Wenn Sie den Wert 1 festlegen, wird der Produktaktivierungsdialog nach dem ersten Start nicht angezeigt
ADMINCFG=	<Pfad>	Pfad zur exportierten XML-Konfiguration (Standardwert *cfg.xml*)

LiveGrid® Eigenschaft

Wenn Sie ESET Endpoint Antivirus mit CFG_LIVEGRID_ENABLED installieren, verhält sich das Produkt nach der Installation wie folgt:

Funktion	CFG_LIVEGRID_ENABLED=0	CFG_LIVEGRID_ENABLED=1
ESET LiveGrid®-Reputationssystem	Ein	Ein
ESET LiveGrid®-System	Aus	Ein
Anonyme Statistiken senden	Aus	Ein

ACTIVATION_DATA-Eigenschaft

Format	Methoden
ACTIVATION_DATA=key:AAAA-BBBB-CCCC-DDDD-EEEE	Aktivierung mit ESET-Lizenzschlüssel (Internetverbindung erforderlich)
ACTIVATION_DATA=offline:C:\ProgramData\ESET\ESET Security\license.lf	Aktivierung mit Offline-Lizenzdatei

Spracheigenschaften

ESET Endpoint Antivirus-Sprache (Sie müssen beide Eigenschaften angeben).

Eigenschaft	Wert
PRODUCT_LANG=	LCID-Dezimalwert (Spracheinstellungs-ID), z. B. 1033 für Englisch (USA), beachten Sie die Liste der Sprachcodes.
PRODUCT_LANG_CODE=	LCID-Zeichenfolge (Language Culture Name) in Kleinbuchstaben, z. B. „en-us“ für Englisch (USA), beachten Sie die Liste der Sprachcodes.

Beispiele für die Kommandozeileninstallation

Wichtig
Stellen Sie vor der Installation sicher, dass Sie die Endbenutzer-Lizenzvereinbarung gelesen haben und dass Sie über Administratorberechtigungen verfügen.

Beispiel
Schließen Sie den Abschnitt **NetworkProtection** von der Installation aus (dazu müssen Sie ebenfalls alle untergeordneten Funktionen angeben):

```
msiexec /qn /i ees_nt64.msi ADDEXCLUDE=Network,Firewall,IdsAndBotnetProtection
```

Beispiel
Wenn Sie Ihr ESET Endpoint Antivirus nach der Installation automatisch konfigurieren möchten, können Sie grundlegende Installationsparameter direkt im Installationsbefehl angeben.
Installation von ESET Endpoint Antivirus mit aktiviertem ESET LiveGrid®:

```
msiexec /qn /i ees_nt64.msi CFG_LIVEGRID_ENABLED=1
```

Beispiel
Installation in ein Installationsverzeichnis, das vom Standard abweicht.

```
msiexec /qn /i ees_nt64_enu.msi APPDIR=C:\ESET\
```

Beispiel
Installation und Aktivierung von ESET Endpoint Antivirus mit Ihrem ESET-Lizenzschlüssel.

```
msiexec /qn /i ees_nt64_enu.msi ACTIVATION_DATA=key:AAAA-BBBB-CCCC-DDDD-EEEE
```

Beispiel
Unbeaufsichtigte Installation mit ausführlichem Logging (hilfreich für die Fehlerbehebung), und RMM nur mit obligatorischen Komponenten:

```
msiexec /qn /i ees_nt64.msi /l*xv msi.log ADDLOCAL=_Base,Rmm
```

Beispiel
Erzwungene unbeaufsichtigte vollständige Installation mit einer ausgewählten Sprache.

```
msiexec /qn /i ees_nt64.msi ADDLOCAL=ALL PRODUCT_LANG=1033 PRODUCT_LANG_CODE=en-us
```

Kommandozeilenoptionen nach der Installation

- ESET CMD - Importieren Sie eine .xml-Konfigurationsdatei, um eine Sicherheitsfunktion zu aktivieren oder zu deaktivieren
- Kommandozeilen-Scanner - Führen Sie einen Computer-Scan in der Kommandozeile aus

Remote-Bereitstellung per GPO oder SCCM

Neben der direkten Installation von ESET Endpoint Antivirus auf einer Client-Workstation oder der Remotebereitstellung mit einem Server-Task in ESMC können Sie für die Installation auch Verwaltungs-Tools wie Gruppenrichtlinienobjekte (GPO), Software Center Configuration Manager (SCCM), Symantec Altiris oder Puppet verwenden.

Verwaltet (empfohlen)

Auf verwalteten Computern installieren wir zunächst den ESET Management Agent und stellen ESET Endpoint Antivirus anschließend mit ESET Security Management Center (ESMC) bereit. ESMC muss in Ihrem Netzwerk installiert sein.

1. Laden Sie das eigenständige Installationsprogramm für den ESET Management Agent herunter.
2. Bereiten Sie das Remotebereitstellungsskript für GPO/SCCM vor.
3. Stellen Sie den ESET Management Agent entweder mit GPO oder mit SCCM bereit.
4. Vergewissern Sie sich, dass die Clientcomputer zu ESMC hinzugefügt wurden.
5. Installieren und aktivieren Sie ESET Endpoint Antivirus auf Ihren Clientcomputern.

Illustrierte Anweisungen
Die folgenden Artikel in der ESET-Knowledgebase sind möglicherweise nur auf Englisch verfügbar:
- Bereitstellen des ESET Management Agent mit SCCM oder GPO (7.x)
- Bereitstellen des ESET Management Agent mit einem Gruppenrichtlinienobjekt (GPO)

??

Upgrade auf eine aktuellere Version

Neuere Versionen von ESET Endpoint Antivirus werden veröffentlicht, um Verbesserungen oder Patches durchzuführen, die ein automatisches Update der Programmmodule nicht leisten kann. Es gibt verschiedene Möglichkeiten, ein Upgrade auf eine aktuellere Version durchzuführen:

1. Automatisch mit ESET Security Management Center, ESET Remote Administrator (nur ESET-Endpunktprodukte 6.x) oder ESET PROTECT Cloud.

2. Manuelle Aktualisierung durch Herunterladen und Installieren der aktuelleren Version (ohne Deinstallation der vorherigen Version)

Empfohlene Upgradeszenarien

- Remote-Upgrade

Falls Sie mehr als 10 ESET Endpoint-Produkte verwalten, sollten Sie Upgrades unter Umständen mit ESET Security Management Center oder ESET PROTECT Cloud , verwalten. Beachten Sie dazu die folgende Dokumentation:

- ESET Security Management Center | Aufbau und Größenbemessung der Infrastruktur
- ESET Remote Administrator | Prozeduren für Upgrade, Migration und erneute Installation
- ESET Security Management Center | Prozeduren für Upgrade, Migration und erneute Installation
- Einführung in ESET PROTECT Cloud

- Manuelles Upgrade auf einem Client-Computer

Falls Sie vorhaben, Upgrades auf einzelnen Client-Computern manuell durchzuführen:

1. Überprüfen Sie zunächst die Voraussetzungen für das Upgrade von ESET Endpoint Antivirus:

Upgrade von	Upgrade auf	Voraussetzungen für das Upgrade
6.x	7.x	• Keine Voraussetzungen • Hinweis: ESET Endpoint Antivirus Version 7 kann nicht mit ESET Remote Administrator verwaltet werden
6.x	6.6.x	• Keine Voraussetzungen
5.x	7.x	• Vergewissern Sie sich, dass Ihr Betriebssystem unterstützt wird. Windows XP wird für Version 7 beispielsweise nicht unterstützt. • Überprüfen Sie, ob Ihre Versionen der ESET Endpoint-Produkte ein Upgrade von Version 5.x unterstützen.
4.x	7.x	• Vergewissern Sie sich, dass Ihr Betriebssystem unterstützt wird. • Deinstallieren Sie ESET NOD32 Antivirus Business Edition oder ESET Smart Security Business Edition. Installieren Sie Version 7 nicht über eine 4.x-Version.

2. Laden Sie eine neuere Version herunter und installieren Sie sie über die vorherige Version.

Bekannte Probleme bei der Installation

In unserer Liste mit Lösungen für bekannte Probleme bei der Installation finden Sie Hilfestellungen, falls Probleme bei der Installation auftreten.

Fehler bei der Aktivierung

Falls bei der Aktivierung von ESET Endpoint Antivirus Probleme auftreten, finden Sie hier eine Liste der häufigsten Ursachen:

- Lizenzschlüssel wird bereits verwendet
- Ungültiger Lizenzschlüssel. Fehler im Produktaktivierungsformular
- Weitere für die Aktivierung erforderliche Informationen fehlen oder sind ungültig
- Bei der Kommunikation mit der Aktivierungsdatenbank ist ein Fehler aufgetreten. Warten Sie 15 Minuten und versuchen Sie dann erneut, das Produkt zu aktivieren
- Verbindung zu den ESET-Aktivierungsservern nicht vorhanden oder deaktiviert

Vergewissern Sie sich, dass Sie den richtigen Lizenzschlüssel eingegeben oder eine Offline-Lizenz angehängt haben und versuchen Sie es erneut.

Falls Sie Ihr Produkt nicht aktivieren können, finden Sie in unserem Willkommenspaket Hinweise zu häufig gestellten Fragen, Fehlern und Problemen bei Aktivierung und Lizenzierung (verfügbar auf Englisch und in verschiedenen anderen Sprachen).

- Fehlerbehebung für ESET-Produktaktivierung starten

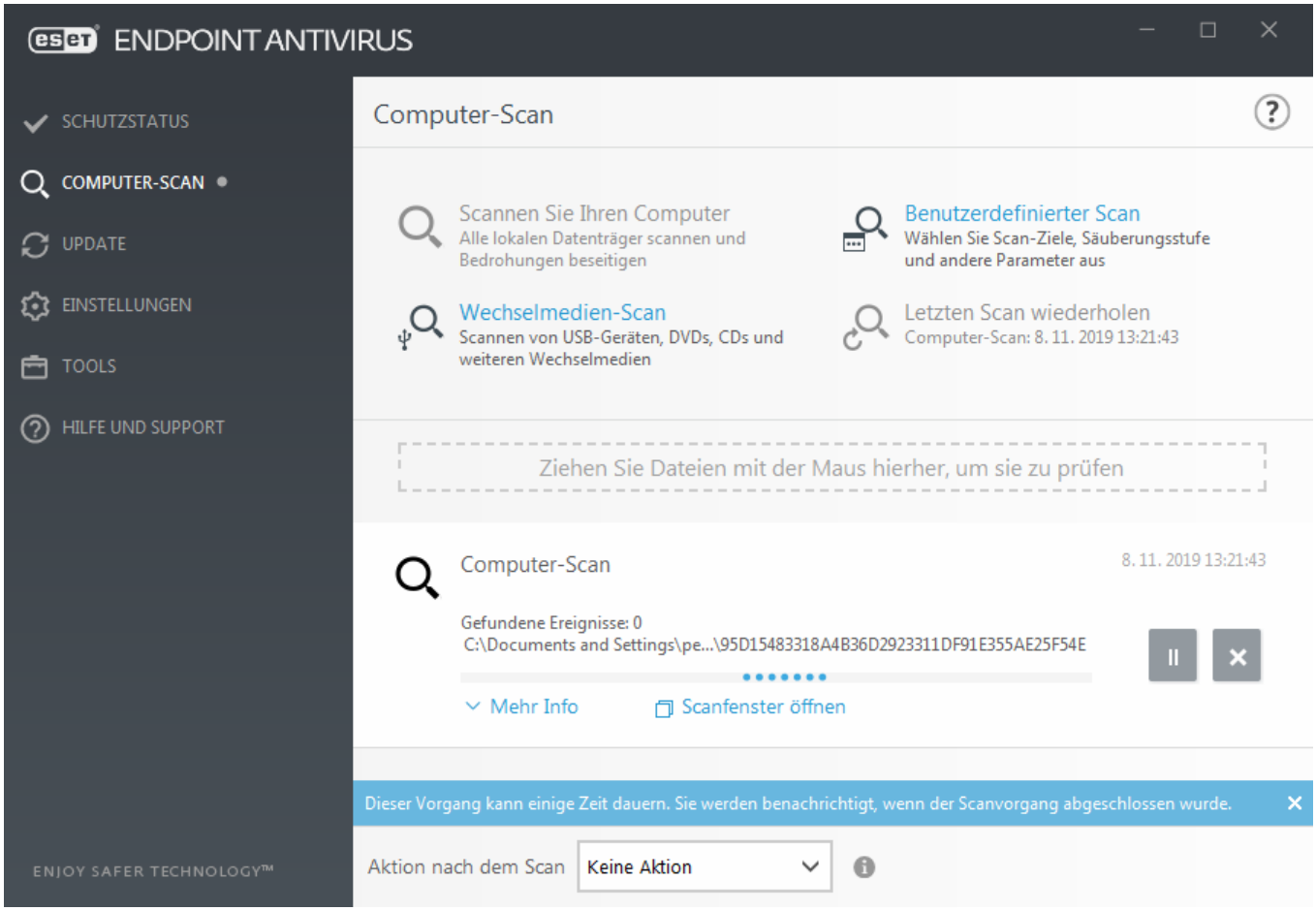
Produktaktivierung

Nach Abschluss der Installation werden Sie aufgefordert, Ihr Produkt zu aktivieren.

Aktivieren Sie ESET Endpoint Antivirus mit einer der verfügbaren Methoden. Weitere Informationen finden Sie unter So aktivieren Sie ESET Endpoint Antivirus.

Computer-Scan

Sie sollten Ihren Computer regelmäßigen Prüfungen unterziehen oder eine regelmäßige Prüfung planen, um Bedrohungen stets rechtzeitig zu erkennen. Klicken Sie dazu im Hauptprogrammfenster auf **Computer prüfen** und dann auf **Smart-Prüfung**. Weitere Informationen zur Prüfung des Computers finden Sie im Abschnitt Computer prüfen.



Erste Schritte

Dieses Kapitel enthält eine einführende Übersicht über ESET Endpoint Antivirus und die Grundeinstellungen des Programms.

Die Benutzeroberfläche

Das Hauptprogrammfenster von ESET Endpoint Antivirus ist in zwei Abschnitte unterteilt. Das primäre Fenster (rechts) zeigt Informationen zu den im Hauptmenü (links) ausgewählten Optionen an.

Im Folgenden werden die Optionen des Hauptmenüs beschrieben:

Schutzstatus - Informationen zum Schutzstatus von ESET Endpoint Antivirus.

Computer prüfen - In diesem Abschnitt können Sie entweder eine Smart-Prüfung, eine Prüfung mit speziellen Einstellungen oder eine Prüfung von Wechselmedien starten. Außerdem können Sie die zuletzt durchgeführte Prüfung wiederholen.

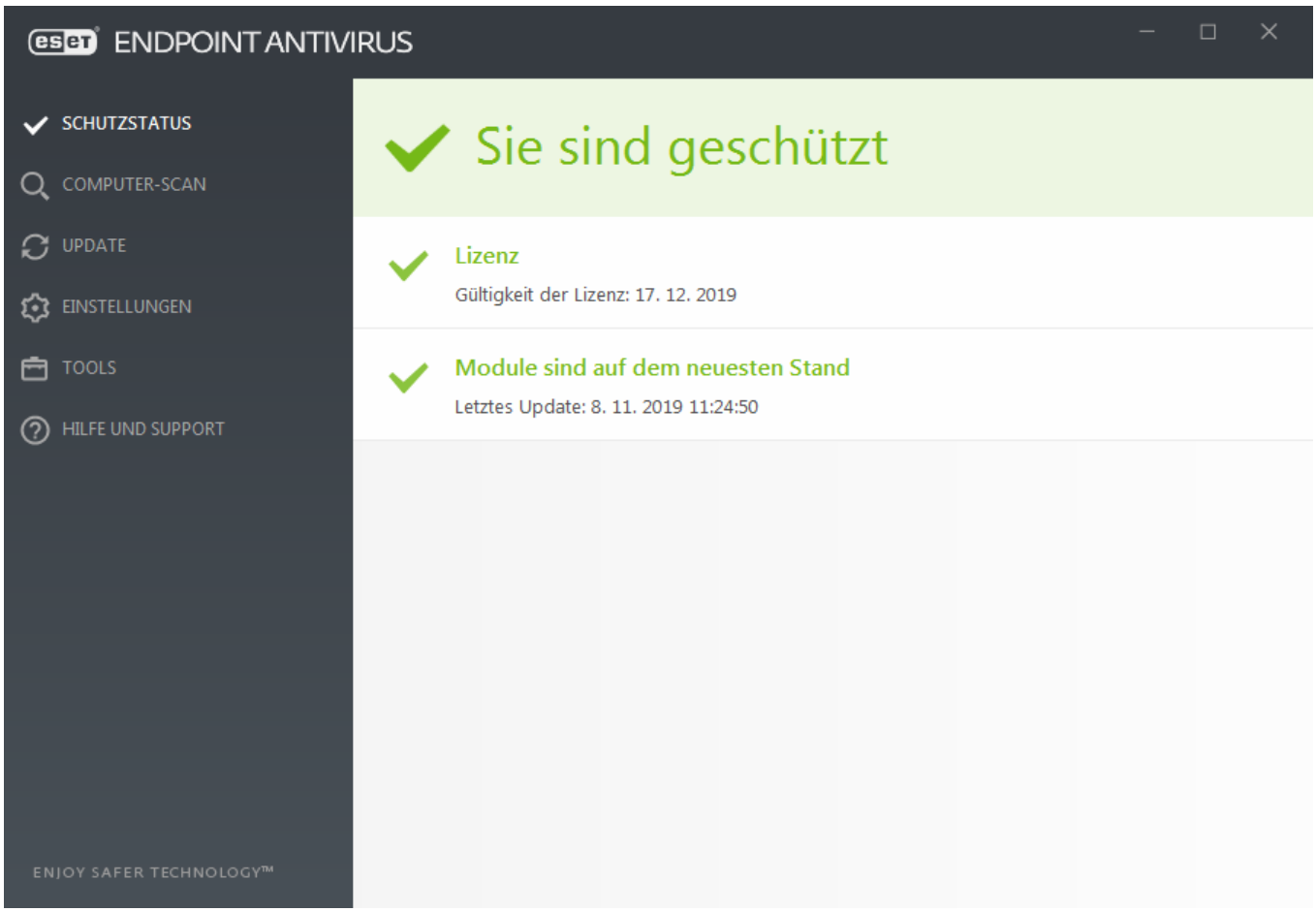
Update – In diesem Abschnitt können Sie Informationen über die Erkennungsroutine anzeigen und manuell nach Updates suchen.

Einstellungen - Hiermit können Sie die Sicherheitseinstellungen Ihres Computers, des oder von Web und E-Mail anpassen.

Tools - Zugang zu den Log-Dateien, der Anzeige der Schutzstatistik, den Funktionen „Aktivität beobachten“ und

„Ausgeführte Prozesse“, dem Taskplaner, der Quarantäne, ESET SysInspector sowie ESET SysRescue zur Erstellung einer Rettungs-CD. Außerdem können Sie eine Probe zur Analyse einreichen.

Hilfe und Support - Bietet Zugriff auf Hilfedateien, die ESET Knowledgebase und die ESET-Website sowie Links zum Öffnen einer Supportanfrage, Support-Tools und Informationen zur Produktaktivierung.

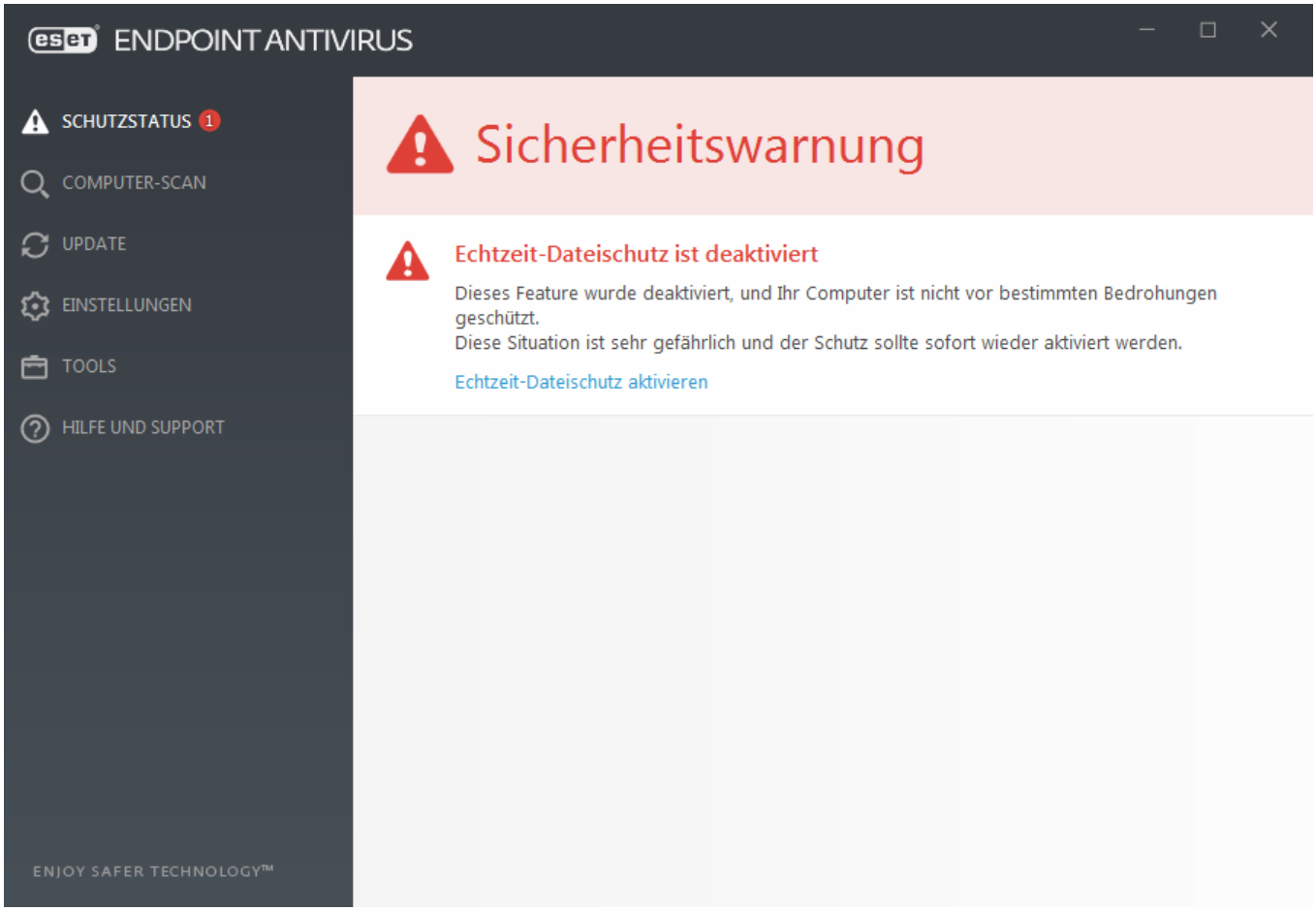


Der Bildschirm **Schutzstatus** enthält Informationen über die Sicherheit und die aktuelle Schutzstufe Ihres Computers. Das grüne Schutzstatussymbol zeigt an, dass **Maximaler Schutz** gewährleistet ist.

Das Statusfenster enthält außerdem Quicklinks zu häufig in ESET Endpoint Antivirus verwendeten Funktionen sowie Informationen zum neuesten Update.

Vorgehensweise bei fehlerhafter Ausführung des Programms

Neben allen voll funktionsfähigen Programmmodulen wird ein grünes Häkchen angezeigt. Ein rotes Ausrufezeichen oder ein orangefarbenes Warnsymbol weist darauf hin, dass ein Modul Ihre Aufmerksamkeit erfordert. Weitere Informationen zum Modul inklusive unserer Empfehlungen zur Wiederherstellung der Funktionstüchtigkeit werden im oberen Teil des Fensters angezeigt. Um den Status eines Moduls zu ändern, klicken Sie im Hauptmenü auf **Einstellungen** und wählen Sie das gewünschte Modul aus.



Ein rotes Ausrufezeichen (!) weist darauf hin, dass der maximale Schutz Ihres Computers nicht gewährleistet ist. Diese Benachrichtigung kann in den folgenden Fällen auftreten:

- **Viren- und Spyware-Schutz sind angehalten**– Klicken Sie auf **Alle Module des Viren- und Spyware-Schutzes aktivieren**, um den Viren- und Spyware-Schutz im Bereich **Schutzstatus** zu aktivieren, oder im Hauptprogrammfenster im Bereich **Einstellungen** auf **Viren- und Spyware-Schutz aktivieren**.
- **Virenschutz ist nicht funktionsfähig**– Fehler bei der Virenschutz-Initialisierung. Die meisten ESET Endpoint Antivirus-Module funktionieren nicht ordnungsgemäß.
- **Phishing-Schutz ist nicht funktionsfähig**– Dieses Feature ist nicht funktionsfähig, da andere benötigte Programmmodule nicht aktiv sind.

- **Erkennungsroutine ist veraltet** - Dieser Fehler wird angezeigt, wenn die Erkennungsroutine (ehemals Signaturdatenbank) trotz wiederholter Versuche nicht aktualisiert werden konnte. Überprüfen Sie in diesem Fall die Update-Einstellungen. Die häufigste Fehlerursache sind falsch eingegebene Lizenzdaten oder fehlerhaft konfigurierte Verbindungseinstellungen.

- **Produkt ist nicht aktiviert** oder **Lizenz abgelaufen** - In diesem Zustand ist das Schutzstatussymbol rot. Nach Ablauf der Lizenz kann das Programm keine Updates mehr durchführen. Führen Sie Anweisungen in der Warnmeldung aus, um Ihre Lizenz zu verlängern.

- **Host Intrusion Prevention System (HIPS) ist deaktiviert** – Dieses Problem wird angezeigt, wenn HIPS in den erweiterten Einstellungen deaktiviert wurde. Ihr Computer ist nicht vor bestimmten Bedrohungen geschützt, und Sie sollten den Schutz sofort erneut aktivieren, indem Sie auf **HIPS aktivieren** klicken.

- **ESET LiveGrid®ist deaktiviert**– Dieses Problem wird angezeigt, wenn ESET LiveGrid® in den erweiterten Einstellungen deaktiviert wurde.

- **Keine regelmäßigen Updates geplant**–ESET Endpoint Antivirus sucht nicht nach und erhält keine wichtigen Updates, wenn Sie keinen Update-Task geplant haben.

- **Anti-Stealth ist deaktiviert**– Klicken Sie auf **Anti-Stealth aktivieren**, um diese Funktion erneut zu aktivieren.

- **Netzwerkzugriff blockiert** - Wird angezeigt, wenn der Clienttask **Computer vom Netzwerk isolieren** auf dieser Arbeitsstation in ESMC ausgelöst wird. Weitere Informationen erhalten Sie von Ihrem Systemadministrator.

- **Echtzeit-Dateischutz ist angehalten**– Der Echtzeit-Dateischutz wurde vom Benutzer deaktiviert. Ihr Computer ist nicht vor Bedrohungen geschützt. Klicken Sie auf**Echtzeit-Dateischutz aktivieren**, um diese Funktion erneut zu aktivieren.

 Das orangefarbene „i“ weist darauf hin, dass Ihr ESET-Produkt der Aufmerksamkeit bei einem nicht-kritischen Problem bedarf. Mögliche Gründe dafür sind:

- **Web-Schutz ist deaktiviert**– Klicken Sie auf die Sicherheitsnachricht, um den Web-Schutz erneut zu aktivieren, und klicken Sie anschließend auf **Web-Schutz aktivieren**.

- **Lizenz läuft bald ab**– Das Schutzstatussymbol weist mit einem Ausrufezeichen auf dieses Problem hin. Nach dem Ablaufen der Lizenz ist kein Programm-Update mehr möglich und das Schutzstatussymbol ist rot.

- **Spam-Schutz ist angehalten** – Klicken Sie auf **Spam-Schutz aktivieren, um diese Funktion erneut zu aktivieren**.

- **Web-Kontrolle ist angehalten** – Klicken Sie auf **Web-Kontrolle aktivieren, um diese Funktion erneut zu aktivieren**.

- **Policy-Override aktiv**– Die von der Policy festgelegte Konfiguration wurde vorübergehend außer Kraft gesetzt, möglicherweise bis zum Abschluss der Problembehandlung. Nur autorisierte Benutzer können die Policy-Einstellungen außer Kraft setzen. Weitere Informationen finden Sie unter Verwenden des Override-Modus.

- **Medienkontrolle ist angehalten** – Klicken Sie auf **Medienkontrolle aktivieren**, um diese Funktion erneut zu aktivieren.

Hinweise zum Anpassen der Sichtbarkeit des produktinternen Status im ersten Bereich von ESET Endpoint Antivirus finden Sie unter Anzuzeigende Hinweise.

Wenn Sie ein Problem mit den vorgeschlagenen Lösungen nicht beheben können, klicken Sie auf **Hilfe und Support**, um die Hilfedateien zu öffnen oder die ESET-Knowledgebase zu durchsuchen. Wenn Sie weiterhin Unterstützung benötigen, können Sie eine Anfrage an den ESET-Support senden. Der ESET-Support wird sich umgehend mit bei Ihnen melden, um Ihre Fragen zu beantworten und Lösungen für Ihr Problem zu finden.



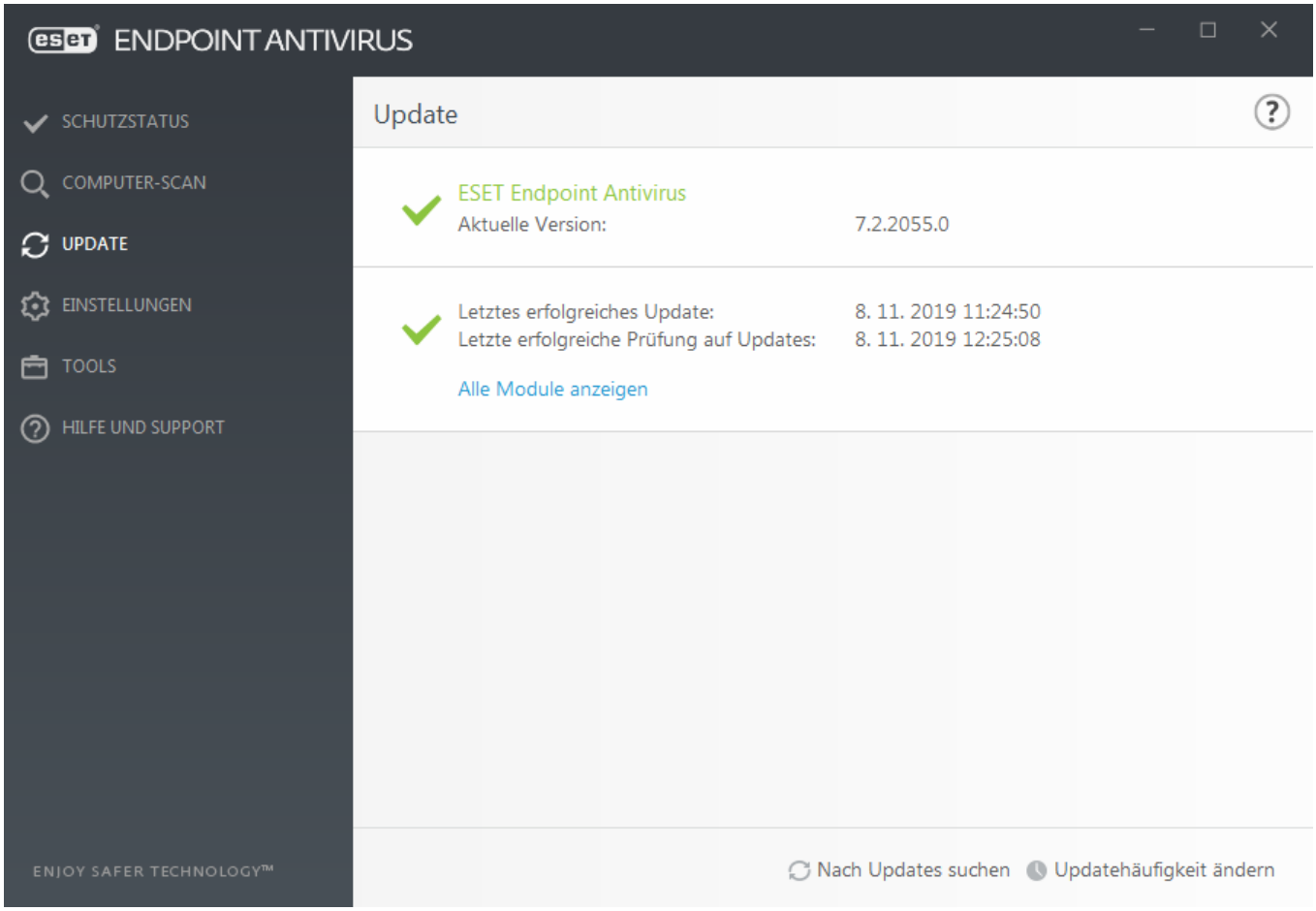
Hinweis

Wenn ein Status zu einem Feature gehört, das von einer ESMC-Policy blockiert wurde, kann der Link nicht angeklickt werden.

Einstellungen für Updates

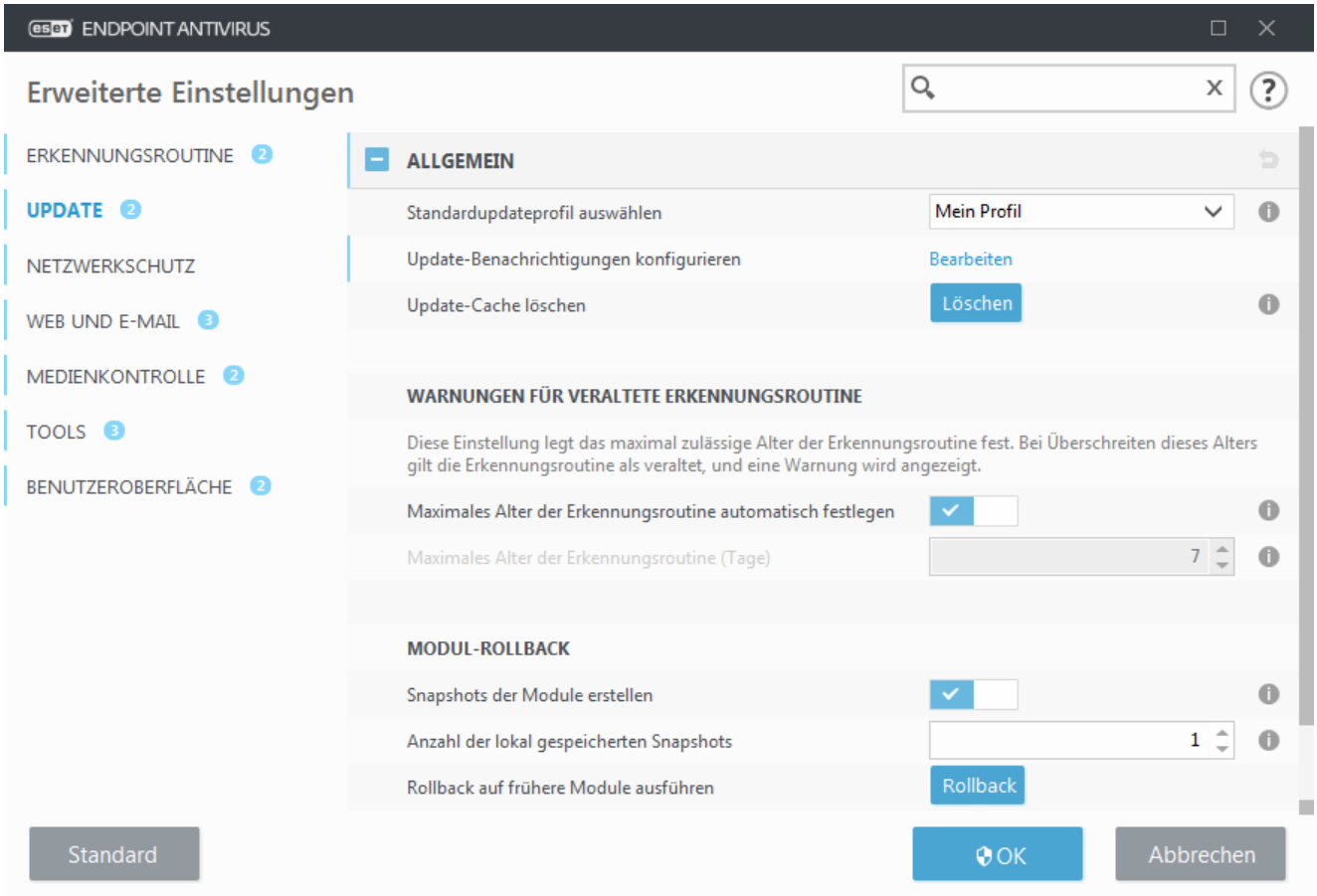
Modul-Updates sind entscheidend für einen möglichst umfassenden Schutz vor Schadcode. Achten Sie deshalb besonders darauf, die Updates passend zu konfigurieren und einzusetzen. Klicken Sie im Hauptmenü auf **Update** > **Nach Updates suchen**, um nach aktuellen Modulupdates zu suchen.

Wenn Sie den **Lizenzschlüssel** noch nicht eingegeben haben, können Sie keine Updates empfangen und werden zur Aktivierung des Produkts aufgefordert.



Das Fenster „Erweiterte Einstellungen“ (klicken Sie auf **Einstellungen** > **Erweiterte Einstellungen im Hauptmenü** oder drücken Sie **F5**) enthält zusätzliche Update-Optionen. Um erweiterte Update-Optionen wie Update-Modus, Proxyserverzugriff, LAN-Verbindungen und die Erstellung von Kopien der Erkennungsroutine zu konfigurieren, klicken Sie in den erweiterten Einstellungen auf **Update**.

- Wenn bei einem Update Fehler auftreten, klicken Sie auf **Löschen**, um den temporären Update-Cache zu löschen.



- Die Option **Automatisch wählen** unter **Profile** > **Updates** > **Modulupdates** ist standardmäßig aktiviert. Wenn Sie Ihre Updates von einem ESET Update-Server beziehen, sollten Sie diese Einstellung beibehalten.

- Falls Sie nicht möchten, dass bei einem erfolgreichen Update eine Benachrichtigung in der Taskleiste unten rechts auf dem Bildschirm angezeigt wird, erweitern Sie **Profile** > **Updates**, klicken Sie auf **Bearbeiten** neben **Empfangene Update-Benachrichtigungen auswählen** und passen Sie die Kontrollkästchen für die Benachrichtigung **Erkennungsroutine wurde erfolgreich aktualisiert** an.

Damit alle Funktionen optimal genutzt werden können, sollte das Programm automatisch aktualisiert werden. Dies ist nur möglich, wenn der richtige **Lizenzschlüssel** unter **Hilfe und Support** > **Produkt aktivieren** eingegeben wurde.

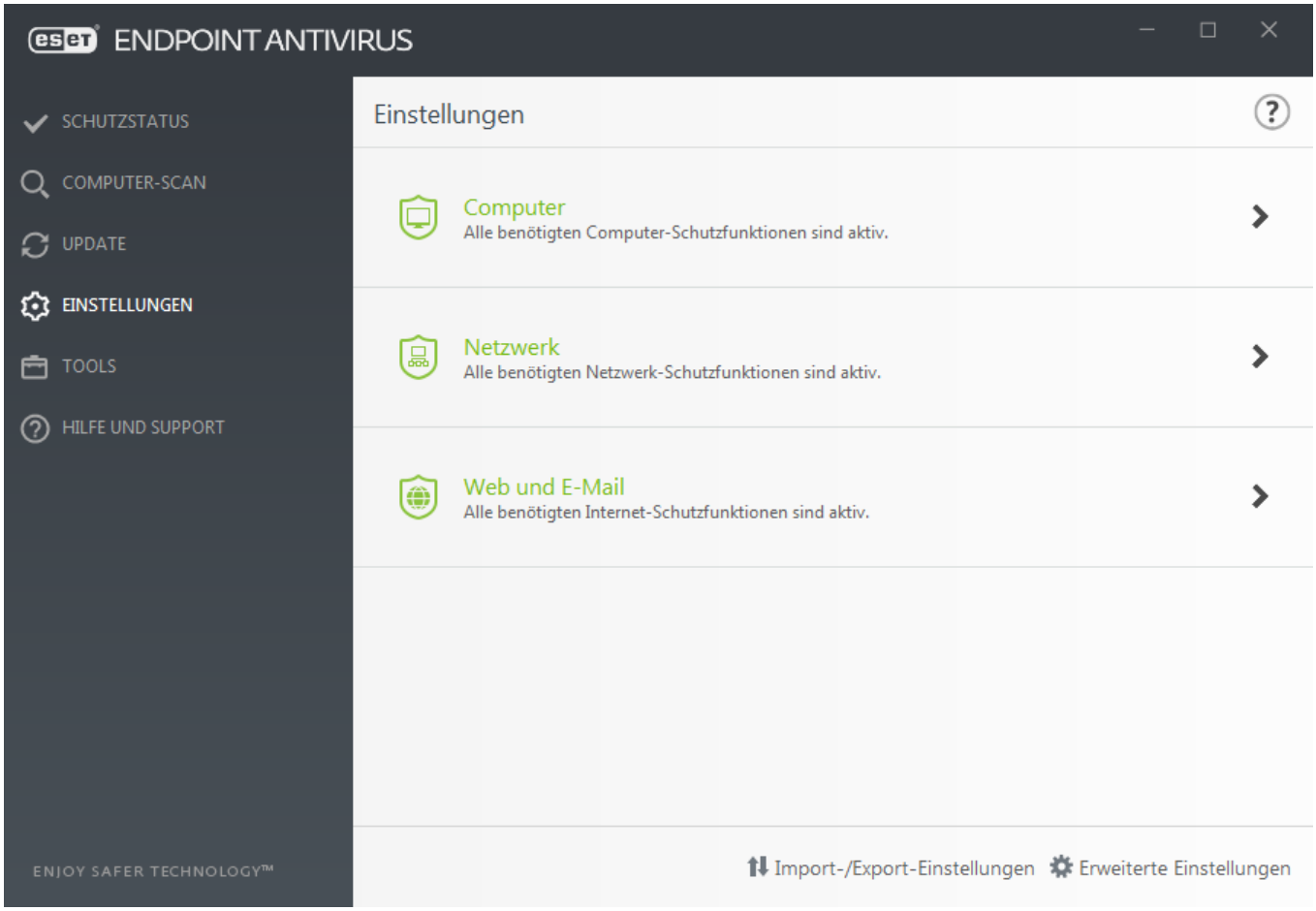
Wenn Sie Ihren **Lizenzschlüssel** nicht nach der Installation eingegeben haben, können Sie dies jederzeit nachholen. Weitere Informationen zur Aktivierung finden Sie unter So aktivieren Sie ESET Endpoint Antivirus. Geben Sie die Anmeldedaten, die Sie für Ihr ESET Security-Produkt erhalten haben, im Fenster **Lizenzdetails** ein.

Arbeiten mit ESET Endpoint Antivirus

Über das ESET Endpoint Antivirus-Menü „Einstellungen“ können Sie die Schutzstufe für Computer, Web und E-Mail anpassen.

Hinweis

Wenn Sie eine Policy in der ESET Security Management Center-Web-Konsole erstellen, können Sie Markierungen für einzelne Einstellungen auswählen. Einstellungen mit der Markierung „Erzwingen“ haben Vorrang und können nicht durch eine spätere Policy überschrieben werden (auch wenn diese ebenfalls die Markierung „Erzwingen“ hat). Dies gewährleistet, dass die Einstellung nicht durch Benutzer oder beim Zusammenführen durch spätere Policies geändert wird. Weitere Informationen finden Sie unter Markierungen in der ESMC-Onlinehilfe.



Folgende Abschnitte stehen im Menü **Einstellungen** zur Verfügung:

- **Computer**
- **Netzwerk**
- **Web und E-Mail**

Im Bereich **Computer** können Sie die folgenden Komponenten aktivieren oder deaktivieren:

- **Echtzeit-Dateischutz** - Alle Dateien werden beim Öffnen, Erstellen oder Ausführen auf Schadcode gescannt.
- **Medienkontrolle** - Bietet Methoden zur automatischen Prüfung von Geräten (CD/DVD/USB/...). Mit diesem Modul können Sie erweiterte Filter- und Berechtigungseinstellungen anpassen und definieren, wie die Benutzer auf bestimmte Geräte zugreifen und mit ihnen arbeiten dürfen.
- **Host Intrusion Prevention System (HIPS)** - Das HIPS-System überwacht Ereignisse auf

Betriebssystemebene und führt Aktionen gemäß individueller Regeln aus.

• Die **Erweiterte Speicherprüfung** bietet im Zusammenspiel mit dem Exploit-Blocker stärkeren Schutz vor Malware, die darauf ausgelegt ist, der Erkennung durch Anti-Malware-Produkte mittels Verschleierung oder Verschlüsselung zu entgehen. Die erweiterte Speicherprüfung ist standardmäßig aktiviert. Weitere Informationen zu dieser Art des Schutzes finden Sie in unserem Glossar.

• **Exploit-Blocker aktivieren** - Dieses Modul sichert besonders anfällige Anwendungstypen wie Webbrowser, PDF-Leseprogramme, E-Mail-Programme und MS Office-Komponenten ab. Der Exploit-Blocker ist standardmäßig aktiviert. Weitere Informationen zu diesem Schutztyp finden Sie in unserem Glossar.

• Der **Ransomware-Schutz** ist eine weitere Schutzebene im Rahmen der HIPS-Funktion. Sie müssen das ESET LiveGrid®-Reputationssystem aktivieren, um den Ransomware-Schutz verwenden zu können. Weitere Informationen zu diesem Schutztyp finden Sie hier.

• **Präsentationsmodus** - Eine Funktion für Benutzer, die ihre Software ununterbrochen nutzen, nicht durch Popup-Fenster gestört werden und die CPU-Auslastung reduzieren möchten. Nach der Aktivierung des Präsentationsmoduswird eine Warnung angezeigt (erhöhtes Sicherheitsrisiko) und das Hauptfenster wird orange.

Im Bereich **Netzwerk-Schutz** können Sie die Funktionen Netzwerkangriffsschutz (IDS) und Botnet-Erkennung konfigurieren.

In den Einstellungen für **Web und E-Mail-Schutz** können Sie folgende Komponenten aktivieren oder deaktivieren:

• **Web-Schutz** - Wenn diese Option aktiviert ist, werden alle Daten geprüft, die über HTTP oder HTTPS übertragen werden.
• **E-Mail-Client-Schutz** - Überwacht eingehende E-Mails, die mit dem POP3- oder dem IMAP-Protokoll übertragen werden.
• **Phishing-Schutz** - Schützt Sie vor Versuchen unseriöser Webseiten, an Passwörter, Bankdaten und andere sicherheitsrelevante Informationen zu gelangen, indem sie sich als seriöse Webseiten ausgeben.

Zur vorübergehenden Deaktivierung einzelner Module klicken Sie auf den**grünen Schalter**  neben dem gewünschten Modul. Beachten Sie, dass dies den Schutz Ihres Computers beeinträchtigen kann.

Zur Reaktivierung des Schutzes einer deaktivierten Sicherheitskomponente klicken Sie auf den roten Schalter  . Hiermit wird wird die Komponente erneut aktiviert.

Wenn eine ESMC/ERA-Policy angewendet wurde, sehen Sie ein Sperrsymbol  neben der jeweiligen Komponente. Die von ESET Security Management Center angewendete Policy kann nach der Authentifizierung durch einen protokollierten Benutzer (z. B. den Administrator) außer Kraft gesetzt werden. Weitere Informationen finden Sie in der ESMC-Onlinehilfe.



Hinweis
Alle auf diese Weise deaktivierten Schutzmaßnahmen werden nach einem Neustart des Computers wieder aktiviert.

Zugriff auf detaillierte Einstellungen zu einer bestimmten Sicherheitskomponente erhalten Sie, indem Sie auf das Zahnradsymbol  neben der betreffenden Komponenten klicken.

Am unteren Rand des Fensters „Einstellungen“ finden Sie weitere Optionen. Verwenden Sie die Option **Import-/Export-Einstellungen**, um die Einstellungen aus einer *.xml*-Konfigurationsdatei zu laden oder die aktuellen

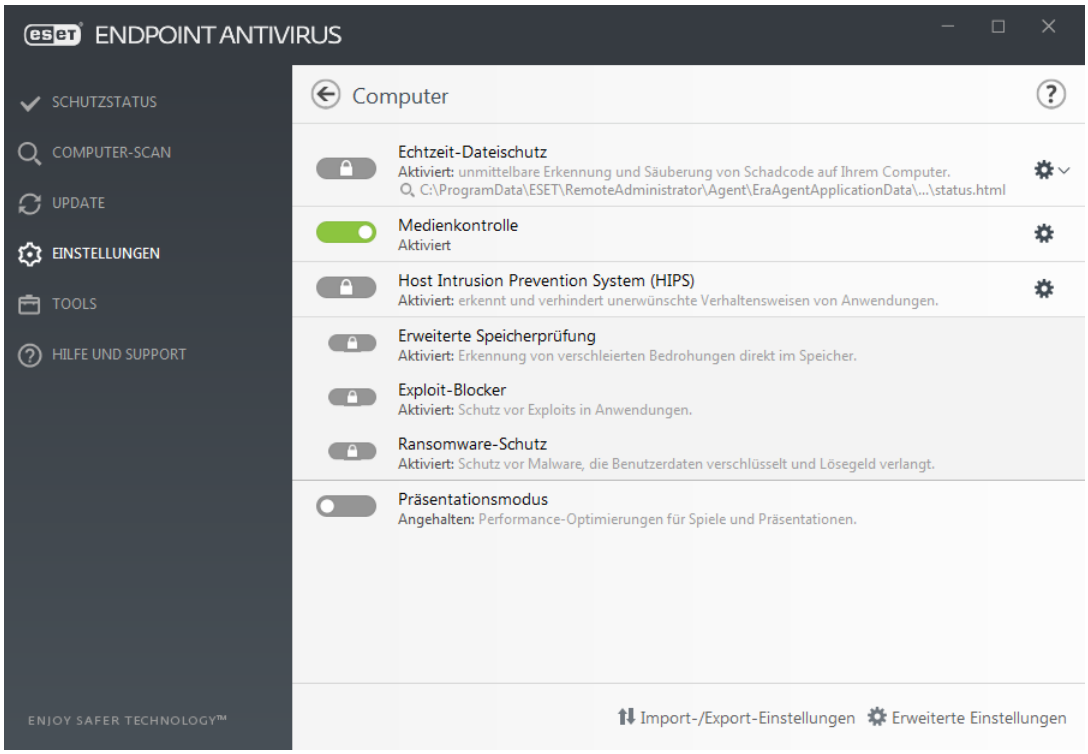
Einstellungen in einer Konfigurationsdatei zu speichern. Ausführliche Informationen hierzu finden Sie unter Import-/Export-Einstellungen.

Klicken Sie auf **Erweiterte Einstellungen** oder drücken Sie **F5**, um weitere Optionen anzuzeigen.

Computer

Das Modul **Computer** befindet sich unter **Einstellungen** > **Computer**. Es enthält eine Übersicht über die im vorherigen Kapitel beschriebenen Schutzmodule. In diesem Bereich stehen die folgenden Einstellungen zur Verfügung:

Klicken Sie auf das Zahnrad neben **Echtzeit-Dateischutz** und anschließend auf **Ausschlussfilter bearbeiten**, um das Fenster für die Ausschlussfilter-Einstellungen zu öffnen. Hier können Sie Dateien und Ordner vom Scannen ausschließen.



Im Bereich **Computer** können Sie die folgenden Komponenten aktivieren oder deaktivieren:

- **Echtzeit-Dateischutz** - Alle Dateien werden beim Öffnen, Erstellen oder Ausführen auf Ihrem Computer auf Schadcode geprüft.

- **Medienkontrolle** - Bietet Methoden zur automatischen Prüfung von Geräten (CD/DVD/USB/...). Mit diesem Modul können Sie erweiterte Filter- und Berechtigungseinstellungen anpassen und definieren, wie die Benutzer auf bestimmte Geräte zugreifen und mit ihnen arbeiten dürfen.

- **Host Intrusion Prevention System (HIPS)** - Das HIPS-System überwacht Ereignisse auf Betriebssystemebene und führt Aktionen gemäß individueller Regeln aus.

- Die **Erweiterte Speicherprüfung** bietet im Zusammenspiel mit dem Exploit-Blocker stärkeren Schutz vor Malware, die darauf ausgelegt ist, der Erkennung durch Anti-Malware-Produkte mittels Verschleierung oder Verschlüsselung zu entgehen. Die erweiterte Speicherprüfung ist standardmäßig aktiviert. Weitere Informationen zu dieser Art des Schutzes finden Sie in unserem Glossar.

- **Exploit-Blocker aktivieren** - Dieses Modul sichert besonders anfällige Anwendungstypen wie Webbrowser, PDF-Leseprogramme, E-Mail-Programme und MS Office-Komponenten ab. Der Exploit-Blocker ist standardmäßig aktiviert. Weitere Informationen zu diesem Schutztyp finden Sie in unserem Glossar.

- Der **Ransomware-Schutz** ist eine weitere Schutzebene im Rahmen der HIPS-Funktion. Sie müssen das ESET LiveGrid®-Reputationssystem aktivieren, um den Ransomware-Schutz verwenden zu können. Weitere Informationen zu diesem Schutztyp finden Sie hier.

- **Präsentationsmodus** - Eine Funktion für Benutzer, die ihre Software ununterbrochen nutzen, nicht durch Popup-Fenster gestört werden und die CPU-Auslastung reduzieren möchten. Nach der Aktivierung des Präsentationsmoduswird eine Warnung angezeigt (erhöhtes Sicherheitsrisiko) und das Hauptfenster wird orange.

Viren- und Spyware-Schutz vorübergehend deaktivieren- Bei der vorübergehenden Deaktivierung des Viren- und Spyware-Schutzes können Sie im entsprechenden Dropdown-Menü den Zeitraum wählen, in dem die jeweilige Komponente deaktiviert werden soll. Klicken Sie anschließend auf **Übernehmen**, um die Sicherheitskomponente zu deaktivieren. Durch Klicken auf **Viren- und Spyware-Schutz aktivieren** wird der Schutz wieder aktiviert.

Erkennungsroutine (7.2 und höher)

Die Erkennungsroutine schützt Sie vor bösartigen Systemangriffen, indem Dateien, E-Mails und die Internetkommunikation kontrolliert werden. Wenn ein als Malware klassifiziertes Objekt gefunden wird, beginnt die Säuberung. Die Erkennungsroutine kann das Objekt zunächst blockieren und anschließend säubern, löschen oder in die Quarantäne verschieben.

Klicken Sie auf **Erweiterte Einstellungen** oder drücken Sie die Taste **F5**, um die Einstellungen für die Erkennungsroutine im Detail zu konfigurieren.

In diesem Abschnitt:

- Kategorien Echtzeit- & Machine-Learning-Schutz
- Malware-Scans
- Einrichten der Berichterstellung
- Einrichten des Schutzes
- Best Practices

> **Änderungen an der Scannerkonfiguration der Erkennungsroutine**
> Ab Version 7.2 enthält der Abschnitt „Erkennungsroutine“ keine EIN-/AUS-Schalter mehr wie in Version 7.1 und niedriger. Die EIN-/AUS-Schalter wurden durch vier Schwellenwerte ersetzt: Aggressiv, Ausgewogen, Vorsichtig und Aus.

Kategorien Echtzeit- & Machine-Learning-Schutz

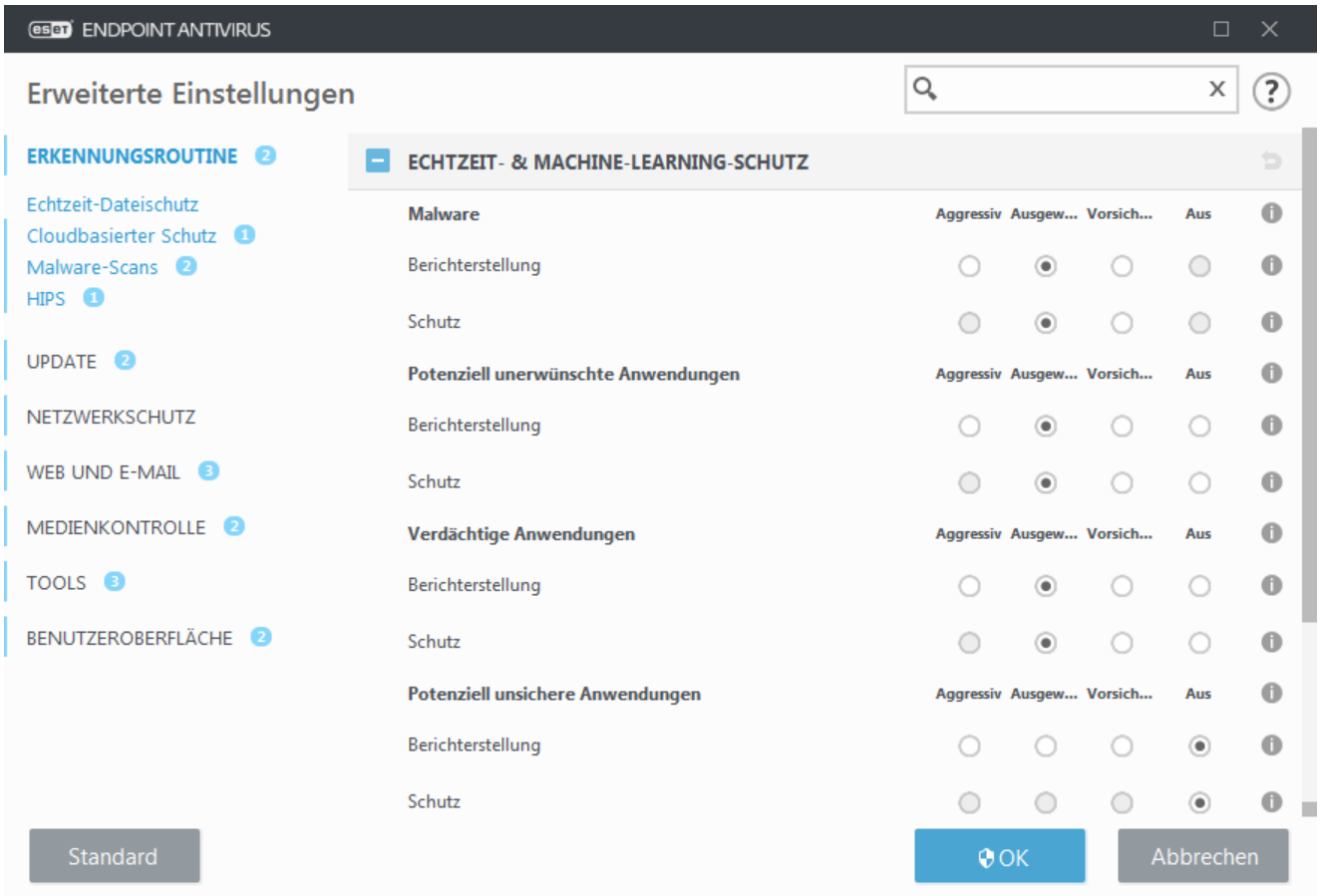
Mit dem **Echtzeit- & Machine-Learning-Schutz** für alle Schutzmodule (z. B. Echtzeit-Dateischutz, Web-Schutz usw.) können Sie Berichte und Schutzebenen für die folgenden Kategorien konfigurieren:

- **Malware** - Computerviren sind Schadcode, der den vorhandenen Dateien auf Ihrem Computer vorangestellt oder angefügt wird. Allerdings wird der Begriff „Virus“ oft missbraucht. „Malware“ (Schadcode) ist ein präziserer Begriff. Die Malware-Erkennung wird von der Erkennungsroutine zusammen mit der Machine-Learning-Komponente ausgeführt.
Weitere Informationen zu diesem Anwendungstyp finden Sie im Glossar.

- **Potenziell unerwünschte Anwendungen** - Grayware oder potenziell unerwünschte Anwendungen (PUA) sind verschiedenste Arten von Software, deren Ziel nicht so eindeutig bösartig ist wie bei anderen Arten von Malware wie Viren oder Trojanern. Diese Art von Software kann jedoch weitere unerwünschte Software installieren, das Verhalten des digitalen Geräts ändern oder Aktionen ausführen, denen der Benutzer nicht zugestimmt hat oder die er nicht erwartet.
Weitere Informationen zu diesem Anwendungstyp finden Sie im Glossar.

- **Potenziell unsichere Anwendungen** sind gewerbliche Anwendungen, die zu böswilligen Zwecken missbraucht werden können. Beispiele für potenziell unsichere Anwendungen (PUA) sind Programme zum Fernsteuern von Computern (Remotedesktopverbindung), Programme zum Entschlüsseln von Passwörtern und Keylogger (Programme, die Tastendrücke der Benutzer aufzeichnen).
Weitere Informationen zu diesem Anwendungstyp finden Sie im Glossar.

- **Verdächtige Anwendungen** umfassen Programme, die mit Packprogrammen oder Schutzprogrammen komprimiert wurden. Diese Schutzarten werden oft von Verfassern von Schadcode eingesetzt, um die Erkennung zu umgehen.





Verbesserter Schutz

Das erweiterte Machine Learning ist jetzt als zusätzliche Schutzebene in der Erkennungsroutine enthalten und verbessert die Erkennung auf Basis von Machine Learning. Weitere Informationen zu diesem Schutztyp finden Sie im Glossar.

Malware-Scans

Die Scaneinstellungen für Echtzeit-Scanner und On-Demand-Scanner können separat konfiguriert werden. Die Option **Einstellungen für den Echtzeit-Schutz verwenden** ist standardmäßig aktiviert. Wenn diese Option aktiviert ist, werden die On-Demand-Scaneinstellungen aus dem Bereich **Echtzeit- & Machine-Learning-Schutz** übernommen.

Einrichten der Berichterstellung

Bei einem Ereignis (z. B. eine Bedrohung wird gefunden und als Malware klassifiziert) werden Informationen im Ereignis-Los aufgezeichnet, und Desktophinweise werden angezeigt, wenn dies in ESET Endpoint Antivirus konfiguriert wurde.

Der Schwellenwert für die Berichterstellung kann pro Kategorie konfiguriert werden (bezeichnet als „KATEGORIE“):

1. Malware
2. Potenziell unerwünschte Anwendungen
3. Potenziell unsicher
4. Verdächtige Anwendungen

Die Berichterstellung wird mit der Erkennungsroutine ausgeführt, inklusive der Machine-Learning-Komponente. Sie können einen höheren Schwellenwert für die Berichterstellung als die aktuelle Schutzstufe festlegen. Diese Einstellungen für die Berichterstellung haben keinen Einfluss darauf, ob Objekte blockiert, gesäubert oder gelöscht werden.

Lesen Sie die folgenden Artikel, bevor Sie Änderungen an Schwellenwerten (oder Ebenen für KATEGORIE-Berichte vornehmen:

Schwellenwert	Erklärung
Aggressiv	KATEGORIE-Berichte mit maximaler Empfindlichkeit. Mehr Bedrohungen werden gemeldet. Die **aggressive** Einstellung kann Objekte fälschlicherweise als KATEGORIE klassifizieren.
Ausgewogen	Ausgewogen konfigurierte KATEGORIE-Berichte. Diese Einstellung bietet einen optimalen Ausgleich zwischen Leistung und Genauigkeit der Erkennungsraten und der Anzahl der fälschlich gemeldeten Objekte.

Vorsichtig	KATEGORIE-Berichte zur Minimierung falsch erkannter Objekte mit ausreichendem Schutzniveau. Objekte werden nur gemeldet, wenn die Erkennung sehr wahrscheinlich ist und mit dem Verhalten von KATEGORIE übereinstimmt.
Aus	Die Berichterstellung für KATEGORIE ist nicht aktiv und diese Ereignisse werden nicht erkannt, gemeldet oder gesäubert. Diese Einstellung deaktiviert daher den Schutz vor diesem Ereignistyp. Off ist nicht verfügbar für Malware-Berichte und ist der Standardwert für potenziell unsichere Anwendungen.

Verfügbarkeit der ESET Endpoint Antivirus-Schutzmodule

Verfügbarkeit (aktiviert oder deaktiviert) eines Schutzmoduls für einen ausgewählten KATEGORIE-Schwellenwert:

	Aggressiv	Ausgewogen	Vorsichtig	Aus**
Erweitertes Machine Learning-Modul*	✔ (aggressiver Modus)	✔ (zurückhaltender Modus)	X	X
Modul der Erkennungsroutine	✔	✔	✔	X
Andere Schutzmodule	✔	✔	✔	X

* Verfügbar in ESET Endpoint Antivirus Version 7.2 und höher.
** Nicht empfohlen

Ermitteln von Produktversion, Versionen der Programmmodule und Builddaten

1. Klicken Sie auf **Hilfe und Support** > **Über ESET Endpoint Antivirus**.
2. Im Abschnitt **Über** wird in der ersten Zeile die Versionsnummer Ihres ESET-Produkts angezeigt.
3. Klicken Sie auf **Installierte Komponenten**, um Informationen zu einzelnen Modulen anzuzeigen.

Wichtige Hinweise

Einige Hinweise zum Festlegen angemessener Schwellenwerte für Ihre Umgebung:

- Der Schwellenwert **Ausgewogen** wird für die meisten Einrichtungen empfohlen.
- Der Schwellenwert **Vorsichtig** bietet eine Schutzebene, die mit den Vorgängerversionen von ESET Endpoint Antivirus (7.1 und niedriger) vergleichbar ist. Diese Ebene wird empfohlen für Umgebungen, in denen es wichtig ist, die von der Sicherheitssoftware fälschlich identifizierten Objekte zu minimieren.
- Je höher der Schwellenwert für die Berichterstellung, desto höher ist die Erkennungsrate, aber auch die Rate der fälschlich identifizierten Objekte.
- In der Praxis ist es nicht möglich, eine Erkennungsrate von 100 % oder eine Rate von 0 % für fälschlicherweise als Malware erkannte saubere Objekte zu garantieren.
- Aktualisieren Sie ESET Endpoint Antivirus und die Module fortlaufend, um die Balance zwischen Leistung und Genauigkeit der Erkennungsraten und der Anzahl der fälschlicherweise gemeldeten Objekte zu optimieren.

Einrichten des Schutzes

Als KATEGORIE klassifizierte Objekte werden vom Programm blockiert, und das Objekt wird anschließend gesäubert, gelöscht oder in die Quarantäne verschoben.

Lesen Sie die folgenden Artikel, bevor Sie Änderungen an Schwellenwerten (oder Ebenen für den KATEGORIE-Schutz vornehmen:

Schwellenwert	Erklärung
Aggressiv	Gemeldete aggressive (oder niedrigere) Ereignisse werden blockiert und die automatische Behebung (z. B. Säuberung) wird gestartet. Diese Einstellung wird empfohlen, wenn alle Endpoints mit aggressiven Einstellungen gescannt wurden und fälschlicherweise gemeldete Objekte zu den Erkennungsausschlüssen hinzugefügt wurden.
Ausgewogen	Gemeldete ausgewogene (oder niedrigere) Ereignisse werden blockiert und die automatische Behebung (z. B. Säuberung) wird gestartet.
Vorsichtig	Gemeldete ausgewogene Ereignisse werden gesperrt und die automatische Behebung (z. B. Säuberung) wird gestartet.
Aus	Nützlich, um fälschlich gemeldete Objekte zu identifizieren und auszuschließen. Off ist nicht verfügbar für den Malware-Schutz und ist der Standardwert für potenziell unsichere Anwendungen.

Konvertierungstabelle für ESMC-Policies in ESET Endpoint Antivirus 7.1 und niedriger

Der ESMC-Policy-Editor für die Scannereinstellungen enthält keine EIN-/AUS-Schalter mehr pro KATEGORIE. Die folgende Tabelle zeigt die Konvertierung zwischen dem Schutz-Schwellenwert und der entsprechenden Position des Schalters in ESET Endpoint Antivirus 7.1 und niedriger.

Status des KATEGORIE-Schwellenwerts	Aggressiv	Ausgewogen	Vorsichtig	Aus
Schalterposition für KATEGORIE	✓	✓	✓	✗

Beim Upgrade von Version 7.1 und niedriger auf Version 7.2 und höher gilt der folgende neue Schwellenwertstatus:

Kategorieschalter vor dem Upgrade	✓	✗
Neuer KATEGORIE-Schwellenwert nach dem Upgrade	Ausgewogen	Aus

Best Practices

NICHT VERWALTET (einzelne Client-Workstation)

Behalten Sie die empfohlenen Standardwerte bei.

VERWALTETE UMGEBUNG

Diese Einstellungen werden normalerweise mit einer Policy auf Workstations angewendet.

1. Anfangsphase

Diese Phase kann bis zu einer Woche dauern.

- Legen Sie alle **Berichterstellungs**-Schwellenwerte auf **Ausgewogen** fest.
HINWEIS: Legen Sie die Werte bei Bedarf auf **Aggressiv** fest.
- Legen Sie den Malware-**Schutz** auf **Ausgewogen** fest.
- Legen Sie den **Schutz** für andere KATEGORIEN auf **Vorsichtig** fest.
HINWEIS: Wir raten davon ab, den **Schutz**-Schwellenwert in dieser Phase auf **Aggressiv** festzulegen, da andernfalls alle gefundenen Ereignisse behoben werden, inklusive fälschlich identifizierter Ereignisse.
- Identifizieren Sie daher zunächst die fälschlich identifizierten Objekte im Erkennungs-Log und fügen Sie sie zu den Ereignisausschlüssen hinzu.

2. Übergangsphase

- Implementieren Sie die „Produktionsphase“ als Test auf einigen Workstations (nicht auf allen Workstations im Netzwerk).

3. Produktionsphase

- Legen Sie alle **Schutz**-Schwellenwerte auf **Ausgewogen** fest.
- Verwenden Sie in remote verwalteten Umgebungen eine passende vordefinierter Virenschutz-Policy für ESET Endpoint Antivirus.
- Verwenden Sie den Schutz-Schwellenwert **Aggressiv**, wenn Sie die Erkennungsrate maximieren möchten und bereit sind, fälschlich identifizierte Objekte zu akzeptieren.
- Überprüfen Sie das Erkennungs-Log oder die ESMC-Berichte auf mögliche fehlende Erkennungen.

Erweiterte Einstellungen für die Erkennungsroutine

Die **Anti-Stealth-Technologie** ist ein fortschrittliches System zur Erkennung gefährlicher Programme wie Rootkits, die sich vor dem Betriebssystem verstecken können. Aus diesem Grund ist es nahezu unmöglich, sie mit herkömmlichen Prüfmethoden zu erkennen.

Erweiterte AMSI-Prüfung aktivieren–Mit der Anti-Malware-Prüfschnittstelle von Microsoft können Anwendungsentwickler neue Verteidigungsmaßnahmen entwickeln (nur Windows 10).

Erkennungsroutine (7.1 und niedriger)

Die Erkennungsroutine schützt Sie vor bösartigen Systemangriffen, indem Dateien, E-Mails und die Internetkommunikation kontrolliert werden. Wenn ein als Malware klassifiziertes Objekt gefunden wird, beginnt die Säuberung. Die Erkennungsroutine kann das Objekt zunächst blockieren und anschließend säubern, löschen oder in die Quarantäne verschieben.

Klicken Sie auf **Erweiterte Einstellungen** oder drücken Sie die Taste **F5**, um die Einstellungen für die Erkennungsroutine im Detail zu konfigurieren.

> **Änderungen an der Scannerkonfiguration der Erkennungsroutine**
> Mit Version 7.2 hat sich das Erscheinungsbild der Erkennungsroutine geändert.

In den **Scan-Einstellungen** für die verschiedenen Schutzmodule (Echtzeit-Dateischutz, Web-Schutz usw.) können Sie die Erkennung folgender Elemente aktivieren und deaktivieren:

- **Potenziell unerwünschte Anwendungen**– Grayware oder potenziell unerwünschte Anwendungen sind verschiedenste Arten von Software, deren Ziel nicht so eindeutig bösartig ist wie bei anderen Arten von Malware wie Viren oder Trojanern. Diese Art von Software kann jedoch weitere unerwünschte Software installieren, das Verhalten des digitalen Geräts ändern oder Aktionen ausführen, denen der Benutzer nicht zugestimmt hat oder die er nicht erwartet.
  Weitere Informationen zu diesem Anwendungstyp finden Sie im Glossar.

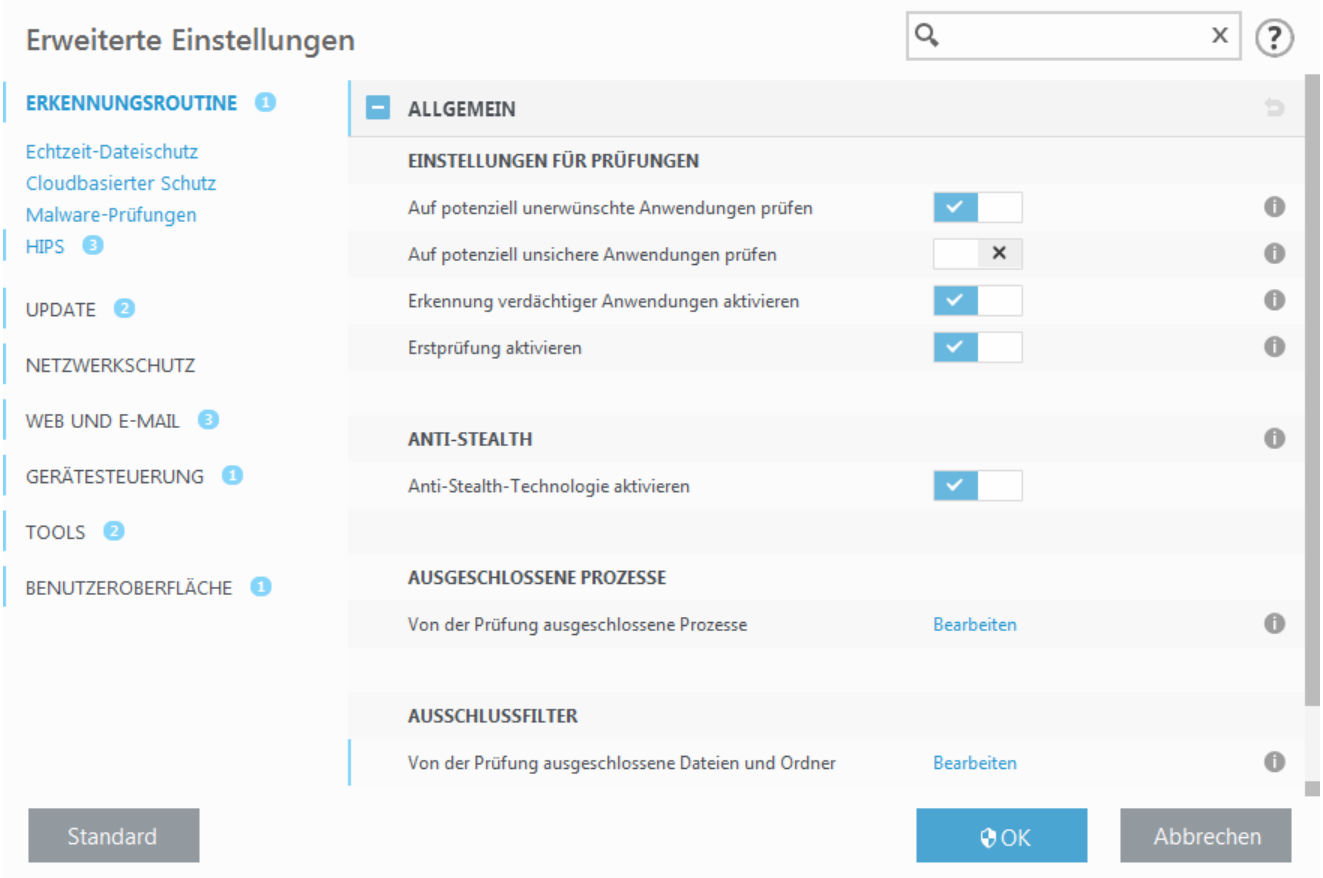
- **Potenziell unsichere Anwendungen** stellen gewerbliche Software dar, die zu einem böswilligen Zweck missbraucht werden kann. Beispiele für potenziell unsichere Anwendungen sind Programme für das Fernsteuern von Computern (Remotedesktopverbindung), Programme zum Entschlüsseln von Passwörtern und Keylogger (Programme, die aufzeichnen, welche Tasten vom Benutzer gedrückt werden). Diese Option ist in der Voreinstellung deaktiviert.
  Weitere Informationen zu diesem Anwendungstyp finden Sie im Glossar.

- **Verdächtige Anwendungen** umfassen Programme, die mit Packprogrammen oder Schutzprogrammen komprimiert wurden. Diese Schutzarten werden oft von Verfassern von Schadcode eingesetzt, um die Erkennung zu umgehen.

Die **Anti-Stealth-Technologie** ist ein fortschrittliches System zur Erkennung gefährlicher Programme wie Rootkits, die sich vor dem Betriebssystem verstecken können. Aus diesem Grund ist es nahezu unmöglich, sie mit herkömmlichen Prüfmethoden zu erkennen.

Mit **Ausschlüssen** können Sie Objekte von den Scans ausschließen. Weitere Informationen finden Sie unter Ausschlüsse.

Erweiterte AMSI-Prüfung aktivieren–Mit der Anti-Malware-Prüfschnittstelle von Microsoft können Anwendungsentwickler neue Verteidigungsmaßnahmen entwickeln (nur Windows 10).



Eingedrungene Schadsoftware wurde erkannt

Schadsoftware kann auf vielen Wegen in das System gelangen. Mögliche Eintrittsstellen sind Websites, freigegebene Ordner, E-Mails oder Wechselmedien (USB-Sticks, externe Festplatten, CDs, DVDs, usw.).

Standardmäßiges Verhalten

ESET Endpoint Antivirus kann Bedrohungen mit einem der folgenden Module erkennen:

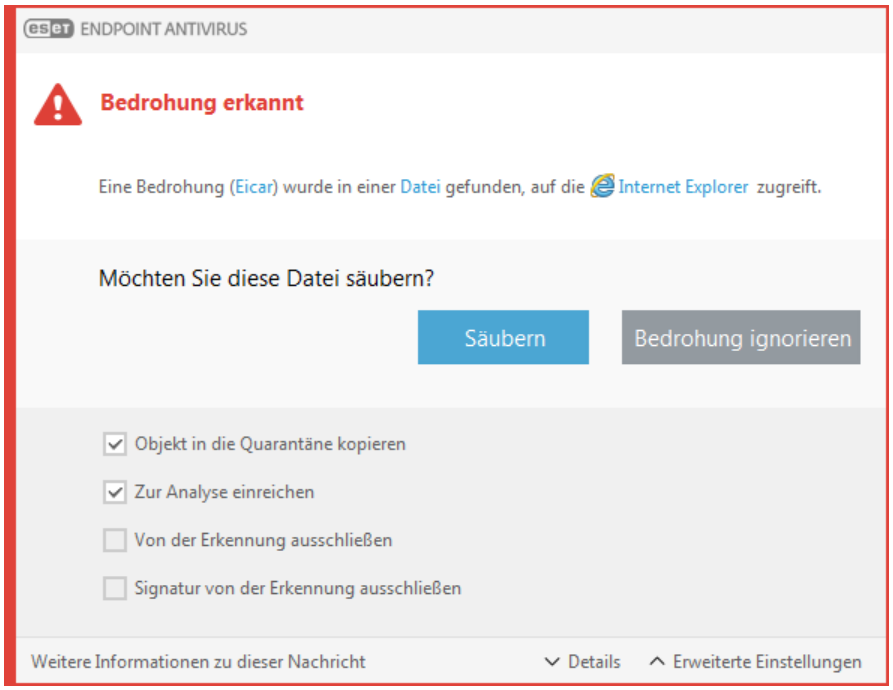
- Echtzeit-Dateischutz
- Web-Schutz
- E-Mail-Client-Schutz
- On-Demand-Scan

Standardmäßig wenden die Module die normale Säuberungsstufe an und versuchen, die Datei zu säubern und in die Quarantäne zu verschieben, oder die Verbindung zu beenden. Im Infobereich der Taskleiste rechts unten auf dem Bildschirm wird ein Hinweisfenster angezeigt. Weitere Informationen zu den Säuberungsstufen und zum Verhalten des Produkts finden Sie unter Säubern.



Säubern und löschen

Ist für den Echtzeit-Dateischutz keine vordefinierte Aktion angegeben, werden Sie in einem Warnungsfenster aufgefordert, zwischen verschiedenen Optionen zu wählen. In der Regel stehen die Optionen **Säubern**, **Löschen** und **Keine Aktion** zur Auswahl. Die Auswahl der Option **Keine Aktion** ist nicht empfehlenswert, da infizierte Dateien mit dieser Einstellung nicht gesäubert werden. Einzige Ausnahme: Sie sind sich sicher, dass die Datei harmlos ist und versehentlich erkannt wurde.



Wenden Sie die Option „Säubern“ an, wenn eine Datei von einem Virus mit Schadcode infiziert wurde. In einem solchen Fall sollten Sie zuerst versuchen, den Schadcode aus der infizierten Datei zu entfernen und ihren Originalzustand wiederherzustellen. Wenn die Datei ausschließlich Schadcode enthält, wird sie gelöscht.

Wenn eine infizierte Datei „gesperrt“ ist oder von einem Systemprozess verwendet wird, muss die Datei in der Regel erst freigegeben werden (häufig ist dazu ein Systemneustart erforderlich), bevor sie gelöscht werden kann.

Mehrere Bedrohungen

Falls infizierte Dateien während der Prüfung des Computers nicht gesäubert wurden (oder die Säuberungsstufe auf **Nicht säubern** festgelegt wurde), so wird ein Warnfenster angezeigt. In diesem wird danach gefragt, wie mit den Dateien verfahren werden soll.

Dateien in Archiven löschen

Im Standard-Säuberungsmodus wird das gesamte Archiv nur gelöscht, wenn es ausschließlich infizierte Dateien enthält. Archive, die auch nicht infizierte Dateien enthalten, werden also nicht gelöscht. Die Option „Immer versuchen, automatisch zu entfernen“ sollten Sie mit Bedacht einsetzen, da in diesem Modus alle Archive gelöscht werden, die mindestens eine infizierte Datei enthalten, und dies unabhängig vom Status der übrigen Archivdateien.

Wenn Ihr Computer die Symptome einer Malware-Infektion aufweist (beispielsweise langsamer als gewöhnlich arbeitet oder häufig nicht reagiert), sollten Sie folgendermaßen vorgehen:

- Öffnen Sie ESET Endpoint Antivirus und klicken Sie auf „Computer prüfen“
- Klicken Sie auf **Smart-Prüfung** (weitere Informationen siehe Abschnitt Computer prüfen)
- Nachdem die Prüfung abgeschlossen ist, überprüfen Sie im Log die Anzahl der geprüften, infizierten und wiederhergestellten Dateien

Wenn Sie nur einen Teil Ihrer Festplatte prüfen möchten, wählen Sie **Benutzerdefinierte Prüfung** und anschließend die Bereiche, die auf Viren geprüft werden sollen.

Gemeinsam genutzter lokaler Cache

Der gemeinsam genutzte lokale Cache kann die Leistung in isolierten Umgebungen (z. B. virtuelle Computer) verbessern, indem doppelte Scans im Netzwerk vermieden werden. Jede Datei wird nur einmal gescannt und im gemeinsamen Cache gespeichert.

Der ESET Shared Local Cache muss zuerst installiert und konfiguriert werden.

- ESET Shared Local Cache herunterladen.
- Weitere Informationen finden Sie im Handbuch für den ESET Shared Local Cache.

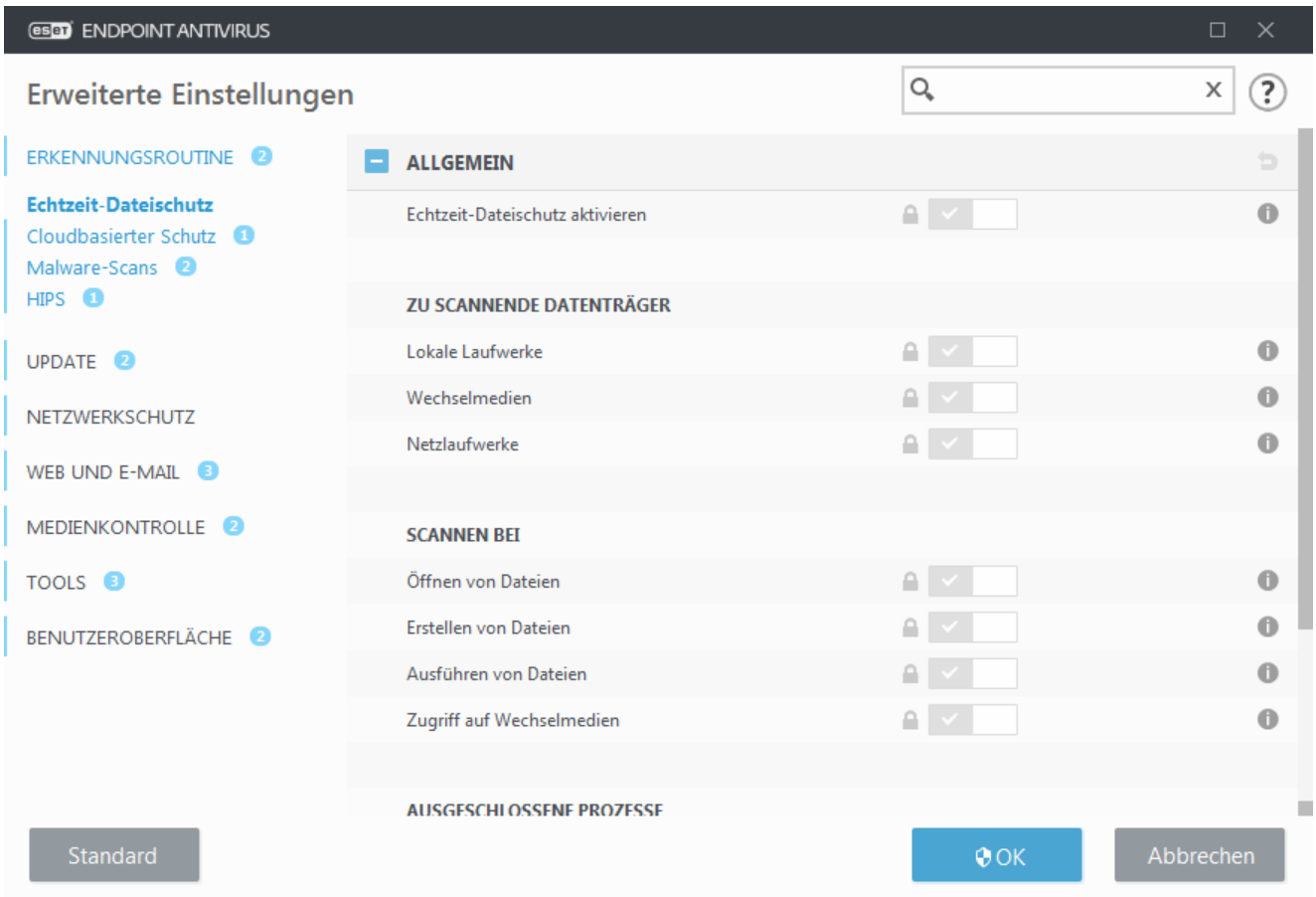
Aktivieren Sie den Schalter **Caching-Option**, um Informationen zu gescannten Dateien und Ordnern in Ihrem Netzwerk im ESET Shared Local Cache zu speichern. Wenn Sie einen neuen Scan ausführen, sucht ESET Endpoint Antivirus im ESET Shared Local Cache nach gescannten Dateien. Gefundene Übereinstimmungen werden vom Scannen ausgeschlossen.

Zu den Einstellungen des **Cache-Servers** gehören die folgenden Elemente:

- **Hostname** - Hostname oder IP-Adresse des Computers, auf dem sich der ESET Shared Local Cache befindet.
- **Port** - Portnummer für die Kommunikation (die gleiche Nummer, die auch für den ESET Shared Local Cache festgelegt wurde).
- **Passwort** - Geben Sie bei Bedarf das Passwort für ESET Shared Local Cache an.

Echtzeit-Dateischutz

Der Echtzeit-Dateischutz kontrolliert alle Dateien im Dateisystem beim Öffnen, Erstellen und Ausführen auf bösartigen Code.



Der Echtzeit-Dateischutz wird standardmäßig beim Systemstart gestartet und fortlaufend ausgeführt. Wir empfehlen, die Option **Echtzeit-Dateischutz aktivieren** unter **Erweiterte Einstellungen** > **Erkennungsroutine** > **Echtzeit-Dateischutz** > **Einfach** nicht zu deaktivieren.

Zu scannende Datenträger

In der Standardeinstellung werden alle Datenträger auf mögliche Bedrohungen geprüft:

- **Lokale Laufwerke** - Scannt alle System- und fest installierten Laufwerke (Beispiel: *C:*\, *D:*\).
- **Wechselmedien** - Scannt CD/DVDs, USB-Sticks, Speicherkarten usw.
- **Netzlaufwerke** - Scannt alle zugeordneten Netzlaufwerke (Beispiel: *H:*\ als *store04*) oder Netzlaufwerke mit direktem Zugriff (Beispiel: *store08*).

Es wird empfohlen, diese Einstellungen nur in Ausnahmefällen zu ändern, z. B. wenn die Prüfung bestimmter Datenträger die Datenübertragung deutlich verlangsamt.

Scannen bei

Standardmäßig werden alle Dateien beim Öffnen, Erstellen und Ausführen geprüft. Wir empfehlen Ihnen, die

Standardeinstellungen beizubehalten. So bietet der Echtzeit-Dateischutz auf Ihrem Computer maximale Sicherheit:

- **Öffnen von Dateien** - Scannen, wenn eine Datei geöffnet wird.
- **Erstellen von Dateien** - Scannen, wenn Dateien erstelle oder geändert werden.
- **Ausführen von Dateien** - Scannen, wenn eine Datei ausgeführt oder gestartet wird.
- **Zugriff auf Wechselmedien-Bootsektor** - Wenn ein Wechselmedium mit Bootsektor an ein Gerät angeschlossen wird, wird der Bootsektor sofort gescannt. Diese Option aktiviert keine Scans für Dateien auf Wechselmedien. Scans für Dateien auf Wechselmedien können unter **Zu scannende Datenträger** > **Wechselmedien** aktiviert werden. Für den **Zugriff auf den Wechselmedien-Bootsektor** muss die Option **Bootsektoren/UEFI** in den ThreatSense-Parametern aktiviert sein.

Vom Scannen ausgeschlossene Prozesse - Weitere Informationen zu diesem Ausschlusstyp finden Sie im Kapitel Ausgeschlossene Prozesse.

Der Echtzeit-Dateischutz überwacht alle Datenträger auf das Eintreten bestimmter Ereignisse wie den Zugriff auf eine Datei. Durch die Verwendung der ThreatSense-Erkennungsmethoden (siehe Abschnitt Einstellungen für ThreatSense) kann der Echtzeit-Dateischutz so konfiguriert werden, dass neu erstellte und vorhandene Dateien unterschiedlich behandelt werden. Sie können den Echtzeit-Dateischutz z. B. so konfigurieren, dass neuere Dateien genauer überwacht werden.

Bereits geprüfte Dateien werden nicht erneut geprüft (sofern sie nicht geändert wurden), um die Systembelastung durch den Echtzeit-Dateischutz möglichst gering zu halten. Nach jedem Update der Erkennungsroutine werden die Dateien sofort erneut geprüft. Dieses Verhalten wird mit der **Smart-Optimierung** gesteuert. Wenn die **Smart-Optimierung** deaktiviert ist, werden alle Dateien bei jedem Zugriff gescannt. Um diese Einstellung zu ändern, öffnen Sie das Fenster mit den erweiterten Einstellungen durch Drücken der Taste **F5** und öffnen Sie anschließend **Erkennungsroutine** > **Echtzeit-Dateischutz**. Klicken Sie auf **ThreatSense-Einstellungen** > **Sonstige** und aktivieren bzw. deaktivieren Sie die Option **Smart-Optimierung aktivieren**.

Echtzeit-Dateischutz prüfen

Um sicherzustellen, dass der Echtzeit-Dateischutz aktiv ist und Viren erkennt, verwenden Sie eine Testdatei von eicar.com. Diese Testdatei ist harmlos und wird von allen Virenschutzprogrammen erkannt. Die Datei wurde von der Firma EICAR (European Institute for Computer Antivirus Research) erstellt, um die Funktionalität von Virenschutzprogrammen zu testen.

Die Datei kann unter http://www.eicar.org/download/eicar.com heruntergeladen werden.
Wenn Sie diese URL in Ihrem Browser eingeben, sollten Sie eine Nachricht erhalten, dass die Bedrohung entfernt wurde.

Wann sollten die Einstellungen für den Echtzeit-Dateischutz geändert werden?

Der Echtzeit-Systemschutz ist die wichtigste Komponente für ein sicheres System. Daher sollte gründlich geprüft werden, ob eine Änderung der Einstellungen wirklich notwendig ist. Es wird empfohlen, seine Parameter nur in einzelnen Fällen zu verändern.

Bei der Installation von ESET Endpoint Antivirus werden alle Einstellungen optimal eingerichtet, um dem Benutzer die größtmögliche Schutzstufe für das System zu bieten. Wenn Sie die Standardeinstellungen wiederherstellen möchten, klicken Sie neben den Registerkarten im Fenster (**Erweiterte Einstellungen** > **Erkennungsroutine** > **Echtzeit-Dateischutz**) auf .

Vorgehensweise bei fehlerhaftem Echtzeit-Dateischutz

In diesem Kapitel werden mögliche Probleme mit dem Echtzeit-Dateischutz sowie Lösungsstrategien beschrieben.

Echtzeit-Dateischutz ist deaktiviert

Der Echtzeit-Dateischutz wurde versehentlich von einem Benutzer deaktiviert und muss reaktiviert werden. Um den Echtzeit-Dateischutz erneut zu aktivieren, klicken Sie auf **Einstellungen** und dann auf den Bereich **Echtzeit-Dateischutz** im Hauptprogrammfenster.

Wenn der Echtzeit-Dateischutz beim Systemstart nicht gestartet wird, ist wahrscheinlich die Option **Echtzeit-Dateischutz automatisch starten** deaktiviert. Um diese Option zu aktivieren, klicken Sie unter **Erweiterte Einstellungen** (**F5**) auf **Erkennungsroutine** > **Echtzeit-Dateischutz** > **Einfach**. Achten Sie darauf, dass die Option **Echtzeit-Dateischutz automatisch starten** aktiviert ist.

Echtzeit-Dateischutz erkennt und entfernt keinen Schadcode

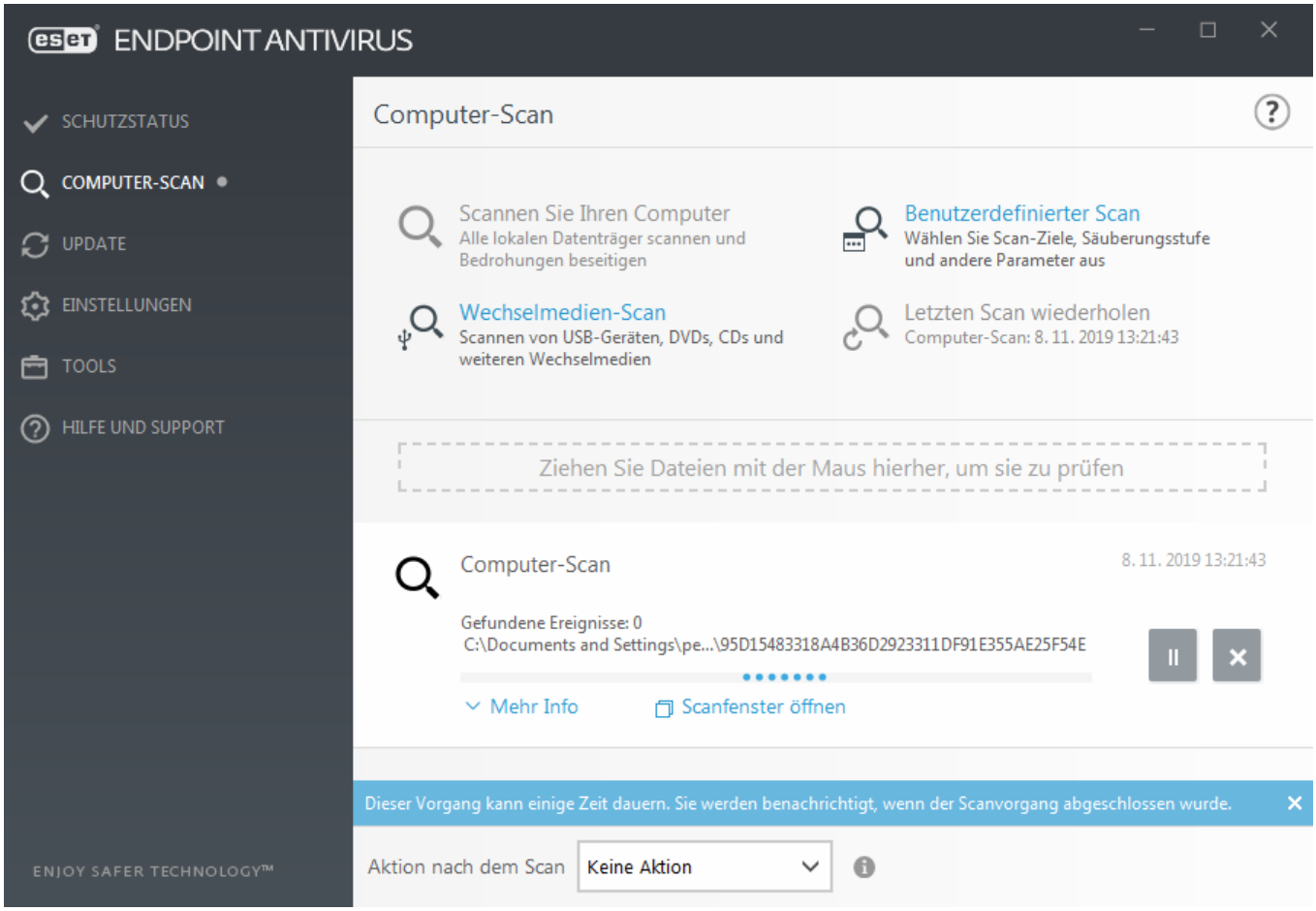
Stellen Sie sicher, dass keine anderen Virenschutzprogramme auf Ihrem Computer installiert sind. Zwei parallel ausgeführte Schutzprogramme können miteinander in Konflikt geraten. Wir empfehlen Ihnen, vor der Installation von ESET alle anderen Virusschutzprogramme zu deinstallieren.

Echtzeit-Dateischutz startet nicht

<Wenn der Echtzeit-Dateischutz beim Systemstart nicht initialisiert wird (und die Option **Echtzeit-Dateischutz aktivieren** aktiviert ist), kann dies an Konflikten mit anderen Programmen liegen. Sollte dies der Fall sein, wenden Sie sich an den ESET-Support.

Computer-Scan

Die manuelle Prüfung ist ein wichtiger Teil von ESET Endpoint Antivirus. Sie dient zur Prüfung von Dateien und Ordnern auf dem Computer. Aus Sicherheitsgründen ist es dringend erforderlich, dass Sie Ihren Computer nicht nur bei Infektionsverdacht prüfen, sondern diese Prüfung in die allgemeinen Sicherheitsroutinen integrieren. Es wird empfohlen, regelmäßig eine gründliche Prüfung des Computers vorzunehmen, um mögliche Viren zu entdecken, die nicht vom Echtzeit-Dateischutz erfasst wurden. Dies kommt z. B. vor, wenn der Echtzeit-Dateischutz zu diesem Zeitpunkt deaktiviert war, die Erkennungsroutine nicht auf dem neuesten Stand war oder die Datei nicht als Virus erkannt wurde, als sie auf dem Datenträger gespeichert wurde.



Sie haben zwei Arten von **Computer-Scans** zur Auswahl. Beim **Smart-Scan** wird das System schnell gescannt, ohne dass Sie weitere Scan-Parameter konfigurieren müssen. Beim **benutzerdefinierten Scan** können Sie ein vordefiniertes Scan-Profil und die Scan-Ziele auswählen.

Weitere Informationen zum Prüfprozess finden Sie im Abschnitt Stand der Prüfung.

Scannen Sie Ihren Computer

Mit der Smart-Prüfung können Sie den Computer schnell überprüfen und infizierte Dateien entfernen, ohne eingreifen zu müssen. Ihr Vorteil ist die einfache Bedienung, bei der Sie keine detaillierten Prüfeinstellungen festlegen müssen. Bei der Smart-Prüfung werden alle Dateien auf lokalen Laufwerken geprüft, und erkannte eingedrungene Schadsoftware wird automatisch entfernt. Als Säuberungsstufe wird automatisch der Standardwert festgelegt. Weitere Informationen zu den Säuberungstypen finden Sie unter Säubern.

Benutzerdefinierter Scan

Über die Option „Prüfen mit speziellen Einstellungen“ können Sie Prüfparameter wie die zu prüfenden Objekte oder Prüfmethoden angeben. Der Vorteil dieser Methode ist die Möglichkeit zur genauen Parameterkonfiguration. Verschiedene Konfigurationen können in benutzerdefinierten Prüfprofilen gespeichert werden. Das ist sinnvoll, wenn Prüfungen wiederholt mit denselben Parametern ausgeführt werden.

Mit der Option **Computer-Scan** > **Benutzerdefinierter Scan** können Sie **Zu prüfende Objekte** aus der Liste oder in der Baumstruktur auswählen. Sie können ein zu prüfendes Objekt auch bestimmen, indem Sie den Pfad zum Ordner oder zu den Dateien eingeben, die geprüft werden sollen. Wenn Sie nur das System ohne zusätzliche Säuberung prüfen möchten, wählen Sie die Option **Nur prüfen, keine Aktion**. Sie können bei der Prüfung zwischen drei Säuberungsebenen wählen. Klicken Sie hierfür auf **Einstellungen ...** > **ThreatSense-Parameter** >

Säuberung.

Eine Prüfung des Computers mit dieser Methode ist für fortgeschrittene Benutzer geeignet, die Erfahrung im Umgang mit Virenschutzprogrammen haben.

Mit der Funktion **Prüfen per Ziehen und Ablegen** können Sie Dateien und Ordner manuell prüfen. Klicken Sie dazu auf die Datei bzw. den Ordner, bewegen Sie den Mauszeiger bei gedrückter Maustaste über den markierten Bereich, und lassen Sie die Maustaste los. Anschließend wird die Anwendung in den Vordergrund verschoben.

Wechselmedien-Scan

Diese Prüfung ähnelt der Option „**Computerprüfung**“ und ermöglicht ein schnelles Prüfen der aktuell an den Computer angeschlossenen Wechselmedien (wie CD/DVD/USB). Dies ist hilfreich, wenn Sie beispielsweise ein USB-Speichergerät an den Computer anschließen und den Inhalt auf Schadcode und sonstige mögliche Bedrohungen untersuchen möchten.

Sie können diese Prüfung auch über **Benutzerdefinierter Scan** starten, indem Sie im Dropdown-Menü **Zu prüfende Objekte** den Eintrag **Wechselmedien** auswählen und auf **Scan** klicken.

Letzten Scan wiederholen

Mit dieser Option können Sie die zuletzt ausgeführte Prüfung mit denselben Parametern wiederholen.

Im Dropdownmenü **Aktion nach dem Scan** können Sie die Optionen **Keine Aktion**, **Herunterfahren** oder **Neu starten** auswählen. Die Verfügbarkeit der Aktionen **Energiesparmodus** und **Ruhezustand** hängt von Ihren Energieeinstellungen im Betriebssystem und vom Funktionsumfang Ihres Computers ab. Die ausgewählte Aktion wird gestartet, nachdem alle laufenden Scans abgeschlossen wurden. Wenn Sie **Herunterfahren** auswählen, wird ein 30-sekündiger Countdown in einem Bestätigungsdialog angezeigt und Sie können auf **Abbrechen** klicken, um das Herunterfahren abzubrechen. Weitere Details finden Sie unter Erweiterte Optionen für Scans.

> **Hinweis**
> Sie sollten Ihren Computer mindestens einmal im Monat scannen. Sie können diesen Scan als geplanten Task unter **Tools** > **Taskplaner** konfigurieren. So planen Sie einen wöchentlichen Computer-Scan

Benutzerdefinierte Prüfung

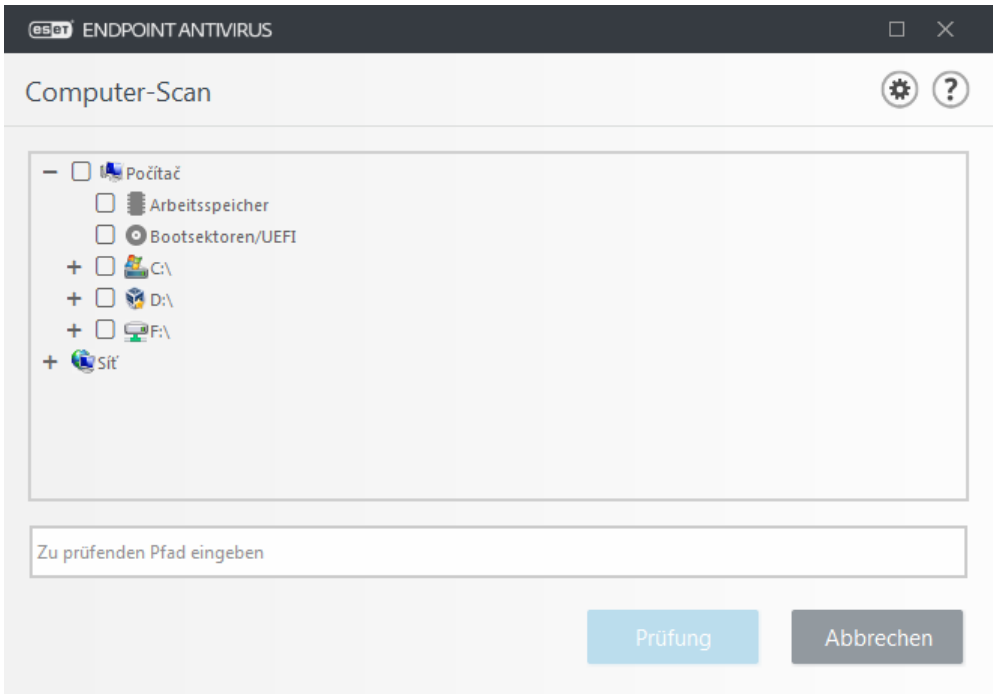
Wenn Sie nur bestimmte Objekte prüfen möchten, klicken Sie auf **Computer prüfen** > **Benutzerdefinierte Prüfung**. Wählen Sie die zu prüfenden Objekte aus dem Dropdown-Menü **Zu prüfende Objekte** oder in der Ordnerstruktur (Baumstruktur) aus.

Im Fenster mit den zu prüfenden Objekten können Sie definieren, welche Objekte (Arbeitsspeicher, Laufwerke, Dateien und Ordner) auf Schadcode geprüft werden. Wählen Sie die zu prüfenden Objekte aus der Baumstruktur aus, in der alle auf dem Computer verfügbaren Ordner aufgelistet werden. Im Dropdown-Menü **Zu prüfende Objekte** können Sie vordefinierte Optionen für die zu prüfenden Objekte auswählen.

- **Nach Profileinstellungen** - Wählt die im Prüfprofil ausgewählten Ziele aus.

- **Wechselmedien** - Wählt Disketten, USB-Speichergeräte, CDs/DVDs aus.
- **Lokale Laufwerke** - Alle lokalen Systemlaufwerke
- **Netzlaufwerke** - Alle zugeordneten Netzlaufwerke
- **Benutzerdefinierte Auswahl** - Mit dieser Option können Sie eine benutzerdefinierte Auswahl von Zielen erstellen.

Geben Sie das Zielverzeichnis in das leere Textfeld unter der Ordnerliste ein, um schnell zu einem Prüfziel zu navigieren oder um Ordner oder Dateien hinzuzufügen. Dies ist nur möglich, wenn keine Objekte aus der Baumstruktur zur Prüfung ausgewählt wurden und im Menü **Scan-Ziele** die Option **Keine Auswahl** festgelegt ist.



Infizierte Objekte werden nicht automatisch gesäubert. Mit einer Prüfung ohne Aktion können Sie den aktuellen Schutzstatus abrufen. Außerdem können Sie unter **Erweiterte Einstellungen** > **Erkennungsroutine** > **On-demand-Scan** > **ThreatSense-Einstellungen** > **Säuberung** zwischen drei Säuberungsstufen wählen. Wählen Sie **Nur scannen, keine Aktion aus**, um einen Scan ohne Säuberungsaktion durchzuführen. Der Scanfortschritt wird im Scan-Log gespeichert.

Mit der Option **Ausschlüsse ignorieren** werden Dateien mit den zuvor ausgeschlossenen Erweiterungen ohne Ausnahme geprüft.

Im Dropdown-Menü **Scan-Profil** können Sie ein Profil auswählen, um ausgewählte Objekte zu scannen. Das Standardprofil ist **Smart-Prüfung**. Es stehen außerdem zwei weitere vordefinierte Prüfprofile zur Verfügung: **Tiefen-Scan** und **Kontextmenü-Scan**. Diese Scan-Profile verwenden unterschiedliche ThreatSense-Einstellungen. Sie finden eine Beschreibung der verfügbaren Optionen unter **Erweiterte Einstellungen** > **Erkennungsroutine** > **Schadsoftware-Scans** > **On-demand-Scan** > ThreatSense-Einstellungen.

Klicken Sie auf **Prüfen**, um die Prüfung mit den von Ihnen festgelegten Parametern auszuführen.

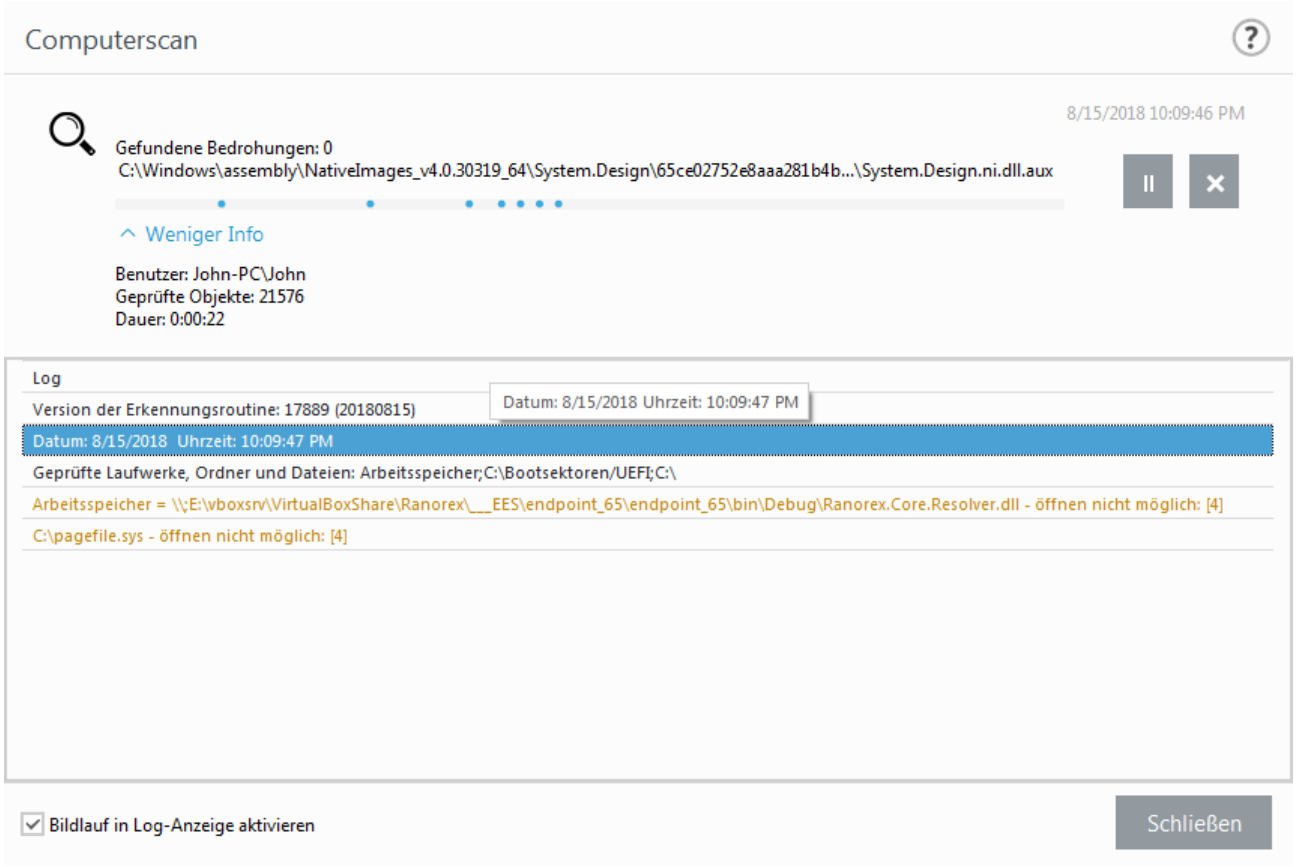
Mit der Schaltfläche Als Administrator prüfen können Sie die Prüfung mit dem Administratorkonto ausführen. Wählen Sie diese Option, wenn der aktuell angemeldete Benutzer keine ausreichenden Zugriffsrechte auf die zu prüfenden Dateien hat. Diese Schaltfläche ist nur verfügbar, wenn der aktuell angemeldete Benutzer UAC-

Vorgänge als Administrator aufrufen kann.

> **Hinweis**
> Klicken Sie auf **Logs anzeigen**.

Stand der Prüfung

Die Fortschrittsanzeige enthält den aktuellen Stand der Prüfung sowie die Anzahl der bisher gefundenen infizierten Dateien.



> **Hinweis**
> Es ist normal, dass u. a. passwortgeschützte Dateien oder Dateien, die ausschließlich vom System genutzt werden (in der Regel sind das *pagefile.sys* und bestimmte Log-Dateien), nicht geprüft werden können.

Stand der Prüfung - Die Fortschrittsanzeige zeigt den Status der bereits geprüften Objekte in Bezug auf die noch zu prüfenden Objekte an. Der Status des Scan-Fortschritts ergibt sich aus der Gesamtzahl der Objekte, die in den Scan einbezogen werden.

Zu prüfende Objekte - Der Name und Speicherort des aktuell geprüften Objekts werden angezeigt.

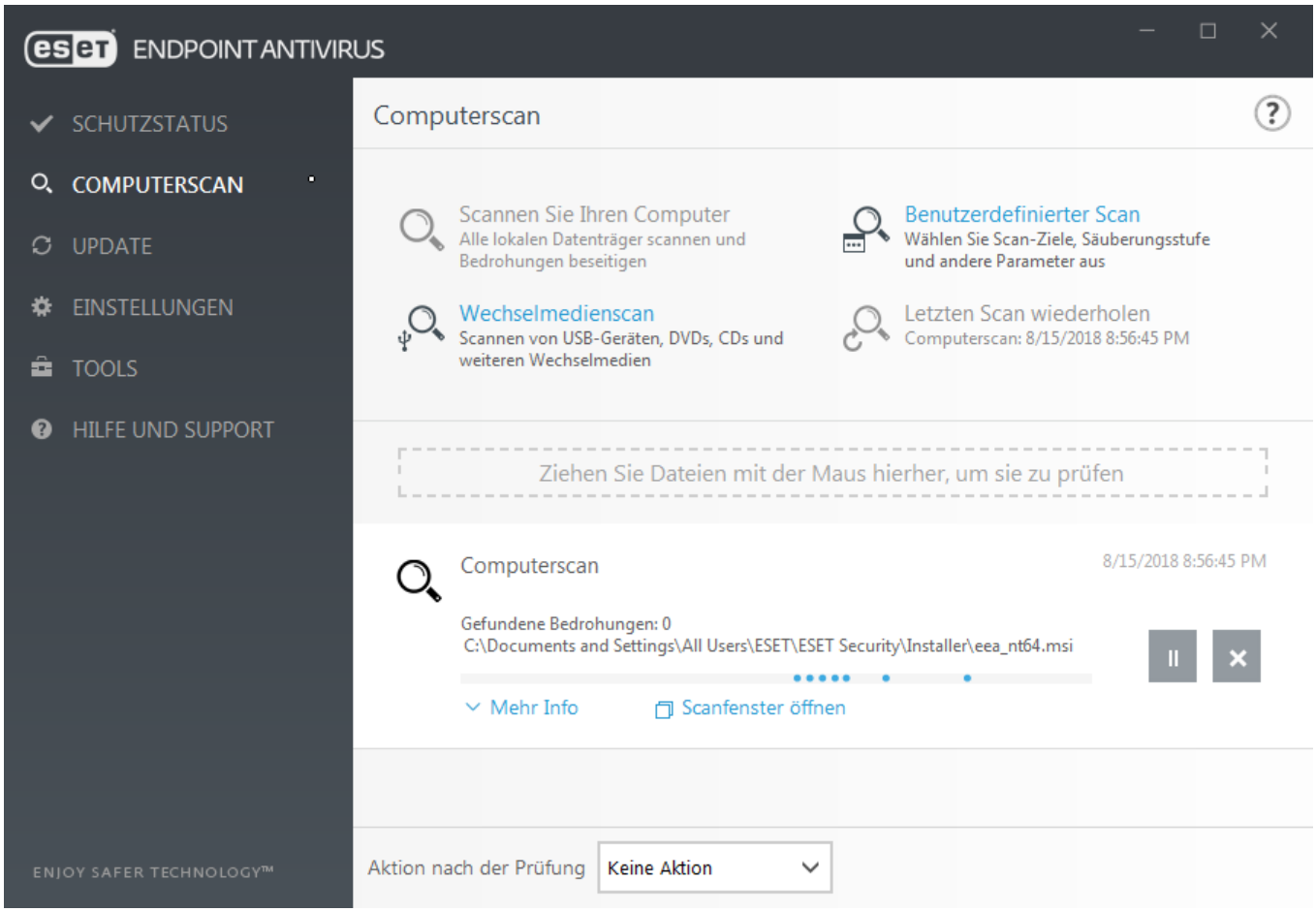
Bedrohungen erkannt - Die Gesamtzahl der Bedrohungen, die während einer Prüfung erkannt wurden, wird angezeigt.

Anhalten - Unterbrechen der Prüfung.

Fortsetzen - Diese Option ist wählbar, wenn die Prüfung angehalten wurde. Klicken Sie auf **Fortsetzen**, um mit der Prüfung fortzufahren.

Beenden - Beenden der Prüfung.

Bildlauf in Log-Anzeige aktivieren - Wenn diese Option aktiviert ist, fährt der Bildlauf automatisch nach unten, um die neuesten Einträge der sich verlängernden Liste anzuzeigen.



Computerprüfungs-Log

Das Computerprüfungs-Log enthält allgemeine Informationen zur Überprüfung, z. B.:

- Datum und Uhrzeit der Prüfung
- Geprüfte Laufwerke, Ordner und Dateien
- Anzahl geprüfter Objekte
- Anzahl erkannter Bedrohungen
- Abschlusszeit
- Prüfdauer

Malware-Scans

Der Bereich **Schadsoftware-Scans** befindet sich in den erweiterten Einstellungen. Drücken Sie die Taste **F5**, und klicken Sie auf **Erkennungsroutine** > **Schadsoftware-Scans**. In diesem Abschnitt können Sie die folgenden Optionen für die Scan-Parameter festlegen:

- **Ausgewähltes Profil** - Eine Gruppe von Parametern für den On-Demand-Scanner.
  Klicken Sie auf **Bearbeiten** neben **Profilliste**, um ein neues Profil zu erstellen. Weitere Details finden Sie unter Scan-Profile.
- **On-demand- & Machine-Learning-Schutz** - siehe Erkennungsroutine (7.2 und höher).
- **Scan-Ziele** - Falls Sie ein bestimmtes Ziel scannen möchten, klicken Sie auf **Bearbeiten** neben **Scan-Ziele** und wählen Sie eine Option im Dropdownmenü aus oder wählen Sie einzelne Ziele in der Ordnerstruktur aus. Weitere Details finden Sie unter Scan-Ziele.
- **ThreatSense-Parameter** - Dieser Bereich enthält erweiterte Einstellungen wie zu scannende Dateierweiterungen, verwendete Erkennungsmethoden usw. Hier finden Sie eine Registerkarte mit erweiterten Scan-Einstellungen.

Scan im Leerlaufbetrieb

Sie können das Scannen im Leerlaufbetrieb in den **erweiterten Einstellungen** unter **Erkennungsroutine** > **Schadsoftware-Scans** > **Scannen im Leerlaufbetrieb aktivieren.**

Scan im Leerlaufbetrieb

Stellen Sie den Schalter neben Scannen im Leerlaufbetrieb aktivieren auf **Ein**, um diese Funktion zu aktivieren. Wenn der Computer im Leerlauf ist, wird ein Computer-Scan für alle lokalen Laufwerke ausgeführt.

Diese Prüfung wird nur dann ausgeführt, wenn der Computer (Notebook) an die Netzversorgung angeschlossen ist. Sie können diese Einstellung überschreiben, indem Sie die Option neben **Auch ausführen, wenn der Computer im Akkubetrieb läuft** in den erweiterten Einstellungen aktivieren.

Aktivieren Sie **Erstellen von Logs aktivieren** in den erweiterten Einstellungen, um die Ausgabe einer Computerprüfung in den Log-Dateien abzulegen (Klicken Sie im Hauptprogrammfenster auf **Tools** > **Log-Dateien** und wählen Sie **Computer prüfen** im Dropdown-Menü **Log** aus).

Leerlauferkennung

Unter Auslöser für das Scannen im Leerlaufbetrieb finden Sie eine Liste der Bedingungen, die das Scannen im Leerlaufbetrieb auslösen.

Klicken Sie auf Einstellungen für ThreatSense, um die Einstellungen (z. B. die Erkennungsmethoden) für die Prüfung im Leerlaufbetrieb zu ändern.

Prüfprofile

Ihre bevorzugten Einstellungen können für zukünftige Prüfungen gespeichert werden. Wir empfehlen Ihnen, für jede regelmäßig durchgeführte Prüfung ein eigenes Profil zu erstellen (mit verschiedenen zu prüfenden Objekten, Prüfmethoden und anderen Parametern).

Um ein neues Profil zu erstellen, öffnen Sie die erweiterten Einstellungen (F5) und klicken auf **Erkennungsroutine** > **Schadsoftware-Prüfungen** > **On-Demand-Prüfung** > **Profilliste**. Im Fenster **Profil-Manager** finden Sie das Dropdownmenü **Ausgewähltes Profil** mit den vorhandenen Prüfprofilen und der Option zum Erstellen eines neuen Profils. Eine Beschreibung der einzelnen Prüfeinstellungen finden Sie im Abschnitt Einstellungen für ThreatSense. So können Sie ein Prüfprofil erstellen, das auf Ihre Anforderungen zugeschnitten ist.



Hinweis

Nehmen wir an, Sie möchten Ihr eigenes Prüfprofil erstellen. Die Option **Computerprüfung** eignet sich in gewissem Maße, aber Sie möchten keine laufzeitkkomprimierten Dateien oder potenziell unsichere Anwendungen prüfen. Außerdem möchten Sie die Option **Immer versuchen, automatisch zu entfernen** anwenden. Geben Sie den Namen des neuen Profils im **Profilmanager** ein und klicken Sie auf **Hinzufügen**. Wählen Sie das neue Profil im Dropdownmenü **Ausgewähltes Profil** aus, passen Sie die restlichen Parameter nach Ihren Anforderungen an und klicken Sie auf **OK**, um das neue Profil zu speichern.

Zu prüfende Objekte

Im Fenster mit den zu prüfenden Objekten können Sie definieren, welche Objekte (Arbeitsspeicher, Laufwerke, Dateien und Ordner) auf Schadcode geprüft werden. Wählen Sie die zu prüfenden Objekte aus der Baumstruktur aus, in der alle auf dem Computer verfügbaren Ordner aufgelistet werden. Im Dropdown-Menü **Zu prüfende Objekte** können Sie vordefinierte Optionen für die zu prüfenden Objekte auswählen.

- **Nach Profileinstellungen** - Wählt die im Prüfprofil ausgewählten Ziele aus.
- **Wechselmedien** - Wählt Disketten, USB-Speichergeräte, CDs/DVDs aus.
- **Lokale Laufwerke** - Alle lokalen Systemlaufwerke
- **Netzlaufwerke** - Alle zugeordneten Netzlaufwerke
- **Benutzerdefinierte Auswahl** - Mit dieser Option können Sie eine benutzerdefinierte Auswahl von Zielen erstellen.

Erweiterte Optionen für Scans

In diesem Fenster können Sie erweiterte Einstellungen für einen geplanten Task zur Prüfung des Computers festlegen. Im Dropdownmenü können Sie eine Aktion festlegen, die nach dem Abschließen des Scans automatisch ausgeführt wird.

- **Herunterfahren**- Der Computer wird nach dem Scan heruntergefahren.
- **Neustart**- Nach dem Scan werden alle offenen Programme geschlossen und der Computer wird neu

gestartet.

- **Energiesparmodus**- Der Computer wird in einen Energiesparmodus versetzt und Ihre Sitzung gespeichert, damit Sie Ihre Arbeit schnell wieder aufnehmen können.

- **Ruhezustand**- Alle im Arbeitsspeicher ausgeführten Aufgaben werden in eine besondere Datei auf der Festplatte verschoben. Der Computer wird heruntergefahren, kehrt jedoch beim nächsten Starten zum zuletzt aktiven Zustand zurück.

- **Keine Aktion** - Nach dem Scan wird keine Aktion ausgeführt.

> **Hinweis**
> Beachten Sie, dass der Computer im Energiesparmodus weiter arbeitet. Er führt weiterhin grundlegende Funktionen aus und verbraucht Strom. Um die Akkubetriebsdauer beispielsweise unterwegs zu verlängern, empfiehlt es sich, den Ruhezustand zu verwenden.

Wählen Sie**Aktion kann nicht vom Benutzer abgebrochen werden** aus, um zu verhindern, dass nicht berechtigte Benutzer Aktionen nach der Prüfung stoppen können.

Wählen Sie die Option **Benutzer darf die Prüfung anhalten (Minuten):** aus, wenn Sie zulassen möchten, dass der Benutzer den Computer-Scan für einen bestimmten Zeitraum anhalten kann.

Weitere Informationen finden Sie im Kapitel Scan-Fortschritt.

Medienkontrolle

ESET Endpoint Antivirus bietet Methoden zur automatischen Prüfung von Geräten (CD/DVD/USB/...). Mit diesem Modul können Sie Medien bzw. Geräte sperren oder erweiterte Filter- und Berechtigungseinstellungen anpassen und definieren, wie ein Benutzer auf diese Geräte zugreifen und mit ihnen arbeiten kann. Dies ist sinnvoll, wenn der Administrator verhindern möchte, dass Benutzer Geräte mit unerwünschten Inhalten verwenden.

Unterstützte externe Geräte:

- Datenträgerspeicher (Festplatten, USB-Wechselmedien)
- CD/DVD
- USB-Drucker
- FireWire-Speicher
- Bluetooth-Gerät
- Smartcard-Leser
- Bildverarbeitungsgerät
- Modem
- LPT/COM-Port

- Tragbares Gerät
- Alle Gerätetypen

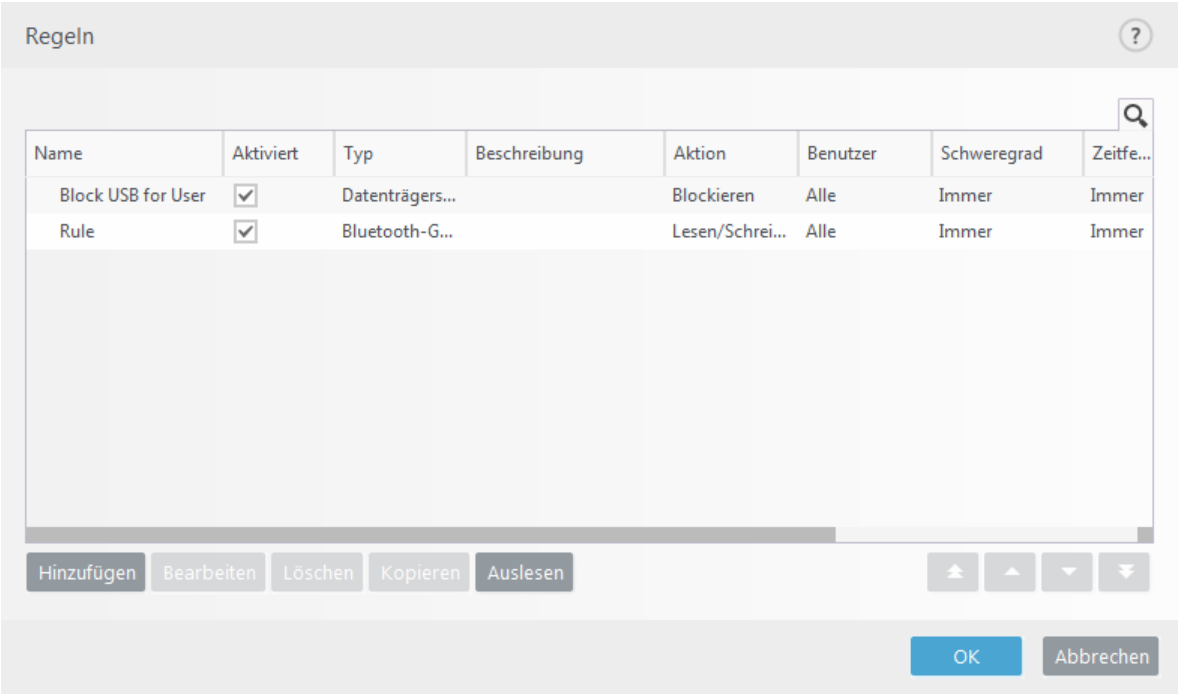
Die Einstellungen für die Medienkontrolle können unter **Erweiterte Einstellungen** (F5) > **Medienkontrolle** geändert werden.

Über das Kontrollkästchen **Systemintegration** aktivieren Sie die Funktion Medienkontrolle in ESET Endpoint Antivirus. Sie müssen Ihren Computer neu starten, um die Änderungen zu übernehmen. Wenn die Medienkontrolle aktiviert ist, wird die Option **Regeln** verfügbar, über die Sie das Fenster Regel-Editor öffnen können.

Wenn ein von einer bestehenden Regel blockiertes Gerät eingefügt wird, wird ein Hinweisfenster angezeigt und es wird kein Zugriff auf das Gerät gewährt.

Regel-Editor für die Medienkontrolle

Im Fenster **Regel-Editor für die Medienkontrolle** können Sie bestehende Regeln anzeigen und präzise Regeln für Geräte erstellen, die Benutzer an den Computer anschließen.



Bestimmte Gerätetypen können je nach Benutzer oder Benutzergruppen oder auf Grundlage weiterer, in der Regelkonfiguration festgelegter Parameter zugelassen oder gesperrt werden. Die Liste der Regeln enthält verschiedene Angaben wie Regelname, Art des externen Geräts, auszuführende Aktion beim Anschließen eines externen Geräts und Log-Schweregrad.

Klicken Sie zum Bearbeiten von Regeln auf **Hinzufügen** oder **Bearbeiten**. Deaktivieren Sie neben einer Regel das Kontrollkästchen **Aktiviert**, um die Regel zu deaktivieren, bis Sie sie später verwenden möchten. Wählen Sie eine oder mehrere Regeln aus und klicken Sie auf **Löschen**, um die Regel(n) dauerhaft zu löschen.

Kopieren– Erstellt eine neue Regel mit vordefinierten Optionen auf Grundlage der ausgewählten Regel.

Klicken Sie auf die Option **Auffüllen**, um automatisch die Parameter für am Computer angeschlossene

Wechselmedien zu übernehmen.

Die Regeln sind nach absteigender Priorität geordnet (Regeln mit höchster Priorität werden an oberster Stelle angezeigt). Sie können die Regeln durch Klicken auf  **Anfang/Aufwärts/Abwärts/Ende einzeln oder in Gruppen verschieben**.

Im Log der Medienkontrolle werden alle ausgelösten Vorkommnisse der Medienkontrolle aufgezeichnet. Um Log-Einträge anzuzeigen, klicken Sie im Hauptfenster von ESET Endpoint Antivirus auf **Tools** > Log-Dateien.

Erkannte Geräte

Die Schaltfläche **Auffüllen** bietet einen Überblick über alle aktuell angeschlossenen Geräte nebst Informationen zu Gerätetyp, Gerätehersteller, Modell und Seriennummer (sofern verfügbar).

Wenn Sie ein Gerät aus der Liste der erkannten Geräte auswählen und auf **OK** klicken, wird das Fenster für den Regel-Editor mit vordefinierten Informationen angezeigt (die Einstellungen können alle angepasst werden).

Gerätegruppen

Warnung
Ein Gerät, das an den Computer angeschlossen wird, kann ein Sicherheitsrisiko darstellen.

Das Fenster „Gerätegruppen“ ist in zwei Bereiche unterteilt. Im rechten Bereich des Fensters wird eine Liste der Geräte angezeigt, die in der betroffenen Gruppe enthalten sind. Links werden die erstellten Gruppen angezeigt. Wählen Sie eine Gruppe mit einer Liste von Geräten aus, die Sie rechts anzeigen möchten.

Wenn Sie das Gerätegruppenfenster öffnen und eine Gruppe auswählen, können Sie Geräte zur Liste hinzufügen oder aus der Liste entfernen. Sie können Geräte auch über eine Datei importieren, um sie zur Gruppe hinzuzufügen. Alternativ können Sie auf die Schaltfläche **Auffüllen** klicken. Alle an den Computer angeschlossenen Geräte werden im Fenster **Erkannte Geräte** angezeigt. Wählen Sie ein Gerät aus der aufgefüllten Liste aus und klicken Sie auf **OK**, um es zur Gruppe hinzuzufügen.

Steuerelemente

Hinzufügen– Je nachdem, in welchem Fensterbereich Sie auf diese Schaltfläche klicken, können Sie eine Gruppe durch Eingabe ihres Namens hinzufügen oder einer vorhandenen Gruppe ein Gerät hinzufügen (optional können Sie auch Details wie den Herstellernamen, das Modell und die Seriennummer eingeben).

Bearbeiten– Mit dieser Option können Sie die ausgewählte Gruppe oder die Geräteparameter (Hersteller, Modell, Seriennummer) ändern.

Löschen – Löscht die ausgewählte Gruppe bzw. das ausgewählte Gerät, je nachdem, in welchem Bereich des Fensters Sie auf die Schaltfläche klicken.

Importieren– Importiert eine Geräteliste aus einer Datei.

Die Schaltfläche **Auffüllen** bietet einen Überblick über alle aktuell angeschlossenen Geräte nebst Informationen zu Gerätetyp, Gerätehersteller, Modell und Seriennummer (sofern verfügbar).

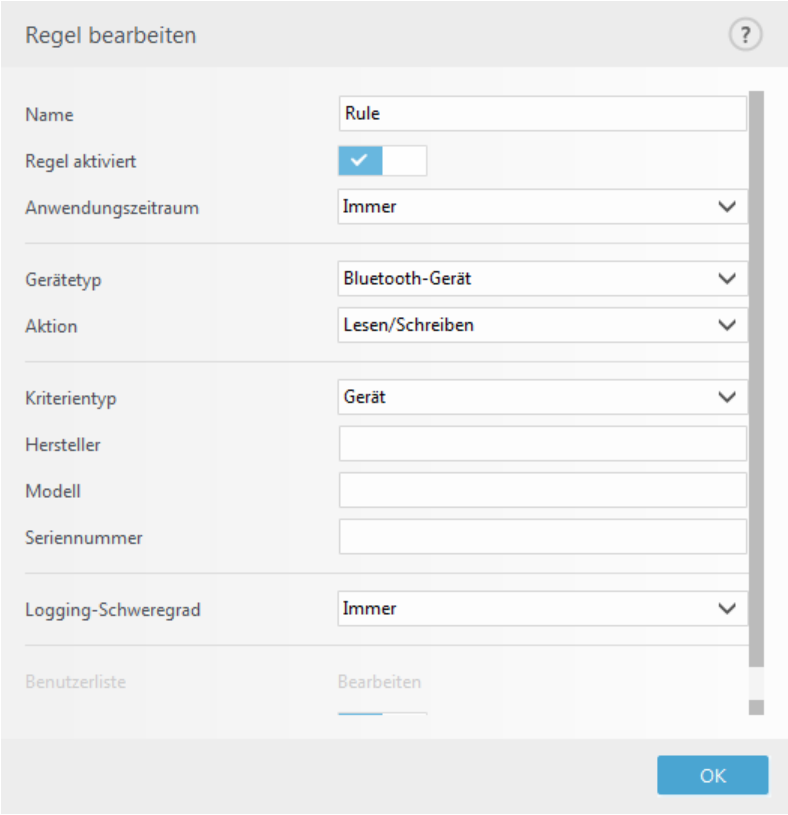
Klicken Sie auf **OK**, wenn Sie die Bearbeitung abgeschlossen haben. Klicken Sie auf **Abbrechen**, wenn Sie das Fenster **Gerätegruppen** schließen möchten, ohne die Änderungen zu speichern.

> **Beispiel**
> Sie können unterschiedliche Gerätegruppen für Geräte erstellen, auf die jeweils unterschiedliche Regeln angewendet werden sollen. Sie können auch nur eine einzige Gerätegruppe erstellen, auf die die Regel mit der Aktion **Lesen/Schreiben** oder **Schreibgeschützt** angewendet wird. So werden nicht erkannte Geräte durch die Medienkontrolle gesperrt, wenn sie an den Computer angeschlossen werden.

Beachten Sie, dass bestimmte Aktionen (Berechtigungen) nur für bestimmte Gerätetypen verfügbar sind. Bei einem Speichergerät sind alle vier Aktionen verfügbar. Bei anderen Geräten als Speichergeräten sind nur drei Aktionen verfügbar. (Die Aktion **Schreibgeschützt** ist beispielsweise für Bluetooth-Geräte nicht verfügbar. Bluetooth-Geräte können daher nur entweder gesperrt oder zugelassen werden oder eine Warnung auslösen.)

Hinzufügen von Regeln für die Medienkontrolle

Eine Regel für die Medienkontrolle definiert die Aktion, die ausgeführt wird, wenn ein Gerät, das die Regelkriterien erfüllt, an den Computer angeschlossen wird.



Geben Sie zur leichteren Identifizierung der Regel im Feld **Name** eine Beschreibung ein. Über den Schalter neben **Regel aktiviert** wird die Regel deaktiviert bzw. aktiviert. Dies ist beispielsweise nützlich, wenn Sie eine Regel deaktivieren, jedoch nicht dauerhaft löschen möchten.

Anwendungszeitraum – Wenden Sie die erstellte Regel während eines angegebenen Zeitraums an. Wählen Sie ein erstelltes Zeitfenster im Dropdownmenü aus. Weitere Informationen finden Sie hier.

Gerätetyp

Wählen Sie im Dropdown-Menü den Typ des externen Geräts aus (Datenträgerspeicher/tragbares Gerät/Bluetooth/FireWire/...). Die Gerätetypen werden vom Betriebssystem erfasst und können im Geräte-Manager angezeigt werden, sofern ein Gerät an den Computer angeschlossen ist. Speichergeräte umfassen externe Datenträger oder herkömmliche Kartenlesegeräte, die über den USB- oder FireWire-Anschluss an den Computer angeschlossen sind. Smartcard-Lesegeräte umfassen Kartenlesegeräte für Smartcards mit eingebettetem integriertem Schaltkreis, beispielsweise SIM-Karten oder Authentifizierungskarten. Bildverarbeitungsgeräte sind beispielsweise Scanner oder Kameras. Diese Geräte stellen nur Informationen zu den eigenen Aktionen bereit, keine Benutzerinformationen. Daher können diese Geräte nur global blockiert werden.

> **Hinweis**
> Die Benutzerlistenfunktion ist für den Modem-Gerätetyp nicht verfügbar. Diese Regel wird für alle Benutzer übernommen und die aktuelle Benutzerliste wird gelöscht.

Aktion

Der Zugriff auf andere Geräte als Speichergeräte kann entweder zugelassen oder gesperrt werden. Im Gegensatz dazu ist es für Speichergeräte möglich, eines der folgenden Rechte für die Regel auszuwählen:

- **Lese-/Schreibzugriff**– Der vollständige Zugriff auf das Gerät wird zugelassen.
- **Sperren**– Der Zugriff auf das Gerät wird gesperrt.
- **Nur Lesezugriff**– Nur Lesezugriff auf das Gerät wird zugelassen.
- **Warnen**– Jedes Mal, wenn ein Gerät angeschlossen wird, erhält der Benutzer eine Benachrichtigung, die angibt, ob das Gerät zugelassen oder gesperrt ist. Außerdem wird ein Log-Eintrag erstellt. Die Geräteinformationen werden nicht gespeichert, d. h. bei einem erneuten, späteren Anschluss des gleichen Geräts wird die Benachrichtigung erneut angezeigt.

Beachten Sie, dass bestimmte Aktionen (Berechtigungen) nur für bestimmte Gerätetypen verfügbar sind. Bei einem Speichergerät sind alle vier Aktionen verfügbar. Bei anderen Geräten als Speichergeräten sind nur drei Aktionen verfügbar. (Die Aktion **Schreibgeschützt** ist beispielsweise für Bluetooth-Geräte nicht verfügbar. Bluetooth-Geräte können daher nur entweder gesperrt oder zugelassen werden oder eine Warnung auslösen.)

Kriterientyp – Wählen Sie Gerätegruppe oder Gerät aus.

Weitere Parameter zur Feinanpassung der Regeln und Anpassung an bestimmte Geräte. (die Groß-/Kleinschreibung muss nicht beachtet werden):

- **Hersteller**– Filtern Sie die Liste nach Herstellername oder -ID.
- **Modell**– Die Bezeichnung des Geräts.
- **Seriennummer**– Externe Geräte verfügen üblicherweise über eigene Seriennummern. Bei CDs/DVDs bezieht sich die Seriennummer auf das Exemplar, nicht auf das Laufwerk.

> **Hinweis**
> Wenn diese Parameter nicht definiert werden, ignoriert die Regel dieser Felder bei der Abstimmung. Bei Filterparametern mit Textfeldern braucht die Groß-/Kleinschreibung nicht beachtet zu werden. Platzhalter (*, ?) werden nicht unterstützt.

Hinweis
Um Informationen zu einem Gerät anzuzeigen, erstellen Sie eine Regel für den entsprechenden Gerätetyp, schließen Sie das Gerät an den Computer an und überprüfen Sie dann die Gerätedetails im Medienkontrolle-Log.

Logging-Schweregrad

- **Immer**– Alle Ereignisse werden protokolliert.
- **Diagnose**– Informationen, die für die Feineinstellung des Programms benötigt werden, werden protokolliert.
- **Informationen**– Meldungen wie erfolgreiche Updates und alle Meldungen höherer Stufen werden protokolliert.
- **Warnungen**– Erfasst kritische Fehler und Warnungen und sendet sie an den ERA Server.
- **Keine** – Es werden keine Logs aufgezeichnet.

Die Regeln können auf bestimmte Benutzer oder Benutzergruppen beschränkt werden, indem Sie diese zur **Benutzerliste** hinzufügen:

- **Hinzufügen**– Öffnet das Dialogfenster **Objekttypen: Benutzer oder Gruppen**, in dem Sie bestimmte Benutzer auswählen können.
- **Entfernen** – Entfernt den ausgewählten Benutzer aus dem Filter.

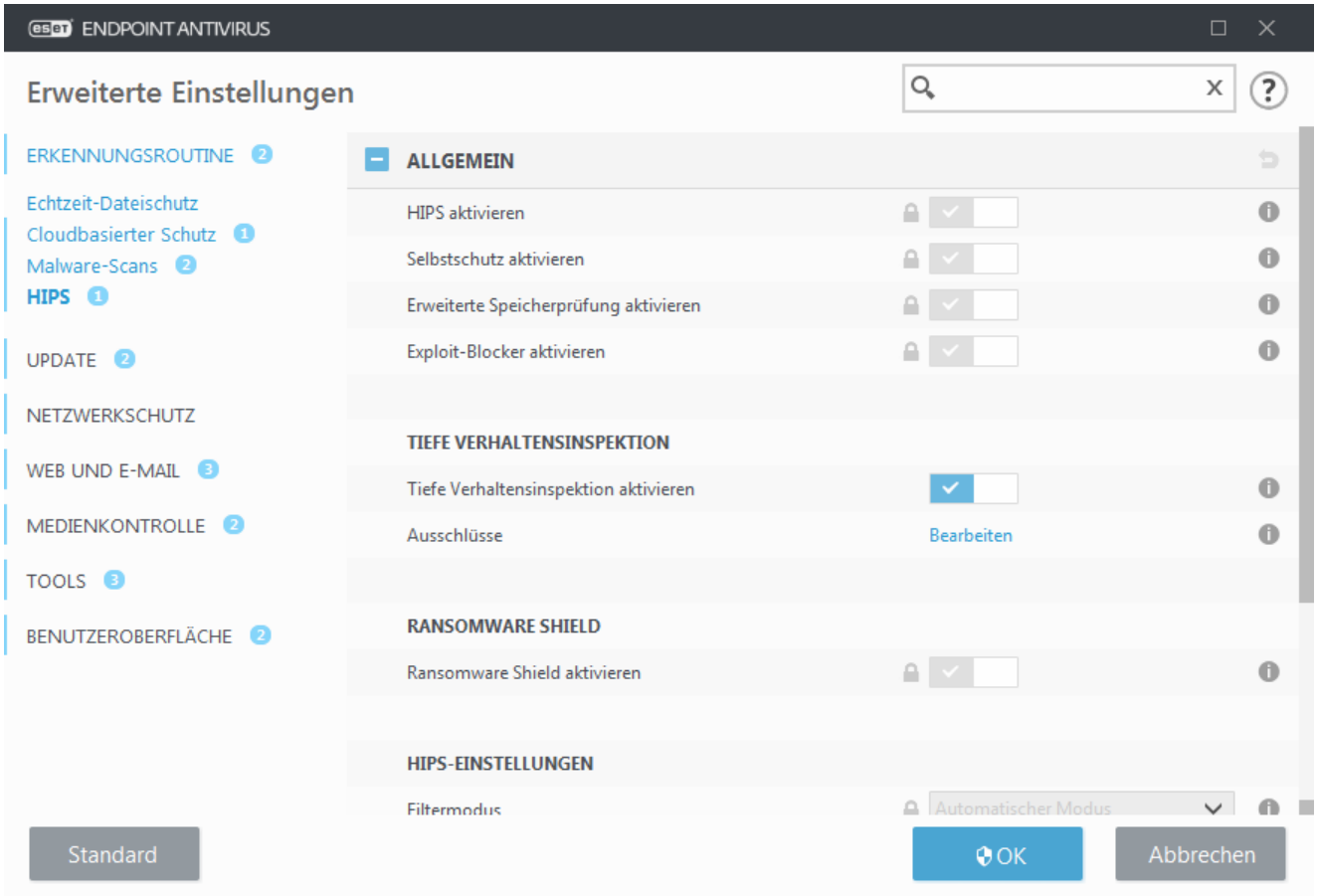
Hinweis
Nicht alle Geräte können über Benutzerregeln eingeschränkt werden (Bildverarbeitungsgeräte liefern beispielsweise keine Informationen über Benutzer, sondern nur über ausgeführte Aktionen).

Host-based Intrusion Prevention System (HIPS)

Warnung
Nur erfahrene Benutzer sollten die Einstellungen von HIPS ändern. Eine falsche Konfiguration der HIPS-Einstellungen kann eine Instabilität des Systems verursachen.

DasHost Intrusion Prevention System (HIPS) schützt Ihr System vor Schadsoftware und unerwünschten Programmaktivitäten, die negative Auswirkungen auf Ihren Computer haben könnten. HIPS analysiert das Verhalten von Programmen genau und nutzt Netzwerkfilter zur Überwachung von laufenden Prozessen, Dateien und Registrierungsschlüsseln. HIPS stellt eine zusätzliche Funktion zum Echtzeit-Dateischutz dar und ist keine Firewall, da nur die im Betriebssystem ausgeführten Prozesse überwacht werden.

Die HIPS-Einstellungen finden Sie unter **Erweiterte Einstellungen** (F5) > **Erkennungsroutine** > **HIPS** > **Einfach**. Der HIPS-Status (aktiviert/deaktiviert) wird im Hauptprogrammfenster von ESET Endpoint Antivirus unter **Einstellungen** > **Computer** angezeigt.



Einfach

HIPS aktivieren - HIPS ist in ESET Endpoint Antivirus standardmäßig aktiviert. Wenn Sie HIPS deaktivieren, werden auch die anderen HIPS-Funktionen wie etwa der Exploit-Blocker deaktiviert.

Selbstschutz aktivieren - ESET Endpoint Antivirus verwendet die in HIPS integrierte **Selbstschutztechnologie**, um Ihren Viren- und Spyware-Schutz vor Beschädigung und Deaktivierung durch Schadsoftware zu schützen. Diese Technologie schützt wichtige System- und ESET-Prozesse sowie Registrierungsschlüssel und Dateien vor Manipulation. Wenn der ESET Management Agent installiert ist, wird dieser ebenfalls geschützt.

Protected Service aktivieren - Aktiviert den Schutz für den ESET-Dienst (ekrn.exe). Wenn Sie diese Option aktivieren, wird der Dienst als geschützter Windows-Prozess gestartet, um ihn vor Malware-Angriffen zu schützen. Diese Option ist in Windows 8.1 und Windows 10 verfügbar.

Erweiterten Speicher-Scanner aktivieren- Diese Funktion bietet im Zusammenspiel mit dem Exploit-Blocker einen besseren Schutz vor Malware, die versucht, der Erkennung durch Anti-Malware-Produkte mittels Verschleierung oder Verschlüsselung zu entgehen. Der erweiterte Speicher-Scanner ist standardmäßig aktiviert. Weitere Informationen zu diesem Schutztyp finden Sie in unserem Glossar.

Exploit-Blocker aktivieren - Dieses Modul sichert besonders anfällige Anwendungstypen wie Webbrowser, PDF-Leseprogramme, E-Mail-Programme und MS Office-Komponenten ab. Der Exploit-Blocker ist standardmäßig aktiviert. Weitere Informationen zu diesem Schutztyp finden Sie in unserem Glossar.

Tiefe Verhaltensinspektion

Tiefe Verhaltensinspektion aktivieren - Dieses Modul bietet eine weitere Schutzebene im Rahmen der HIPS-Funktion. Diese HIPS-Erweiterung analysiert das Verhalten aller auf dem Computer ausgeführten Programme und

warnt Sie, falls sich ein Prozess bösartig verhält.

Mit den HIPS-Ausschlüssen für die tiefe Verhaltensinspektion können Sie festlegen, welche Prozesse von der Analyse ausgenommen werden sollen. Um zu gewährleisten, dass alle Prozesse auf Bedrohungen gescannt werden, sollten Sie Ausnahmen nur in dringenden Fällen erstellen.

Ransomware-Schutz

Ransomware-Schutz aktivieren - Dieses Modul ist eine weitere Schutzebene im Rahmen der HIPS-Funktion. Sie müssen das ESET LiveGrid®-Reputationssystem aktivieren, um den Ransomware-Schutz verwenden zu können. Weitere Informationen zu diesem Schutztyp finden Sie hier.

Audit-Modus aktivieren - Die vom Ransomware Shield gefundenen Ereignisse werden nicht automatisch blockiert, sondern mit dem Schweregrad „Warnung“ geloggt und mit dem Flag „AUDIT-MODUS“ an die Verwaltungskonsole übertragen. Ein Administrator kann anschließend entscheiden, ob das Ereignis ausgeschlossen werden soll, um weitere Erkennungen zu vermeiden, oder ob das Ereignis aktiv bleiben soll, um es nach Ende des Audit-Modus zu blockieren und zu entfernen. Die Aktivierung/Deaktivierung des Audit-Modus wird auch in ESET Endpoint Antivirus geloggt. Diese Option ist nur in ESMC oder im Policy-Konfigurations-Editor in ESET PROTECT Cloud verfügbar.

HIPS-Einstellungen

Für den **Filtermodus** haben Sie die folgenden Optionen zur Auswahl:

Filtermodus	Beschreibung
Automatischer Modus	Vorgänge werden ausgeführt, mit Ausnahme der Vorgänge, die durch vorab definierte Regeln zum Schutz Ihres Systems blockiert wurden.
Smart-Modus	Der Benutzer wird nur über sehr verdächtige Ereignisse benachrichtigt.
Interaktiver Modus	Der Benutzer wird zur Bestätigung von Vorgängen aufgefordert.
Regelbasierter Modus	Blockiert alle Vorgänge, die nicht explizit durch eine Regel erlaubt sind.
Trainingsmodus	Vorgänge werden ausgeführt und nach jedem Vorgang wird eine Regel erstellt. Die in diesem Modus erstellten Regeln können im Editor für **HIPS-Regeln** angezeigt werden, haben jedoch eine geringere Priorität als manuell erstellte Regeln oder Regeln, die im automatischen Modus erstellt wurden. Wenn Sie die Option **Trainingsmodus** im Dropdownmenü **Filtermodus** auswählen, wird die Einstellung **Ende des Trainings Modus**verfügbar. Wählen Sie eine Zeitdauer für den Trainingsmodus aus. Die maximale Dauer beträgt 14 Tage. Wenn die festgelegte Dauer verstrichen ist, werden Sie aufgefordert, die von HIPS im Trainingsmodus erstellten Regeln zu bearbeiten. Sie können auch einen anderen Filtermodus auswählen oder die Entscheidung verschieben und den Trainingsmodus weiterverwenden.

Zu verwendender Modus nach Ablauf des Trainingsmodus - Wählen Sie aus, welcher Filtermodus nach Ablauf des Trainingsmodus verwendet werden soll. Nach Ablauf des Modus sind für die Option **Benutzer fragen** Administratorrechte erforderlich, um Änderungen am HIPS-Filtermodus vorzunehmen.

HIPS überwacht Ereignisse auf Betriebssystemebene und führt Aktionen gemäß Regeln aus, die den Regeln für die Firewall ähneln. Klicken Sie auf **Bearbeiten** neben **Regeln**, um die den Editor für **HIPS-Regeln** zu öffnen. Im Fenster „HIPS-Regeln“ können Sie Regeln auswählen, hinzufügen, bearbeiten oder entfernen. Weitere Informationen zur Erstellung von Regeln und zu HIPS-Operationen finden Sie unter HIPS-Regel bearbeiten.

HIPS-Interaktionsfenster

Im HIPS-Benachrichtigungsfenster können Sie Regeln für die von HIPS erkannten Aktionen erstellen und Bedingungen festlegen, unter denen diese Aktion zugelassen oder blockiert wird.

Die im Benachrichtigungsfenster erstellten Regeln sind gleichwertig mit den manuell erstellten Regeln. Die im Benachrichtigungsfenster erstellten Regeln können allgemeiner sein als die Regel, die das Dialogfenster ausgelöst hat. Wenn Sie also eine Regel im Dialogfeld erstellen, kann es passieren, dass diese Operation dasselbe Fenster auslöst. Weitere Informationen finden Sie unter Priorität für HIPS-Regeln.

Wenn für eine Regel die Standardaktion **Jedes Mal fragen** festgelegt ist, wird bei jedem Auslösen der Regel ein Dialogfeld angezeigt. Dort können Sie den Vorgang entweder **Blockieren** oder **Zulassen**. Wenn Sie innerhalb des vorgegebenen Zeitrahmens keine Aktion auswählen, wird gemäß der Regeln eine neue Aktion ausgewählt.

Mit der Option Bis zum Beenden der Anwendung merken wird die Aktion (**Zulassen/Blockieren**) so lange angewendet, bis die Regeln oder der Filtermodus geändert werden, ein Update des HIPS-Moduls ausgeführt wird oder das System neu gestartet wird. Wenn eine dieser drei Aktionen (Regel- oder Filtermodusänderung, Update des HIPS-Moduls oder Neustart des Systems) ausgeführt wird, wird die vorübergehende Regel gelöscht.

Wenn Sie die Option **Regel erstellen und dauerhaft merken** auswählen, wird eine neue HIPS-Regel erstellt, die Sie später im Abschnitt HIPS-HIPS-Regelverwaltung bearbeiten können (Administratorberechtigungen erforderlich).

Klicken Sie auf unten auf **Details**, um herauszufinden, welche Anwendung den Vorgang ausgelöst hat, welche Reputation die Datei hat oder welche Art von Vorgang Sie zulassen oder blockieren können.

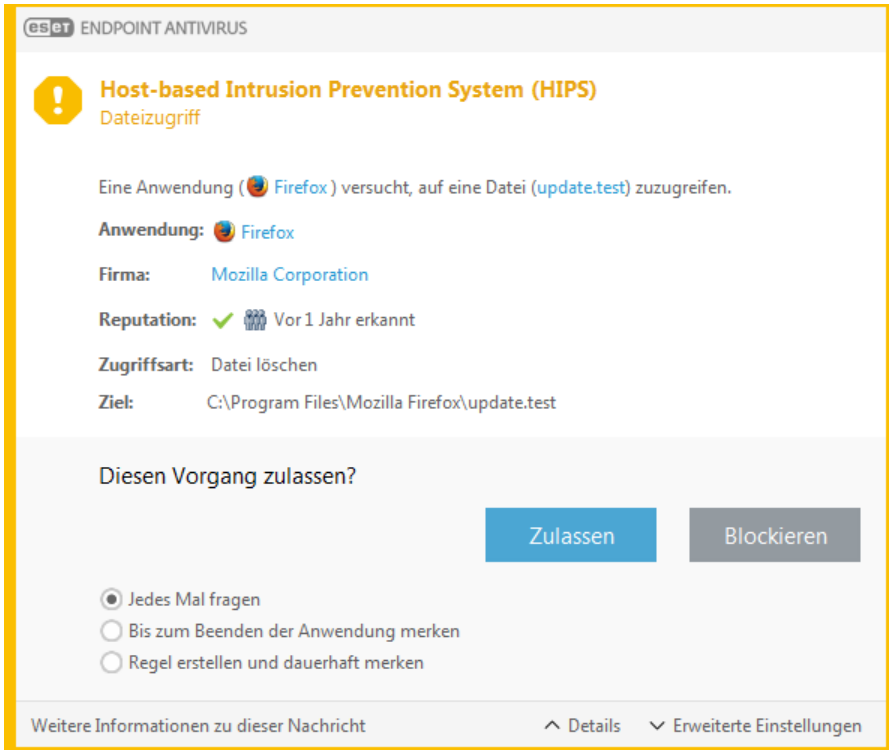
Klicken Sie auf **Erweiterte Optionen**, um die Einstellungen für ausführlichere Regelparameter zu öffnen. Wenn Sie **Regel erstellen und dauerhaft merken** auswählen, haben Sie die folgenden Optionen zur Auswahl:

- **Regel ausschließlich für diese Anwendung erstellen** - Wenn Sie dieses Kontrollkästchen deaktivieren, wird die Regel für alle Quellanwendungen erstellt.
- **Nur für Operation** - Wählen Sie Datei-, Anwendungs- oder Registrierungsoperationen für diese Regel aus. Hier finden Sie eine Beschreibung sämtlicher HIPS-Operationen.
- **Nur für Ziel** - Wählen Sie Datei-, Anwendungs- oder Registrierungsziele für diese Regel aus.



Erhalten Sie zu viele HIPS-Meldungen?

Um die Benachrichtigungen zu deaktivieren, ändern Sie den Filtermodus unter **Erweiterte Einstellungen** (F5) > **Erkennungsroutine** > **HIPS** > **Einfach** zu **Automatischer Modus**.



Mögliches Ransomware-Verhalten erkannt

Dieses interaktive Fenster wird angezeigt, wenn ein potenzielles Ransomware-Verhalten erkannt wird. Dort können Sie den Vorgang entweder **Verweigern** oder **Zulassen**.

Klicken Sie auf **Details, um weitere Erkennungsparameter anzuzeigen.** Im Dialogfeld haben Sie die Optionen **Zur Analyse einreichen** und **Von der Erkennung ausschließen** zur Auswahl.

Wichtig
Für den ordnungsgemäßen Betrieb des Ransomware-Schutzes muss ESET LiveGrid® aktiviert sein.

HIPS-Regelverwaltung

Hier finden Sie eine Liste der von Benutzern erstellten und automatisch hinzugefügten Regeln im HIPS-System. Weitere Details zur Regelerstellung und zu HIPS-Operationen finden Sie im Kapitel Einstellungen für HIPS-Regeln. Siehe auch Funktionsprinzip von HIPS.

Spalten

Regel - Benutzerdefinierter oder automatisch ausgewählter Regelname.

Aktiviert - Deaktivieren Sie diesen Schalter, wenn Sie die Regel nicht verwenden, jedoch nicht aus der Liste löschen möchten.

Aktion - Die Regel definiert eine Aktion (**Zulassen**, **Blockieren** oder **Fragen**), die ausgeführt wird, wenn die Bedingungen erfüllt sind.

Quellen - Die Regel wird nur angewendet, wenn das Ereignis von einer Anwendung ausgelöst wird.

Ziele - Die Regel wird nur angewendet, wenn sich die Operation auf eine bestimmte Datei, eine Anwendung oder einen Registrierungseintrag bezieht.

Log - Wenn Sie diese Option aktivieren, werden Informationen zu dieser Regel im HIPS-Log gespeichert.

Benachrichtigen - In der rechten unteren Ecke wird eine kleine Benachrichtigung angezeigt, wenn ein Ereignis ausgelöst wird.

Steuerelemente

Hinzufügen– Erstellt eine neue Regel.

Bearbeiten - Ausgewählten Eintrag bearbeiten

Löschen – Ausgewählte Einträge entfernen.

Priorität für HIPS-Regeln

Die Priorität der HIPS-Regeln kann nicht mit den Schaltflächen Oben/Unten angepasst werdenwird.

- Alle erstellten Regeln haben dieselbe Priorität
- Je spezifischer eine Regel, desto höher ihre Priorität (eine Regel für eine bestimmte Anwendung hat beispielsweise eine höhere Priorität als eine Regel für alle Anwendungen)
- HIPS enthält einige interne Regeln, auf die Sie keinen Zugriff haben (Sie können die vordefinierten Selbstschutzregeln beispielsweise nicht überschreiben)
- Regeln, die möglicherweise dazu führen, dass Ihr Betriebssystem einfriert, werden nicht ausgeführt (erhalten die niedrigste Priorität)

HIPS-Regeleinstellungen

Lesen Sie zunächst das Kapitel HIPS-Regelverwaltung.

Regelname - Benutzerdefinierter oder automatisch ausgewählter Regelname.

Aktion - Legt eine Aktion fest (**Zulassen**, **Sperren** oder **Fragen**), die bei Eintreten der Bedingungen ausgeführt wird.

Vorgänge in Bezug auf - Wählen Sie die Art des Vorgangs aus, auf den die Regel angewendet werden soll. Die Regel wird nur bei dieser Art Vorgang und für das ausgewählte Ziel angewendet.

Aktiviert - Deaktivieren Sie diesen Schalter, wenn Sie die Regel beibehalten, jedoch derzeit nicht anwenden möchten.

Log - Wenn Sie diese Option aktivieren, werden Informationen zu dieser Regel im HIPS-Log gespeichert.

Benutzer benachrichtigen - In der rechten unteren Ecke wird ein Popup-Fenster angezeigt, wenn ein Ereignis ausgelöst wird.

Die Regel besteht aus mehreren Teilen, mit denen die Auslösebedingungen der Regel beschrieben werden:

Quellanwendungen -Die Regel wird nur angewendet, wenn das Ereignis von dieser/diesen Anwendung(en) ausgelöst wird. Wählen Sie **Bestimmte Anwendungen** aus dem Dropdownmenü aus und klicken Sie auf **Hinzufügen**, um neue Dateien oder Ordner hinzuzufügen, oder wählen Sie **Alle Anwendungen** aus, um alle Anwendungen hinzuzufügen.

Dateien - Die Regel wird nur angewendet, wenn sich der Vorgang auf eines dieser Ziele bezieht. Wählen Sie **Bestimmte Dateien** aus dem Dropdownmenü aus und klicken Sie auf **Hinzufügen**, um neue Dateien oder Ordner hinzuzufügen. Sie können auch den Eintrag **Alle Dateien** aus dem Dropdownmenü auswählen, um alle Dateien hinzuzufügen.

Anwendungen - Die Regel wird nur angewendet, wenn sich der Vorgang auf eines dieser Ziele bezieht. Wählen Sie **Bestimmte Anwendungen** aus dem Dropdownmenü aus und klicken Sie auf **Hinzufügen**, um neue Dateien oder Ordner hinzuzufügen. Sie können auch den Eintrag **Alle Anwendungen** aus dem Dropdownmenü auswählen, um alle Anwendungen hinzuzufügen.

Registrierungseinträge - Die Regel wird nur angewendet, wenn sich der Vorgang auf eines dieser Ziele bezieht. Wählen Sie **Bestimmte Einträge** aus dem Dropdownmenü aus und klicken Sie auf **Hinzufügen**, um neue Dateien oder Ordner hinzuzufügen. Sie können auch den Eintrag **Alle Einträge** aus dem Dropdownmenü auswählen, um alle Anwendungen hinzuzufügen.



Hinweis

Bestimmte, von HIPS vordefinierte Regeln und die aus ihnen resultierenden Vorgänge können nicht blockiert werden, da sie standardmäßig zugelassen sind. Hinzu kommt, dass nicht alle Systemvorgänge von HIPS überwacht werden. HIPS überwacht Vorgänge, die als unsicher eingestuft werden könnten.

Beschreibungen der wichtigsten Vorgänge:

Dateibezogene Vorgänge

- **Datei löschen** - Anwendung versucht, die Zieldatei zu löschen.
- **In Datei schreiben** - Anwendung versucht, in die Zieldatei zu schreiben.
- **Direkter Zugriff auf Datenträger** - Die Anwendung versucht, einen Datenträger auf nicht standardmäßige Art auszulesen oder zu beschreiben (die üblichen Windows-Verfahren werden umgangen). So könnten Dateien verändert werden, ohne dass die entsprechenden Regeln in Kraft treten. Verursacher dieses Vorgangs könnte Malware sein, die versucht, ihre Erkennung zu verhindern. Es könnte sich aber auch um Backup-Software handeln, die versucht, die genaue Kopie eines Datenträgers herzustellen, oder eine Partitionsverwaltung beim Versuch, Festplattenvolumes zu reorganisieren.
- **Globalen Hook installieren** - Bezieht sich auf das Aufrufen der Funktion SetWindowsHookEx aus der MSDN-Bibliothek.
- **Treiber laden** - Laden und Installieren von Treibern im System.

Anwendungsbezogene Vorgänge

- **Andere Anwendung debuggen** - Verknüpfen eines Debuggers mit dem Prozess. Beim Debuggen einer Anwendung können Informationen zu deren Verhalten angezeigt und verändert werden. Ebenso ist der Zugriff auf die Daten der Anwendung möglich.
- **Ereignisse von anderer Anwendung abfangen** - Die Quellanwendung versucht, für die Zielanwendung

bestimmte Ereignisse abzufangen (Beispiel: ein Keylogger versucht, Ereignisse im Browser aufzuzeichnen).

- **Andere Anwendung beenden/unterbrechen** - Die Anwendung unterbricht einen Prozess bzw. setzt ihn fort oder beendet ihn (direkter Zugriff aus dem Process Explorer oder im Bereich „Prozesse“ möglich).
- **Neue Anwendung starten** - Starten neuer Anwendungen oder Prozesse
- **Zustand anderer Anwendung ändern**- Die Quellanwendung versucht, in den Speicher der Zielanwendung zu schreiben oder in ihrem Namen bestimmten Code auszuführen. Diese Funktion ist geeignet, um wichtige Anwendungen zu schützen. Fügen Sie die zu schützende Anwendung hierzu als Zielanwendung zu einer Regel hinzu, die diese Art Vorgang (Ändern des Zustands einer anderen Anwendung) blockiert.

> **Hinweis**
> In der 64-Bit-Version von Windows XP können prozessbezogene Vorgänge nicht abgefangen werden.

Registrierungsvorgänge

- **Starteinstellungen ändern** - Alle Veränderungen der Einstellungen, die festlegen, welche Anwendungen beim Windows-Start ausgeführt werden. Diese können beispielsweise über den Schlüssel Run in der Windows-Registrierung ermittelt werden.
- **Registrierungsinhalte löschen** - Registrierungsschlüssel oder seinen Wert löschen
- **Registrierungsschlüssel umbenennen** - Umbenennen von Registrierungsschlüsseln.
- **Registrierungsdatenbank ändern** - Neue Werte für Registrierungsschlüssel erstellen, vorhandene Werte ändern, Daten im Verzeichnisbaum der Datenbank verschieben oder Benutzer- bzw. Gruppenrechte für Registrierungsschlüssel einrichten.

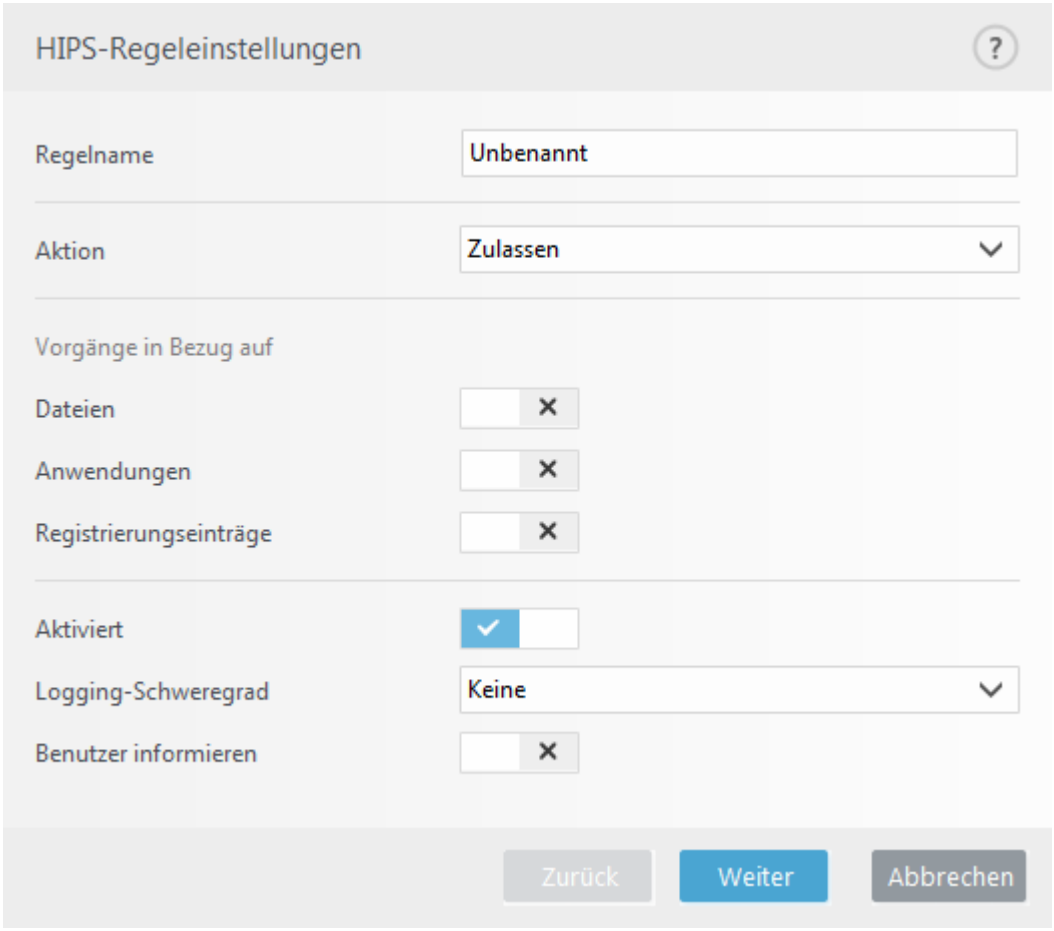
> **Hinweis**
> Verwenden von Platzhaltern in Regeln
> Sternchen können in Regeln nur verwendet werden, um einen bestimmten Schlüssel zu ersetzen, z. B. „HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet*\Start“. Andere Anwendungsformen von Platzhaltern werden nicht unterstützt.
> Erstellen von Regeln mit dem Schlüssel „HKEY_CURRENT_USER“ als Ziel
> Dieser Schlüssel ist lediglich eine Verknüpfung zum entsprechenden Unterschlüssel von „HKEY_USERS“ für den jeweiligen Benutzer anhand des SID (sicherer Bezeichner). Verwenden Sie einen Pfad in Form von „HKEY_USERS\%SID%“ anstelle von „HKEY_CURRENT_USER“, um eine Regel nur für den aktuellen Benutzer zu erstellen. Geben Sie ein Sternchen anstelle des SID ein, um die Regel für alle Benutzer anzuwenden.

> **Warnung**
> Wenn Sie eine sehr allgemeine Regel erstellen, wird eine Warnung zu dieser Art Regel angezeigt.

Das folgende Beispiel zeigt, wie Sie unerwünschte Verhaltensweisen einer bestimmten Anwendung einschränken können:

1. Geben Sie der Regel einen Namen und wählen Sie **Blockieren** (oder **Fragen**, falls Sie sich später entscheiden möchten) im Dropdownmenü **Aktion** aus.
2. Aktivieren Sie die Option **Benutzer informieren**, damit bei jeder Anwendung einer Regel ein Benachrichtigungsfenster angezeigt wird.
3. Wählen Sie mindestens eine Operation im Abschnitt **Vorgänge in Bezug auf** aus, für die die Regel angewendet werden soll.
4. Klicken Sie auf **Weiter**.

5.Wählen Sie im Fenster **Quellanwendungen** die Option **Bestimmte Anwendungen** im Dropdownmenü aus, um Ihre neue Regel für alle Anwendungen anzuwenden, die versuchen, eine der ausgewählten Anwendungsoperationen für die angegebenen Anwendungen auszuführen.
6.Klicken Sie auf **Hinzufügen** und dann auf **...**, um einen Pfad zu einer Anwendung auszuwählen, und klicken Sie dann auf **OK**. Fügen Sie bei Bedarf weitere Anwendungen hinzu.
Beispiel: *C:\Program Files (x86)\Untrusted application\application.exe*
7.Wählen Sie die Operation **In Datei schreiben** aus.
8.Wählen Sie **Alle Dateien** im Dropdownmenü aus. Auf diese Weise werden Schreibversuche in alle Dateien von den Anwendungen blockiert, die Sie im vorherigen Schritt ausgewählt haben.
9.Klicken Sie auf **Fertig stellen**, um die neue Regel zu speichern.



Erweiterte HIPS-Einstellungen

Die folgenden Optionen helfen bei der Fehlerbehebung und der Analyse des Verhaltens einer Anwendung:

Treiber dürfen immer geladen werden - Ausgewählte Treiber werden unabhängig vom konfigurierten Filtermodus immer zugelassen, sofern sie nicht durch eine Benutzerregel ausdrücklich blockiert werden.

Alle blockierten Vorgänge in Log aufnehmen - Alle blockierten Vorgänge werden in den HIPS-Log geschrieben.

Änderungen an Autostart-Einträgen melden - Zeigt einen Desktophinweis an, wenn eine Anwendung vom Systemstart entfernt bzw. zum Systemstart hinzugefügt wird.

Treiber dürfen immer geladen werden

In dieser Liste angezeigte Treiber werden unabhängig vom HIPS-Filtermodus immer zugelassen, sofern sie nicht ausdrücklich durch eine Benutzerregel blockiert werden.

Hinzufügen - Neuen Treiber hinzufügen.

Bearbeiten - Ausgewählten Treiber bearbeiten.

Entfernen - Treiber aus der Liste entfernen.

Zurücksetzen - Systemtreiber werden erneut geladen.

> **Hinweis**
> Klicken Sie nur auf **Zurücksetzen**, wenn Sie keine manuell hinzugefügten Treiber einschließen möchten. Diese Funktion kann nützlich sein, wenn Sie mehrere Treiber hinzugefügt haben und sie nicht manuell aus der Liste löschen können.

Präsentationsmodus

Der Präsentationsmodus ist eine Funktion für Benutzer, die ihre Software ununterbrochen nutzen, nicht durch Popup-Fenster gestört werden und die CPU-Auslastung reduzieren möchten. Der Präsentationsmodus kann auch während Präsentationen verwendet werden, die nicht durch eine Aktion des Virenschutzes unterbrochen werden dürfen. Wenn er aktiviert ist, werden alle Popup-Fenster deaktiviert und geplante Tasks werden nicht ausgeführt. Der Systemschutz läuft weiter im Hintergrund, doch es sind keine Eingaben durch Benutzer erforderlich.

Klicken Sie auf **Einstellungen** > **Computer** und anschließend in das Kontrollkästchen **Präsentationsmodus, um den Präsentationsmodus manuell zu aktivieren. Klicken Sie in Erweiterte Einstellungen** (F5) auf **Tools** > **Präsentationsmodus** und anschließend in das Kontrollkästchen neben **Präsentationsmodus automatisch aktivieren, wenn Anwendungen im Vollbildmodus ausgeführt werden, damit ESET Endpoint Antivirus automatisch in den Präsentationsmodus wechselt, wenn Anwendungen im Vollbildmodus ausgeführt werden**. Im Präsentationsmodus besteht ein erhöhtes Risiko. Daher wird das Schutzstatus-Symbol in der Taskleiste orange und mit einer Warnung angezeigt. Diese Warnung wird auch im Hauptprogrammfenster angezeigt (**Präsentationsmodus aktiviert** wird orangefarben dargestellt).

Wenn Sie die Option **Präsentationsmodus automatisch aktivieren, wenn Anwendungen im Vollbildmodus ausgeführt werden aktivieren,** wird der Präsentationsmodus gestartet, sobald Sie eine Anwendung im Vollbildmodus ausführen. Der Präsentationsmodus wird beendet, sobald Sie die Anwendung beenden. Dies ist besonders hilfreich, um den Präsentationsmodus direkt nach dem Start eines Computerspiels, einer Anwendung im Vollbildmodus oder einer Präsentation starten zu lassen.

Mit der Option **Präsentationsmodus automatisch deaktivieren nach** können Sie außerdem die Zeit in Minuten festlegen, nach der der Präsentationsmodus automatisch deaktiviert wird.

Scan der Systemstartdateien

Die automatische Prüfung der Systemstartdateien wird standardmäßig beim Systemstart und bei Updates von Modulen ausgeführt. Die Ausführung der Prüfung ist abhängig davon, wie der Taskplaner konfiguriert ist und

welche Tasks eingerichtet wurden.

Die Optionen der Systemstartprüfung sind Bestandteil des Task **Scan der Systemstartdateien** im Taskplaner. Navigieren Sie zum Ändern der Einstellungen für die Systemstartprüfung nach **Tools** > **Taskplaner** und klicken Sie auf **Prüfung Systemstartdateien** und anschließend auf **Bearbeiten**. Nach dem letzten Schritt wird das Fenster Prüfung Systemstartdateien angezeigt. (Weitere Informationen finden Sie im nächsten Kapitel.)

Detaillierte Anweisungen zum Erstellen und Verwalten von Tasks im Taskplaner finden Sie unter Erstellen neuer Tasks.

Prüfung Systemstartdateien

Beim Erstellen eines geplanten Tasks für die Prüfung der Systemstartdateien stehen Optionen zum Anpassen der folgenden Parameter zur Verfügung:

Im Dropdownmenü **Prüfziel** wird die Prüftiefe für Systemstartdateien auf Grundlage eines geheimen, komplizierten Algorithmus festgelegt. Die Dateien werden auf Grundlage der folgenden Kriterien in absteigender Reihenfolge sortiert:

- **Alle registrierten Dateien** (größte Anzahl geprüfter Dateien)
- **Selten verwendete Dateien**
- **Häufig verwendete Dateien**
- **Häufig verwendete Dateien**
- **Nur die am häufigsten verwendeten Dateien** (kleinste Anzahl geprüfter Dateien)

Außerdem stehen zwei besondere Gruppen zur Verfügung:

- **Dateien, die vor der Benutzeranmeldung gestartet werden**– Enthält Dateien von Standorten, auf die ohne Benutzeranmeldung zugegriffen werden kann (umfasst nahezu alle Systemstartstandorte wie Dienste, Browserhilfsobjekte, Windows-Anmeldungshinweise, Einträge im Windows-Taskplaner, bekannte DLL-Dateien usw.).
- **Dateien, die nach der Benutzeranmeldung gestartet werden**- Enthält Dateien von Standorten, auf die erst nach einer Benutzeranmeldung zugegriffen werden kann (umfasst Dateien, die nur für einen bestimmten Benutzer ausgeführt werden, üblicherweise im Verzeichnis *HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run*).

Die Liste der zu prüfenden Dateien ist für jede der zuvor genannten Gruppen unveränderbar.

Scan-Priorität– Die Priorität, mit der der Scan-Beginn ermittelt wird:

- **Bei Leerlauf**– Der Task wird nur ausgeführt, wenn das System im Leerlauf ist,
- **Minimal**– bei minimaler Systemlast
- **Niedrig**– bei geringer Systemlast
- **Normal**– bei durchschnittlicher Systemlast.

Dokumentenschutz

Die Dokumentenschutzfunktion überprüft Microsoft Office-Dokumente vor dem Öffnen sowie automatisch von Internet Explorer heruntergeladene Dateien wie Microsoft ActiveX-Elemente. Der Dokumentenschutz bietet eine zusätzliche Schutzebene zum Echtzeit-Dateischutz und kann deaktiviert werden, um die Leistung auf Systemen zu

verbessern, die keine große Anzahl an Microsoft Office-Dokumenten verarbeiten müssen.

Um den Dokumentenschutz zu aktivieren, navigieren Sie zu **Erweiterte Einstellungen** (F5) > **Erkennungsroutine** > **Schadsoftware-Prüfungen** > **Dokumentenschutz**, und klicken Sie auf den Schalter **Systemintegration**.



Hinweis
Die Funktion wird von Anwendungen aktiviert, die die Microsoft Antivirus API verwenden (z. B. Microsoft Office 2000 und höher oder Microsoft Internet Explorer 5.0 und höher).

Ausschlussfilter

Mit **Ausschlüssen** können Sie festlegen, welche Objekte aus der Erkennungsroutine ausgeschlossen werden sollen. Um zu gewährleisten, dass möglichst alle Objekte gescannt werden, empfehlen wir, nur bei dringendem Bedarf Ausnahmen zu erstellen. In bestimmten Fällen kann es jedoch erforderlich sein, Objekte vom Scannen auszuschließen, beispielsweise bei großen Datenbankeinträgen, deren Scan die Computerleistung zu stark beeinträchtigen würde, oder bei Software, die Konflikte beim Scannen verursacht (z. B. Backup-Software).

Mit Leistungsausschlüssen können Sie Dateien und Ordner vom Scannen ausschließen. Leistungsausschlüsse sind hilfreich, um Gaming-Anwendungen auf Dateiebene auszuschließen, wenn das Systemverhalten beeinträchtigt wird oder um die Leistung zu verbessern.

Mit Ereignisausschlüssen können Sie Objekte nach deren Ereignisname, Pfad oder Hash von der Säuberung ausschließen. Ereignisausschlüsse schließen im Gegensatz zu Leistungsausschlüssen keine Dateien und Ordner vom Scannen aus. Ereignisausschlüsse schließen Objekte nur aus, wenn diese von der Erkennungsroutine erkannt wurden und eine entsprechende Regel in der Ausschlussliste existiert.

In den Ausschlüssen in Version 7.1 und niedriger werden Leistungsausschlüsse und Ereignisausschlüsse zusammengeführt.

Verwechseln Sie diese Ausschlüsse nicht mit den anderen Arten von Ausschlüssen:

- Ausgeschlossene Prozesse - Alle dateibezogenen Vorgänge im Zusammenhang Anwendungsprozessen werden vom Scannen ausgeschlossen (ist unter Umständen erforderlich, um Die Geschwindigkeit und Verfügbarkeit von Backup-Diensten zu verbessern).
- Ausgeschlossene Dateierweiterungen
- HIPS-Ausschlüsse
- Ausschlussfilter für den cloudbasierten Schutz

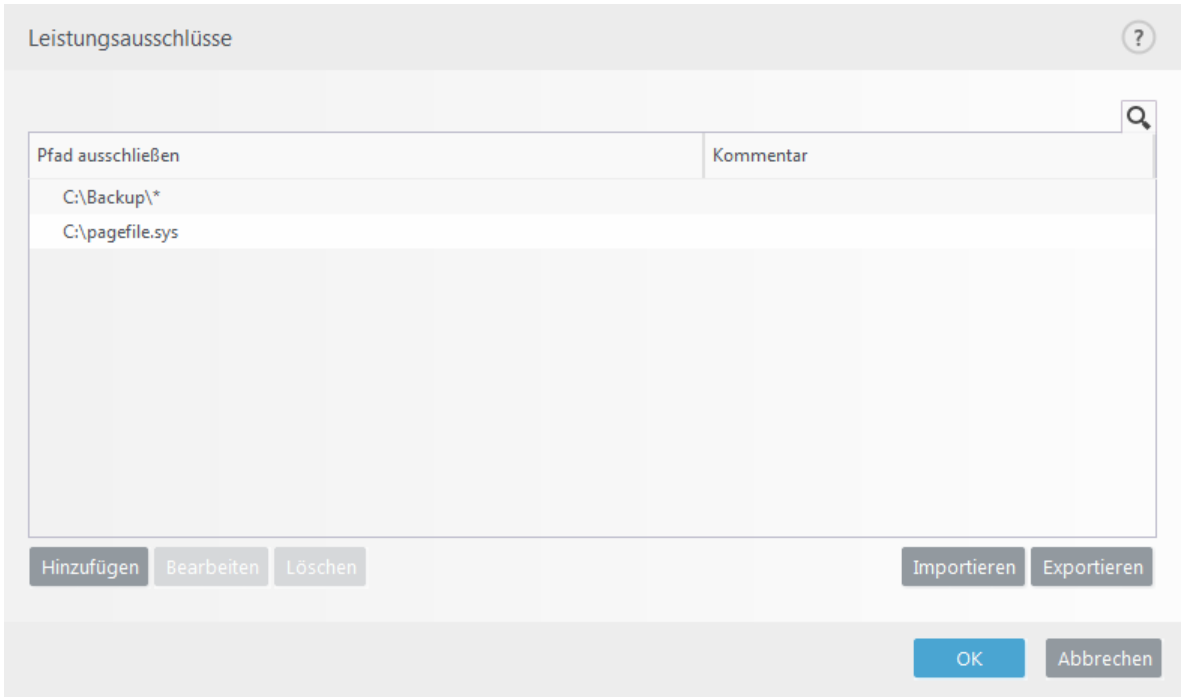
Leistungsausschlüsse

Mit Leistungsausschlüssen können Sie Dateien und Ordner vom Scannen ausschließen.

Um zu gewährleisten, dass möglichst alle Objekte auf Bedrohungen gescannt werden, sollten Sie Leistungsausschlüsse nur bei dringendem Bedarf erstellen. In bestimmten Fällen kann es jedoch erforderlich sein, Objekte vom Scannen auszuschließen, etwa bei großen Datenbankeinträgen, die die Computerleistung beim Scannen zu stark beeinträchtigen würden, oder bei Software, die Konflikte beim Scannen verursacht.

Sie können Dateien und Ordner vom Scannen ausschließen, indem Sie sie unter **Erweiterte Einstellungen** (**F5**) > **Erkennungsroutine** > **Ausschlüsse** > **Leistungsausschlüsse** > **Bearbeiten** zur Liste der Ausschlüsse hinzufügen.

Um ein Objekt vom Scannen auszuschließen (Pfad: Datei oder Ordner), klicken Sie auf **Hinzufügen** und geben Sie den Pfad des Objekts ein oder wählen Sie es in der Baumstruktur aus.



HINWEIS
Eine Bedrohung, die sich in einer Datei befindet, die die Kriterien des Ausschlussfilters erfüllt, kann vom **Echtzeit-Dateischutz** und bei der **Prüfung des Computers** nicht erkannt werden.

Steuerelemente

- **Hinzufügen** - Fügen Sie einen neuen Eintrag hinzu, um Objekte vom Scannen auszuschließen.
- **Bearbeiten** - Ausgewählten Eintrag bearbeiten
- **Löschen** – Ausgewählte Einträge entfernen (CTRL + Klicken, um mehrere Einträge auszuwählen.
- **Importieren/Exportieren** - Das Importieren und Exportieren der Leistungsausschlüsse ist hilfreich, um Ihre aktuellen Ausschlüsse zur späteren Verwendung zu sichern. Die Option zum Exportieren der Einstellungen ist auch hilfreich für Benutzer in nicht verwalteten Umgebungen, die ihre bevorzugte Konfiguration auf mehreren Systemen verwenden möchten. Diese Benutzer können ihre Einstellungen übertragen, indem sie eine .txt-Datei importieren.
  Beispiel für das Import/Export-Dateiformat anzeigen

```
# {"product":"endpoint","version":"7.2.2055","path":"plugins.01000600.settings.Perfo
rmanceExclusions","columns":["Path","Description"]}

C:\Backup\*,custom comment

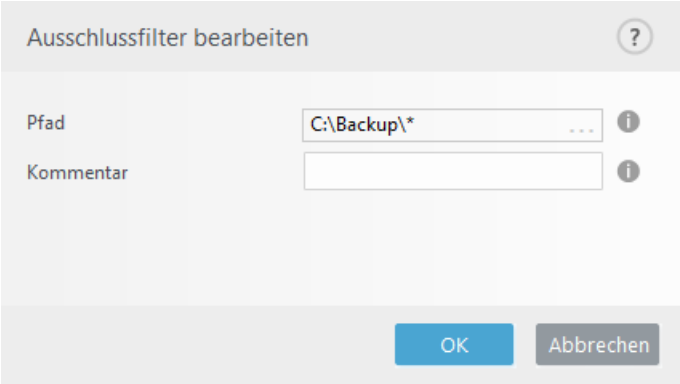
C:\pagefile.sys,
```

Leistungsausschluss hinzufügen oder bearbeiten

In diesem Dialogfeld können Sie einen bestimmten Pfad (Datei oder Ordner) auf diesem Computer ausschließen.

Pfad auswählen oder manuell eingeben

Um den gewünschten Pfad auszuwählen, klicken Sie auf **...** im Feld **Pfad**.
Falls Sie den Pfad manuell eingebe, finden Sie unten weitere Beispiele für Ausschlussformate.



Mit Platzhaltern können Sie Gruppen von Dateien ausschließen. Dabei steht ein Fragezeichen (*?*) für genau ein beliebiges Zeichen, und ein Sternchen (***) steht für null bis beliebig viele Zeichen.

Eingeben von Ausschlussfiltern

- Wenn Sie alle Dateien in einem bestimmten Ordner ausschließen möchten, geben Sie den Pfad zum Ordner mit der Maske **.** ein.
- Wenn nur DOC-Dateien ausgeschlossen werden sollen, verwenden Sie die Maske **.doc*.
- Wenn der Name einer ausführbaren Datei aus einer bestimmten Anzahl von variierenden Zeichen besteht und Sie nur das erste Zeichen mit Sicherheit kennen (z. B. „D“), verwenden Sie das folgende Format:
D????.exe (Die Fragezeichen ersetzen die fehlenden oder unbekannten Zeichen)

Systemvariablen in Ausschlüssen

Sie können Systemvariablen wie *%PROGRAMFILES%* verwenden, um Scan-Ausschlüsse zu definieren.

- Um den Programme-Ordner mit dieser Systemvariable auszuschließen, fügen Sie den Pfad *%PROGRAMFILES%** (mit umgekehrtem Schrägstrich und Sternchen am Ende des Pfads) zu Ihren Ausschlüssen hinzu
- Um alle Dateien und Ordner in einem Unterverzeichnis von *%PROGRAMFILES%* auszuschließen, schließen Sie den Pfad *%PROGRAMFILES%\Ausgeschlossenes_Verzeichnis** aus

Liste der unterstützten Systemvariablen erweitern

Im Format für ausgeschlossene Pfade können Sie die folgenden Variablen verwenden:

- *%ALLUSERSPROFILE%*
- *%COMMONPROGRAMFILES%*
- *%COMMONPROGRAMFILES(X86)%*
- *%COMSPEC%*
- *%PROGRAMFILES%*
- *%PROGRAMFILES(X86)%*
- *%SystemDrive%*
- *%SystemRoot%*
- *%WINDIR%*
- *%PUBLIC%*

Benutzerspezifische Systemvariablen (z. B. *%TEMP%* oder *%USERPROFILE%*) oder Umgebungsvariablen (z. B. *%PATH%*) werden nicht unterstützt.

Pfadausschlüsse mit Sternchen

Hier sehen Sie einige weitere Beispiele für die Verwendung von Sternchen:

*C:\Tools** - Der Pfad muss mit umgekehrtem Schrägstrich und Sternchen enden, um anzugeben, dass es sich um einen Ordner handelt und dann alle Unterordner ausgeschlossen werden sollen.

C:\Tools.dat* - Mit diesem Filter werden .dat-Dateien im Ordner *Tools* ausgeschlossen.

C:\Tools\sg.dat - Dieser Filter schließt eine bestimmte Datei unter einem bestimmten Pfad aus.

Eine Ausnahme für Leistungsausschlüsse:

C:\Tools.** - Dasselbe Verhalten wie *C:\Tools** (Achtung: Die Maske `*.*` schließt nur Dateien mit Erweiterungen im Ordner *Tools* aus).

Beispiel für einen falsch eingegebenen Ausschluss:

C:\Tools - Der Ordner *Tools* wird nicht ausgeschlossen. Aus der Perspektive des Scanners könnte *Tools* auch ein Dateiname sein.

C:\Tools - Vergessen Sie nicht das Sternchen am Ende des Pfads: *C:\Tools**

Platzhalter in der Mitte von Pfaden

Verwenden Sie Platzhalter in der Mitte von Pfaden (z. B. *C:\Tools*\Data\file.dat*) nach Möglichkeit nur, wenn dies für Ihr System unbedingt erforderlich ist. Weitere Informationen finden Sie in diesem Knowledgebase-Artikel.

Bei Ereignisausschlüsse gelten keine Einschränkungen für die Verwendung von Platzhaltern in der Mitte von Pfaden.

Reihenfolge der Ausschlüsse

- Sie können die Priorität der Ausschlüsse nicht mit den Schaltflächen Oben/Unten anpassen
- Wenn die erste anwendbare Regel im Scanner eine Übereinstimmung ergibt, wird die zweite Regel nicht mehr ausgewertet
- Je weniger Regeln, desto besser die Scan-Leistung
- Vermeiden Sie konkurrierende Regeln

Format für ausgeschlossene Pfade

Mit Platzhaltern können Sie Gruppen von Dateien ausschließen. Dabei steht ein Fragezeichen (*?*) für genau ein beliebiges Zeichen, und ein Sternchen (***) steht für null bis beliebig viele Zeichen.

Eingeben von Ausschlussfiltern

- Wenn Sie alle Dateien in einem bestimmten Ordner ausschließen möchten, geben Sie den Pfad zum Ordner mit der Maske **.** ein.
- Wenn nur DOC-Dateien ausgeschlossen werden sollen, verwenden Sie die Maske **.doc*.
- Wenn der Name einer ausführbaren Datei aus einer bestimmten Anzahl von variierenden Zeichen besteht und Sie nur das erste Zeichen mit Sicherheit kennen (z. B. „D“), verwenden Sie das folgende Format:

D????.exe (Die Fragezeichen ersetzen die fehlenden oder unbekannten Zeichen)

Systemvariablen in Ausschlüssen

Sie können Systemvariablen wie *%PROGRAMFILES%* verwenden, um Scan-Ausschlüsse zu definieren.

- Um den Programme-Ordner mit dieser Systemvariable auszuschließen, fügen Sie den Pfad *%PROGRAMFILES%** (mit umgekehrtem Schrägstrich und Sternchen am Ende des Pfads) zu Ihren Ausschlüssen hinzu
- Um alle Dateien und Ordner in einem Unterverzeichnis von *%PROGRAMFILES%* auszuschließen, schließen Sie den Pfad *%PROGRAMFILES%\Ausgeschlossenes_Verzeichnis** aus

Liste der unterstützten Systemvariablen erweitern

Im Format für ausgeschlossene Pfade können Sie die folgenden Variablen verwenden:

- *%ALLUSERSPROFILE%*
- *%COMMONPROGRAMFILES%*
- *%COMMONPROGRAMFILES(X86)%*
- *%COMSPEC%*
- *%PROGRAMFILES%*
- *%PROGRAMFILES(X86)%*
- *%SystemDrive%*
- *%SystemRoot%*
- *%WINDIR%*
- *%PUBLIC%*

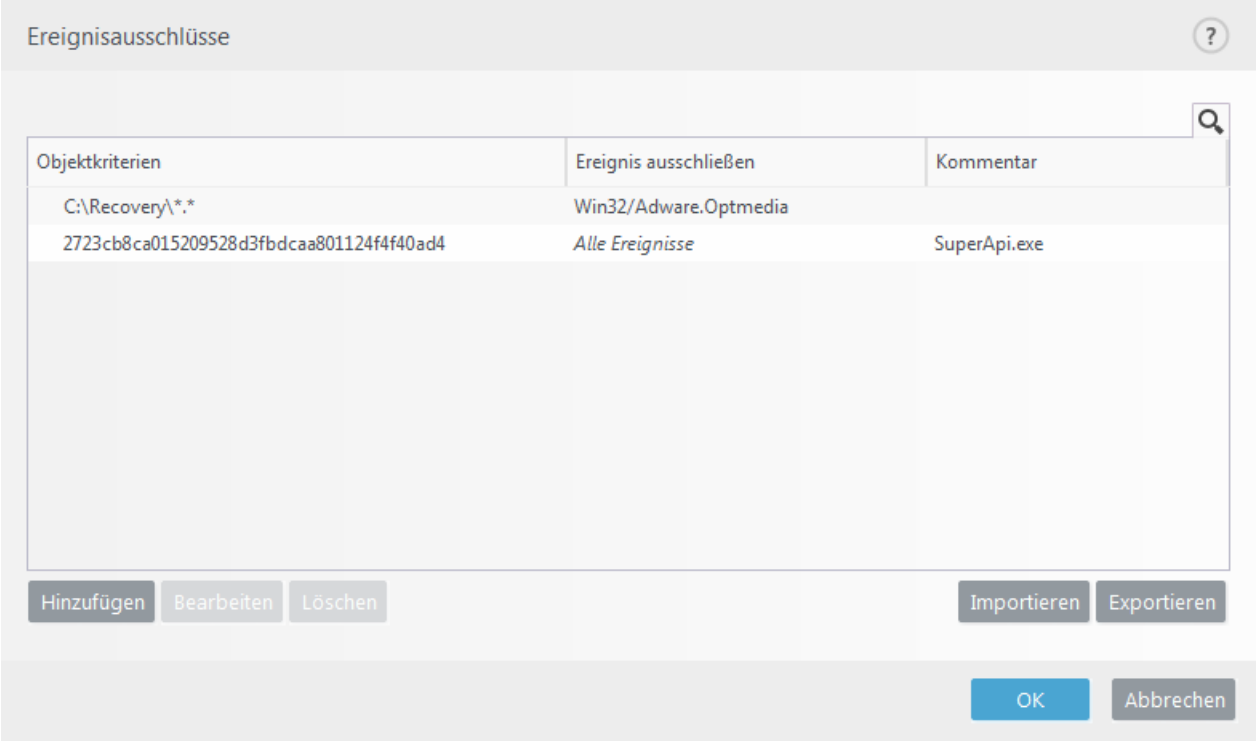
Benutzerspezifische Systemvariablen (z. B. *%TEMP%* oder *%USERPROFILE%*) oder Umgebungsvariablen (z. B. *%PATH%*) werden nicht unterstützt.

Ereignisausschlüsse

Mit Ereignisausschlüssen können Sie Objekte von der Säuberung ausschließen, indem Sie sie nach Ereignisname, Objektpfad oder Hash filtern.

Funktionsweise von Ereignisausschlüssen

Ereignisausschlüsse schließen im Gegensatz zu Leistungsausschlüssen keine Dateien und Ordner vom Scannen aus. Ereignisausschlüsse schließen Objekte nur aus, wenn diese von der Erkennungsroutine erkannt wurden und eine entsprechende Regel in der Ausschlussliste existiert. Zum Beispiel (siehe erste Zeile im Bild unten), Wenn ein Objekt als Win32/Adware.Optmedia erkannt wird und die Datei gleich *C:\Recovery\file.exe* ist. In der zweiten Zeile werden alle Dateien mit dem entsprechenden SHA-1-Hash unabhängig vom Ereignisnamen immer ausgeschlossen.



Um sicherzustellen, dass alle Bedrohungen erkannt werden, sollten Sie Ereignisausschlüsse nur erstellen, wenn dies unbedingt erforderlich ist.

Sie können Dateien und Ordner unter **Erweiterte Einstellungen** (**F5**) > **Erkennungsroutine** > **Ausschlüsse** > **Ereignisausschlüsse** > **Bearbeiten** zur Liste der Ausschlüsse hinzufügen.

Um ein Objekt (nach Ereignisname oder Hash) vom Säubern auszuschließen, klicken Sie auf **Hinzufügen**.

Objektkriterien für Ereignisausschlüsse

- **Pfad** - Beschränkt einen Ereignisausschluss auf einen bestimmten Pfad (oder alle Pfade).
- **Ereignisname** - Steht neben einer ausgeschlossenen Datei der Name eines Ereignisses, dann gilt die Ausnahme nicht generell für die Datei, sondern nur für dieses bestimmte Ereignis. Wird die Datei später durch andere Malware infiziert, wird dies erkannt. Dieser Ausschlusstyp kann nur bei bestimmten Arten eingedrungener Schadsoftware verwendet werden und wird entweder im Warnungsfenster für das Ereignis erstellt (klicken Sie auf **Erweiterte Einstellungen anzeigen** und dann auf **Von der Erkennung ausschließen**) oder indem Sie unter **Tools** > **Quarantäne** mit der rechten Maustaste auf die Datei in der Quarantäne klicken und aus dem Kontextmenü den Befehl **Wiederherstellen und von Scans ausschließen** auswählen.
- **Hash** – Schließt eine Datei auf Basis eines angegebenen Hashs (SHA1) aus, unabhängig von Dateityp, Speicherort, Name oder Erweiterung.

Steuerelemente

- **Hinzufügen** - Fügen Sie einen neuen Eintrag hinzu, um Objekte vom Säubern auszuschließen.
- **Bearbeiten** - Ausgewählten Eintrag bearbeiten
- **Löschen** – Ausgewählte Einträge entfernen (CTRL + Klicken, um mehrere Einträge auszuwählen.
- **Importieren/Exportieren** - Das Importieren und Exportieren der Ereignisausschlüsse ist hilfreich, um Ihre aktuellen Ausschlüsse zur späteren Verwendung zu sichern. Die Option zum Exportieren der Einstellungen ist auch hilfreich für Benutzer in nicht verwalteten Umgebungen, die ihre bevorzugte Konfiguration auf mehreren Systemen verwenden möchten. Diese Benutzer können ihre Einstellungen übertragen, indem sie eine .txt-Datei importieren.
  Beispiel für das Import/Export-Dateiformat anzeigen

```
# {"product":"endpoint","version":"7.2.2055","path":"Settings.ExclusionsManagement.DetectionExclusions","columns":["Id","Path","ThreatName","Description","FileHash"]}

4c59cd02-357c-4b20-a0ac-ca8400000001,,,SuperApi.exe,00117F70C86ADB0F979021391A8AEAA497C2C8DF

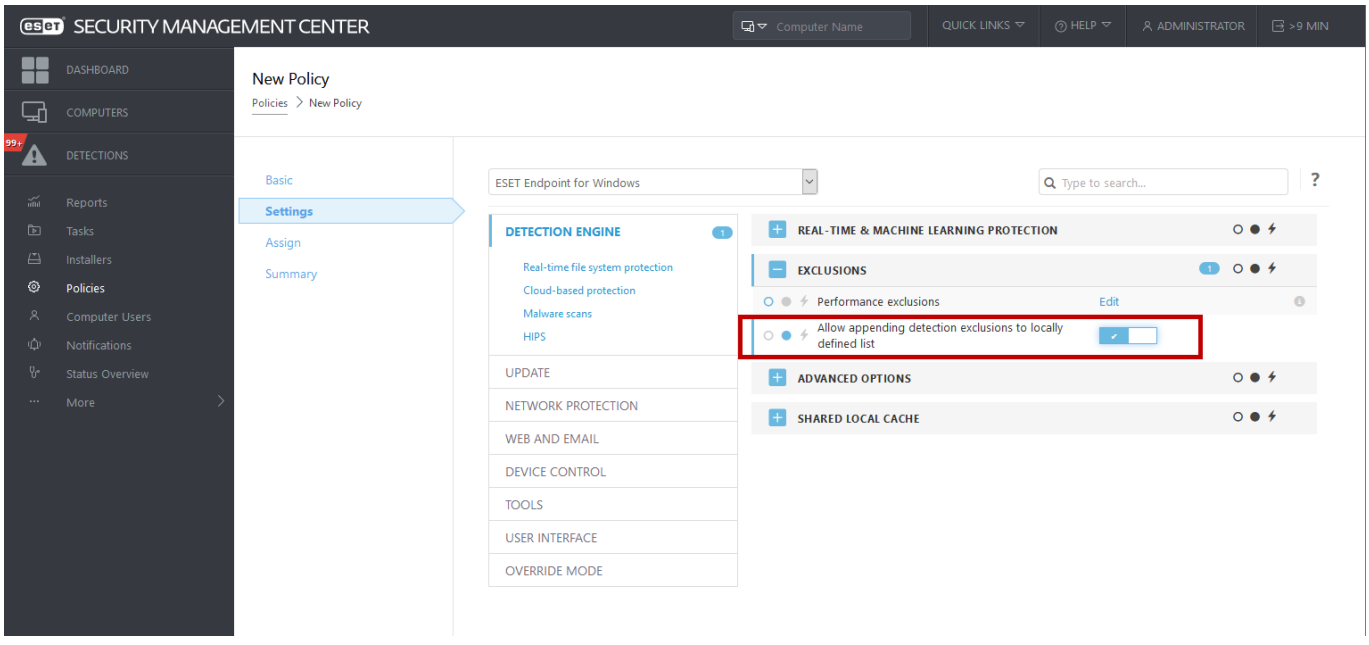
2c362ac8-a630-496e-9665-c76d00000001,C:\Recovery\*.*,Win32/Adware.Optmedia,,
```

Einrichten von Ereignisausschlüssen in ESMC

ESMC 7.1 enthält einen neuen Assistenten zum Verwalten von Ereignisausschlüssen, mit dem Sie einen Ereignisausschluss erstellen und auf mehrere Computer oder Gruppen anwenden können.

Überschreiben möglicher Ereignisausschlüsse in ESMC

Wenn eine lokale Liste mit Ereignisausschlüssen existiert, muss ein Administrator eine Policy mit **Anhängen von Ereignisausschlüssen an lokal definierte Liste erlauben** anwenden. Anschließend funktionieren die Ereignisausschlüsse aus ESMC wie erwartet.

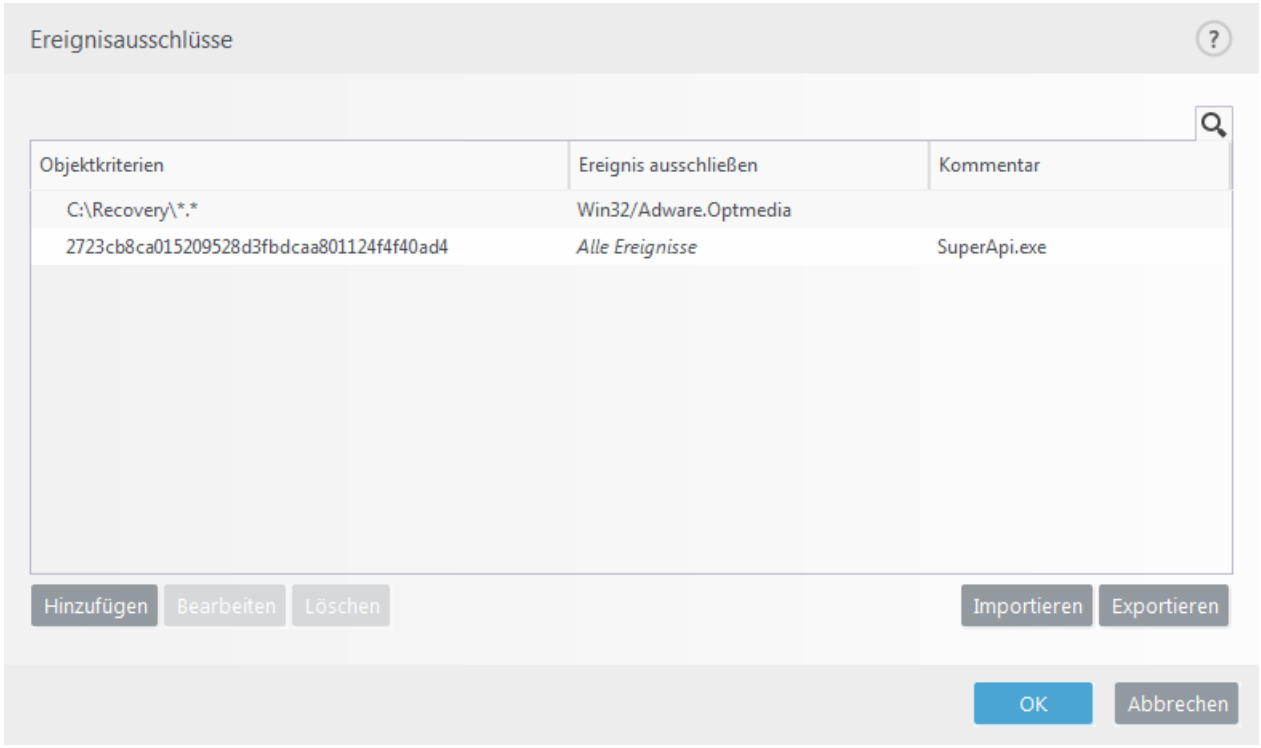


Ereignisausschluss hinzufügen oder bearbeiten

Ereignis ausschließen

Geben Sie einen gültigen Ereignis für ESET an. Sie finden gültige Ereignisnamen unter Log-Dateien > **Ereignisse** im Dropdown-Menü „Log-Dateien“. Dies ist hilfreich, wenn ESET Endpoint Antivirus einen Fehlalarm auslöst. Ausschlüsse für tatsächliche Schadsoftware sind sehr gefährlich, daher sollten Sie nur betroffene Dateien / Verzeichnisse auswählen, indem Sie auf **...** im Feld **Pfad** klicken und diese nur für begrenzte Zeit ausschließen. Ausschlüsse gelten auch für potenziell unerwünschte Anwendungen, potenziell unsichere Anwendungen und verdächtige Anwendungen.

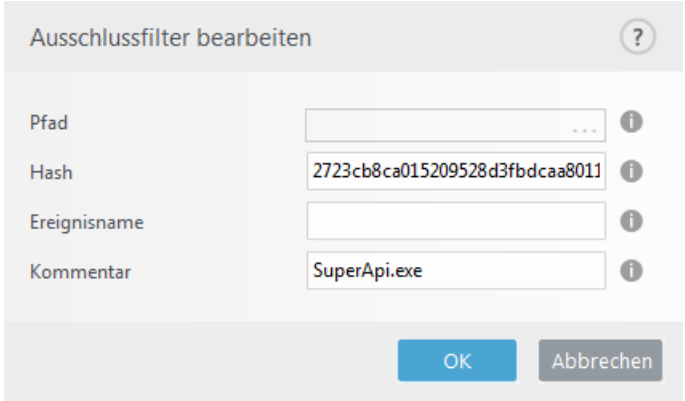
Siehe auch Format für ausgeschlossene Pfade.



Beachten Sie das unten gezeigte Beispiel für Ereignisausschlüsse.

Hash ausschließen

Schließt eine Datei auf Basis eines angegebenen Hashs (SHA1) aus, unabhängig von Dateityp, Speicherort, Name oder Erweiterung.



Ausschlüsse nach Ereignisname

Geben Sie einen gültigen Ereignisnamen ein, um ein bestimmtes Ereignis nach dessen Namen auszuschließen:
Win32/Adware.Optmedia
Sie können auch das folgende Format verwenden, um ein Ereignis im ESET Endpoint Antivirus-Warnungsfenster auszuschließen:
@NAME=Win32/Adware.Optmedia@TYPE=ApplicUnwnt
@NAME=Win32/TrojanDownloader.Delf.QQI@TYPE=Trojan
@NAME=Win32/Bagle.D@TYPE=worm

Steuerelemente

- **Hinzufügen** - Objekte von der Prüfung ausnehmen
- **Bearbeiten** - Ausgewählten Eintrag bearbeiten
- **Löschen** – Ausgewählte Einträge entfernen (CTRL + Klicken, um mehrere Einträge auszuwählen.

Assistent zum Erstellen von Ereignisausschlüssen

Sie können Ereignisausschlüsse auch im Kontextmenü der Log-Dateien erstellen (nicht verfügbar für Malware-Erkennungen):

1. Klicken Sie im Hauptprogrammfenster auf **Tools** > **Log-Dateien**.
2. Klicken Sie mit der rechten Maustaste auf eine Erkennung im **Erkennungs-Log**.
3. Klicken Sie auf **Ausschluss erstellen**.

Um eine oder mehrere Erkennungen auf Basis von **Ausschlusskriterien** auszuschließen, klicken Sie auf **Kriterien ändern**:

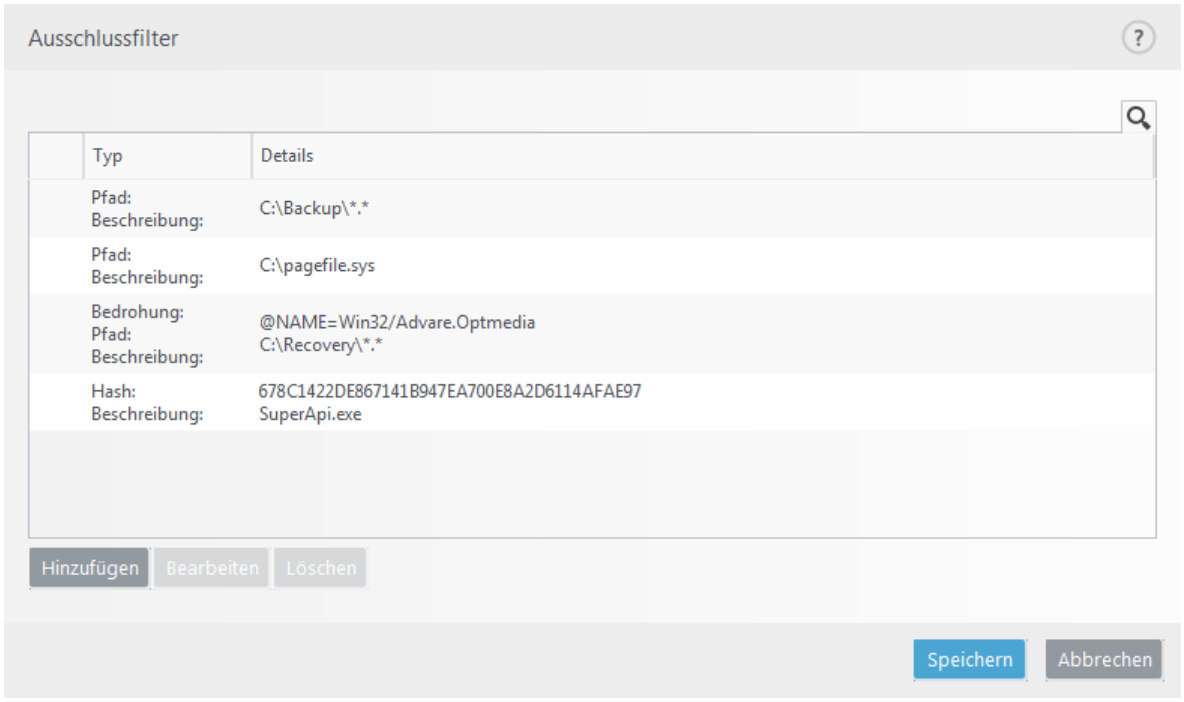
- **Exakte Dateien**- Schließen Sie Dateien nach ihrem SHA-1-Hash aus.
- **Ereignis** - Schließen Sie Dateien nach dem Ereignisnamen aus.
- **Pfad + Ereignis** - Schließen Sie Dateien nach Ereignisname und Pfad aus, inklusive des Dateinamens (z. B. *file:///C:/Users/user/AppData/Local/Temp/34e1824e/ggdsfdgfd.pdf.exe*).

Die empfohlene Option wird anhand des Ereignistyps vorausgewählt.

Optional können Sie einen **Kommentar** eingeben, bevor Sie auf **Ausschluss erstellen** klicken.

Ausschlüsse (7.1 und niedriger)

In den Ausschlüssen in Version 7.1 und niedriger werden Leistungsausschlüsse und Ereignisausschlüsse zusammengeführt.



Ausgeschlossene Prozesse

Mit den ausgeschlossenen Prozessen können Sie Anwendungsprozesse vom Echtzeit-Dateischutz ausschließen. Um Sicherungsgeschwindigkeit, Prozessintegrität und Dienstverfügbarkeit zu verbessern, werden bei der Sicherung bestimmte Techniken eingesetzt, die bekannte Konflikte mit dem Malware-Schutz auf Dateiebene verursachen. Ähnliche Probleme können bei der Live-Migration virtueller Computer auftreten. Eine Deaktivierung der Malware-Schutzsoftware ist der einzig sichere Weg, um beide Situationen zu vermeiden. Wenn Sie bestimmte Prozesse ausschließen (z. B. die der Sicherungslösung), werden alle Dateioperationen dieser Prozesse ignoriert und als sicher betrachtet, um Wechselwirkungen mit dem Sicherungsprozess zu minimieren. Erstellen Sie Ausschlüsse jedoch mit Bedacht: ein ausgeschlossenes Sicherungstool kann auf infizierte Dateien zugreifen, ohne eine Warnung auszulösen. Daher sind erweiterte Berechtigungen nur im Echtzeit-Dateischutzmodul erlaubt.

Mit ausgeschlossenen Prozessen können Sie das Risiko für Konflikte minimieren und die Leistung der ausgeschlossenen Anwendungen verbessern, was sich wiederum auf die Gesamtleistung und Stabilität des Betriebssystems auswirkt. Das Ausschließen von Prozessen und Anwendungen bezieht sich auf deren ausführbare Datei (*.exe*).

Sie können ausführbare Dateien unter **Erweiterte Einstellungen** (**F5**) > **Erkennungsroutine** > **Echtzeit-Dateischutz** > **Ausgeschlossene Prozesse** zur Liste der ausgeschlossenen Prozesse hinzufügen.

Diese Funktion wurde entwickelt, um Sicherungstools auszuschließen. Wenn Sie den Prozess des Sicherungstools vom Scannen ausschließen, verbessern Sie nicht nur die Systemstabilität, sondern auch die Leistung der Sicherungen, da deren Ausführung nicht verlangsamt wird.

Beispiel

Klicken Sie auf **Bearbeiten**, um das Verwaltungsfenster für **ausgeschlossene Prozesse** zu öffnen, in dem Sie Ausschlüsse hinzufügen und nach deren ausführbarer Datei (z. B. *Backup-tool.exe*) suchen können, um sie vom Scannen auszuschließen.
Wenn Sie eine *.exe*-Datei zu den Ausschlüssen hinzufügen, wird deren Prozess nicht mehr von ESET Endpoint Antivirus überwacht, und die ausgeführten Dateioperationen werden nicht gescannt.

Wichtig
Falls Sie nicht die Funktion zum Durchsuchen verwenden, um die ausführbare Datei eines Prozesses auszuwählen, müssen Sie den vollständigen Pfad der ausführbaren Datei angeben. Andernfalls wird die Datei nicht korrekt ausgeschlossen, und in HIPS können Fehler auftreten.

Sie können die vorhandenen Prozesse auch **bearbeiten** oder aus den Ausschlüssen **löschen**.

Hinweis
Der Web-Schutz berücksichtigt diese Ausschlüsse nicht. Wenn Sie also die ausführbare Datei Ihres Webbrowsers ausschließen, werden heruntergeladene Dateien weiterhin gescannt, um Schadsoftware erkennen zu können. Dieses Szenario ist lediglich ein Beispiel und keine Empfehlung, Webbrowser vom Scannen auszuschließen.

Ausgeschlossene Prozesse hinzufügen oder bearbeiten

In diesem Dialogfeld können Sie Prozesse zu den Ausschlüssen für die Erkennungsroutine **hinzufügen**. Mit ausgeschlossenen Prozessen können Sie das Risiko für Konflikte minimieren und die Leistung der ausgeschlossenen Anwendungen verbessern, was sich wiederum auf die Gesamtleistung und Stabilität des Betriebssystems auswirkt. Das Ausschließen von Prozessen und Anwendungen bezieht sich auf deren ausführbare Datei (*.exe*).

Beispiel
Wählen Sie den Pfad einer Anwendung aus, indem Sie auf ... klicken (zum Beispiel *C:\Program Files\Firefox\Firefox.exe*), um eine Ausnahme zu erstellen. Geben Sie NICHT den Namen der Anwendung ein.
Wenn Sie eine *.exe*-Datei zu den Ausschlüssen hinzufügen, wird deren Prozess nicht mehr von ESET Endpoint Antivirus überwacht, und die ausgeführten Dateioperationen werden nicht gescannt.

Wichtig
Falls Sie nicht die Funktion zum Durchsuchen verwenden, um die ausführbare Datei eines Prozesses auszuwählen, müssen Sie den vollständigen Pfad der ausführbaren Datei angeben. Andernfalls wird die Datei nicht korrekt ausgeschlossen, und in HIPS können Fehler auftreten.

Sie können die vorhandenen Prozesse auch **bearbeiten** oder aus den Ausschlüssen **löschen**.

HIPS-Ausschlüsse

Mit den HIPS-Ausschlüssen können Sie Prozesse von der tiefen HIPS-Verhaltensinspektion ausschließen.

Um ein Objekt auszuschließen, klicken Sie auf **Hinzufügen** und geben Sie den Pfad des Objekts ein oder wählen Sie es in der Baumstruktur aus. Sie können ausgewählte Einträge auch bearbeiten oder löschen.

ThreatSense-Parameter

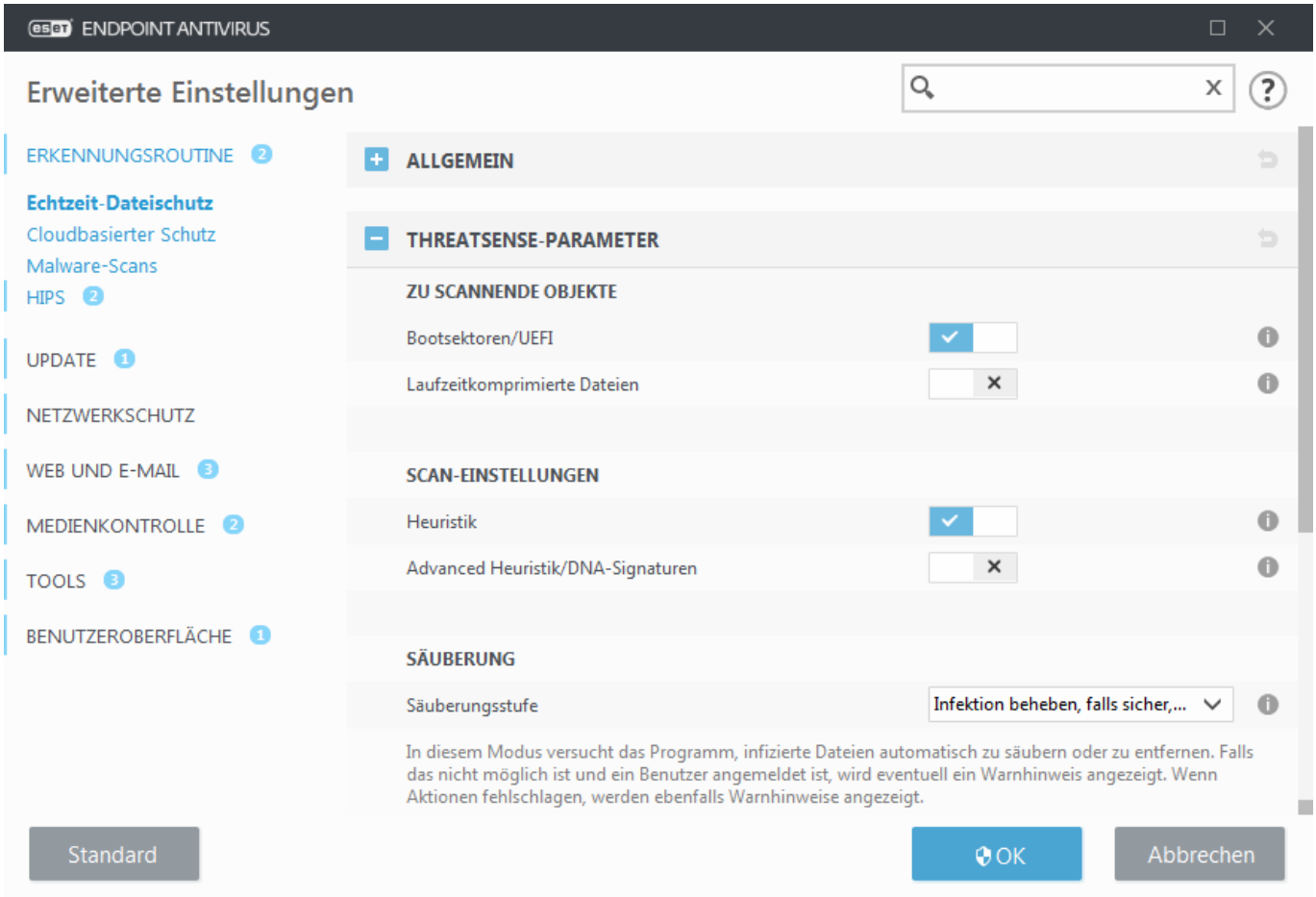
ThreatSense verwendet verschiedene komplexe Methoden zur Bedrohungserkennung. Die Technologie arbeitet proaktiv, d. h. sie schützt das System auch während der ersten Ausbreitung eines neuen Angriffs. Eingesetzt wird eine Kombination aus Code-Analyse, Code-Emulation, allgemeinen Signaturen und Virussignaturen verwendet, die zusammen die Systemsicherheit deutlich erhöhen. Das Prüfmodul kann verschiedene Datenströme gleichzeitig kontrollieren und so die Effizienz und Erkennungsrate steigern. Die ThreatSense-Technologie entfernt auch erfolgreich Rootkits.

in den Einstellungen für ThreatSense können Sie verschiedene Prüfparameter festlegen:

- Dateitypen und -erweiterungen, die geprüft werden sollen
- Die Kombination verschiedener Erkennungsmethoden
- Säuberungsstufen usw.

Um das Fenster für die Einstellungen zu öffnen, klicken Sie auf die **ThreatSense-Parameter** , die im Fenster mit erweiterten Einstellungen für alle Module angezeigt werden, die ThreatSense verwenden (siehe unten). Je nach Anforderung sind eventuell verschiedene Sicherheitseinstellungen erforderlich. Dies sollte bei den individuellen ThreatSense-Einstellungen für die folgenden Schutzmodule berücksichtigt werden:

- Echtzeit-Dateischutz
- Prüfen im Leerlaufbetrieb
- Prüfung der Systemstartdateien
- Dokumentenschutz
- E-Mail-Schutz
- Web-Schutz
- Computerprüfung



ThreatSense-Parameter sind für jedes Modul optimal eingerichtet. Eine Veränderung der Einstellungen kann den Systembetrieb spürbar beeinträchtigen. Änderungen an den Einstellungen für das Prüfen laufzeitkomprimierter Dateien oder die Aktivierung der Advanced Heuristik im Modul „Echtzeit-Dateischutz“ können das System verlangsamen (normalerweise werden mit diesen Methoden nur neu erstellte Dateien geprüft). Es wird empfohlen, die Standard-Parameter für ThreatSense in allen Modulen unverändert beizubehalten. Änderungen sollten nur im Modul „Computer prüfen“ vorgenommen werden.

Zu prüfende Objekte

In diesem Bereich können Sie festlegen, welche Dateien und Komponenten Ihres Computers auf Schadcode gescannt werden sollen.

Arbeitsspeicher - Prüfung auf Bedrohungen für den Arbeitsspeicher des Systems.

Bootsektoren/UEFI - Scannt die Bootsektoren auf Malware im Master Boot Record. Weitere Informationen zu UEFI finden Sie im Glossar.

E-Mail-Dateien – Das Programm unterstützt die folgenden Erweiterungen: DBX (Outlook Express) und EML.

Archive – Das Programm unterstützt die folgenden Erweiterungen: ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE und viele andere.

Selbstentpackende Archive – Selbstentpackende Archive (SFX) sind Archivdateien, die sich selbst extrahieren können.

Laufzeitkomprimierte Dateien – Im Unterschied zu Standardarchiven werden laufzeitkomprimierte Dateien nach dem Starten im Arbeitsspeicher dekomprimiert. Neben statischen laufzeitkomprimierten Dateiformaten (UPX, yoda, ASPack, FSG usw.) kann die Prüfung durch Code-Emulation viele weitere SFX-Typen erkennen.

Prüfungseinstellungen

Wählen Sie die Methoden aus, mit denen das System auf Infiltrationen gescannt werden soll. Folgende Optionen stehen zur Verfügung:

Heuristik - Als heuristische Methoden werden Verfahren bezeichnet, die (bösartige) Aktivitäten von Programmen analysieren. Auf diese Weise können auch bösartige Programme erkannt werden, die noch nicht in der Erkennungsroutine verzeichnet sind. Nachteilig ist, dass es in Einzelfällen zu Fehlalarmen kommen kann.

Advanced Heuristik/DNA-Signaturen - Advanced Heuristik sind besondere heuristische Verfahren, die von ESET entwickelt wurden, um Würmer, Trojaner und Schadprogramme besser zu erkennen, die in höheren Programmiersprachen geschrieben wurden. Mit Advanced Heuristik werden die Fähigkeiten von ESET-Produkten zur Erkennung von Bedrohungen beträchtlich gesteigert. Mit Hilfe von Signaturen können Viren zuverlässig erkannt werden. Mit automatischen Updates sind Signaturen für neue Bedrohungen innerhalb weniger Stunden verfügbar. Nachteilig an Signaturen ist, dass mit ihrer Hilfe nur bekannte Viren und gering modifizierte Varianten bekannter Viren erkannt werden können.

Säubern

Die Säuberungseinstellungen legen fest, wie ESET Endpoint Antivirus beim Säubern von Objekten vorgeht.

Ausschlussfilter

Die Erweiterung ist der Teil des Dateinamens nach dem Punkt. Die Erweiterung definiert den Typ und den Inhalt einer Datei. In diesem Abschnitt der ThreatSense-Einstellungen können Sie die Dateitypen festlegen, die geprüft werden sollen.

Sonstige

Bei der Konfiguration von ThreatSense für eine On-Demand-Prüfung des Computers sind folgende Optionen im Abschnitt **Sonstige** verfügbar:

Alternative Datenströme (ADS) prüfen - Bei den von NTFS-Dateisystemen verwendeten alternativen Datenströmen (ADS) handelt es sich um Datei- und Ordnerzuordnungen, die mit herkömmlichen Prüftechniken nicht erkannt werden können. Eingedrungene Schadsoftware tarnt sich häufig als alternativer Datenstrom, um nicht erkannt zu werden.

Hintergrundprüfungen mit geringer Priorität ausführen - Jede Prüfung nimmt eine bestimmte Menge von Systemressourcen in Anspruch. Wenn Sie mit Anwendungen arbeiten, welche die Systemressourcen stark beanspruchen, können Sie eine Hintergrundprüfung mit geringer Priorität aktivieren, um Ressourcen für die Anwendungen zu sparen.

Alle Objekte in Log aufnehmen - Das Scan-Log enthält alle gescannten Dateien in selbstentpackenden Archiven, auch nicht infizierte Dateien (diese Funktion kann große Mengen an Scan-Log-Daten generieren, und das Scan-Log kann stark anwachsen).

Smart-Optimierung aktivieren - Wenn die Smart-Optimierung aktiviert ist, werden die optimalen Einstellungen verwendet, um die effizienteste Prüfung bei höchster Geschwindigkeit zu gewährleisten. Die verschiedenen Schutzmodule führen eine intelligente Prüfung durch. Dabei verwenden sie unterschiedliche Prüfmethoden für die jeweiligen Dateitypen. Wenn die Smart-Optimierung deaktiviert ist, werden nur die benutzerdefinierten Einstellungen im ThreatSense-Kern der entsprechenden Module für die Prüfung verwendet.

Datum für „Geändert am“ beibehalten - Aktivieren Sie diese Option, um den Zeitpunkt des ursprünglichen

Zugriffs auf geprüfte Dateien beizubehalten (z. B. für die Verwendung mit Datensicherungssystemen), anstatt ihn zu aktualisieren.

Grenzen

Im Bereich „Grenzen“ können Sie die Maximalgröße von Elementen und Stufen verschachtelter Archive festlegen, die geprüft werden sollen:

Einstellungen für Objektprüfung

Maximale Objektgröße - Definiert die Maximalgröße der zu prüfenden Elemente. Der aktuelle Virenschutz prüft dann nur die Elemente, deren Größe unter der angegebenen Maximalgröße liegt. Diese Option sollte nur von fortgeschrittenen Benutzern geändert werden, die bestimmte Gründe dafür haben, dass größere Elemente von der Prüfung ausgeschlossen werden. Der Standardwert ist unbegrenzt.

Maximale Scanzeit pro Objekt (Sek.) - Definiert die maximale Dauer für die Prüfung eines Elements. Wenn hier ein benutzerdefinierter Wert eingegeben wurde, beendet der Virenschutz die Prüfung eines Elements, sobald diese Zeit abgelaufen ist, und zwar ungeachtet dessen, ob die Prüfung abgeschlossen ist oder nicht. Der Standardwert ist unbegrenzt.

Einstellungen für Archivprüfung

Verschachtelungstiefe bei Archiven - Legt die maximale Tiefe der Virenprüfung von Archiven fest. Der Standardwert ist 10.

Maximalgröße von Dateien im Archiv - Hier können Sie die maximale Dateigröße für Dateien in (extrahierten) Archiven festlegen, die geprüft werden sollen. Der Standardwert ist unbegrenzt.

> **Hinweis**
> Die Standardwerte sollten nicht geändert werden; unter normalen Umständen besteht dazu auch kein Grund.

Säuberungsstufen

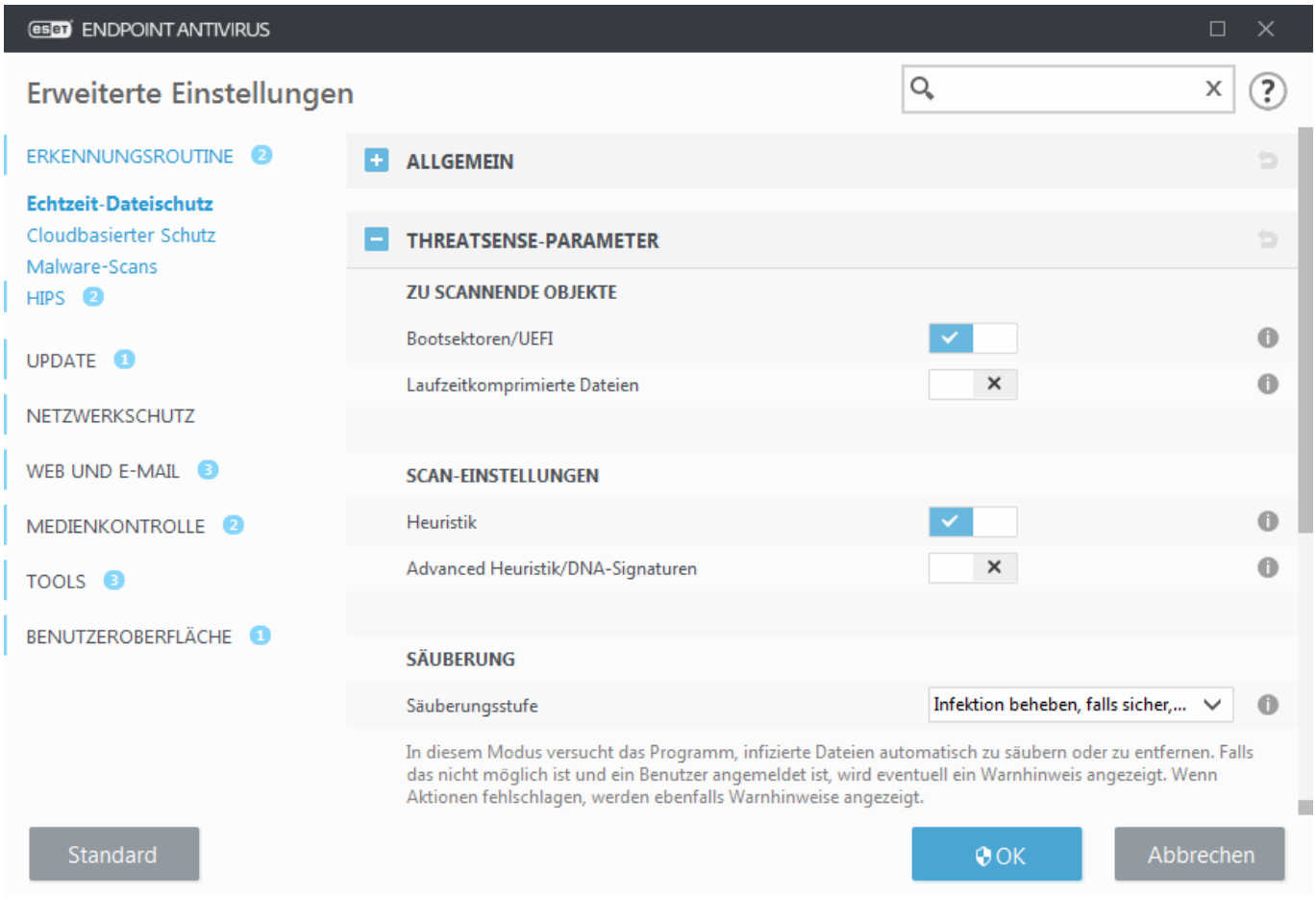
Um die Einstellungen für die Säuberungsstufe eines bestimmten Schutzmoduls zu öffnen, erweitern Sie die **ThreatSense-Parameter** (z. B. den **Echtzeit-Dateischutz**) und klicken Sie auf **Säubern**.

Für den Echtzeit-Dateischutz und andere Schutzmodule sind die folgenden Korrekturstufen (Säuberungsstufen) verfügbar.

Behebung in ESET Endpoint Antivirus 7.2 und höher

Säuberungsstufe	Beschreibung
Ereignis immer beheben	Es wird versucht, Ereignisse beim Säubern von Objekten ohne Eingreifen des Endbenutzers zu beheben. In seltenen Fällen (z. B. Systemdateien) verbleibt das gemeldete Objekt an seinem ursprünglichen Speicherort, falls das Ereignis nicht behoben werden kann. Die Einstellung **Ereignis immer beheben** wird für verwaltete Umgebungen empfohlen.

Ereignis beheben, falls sicher, ansonsten beibehalten	Es wird versucht, Ereignisse beim Säubern von Objekten ohne Eingreifen des Endbenutzers zu beheben. In manchen Fällen (z. B. Systemdateien oder Archive mit sowohl sauberen als auch infizierten Dateien) verbleibt das gemeldete Objekt an seinem ursprünglichen Speicherort, falls das Ereignis nicht behoben werden kann.
Ereignis beheben, falls sicher, andernfalls nachfragen	Es wird versucht, das Ereignis beim Säubern von Objekten zu beheben. Wenn keine Aktion ausgeführt werden kann, erhält der Endbenutzer in manchen Fällen eine interaktive Warnung und kann eine Behebungsaktion auswählen, z. B. löschen oder ignorieren. Diese Einstellung wird in den meisten Fällen empfohlen.
Immer den Endbenutzer fragen	Dem Endbenutzer wird beim Säubern von Objekten ein interaktives Fenster angezeigt, in dem er eine Behebungsaktion auswählen kann, z. B. löschen oder ignorieren). Diese Stufe eignet sich für fortgeschrittene Benutzer, die wissen, wie bei Ereignissen vorzugehen ist.



Säuberungsstufen in ESET Endpoint Antivirus 7.1 und niedriger

Säuberungsstufe	Beschreibung
Nicht säubern	Ereignisse werden nicht automatisch gesäubert. Eine Warnung wird angezeigt, und der Benutzer kann eine Aktion auswählen. Diese Stufe eignet sich für fortgeschrittene Benutzer, die wissen, wie bei Ereignissen vorzugehen ist.
Normale Säuberung	Das Programm versucht, infizierte Dateien automatisch zu säubern oder zu löschen. Es wendet hierzu vordefinierte Aktionen an (je nach Art der Infiltration). Ein Hinweis am unteren rechten Bildschirmrand informiert über die Erkennung und das Löschen infizierter Dateien. Wenn es nicht möglich ist, die angemessene Aktion automatisch zu bestimmen, schlägt das Programm verschiedene Aktionen vor. Dies gilt auch, wenn eine vordefinierte Aktion nicht erfolgreich abgeschlossen werden kann.

Immer versuchen, automatisch zu entfernen	Das Programm säubert oder löscht alle Ereignisse. Ausnahmen gelten nur für Systemdateien. Wenn die Säuberung nicht möglich ist, wird der Benutzer aufgefordert, eine Aktion auszuwählen.

Die genannte Säuberungsstufe wird angewendet, wenn eine ESMC-Policy für ältere Versionen von ESET Endpoint Antivirus eingerichtet wird:

Säuberungsstufe in der ESMC-Policy	Angewendete Säuberungsstufe
Ereignis immer beheben	Immer versuchen, automatisch zu entfernen
Ereignis beheben, falls sicher, ansonsten beibehalten	Normale Säuberung
Ereignis beheben, falls sicher, andernfalls nachfragen	Normale Säuberung
Immer den Endbenutzer fragen	Nicht säubern

* Standardwert beim Upgrade auf Version 7.2 und höher mit der Einstellung **Normale Säuberung** in ESET Endpoint Antivirus.

Von der Prüfung ausgeschlossene Dateiendungen

Die Erweiterung ist der Teil des Dateinamens nach dem Punkt. Die Erweiterung definiert den Typ und den Inhalt einer Datei. In diesem Abschnitt der ThreatSense-Einstellungen können Sie die Dateitypen festlegen, die geprüft werden sollen.



Hinweis
Verwechseln Sie diese Ausschlüsse nicht mit den anderen Arten von Ausschlüssen.

Alle Dateien werden standardmäßig geprüft. Jede Erweiterung kann der Liste ausgeschlossener Dateien hinzugefügt werden.

Der Ausschluss bestimmter Dateien ist dann sinnvoll, wenn die Prüfung bestimmter Dateitypen die Funktion eines Programms beeinträchtigt, das diese Erweiterungen verwendet. So sollten Sie z. B. die Erweiterungen `.edb`, `.eml` und `.tmp` ausschließen, wenn Sie Microsoft Exchange Server verwenden.



Beispiel
Klicken Sie zum Hinzufügen einer neuen Erweiterung zur Liste auf **Hinzufügen**, geben Sie die Erweiterung in das Feld ein (z. B. `tmp`) und klicken Sie auf **OK**. Mit der Option **Mehrere Werte eingeben** können Sie mehrere, durch Zeilen, Komma oder Semikolon getrennte Erweiterungen eingeben (wählen Sie beispielsweise **Semikolon** im Dropdownmenü als Trennzeichen aus und geben Sie `edb;eml;tmp` ein).
Das Sonderzeichen ? (Fragezeichen) steht für ein beliebiges Zeichen (z. B. `?db`).



Hinweis
Um die tatsächliche Erweiterung einer Datei (falls vorhanden) unter Windows anzuzeigen, müssen Sie die Option **Erweiterungen bei bekannten Dateitypen ausblenden** unter **Systemsteuerung** > **Ordneroptionen** > **Ansicht** (Registerkarte) deaktivieren und die Änderung anschließend übernehmen.

Zusätzliche ThreatSense-Parameter

Zusätzliche ThreatSense-Einstellungen für neu erstellte und geänderte Dateien– Das Infektionsrisiko für neu erstellte oder geänderte Dateien ist vergleichsweise größer als für vorhandene Dateien. Daher prüft das Programm solche Dateien mit zusätzlichen Parametern. Zusätzlich zu den üblichen Prüfmethoden auf Signaturbasis wird die Advanced Heuristik verwendet. Diese Methode erkennt neue Bedrohungen, bevor ein Update der Erkennungsroutine veröffentlicht wird. Neben neu erstellten Dateien werden auch selbstentpackende Archive (SFX) und laufzeitkomprimierte Dateien (intern komprimierte, ausführbare Dateien) geprüft. In den Standardeinstellungen werden Archive unabhängig von ihrer eigentlichen Größe bis zur 10. Verschachtelungsebene geprüft. Deaktivieren Sie die Option **Standardeinstellungen Archivprüfung**, um die Archivprüfeinstellungen zu ändern.

Weitere Informationen zu **laufzeitkomprimierten Dateien**, **selbstentpackende Archive** und **Advanced Heuristik** finden Sie unterEinstellungen für ThreatSense.

Zusätzliche ThreatSense-Einstellungen für ausführbare Dateien– Standardmäßig wird bei der Dateiausführung keine Advanced Heuristik verwendet. Wenn diese Option aktiviert ist, sollten Smart-Optimierung und ESET LiveGrid® unbedingt aktiviert bleiben, um die Auswirkungen auf die Systemleistung gering zu halten.

Netzwerk

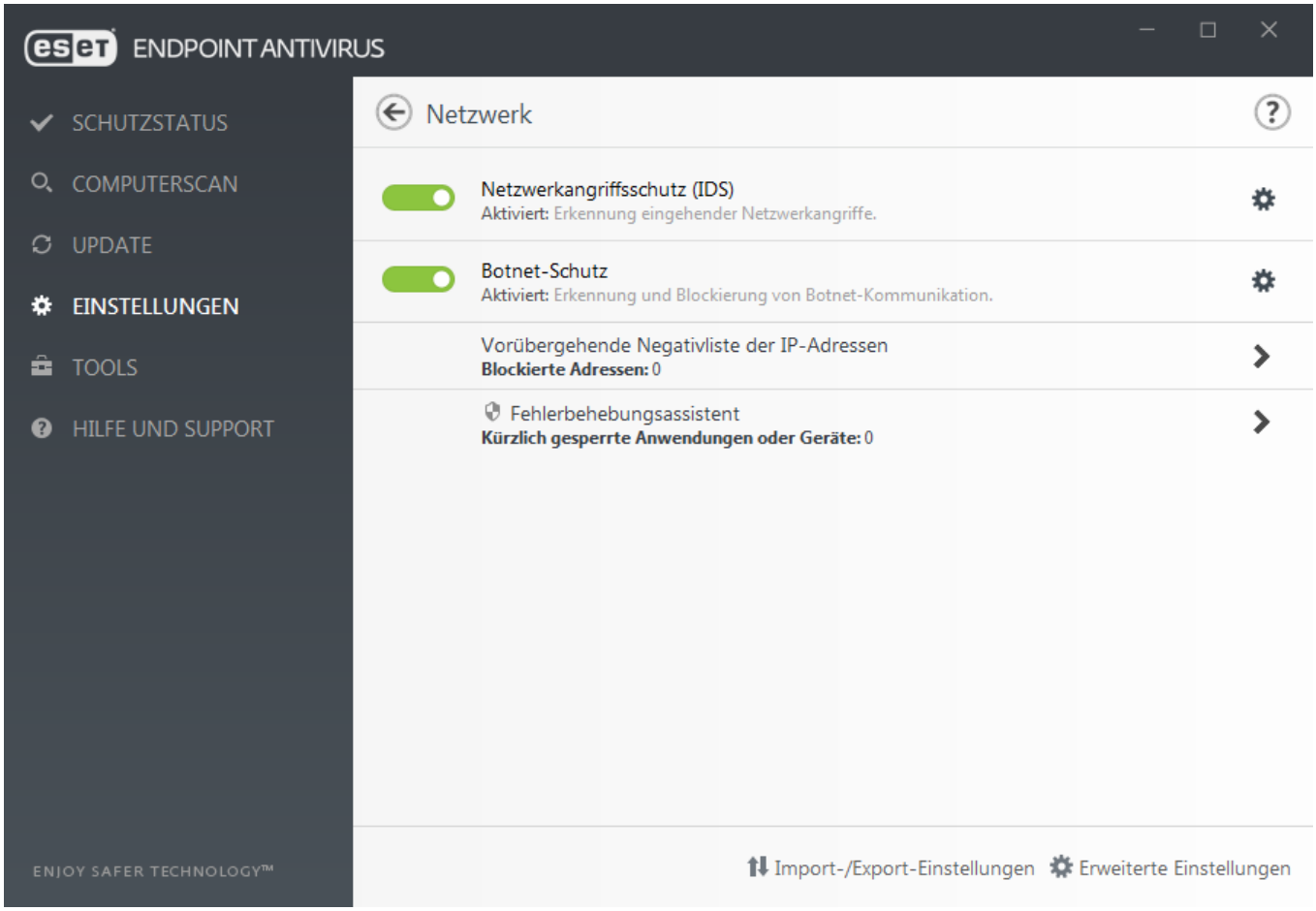
Im Bereich **Netzwerk** können Sie auf die folgenden Komponenten oder Einstellungen aus den erweiterten Einstellungen zugreifen:

- **Netzwerkangriffsschutz (IDS)** - Analysiert den Inhalt des Netzwerkverkehrs und schützt vor Netzwerkangriffen. Jeglicher als schädlich erkannter Verkehr wird blockiert. ESET Endpoint Antivirus informiert Sie, wenn Sie sich mit einem gar nicht oder nur schwach geschützten WLAN-Netzwerk verbinden.

- **Botnet-Erkennung** - Erkennt Schadsoftware auf dem System schnell und präzise. Sie können den Botnet-Schutz für eine bestimmte Dauer deaktivieren, indem Sie auf  klicken. (nicht empfohlen)

- **Vorübergehende Negativliste der IP-Adressen** - Zeigt eine Liste von IP-Adressen an, die als Angriffsquellen identifiziert und zur Negativliste hinzugefügt wurden, um die Verbindung für einen bestimmten Zeitraum zu unterbinden. Für weitere Informationen klicken Sie auf diese Option und drücken Sie die Taste F1.

- **Fehlerbehebungsassistent** – Hilft Ihnen bei der Lösung von Konnektivitätsproblemen, die von der ESET Firewall verursacht wurden. Weitere ausführliche Informationen finden Sie unter Fehlerbehebungsassistent.



Netzwerkangriffsschutz

Schutz vor Netzwerkangriffen (IDS) - Analysiert den Inhalt von Netzwerkverkehr und schützt vor Angriffen aus dem Netzwerk. Jeglicher als schädlich erkannter Verkehr wird blockiert.

Botnet-Erkennung aktivieren - Erkennt auf der Grundlage üblicher Muster die Kommunikation mit schädlichen Steuerungszentralen und blockiert sie auf einem infizierten Computer, wenn ein Bot versucht, zu kommunizieren.Weitere Informationen zur Botnet-Erkennung finden Sie im Glossar.

IDS-Ausnahmen – Mit dieser Option können Sie erweiterte Filtereinstellungen festlegen, um verschiedene Angriffsstrategien auf Ihren Computer zu erkennen.

Erweiterte Filteroptionen

Im Abschnitt „Netzwerkangriffsschutz“ können Sie erweiterte Filteroptionen konfigurieren, um verschiedene Arten von Angriffen und mögliche Schwachstellen auf Ihrem Computer zu erkennen.

Benachrichtigungen und Logging

In bestimmten Fällen erhalten Sie keinen Hinweis zum gesperrten Datenverkehr. Im Abschnitt Erstellen von Logs und Erstellen von Regeln oder Ausnahmen anhand des Logs finden Sie Anweisungen dazu, wie Sie den gesamten blockierten Datenverkehr im Firewall-Log anzeigen.



Verfügbarkeit bestimmter Optionen in dieser Hilfeseite

Die Verfügbarkeit bestimmter Optionen in den erweiterten Einstellungen (**F5**) > **Netzwerkschutz** > **Netzwerkangriffsschutz** hängt von der Art und Version Ihres ESET-Endpunktprodukts und Ihres Firewall-Moduls sowie von der Version Ihres Betriebssystems ab. Manche Optionen sind nur für ESET Endpoint Security verfügbar.

Eindringversuche erkennen

- **SMB-Protokoll** - Erkennt und blockiert verschiedene Sicherheitsprobleme im SMB-Protokoll:
  - **Angriffe über manipulierte Authentifizierungs-Challenge erkennen** - Schützt Sie vor einem Angriff mit einer manipulierten Authentifizierungs-Challenge zum Abschöpfen von Anmeldedaten.
  - **IDS-Umgehungsversuche beim Öffnen von Named Pipes erkennen**– Erkennung bekannter Umgehungsversuche für MSRPC-Named Pipes im SMB-Protokoll.
  - **CVE-Erkennungsmethoden** („Common Vulnerabilities and Exposures“, übliche Schwachstellen und Gefahren) – Bereitgestellte Erkennungsmethoden für verschiedene Angriffe, Formulare, Sicherheitslücken und Exploits über das SMB-Protokoll. Weitere Informationen zu CVE-Identifizierungen finden Sie auf der CVE-Website auf cve.mitre.org.
- **RPC-Protokoll** - Erkennt und blockiert verschiedene CVEs im RPC-System, die für die Umgebung für verteilte Datenverarbeitung (DCE) entwickelt wurden.
- **RDP-Protokoll**– Erkennt und blockiert verschiedene CVEs im RDP-Protokoll (siehe weiter oben).
- **Unsichere Adresse nach erkanntem Angriff blockieren** - Fügt IP-Adressen, die als Angriffsquellen identifiziert wurden, zur Negativliste hinzu, um die Verbindung für einen bestimmten Zeitraum zu unterbinden.
- **Hinweis bei erkanntem Angriff anzeigen** - Aktiviert die Hinweise im Infobereich der Taskleiste rechts unten auf dem Bildschirm.
- **Benachrichtigung auch bei eingehenden Angriffen auf Sicherheitslücken anzeigen** - Zeigt eine Benachrichtigung an, wenn Angriffe auf Sicherheitslücken erkannt werden oder eine Bedrohung versucht, auf diese Weise in das System zu gelangen.

Paketprüfung

- **Eingehende Verbindungen zu administrativen Freigaben per SMB-Protokoll zulassen** - Administrative Freigaben (admin shares) sind Standard-Netzwerkfreigaben für Festplattenpartitionen (*C$*, *D$*, ...) im System zusammen mit dem Systemordner (*ADMIN$*). Die Deaktivierung von Verbindungen zu den administrativen Freigaben unterbindet zahlreiche Sicherheitsrisiken. Der Conficker-Wurm verwendet beispielsweise Wörterbuchangriffe, um sich mit administrativen Freigaben zu verbinden.
- **Alte (nicht unterstützte) SMB-Dialekte blockieren** - SMB-Sitzungen mit alten SMB-Dialekten verhindern, die nicht von IDS unterstützt werden. Moderne Windows-Systeme unterstützen alte SMB-Dialekte aus Kompatibilitätsgründen mit alten Systemen wie z. B. Windows 95. Ein Angreifer kann einen alten Dialekt in einer SMB-Sitzung verwenden, um die Datenprüfung zu umgehen. Blockieren Sie alte SMB-Dialekte, wenn Ihr Computer keine Dateien mit alten Windows-Versionen teilen (oder SMB-Kommunikation allgemein verwenden) muss.

- **SMB-Sitzungen ohne erweiterte Sicherheitsfunktionen blockieren** - Erweiterte Sicherheit kann in SMB-Sitzungen verwendet werden, um einen sichereren Authentifizierungsmechanismus im Vergleich zur LAN Manager Challenge/Response (LM)-Methode zu erhalten. Die LM-Methode gilt als schwach und sollte daher nicht verwendet werden.

- **Verbindungen zur Sicherheitskontenverwaltung (SAM) zulassen** - Weitere Informationen zu diesem Dienst finden Sie unter [MS-SAMR].

- **Verbindungen zur Local Security Authority (LSASS) zulassen** - Weitere Informationen zu diesem Dienst finden Sie unter [MS-LSAD] und [MS-LSAT].

- **Verbindungen zum Dienst „Remoteregistrierung“ zulassen** - Weitere Informationen zu diesem Dienst finden Sie unter [MS-SAMR].

- **Verbindungen zum Service Control Manager (SCM) zulassen** - Weitere Informationen zu diesem Dienst finden Sie unter [MS-SAMR].

- **Verbindungen zum Serverdienst zulassen** - Weitere Informationen zu diesem Dienst finden Sie unter [MS-SAMR].

- **Verbindungen zu anderen Diensten zulassen** – MSRPC ist die Microsoft-Implementierung des DCE RPC-Mechanismus. MSRPC kann außerdem Named Pipes aus dem SMB-Protokoll für den Transport verwenden (ncacn_np transport). MSRPC-Services bieten Schnittstellen für den Fernzugriff und die Verwaltung von Windows-Systemen. Es wurden zahlreiche Schwachstellen im Microsoft MSRPC-System entdeckt und ausgenutzt (Conficker-Wurm, Sasser-Wurm usw). Deaktivieren Sie die Kommunikation mit nicht benötigten MSRPC-Diensten, um zahlreiche Sicherheitsrisiken auszuschließen (z. B. Remote Code Execution oder Service Failure-Angriffe).

- **TCP-Verbindungsstatus prüfen–** Überprüft, ob alle TCP-Pakete zu einer vorhandenen Verbindung gehören. Wenn ein Paket zu keiner Verbindung gehört, wird es verworfen.

- **Inaktive TCP-Verbindungen aufrechterhalten** - Zur ordnungsgemäßen Funktion einiger Anwendungen ist es erforderlich, dass die hergestellte TCP-Verbindung auch dann aufrechterhalten bleibt, wenn sie möglicherweise inaktiv ist. Aktivieren Sie diese Option, um zu vermeiden, dass inaktive TCP-Verbindungen beendet werden.

- **Denial of Service-Angriff auf TCP-Ebene erkennen** – Bei dieser Methode wird der Computer/Server mehreren Anfragen ausgesetzt. Siehe auch Abschnitt DoS (Denial of Service-Angriffe).

- **ICMP-Nachrichten prüfen** - Verhindert Angriffe, die Schwachstellen des ICMP-Protokolls ausnutzen, was zu Problemen mit dem Systemreaktionsverhalten des Computers führen kann - siehe auch DoS (Denial of Service-Angriffe).

- **Im ICMP-Protokoll verborgene Daten (covert channel) entdecken–** Prüft, ob über ICMP Daten übermittelt werden. Viele Schadcode-Methoden nutzen das ICMP-Protokoll, um die Firewall zu umgehen.

Eine aktualisierte Version dieser Hilfeseite finden Sie in diesem ESET-Knowledgebase-Artikel.

IDS-Ausnahmen

Es kann vorkommen, dass der Netzwerkangriffsschutz (IDS) die Kommunikation zwischen Routern oder anderen internen Netzwerkgeräten als potenziellen Angriff meldet. Sie können als sicher bekannte Adressen zu den IDS-Ausschlüssen hinzufügen, um den IDS zu umgehen.

Illustrierte Anweisungen

Die folgenden Artikel in der ESET-Knowledgebase sind möglicherweise nur auf Englisch verfügbar:

- Erstellen von IDS-Ausnahmen auf Client-Arbeitsstationen in ESET Endpoint Antivirus
- Erstellen von IDS-Ausnahmen für Client-Arbeitsstationen in ESET Security Management Center

Spalten

- **Warnung**- Art der Warnung.
- **Anwendung** - Wählen Sie den Pfad einer Anwendung aus, indem Sie auf **...** klicken (zum Beispiel *C:\Program Files\Firefox\Firefox.exe*), um eine Ausnahme zu erstellen. Geben Sie NICHT den Namen der Anwendung ein.
- **Remote-IP**- Eine Liste von Remote-IPv4- oder IPv6-Adressen, Adressbereichen oder Subnetzen. Mehrere Adressen müssen durch ein Komma voneinander getrennt sein.
- **Blockieren**- Jeder Systemprozess hat ein eigenes Standardverhalten und eine eigene zugewiesene Aktion (Blockieren oder Zulassen). Wenn Sie das Standardverhalten für ESET Endpoint Antivirus umgehen möchten, können Sie im Dropdown-Menü die entsprechende Aktion auswählen.
- **Benachrichtigen** - Wählen Sie **Ja** aus, um Desktophinweise auf Ihrem Computer anzuzeigen. Wählen Sie **Nein** aus, falls Sie keine Desktophinweise erhalten möchten. Mögliche Werte sind **Standard**/**Ja**/**Nein**.
- **Log** - Wählen Sie **Ja** aus, um Ereignisse in die ESET Endpoint Antivirus-Log-Dateien zu schreiben. Wählen Sie **Nein** aus, falls Sie keine Ereignisse loggen möchten. Mögliche Werte sind **Standard**/**Ja**/**Nein**.

IDS-Ausnahmen verwalten

- **Hinzufügen** - Erstellen einer neuen IDS-Ausnahme
- **Bearbeiten** - Bearbeiten einer bestehenden IDS-Ausnahme
- **Entfernen** - Entfernen des bzw. der ausgewählten Ausnahmen aus der Liste der IDS-Ausnahmen.
-  **Oben/Nach oben/Nach unten/Unten**- Ermöglicht das Einstellen der Priorität von Ausnahmen (die Ausnahmen werden von oben nach unten bewertet).

Beispiel

Sie möchten bei jedem Vorkommnis des Ereignisses eine Benachrichtigung anzeigen und einen Log-Eintrag erstelle:

1.Klicken Sie auf **Hinzufügen**, um eine neue IDS-Ausnahme hinzuzufügen.
2.Wählen Sie eine bestimmte Warnung im Dropdown-Menü **Warnung** aus.
3.Klicken Sie auf **...** und wählen Sie den Dateipfad der Anwendung aus, für die Sie eine Benachrichtigung einrichten möchten.
4.Lassen Sie den Wert **Standard** im Dropdown-Menü **Sperren** ausgewählt. Auf diese Weise wird die Standardaktion von ESET Endpoint Antivirus vererbt.
5.Wählen Sie in den Dropdown-Menüs **Benachrichtigen** und **Log** jeweils den Wert **Ja** aus.
6.Klicken Sie auf **OK**, um die Benachrichtigung zu speichern.

Beispiel

Sie möchten wiederkehrende Benachrichtigungen für eine Warnung entfernen, die Sie nicht als Bedrohung einstufen:

1.Klicken Sie auf **Hinzufügen**, um eine neue IDS-Ausnahme hinzuzufügen.
2.Wählen Sie eine bestimmte Warnung im Dropdown-Menü **Warnung** aus, zum Beispiel **SMB-Sitzung ohne Sicherheitserweiterungen** oder.
3.Wählen Sie **Eingehend** im Dropdown-Menü „Richtung“ aus, falls es sich um eine eingehende Kommunikation handelt.
4.Wählen Sie im Dropdown-Menü **Benachrichtigen** die Option **Nein** aus.
5.Wählen Sie im Dropdown-Menü **Log** die Option **Ja** aus.
6.Lassen Sie das Feld **Anwendung** leer.
7.Falls die Kommunikation nicht von einer bestimmten IP-Adresse stammt, lassen Sie das Feld **Remote-IP-Adressen** leer.
8.Klicken Sie auf **OK**, um die Benachrichtigung zu speichern.

Verdächtige Bedrohung blockiert

Diese Situation kann auftreten, wenn eine Anwendung auf dem Computer versucht, unter Ausnutzung einer Sicherheitslücke schädlichen Verkehr an einen anderen Computer im Netzwerk zu übertragen, oder wenn versucht wird, Ports zu scannen.

Bedrohung - Name der Bedrohung

Quelle– Quell-Netzwerkadresse

Ziel– Ziel-Netzwerkadresse

Nicht mehr blockieren - Erstellt eine IDS-Ausnahme für die verdächtige Bedrohung und bietet Einstellungen zum Zulassen der Kommunikation.

Weiterhin blockieren - Blockiert die erkannte Bedrohung. Um eine IDS-Ausnahme mit der Einstellung zum Blockieren der Kommunikation für diese Bedrohung zu erstellen, wählen Sie **Nicht mehr benachrichtigen** aus.

Hinweis

Die in diesem Benachrichtigungsfenster angezeigten Informationen hängen von der Art der erkannten Bedrohung ab.
Weitere Informationen zu Bedrohungen und anderen verwandten Begriffen finden Sie unter Angriffe und Arten von Ereignissen.

Fehlerbehebung für den Netzwerkschutz

Der Fehlerbehebungsassistent hilft Ihnen bei der Lösung von Konnektivitätsproblemen, die von der ESET Firewall verursacht wurden. Wählen Sie im Dropdownmenü einen Zeitraum aus, in dem die betreffende Kommunikation gesperrt wurde. Die Liste der kürzlich gesperrten Kommunikationen bietet eine Übersicht über Arten von Anwendungen und Geräten, Reputation und die Gesamtzahl der in diesem Zeitraum gesperrten Anwendungen und Geräte. Klicken Sie auf **Details**, um mehr Informationen zur gesperrten Kommunikation anzuzeigen. Anschließend können Sie die Anwendung bzw. das Gerät freischalten, in der/dem die Verbindungsprobleme aufgetreten sind.

Wenn Sie auf **Entsperren** klicken, wird die zuvor gesperrte Kommunikation erlaubt. Falls weiterhin Probleme mit einer Anwendung auftreten, oder Ihr Gerät nicht wie gewünscht funktioniert, klicken Sie auf **Die Anwendung funktioniert immer noch nicht**, um sämtliche zuvor gesperrte Kommunikation für das entsprechende Gerät zu erlauben. Starten Sie den Computer neu, falls das Problem weiterhin auftritt.

Klicken Sie auf **Änderungen anzeigen**, um die vom Assistenten erstellten Regeln anzuzeigen. Sie finden die vom Assistenten erstellten Regeln auch unter **Erweiterte Einstellungen** > **Netzwerkschutz** > **Firewall** > **Erweitert** > **Regeln**.

Klicken Sie auf **Weitere entsperren, um Kommunikationsprobleme mit weiteren Geräten oder Anwendungen zu beheben.**

Vorübergehende Negativliste der IP-Adressen

IP-Adressen, die als Angriffsquellen identifiziert wurden, werden zur Negativliste hinzugefügt, um die Verbindung für einen bestimmten Zeitraum zu unterbinden. Sie finden diese Adressen in ESET Endpoint Antivirus unter **Einstellungen** > **Netzwerkschutz** > **Vorübergehende Negativliste für IP-Adressen**.

Spalten

IP-Adresse – zeigt eine blockierte IP-Adresse an.

Grund für Blockierung – Zeigt die Angriffsart an, die von dieser Adresse verhindert wurde (z. B. TCP Portscanning-Angriff).

Zeitüberschreitung – Zeigt den Zeitpunkt an, zu dem die Adresse aus der Negativliste entfernt wird.

Steuerelemente

Entfernen – Entfernt eine Adresse vor Ablauf der Zeitüberschreitung aus der Negativliste.

Alle entfernen – Entfernt alle Adressen sofort aus der Negativliste.

Ausnahme hinzufügen – Fügt eine Firewall-Ausnahme zum IDS-Filter hinzu.

Lösen von Problemen mit der ESET Firewall

Wenn bei Computern, auf denen ESET Endpoint Antivirus installiert ist, Konnektivitätsprobleme auftreten, kann auf mehrere Arten festgestellt werden, ob die ESET Firewall die Ursache dafür ist. Darüber hinaus kann Ihnen die ESET Firewall bei der Erstellung neuer Regeln oder Ausnahmen helfen, um Konnektivitätsprobleme zu vermeiden.

In den folgenden Themen finden Sie Hilfe bei Problemen mit der ESET Firewall:

- Fehlerbehebungsassistent
- Erstellen von Logs und Erstellen von Regeln oder Ausnahmen anhand des Logs
- Erstellen von Ausnahmen von Firewall-Hinweisen
- Erweitertes PCAP-Logging

- Lösen von Problemen bei der Protokollfilterung

Fehlerbehebungsassistent

Der Feherbehebungsassistent überwacht im Hintergrund alle blockierten Verbindungen und begleitet Sie durch den Fehlerbehebungsprozess, um Firewall-Probleme bei bestimmten Anwendungen oder Geräten zu lösen. Anschließend schlägt der Assistent eine neue Reihe von Regeln vor, die angewendet werden, wenn Sie sie genehmigen. Der **Fehlerbehebungsassistent** befindet sich im Hauptmenü unter **Einstellungen** > **Netzwerk**.

Erstellen von Logs und Erstellen von Regeln oder Ausnahmen anhand des Logs

Die ESET Firewall protokolliert standardmäßig nicht alle blockierten Verbindungen. Um die von der Firewall blockierten Verbindungen zu sehen, aktivieren Sie das erweiterte Logging für den Netzwerkschutz im Bereich **Diagnose** unter **Erweiterte Einstellungen** > **Tools** > **Diagnose**. Wenn die Log-Datei Einträge enthält, die nicht blockiert werden sollen, können Sie eine Regel oder eine IDS-Ausnahme erstellen. Klicken Sie dazu mit der rechten Maustaste auf den entsprechenden Eintrag und wählen Sie **Ähnliche Ereignisse zukünftig nicht blockieren** aus. Bedenken Sie, dass das Log aller blockierten Verbindungen möglicherweise Tausende von Einträgen enthält und bestimmte Verbindungen somit schwer zu finden sind. Deaktivieren Sie die Log-Erstellung daher, nachdem Sie Ihr Problem gelöst haben.

Weitere Informationen zum Log finden Sie unter Log-Dateien.

> **Hinweis**
> In den Log-Dateien können Sie die Reihenfolge erkennen, in der die Firewall bestimmte Verbindungen blockiert hat. Außerdem können Sie anhand des Logs Regeln erstellen, die sich genau so verhalten, wie Sie es wünschen.

Regel aus Log erstellen

Mit der neuen Version von ESET Endpoint Antivirus können Sie eine Regel im Log erstellen. Klicken Sie im Hauptmenü auf **Tools** > **Log-Dateien**. Wählen Sie **Netzwerkschutz** im Dropdownmenü aus, klicken Sie mit der rechten Maustaste auf den gewünschten Log-Eintrag und wählen Sie **Ähnliche Ereignisse zukünftig nicht blockieren** im Kontextmenü aus. Die neue Regel wird in einem Hinweisfenster angezeigt.

Für die Erstellung neuer Regeln aus dem Log müssen die folgenden Einstellungen in ESET Endpoint Antivirus vorgenommen werden:

- Stellen Sie die Mindestinformation in Logs in **Erweiterte Einstellungen** (F5) > **Tools** > **Log-Dateien** auf **Diagnose** ein.

- Aktivieren Sie die Option **Benachrichtigung auch bei eingehenden Angriffen auf Sicherheitslücken anzeigen** unter **Erweiterte Einstellungen** (F5) > **Netzwerkschutz** > **Netzwerkangriffsschutz** > **Erweiterte Optionen** > **Eindringversuche erkennen**.

Erstellen von Ausnahmen von Firewall-Hinweisen

Wenn die ESET Firewall schädliche Netzwerkaktivitäten erkennt, wird ein Hinweisfenster mit einer Beschreibung des Ereignisses angezeigt. Dieser Hinweis enthält ein Link, der weitere Informationen zum Ereignis enthält und unter dem Sie ggf. eine Ausnahme für dieses Ereignis erstellen können.



Hinweis
Wenn eine Netzwerkanwendung oder ein Gerät Netzwerkstandards nicht ordnungsgemäß implementiert, kann dies dazu führen, dass wiederholte IDS-Hinweise zur Firewall angezeigt werden. Damit die ESET Firewall diese Anwendung bzw. dieses Gerät künftig nicht mehr erkennt, können Sie direkt im Hinweis eine Ausnahme erstellen.

Erweitertes PCAP-Logging

Diese Funktion dient dazu, komplexere Log-Dateien für den ESET-Kundendienst zu liefern. Verwenden Sie sie nur, wenn Sie vom ESET-Kundendienst dazu aufgefordert werden, da hiermit eine möglicherweise sehr große Log-Datei erstellt wird, die die Leistung Ihres Computers beeinträchtigt.

1. Navigieren Sie zu **Erweiterte Einstellungen** > **Tools** > **Diagnose**, und aktivieren Sie die Option **Erweitertes Logging für Protokollfilterung aktivieren**.

2. Versuchen Sie, das aufgetretene Problem zu reproduzieren.

3. Deaktivireren Sie das erweiterte PCAP-Logging.

4. Die PCAP-Log-Datei befindet sich im selben Verzeichnis, in dem Speicherabbilder zur Diagnose erzeugt werden:

- Microsoft Windows Vista oder neuer

C:\ProgramData\ESET\ESET Security\Diagnostics

- Microsoft Windows XP

C:\Dokumente und Einstellungen\Alle Benutzer\...

Lösen von Problemen bei der Protokollfilterung

Wenn Sie Probleme mit dem Browser oder dem E-Mail-Programm haben, überprüfen Sie als erstes, ob die Ursache dafür möglicherweise die Protokollfilterung ist. Deaktivieren Sie hierfür vorübergehend die Anwendungsprotokollfilterung in den erweiterten Einstellungen. Denken Sie daran, sie anschließend wieder zu aktivieren, da Browser un E-Mail-Programm ansonsten nicht geschützt sind. Wenn das Problem hiermit behoben ist, finden Sie nachstehend eine Liste gängiger Probleme nebst deren Lösung:

Probleme mit Updates oder sicheren Verbindungen

Wenn Ihre Anwendung nicht aktualisiert werden kann oder ein Kommunikationskanal nicht sicher ist:

- Wenn die SSL-Protokollfilterung aktiviert ist, deaktivieren Sie sie vorübergehend. Wenn das Problem damit behoben ist, können Sie die SSL-Filterung aktiviert lassen und das Update durch Ausschließen der problematischen Verbindung anwenden:
Setzen Sie den SSL-Protokollfiltermodus auf „interaktiv“. Führen Sie das Update erneut aus. Es sollte ein Dialogfeld angezeigt werden, in dem Sie über verschlüsselten Datenverkehr informiert werden. Vergewissern Sie sich, dass die Anwendung mit jener übereinstimmt, bei der Sie Fehler beheben und dass das Zertifikat von dem Server stammt, von dem auch das Update stammt. Speichern Sie anschließend die Aktion zu diesem Zertifikat und klicken Sie auf „Ignorieren“. Wenn weitere Dialogfelder angezeigt werden, können Sie den Filtermodus wieder auf „automatisch“ setzen. Das Problem sollte nun behoben sein.

- Wenn es sich bei der Anwendung nicht um einen Browser oder ein E-Mail-Programm handelt, können Sie sie komplett aus der Protokollfilterung ausschließen (ein Browser oder ein E-Mail-Programm wäre in diesem Fall ungeschützt). Anwendungen, deren Kommunikation bereits in der Vergangenheit gefiltert wurde, sollten sich bereits in der Liste befinden, die bei Hinzufügen einer Ausnahme angezeigt wird, somit brauchen sie wahrscheinlich nicht manuell hinzugefügt werden.

Problem beim Zugriff auf ein Gerät im Netzwerk

Wenn die Funktionen eines Geräts im Netzwerk nicht genutzt werden können (wenn beispielsweise Webseiten einer Webcam nicht geöffnet oder Videos auf einem Home-Media-Player nicht abgespielt werden können), fügen Sie dessen IPv4- und IPv6-Adressen zur Liste der ausgeschlossenen Adressen hinzu.

Probleme mit einer bestimmten Website

Mithilfe der URL-Adressverwaltung können Sie bestimmte Websites von der Protokollfilterung ausschließen. Wenn Sie beispielsweise nicht auf https://www.gmail.com/intl/en/mail/help/about.html zugreifen können, fügen Sie *gmail.com* zur Liste der ausgeschlossenen Adressen hinzu.

Fehler „Anwendungen, welche das Root-Zertifikat importieren können, sind noch aktiv“

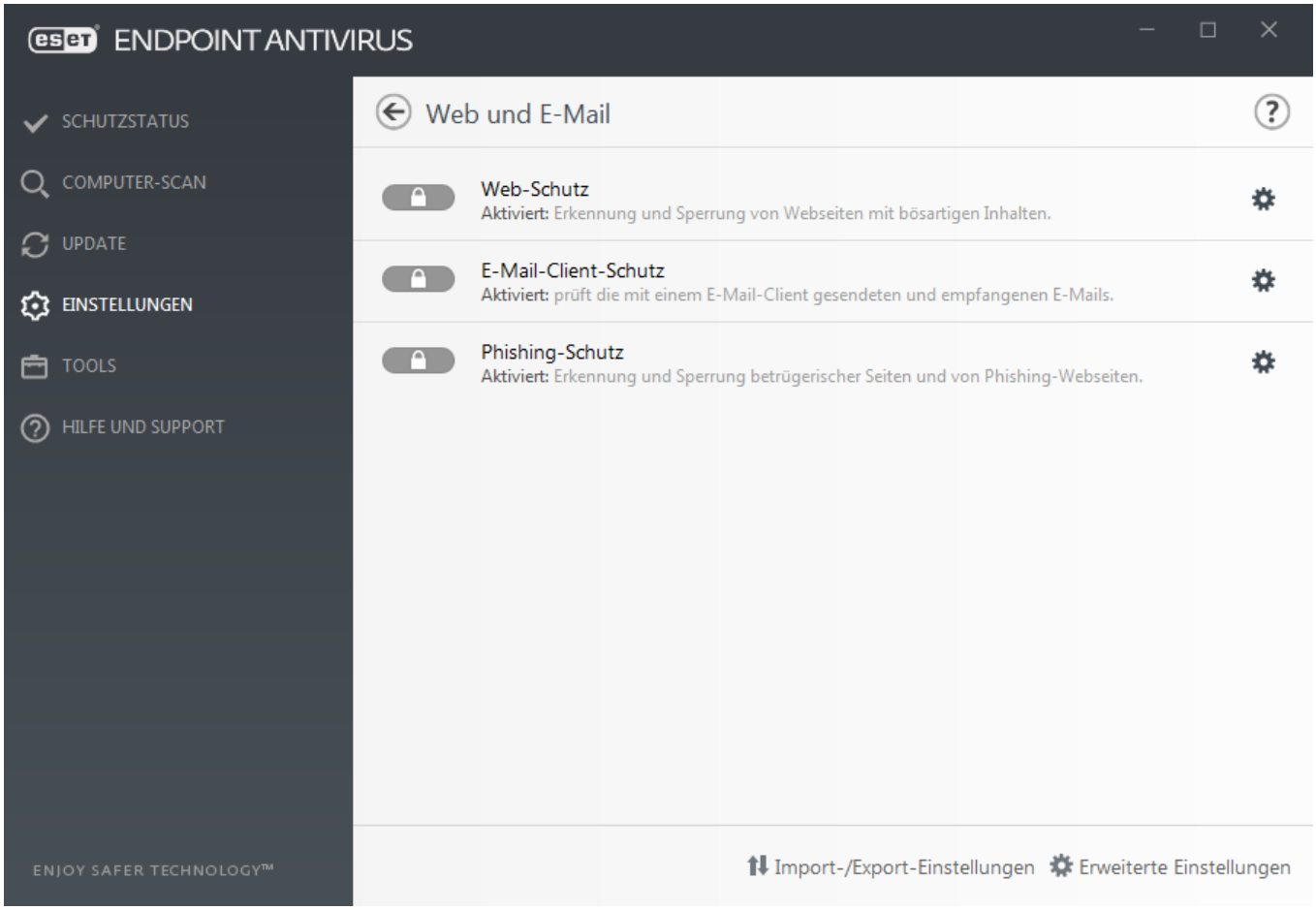
Bei Aktivierung der SSL-Protokollfilterung vergewissert sich ESET Endpoint Antivirus, dass die installierten Anwendungen der Art und Weise der Filterung von SSL-Protokollen vertrauen, indem ein Zertifikat in ihren Zertifikatspeicher importiert wird. Bei einigen Anwendungen wie Firefox und Opera ist dies nicht möglich, während sie ausgeführt werden. Vergewissern Sie sich, dass keine dieser Anwendungen ausgeführt wird (öffnen Sie hierzu den Taskmanager und stellen Sie sicher, dass sich in der Registerkarte „Prozesse“ keine Einträge mit der Bezeichnung „firefox.exe“ oder „opera.exe“ befinden) und wiederholen Sie den Vorgang.

Fehler aufgrund eines nicht vertrauenswürdigen Ausstellers oder einer ungültigen Signatur

Dies bedeutet in den meisten Fällen, dass der oben beschriebene Zertifikatimport fehlgeschlagen ist. Vergewissern Sie sich, dass keine der genannten Anwendungen ausgeführt wird. Deaktivieren Sie anschließend die SSL-Protokollfilterung und aktivieren Sie sie erneut. Hiermit wird der Import erneut durchgeführt.

Web und E-Mail

Die Web- und E-Mail-Konfiguration befindet sich unter **Einstellungen** > **Web und E-Mail**. Von hier aus können Sie auf erweiterte Einstellungen des Programms zugreifen.



Der Internetzugang ist eine Standardfunktion von Computern. Leider ist das Internet mittlerweile auch der wichtigste Weg zur Verbreitung von Schadsoftware. Daher müssen Sie die Einstellungen des **Web-Schutzes** sorgfältig auswählen.

Der **E-Mail-Client-Schutz** dient der Überwachung eingehender E-Mails, die mit dem POP3(S)- und IMAP(S)-Protokollen übertragen werden. Mithilfe der Plug-In-Software für Ihr E-Mail-Programm stellt ESET Endpoint Antivirus Kontrollfunktionen für die gesamte E-Mail-Kommunikation bereit.

Phishing-Schutz stellt eine weitere, verstärkte Schutzebene vor unseriösen Webseiten dar, die versuchen, Passwörter und andere sicherheitsrelevante Daten in Erfahrung zu bringen. Der Phishing-Schutz befindet sich im Bereich **Einstellungenunter Web und E-Mail**. Weitere Informationen finden Sie unter Phishing-Schutz.

Sie können den Web-/E-Mail-/Phishing Schutz kann durch Klicken auf  vorübergehend deaktivieren.

Prüfen von Anwendungsprotokollen

Das ThreatSense-Scan-Modul bietet Virenschutz für Anwendungsprotokolle und integriert alle erweiterten Malware-Scanmethoden nahtlos. Die Protokollprüfung erfolgt unabhängig vom Webbrowser oder E-Mail-Client. Sie können die Verschlüsselungseinstellungen (SSL) unter **Erweiterte Einstellungen** (F5) > **Web und E-Mail** >

SSL/TLS bearbeiten.

Prüfen von anwendungsspezifischen Protokollen aktivieren - Hiermit kann die Protokollprüfung deaktiviert werden. Bedenken Sie jedoch, dass zahlreiche Komponenten von ESET Endpoint Antivirus wie Web-Schutz, E-Mail-Schutz, Phishing-Schutz und Web-Kontrolle von dieser Option abhängen und ohne sie nicht ordnungsgemäß funktionieren.

Ausgeschlossene Anwendungen - Ermöglicht das Ausschließen bestimmter Anwendungen von der Protokollprüfung. Diese Option ist nützlich, wenn es aufgrund der Protokollprüfung zu Kompatibilitätsproblemen kommt.

Ausgeschlossene IP-Adressen - Ermöglicht das Ausschließen bestimmter Remote-Adressen von der Protokollprüfung. Diese Option ist nützlich, wenn es aufgrund der Protokollprüfung zu Kompatibilitätsproblemen kommt.

Beispiel für ausgeschlossene IP-Adressen

IPv4-Adressen und Maske:

- *192.168.0.10* – Hinzufügen der IP-Adresse eines einzelnen Computers, auf den die Regel angewendet werden soll.
- *192.168.0.1* bis *192.168.0.99* – Geben Sie die Start- und Endadresse eines Bereichs von IP-Adressen ein (von mehreren Computern), auf die die Regel angewendet werden soll.
- Subnetz (eine Gruppe von Computern) mit einer IP-Adresse und einer Maske. *255.255.255.0* ist z. B. die Netzwerkmaske für das Präfix *192.168.1.0/24* und steht für den Adressbereich *192.168.1.1* bis 192.168.1.254.

IPv4-Adresse und Maske:

- *2001:718:1c01:16:214:22ff:fec9:ca5* - Die IPv6-Adresse eines einzelnen Computers, auf den die Regel angewendet werden soll.
- *2002:c0a8:6301:1::1/64* - Eine IPv6-Adresse mit einer Präfixlänge von 64 Bit, also *2002:c0a8:6301:0001:0000:0000:0000:0000 bis 2002:c0a8:6301:0001:ffff:ffff:ffff:ffff*

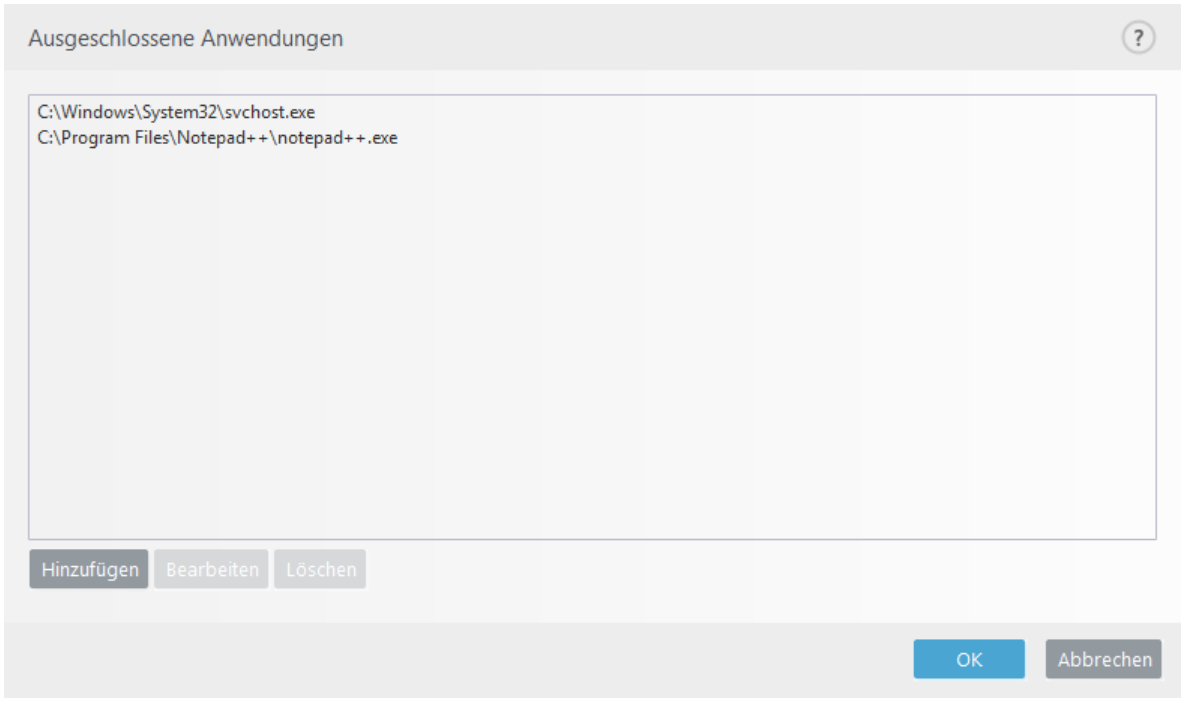
Ausgeschlossene Anwendungen

Netzwerk-Anwendungen, für deren Datenkommunikation keine Protokollprüfung erfolgen soll, können Sie dieser Liste hinzufügen. Dies schließt die HTTP/POP3/IMAP-Datenkommunikation ausgewählter Anwendungen von der Prüfung auf Bedrohungen aus. Es wird empfohlen, diese Technik nur anzuwenden, wenn Anwendungen bei aktivierter Protokollprüfung nicht ordnungsgemäß funktionieren.

Anwendungen und Dienste, die von der Protokollprüfung bereits betroffen waren, werden nach dem Klicken auf **Hinzufügen** automatisch angezeigt.

Bearbeiten - Bearbeiten von ausgewählten Einträgen in der Liste.

Entfernen - Entfernt ausgewählte Einträge aus der Liste.



Ausgeschlossene IP-Adressen

Die IP-Adressen in dieser Liste werden von der Prüfung von Protokollen ausgenommen. Die HTTP/POP3/IMAP-Datenkommunikation von/an die ausgewählten Adressen wird nicht auf Bedrohungen geprüft. Wir empfehlen, diese Option nur für Adressen zu aktivieren, die als vertrauenswürdig bekannt sind.

Hinzufügen - Hier können Sie eine IP-Adresse, einen Bereich von Adressen oder ein Subnetz für die Gegenstelle festlegen, die von der Regel erfasst wird.

Bearbeiten - Bearbeiten von ausgewählten Einträgen in der Liste.

Entfernen - Entfernt ausgewählte Einträge aus der Liste.



SSL/TLS

ESET Endpoint Antivirus kann Verbindungen, die das SSL-Protokoll verwenden, auf Bedrohungen untersuchen. Für die Untersuchung von durch SSL geschützten Verbindungen gibt es verschiedene Prüfmodi mit vertrauenswürdigen und unbekannten Zertifikaten sowie Zertifikaten, die von der Prüfung SSL-geschützter Verbindungen ausgeschlossen sind.

SSL/TLS-Protokollfilterung aktivieren - Die Protokollfilterung ist standardmäßig aktiviert. Sie können die SSL/TLS-Protokollfilterung unter **Erweiterte Einstellungen** > **Web und E-Mail** > **SSL/TLS** oder mit einer Policy deaktivieren. Wenn die Protokollfilterung deaktiviert ist, werden SSL-Verbindungen nicht gescannt.

Für den SSL/TLS-Protokollfiltermodus sind folgende Optionen verfügbar:

Filtermodus	Beschreibung
Automatischer Modus	Der Standardmodus prüft nur relevante Anwendungen wie Webbrowser und E-Mail-Clients. Sie können zusätzliche Anwendungen auswählen, deren Kommunikation geprüft werden soll.
Interaktiver Modus	Bei Eingabe einer neuen, durch SSL geschützten Seite (mit unbekanntem Zertifikat) wird ein Dialogfeld mit möglichen Aktionen angezeigt. In diesem Modus können Sie eine Liste von SSL-Zertifikaten und Anwendungen erstellen, die von der Prüfung ausgeschlossen sind.
Policy-Modus	Policy-Modus – Aktivieren Sie diese Option, um jegliche SSL-geschützte Kommunikation zu prüfen, außer wenn Zertifikate verwendet werden, die von der Prüfung ausgeschlossen sind. Wird eine Verbindung mit einem unbekannten, signierten Zertifikat erstellt, so wird sie ohne gesonderten Hinweis automatisch geprüft. Wenn Sie auf einen Server mit einem nicht vertrauenswürdigen Zertifikat, das sich in der Liste der vertrauenswürdigen Zertifikate befindet und damit als vertrauenswürdig eingestuft wurde, zugreifen, wird die Kommunikation zugelassen und der Inhalt des Kommunikationskanals geprüft.

Mit der **Liste der vom SSL-Filter betroffenen Anwendungen** können Sie das Verhalten von ESET Endpoint Antivirus für bestimmte Anwendungen anpassen.

Mit der **Liste bekannter Zertifikate** können Sie das Verhalten von ESET Endpoint Antivirus für bestimmte SSL-Zertifikate anpassen.

Kommunikation mit vertrauenswürdigen Domains ausschließen – Wenn diese Option aktiviert ist, wird die Kommunikation mit vertrauenswürdigen Domänen von der Prüfung ausgeschlossen. Die Vertrauenswürdigkeit von Domains wird anhand einer integrierten Positivliste ermittelt.

Verschlüsselte Kommunikation sperren, die das obsolete Protokoll SSL v2 verwendet - Verbindungen, die die frühere Version des SSL-Protokolls verwenden, werden automatisch blockiert.

> **Hinweis**
> Wenn die Einstellung **Kommunikation mit vertrauenswürdigen Domains ausschließen** aktiviert ist und die Domäne als vertrauenswürdig gilt, werden keine Adressen gefiltert.

Stammzertifikat

Stammzertifikat - Damit die SSL-Kommunikation in Ihren Browsern/E-Mail-Programmen ordnungsgemäß funktioniert, muss das Stammzertifikat für ESET der Liste der bekannten Stammzertifikate (Herausgeber)

hinzugefügt werden. **Bekannten Browsern das Stammzertifikat hinzufügen** sollte aktiviert sein. Wählen Sie diese Option, um das ESET-Stammzertifikat automatisch zu den bekannten Browsern (z. B. Opera, Firefox) hinzuzufügen. Wenn ein Browser den Systemzertifizierungsspeicher verwendet, wird das Zertifikat automatisch hinzugefügt (z. B. Internet Explorer).

Um das Zertifikat für nicht unterstützte Browser zu übernehmen, klicken Sie auf **Zertifikat anzeigen** > **Details** > **In die Datei kopieren...**, und importieren Sie es anschließend manuell in den Browser.

Gültigkeit des Zertifikats

Falls das Zertifikat nicht über die VSZS-Zertifikatablage geprüft werden kann - In manchen Fällen kann ein Website-Zertifikat nicht über den Speicher vertrauenswürdiger Stammzertifizierungsstellen (VSZS) geprüft werden. Das bedeutet, dass jemand das Zertifikat signiert hat (z. B. der Administrator eines Webservers oder ein Kleinunternehmen). Das Zertifikat als vertrauenswürdig einzustufen, stellt nicht immer ein Risiko dar. Die meisten großen Unternehmen (z. B. Banken) verwenden Zertifikate, die von einer vertrauenswürdigen Stammzertifizierungsstelle signiert sind. Wenn die Option **Gültigkeit des Zertifikats erfragen** ausgewählt ist (Standardeinstellung), muss der Benutzer eine Aktion festlegen, die ausgeführt werden soll, wenn verschlüsselte Verbindungen aufgebaut werden. Sie können die Option **Kommunikation blockieren, die das Zertifikat verwendet** aktivieren, um verschlüsselte Verbindungen zu der Site, die nicht verifizierte Zertifikate verwendet, immer zu beenden.

Wenn das Zertifikat ungültig oder beschädigt ist – Dies bedeutet, dass es entweder abgelaufen ist oder fehlerhaft signiert wurde. Verwenden Sie in diesem Fall die Option **Kommunikation blockieren, die das Zertifikat verwendet**.



Beispiele mit Abbildungen

Die folgenden Artikel in der ESET-Knowledgebase sind möglicherweise nur auf Englisch verfügbar:

- Zertifikatbenachrichtigungen in ESET-Produkten
- Beim Aufrufen von Webseiten wird die Meldung „Verschlüsselte Netzwerkverbindung: Nicht vertrauenswürdiges Zertifikat“ angezeigt

Zertifikate

Damit die SSL-Kommunikation in Ihren Browsern/E-Mail-Programmen ordnungsgemäß funktioniert, muss das Stammzertifikat für ESET der Liste der bekannten Stammzertifikate (Herausgeber) hinzugefügt werden. **Bekannten Browsern das Stammzertifikat hinzufügen** sollte aktiviert sein. Wählen Sie diese Option, um das ESET-Stammzertifikat automatisch zu den bekannten Browsern (z. B. Opera, Firefox) hinzuzufügen. Wenn ein Browser den Systemzertifizierungsspeicher verwendet, wird das Zertifikat automatisch hinzugefügt (z. B. Internet Explorer). Um das Zertifikat für nicht unterstützte Browser zu übernehmen, klicken Sie auf **Zertifikat anzeigen** > **Details** > **In die Datei kopieren...**, und importieren Sie es anschließend manuell in den Browser.

In manchen Fällen kann das Zertifikat nicht über den Speicher vertrauenswürdiger Stammzertifizierungsstellen geprüft werden (z. B. VeriSign). Das bedeutet, dass jemand das Zertifikat selbst signiert hat (z. B. der Administrator eines Webservers oder ein Kleinunternehmen). Das Zertifikat als vertrauenswürdig einzustufen, stellt nicht immer ein Risiko dar. Die meisten großen Unternehmen (z. B. Banken) verwenden Zertifikate, die von einer vertrauenswürdigen Stammzertifizierungsstelle signiert sind. Wenn die Option **Gültigkeit des Zertifikats erfragen** ausgewählt ist (Standardeinstellung), muss der Benutzer eine Aktion festlegen, die ausgeführt werden soll, wenn verschlüsselte Verbindungen aufgebaut werden. Dazu wird ein Aktionsauswahl-Dialogfenster angezeigt, in dem Sie das Zertifikat als vertrauenswürdig markieren oder ausschließen können. Wenn das Zertifikat nicht in der Liste vertrauenswürdiger Stammzertifizierungsstellen enthalten ist, ist das Fenster rot

hinterlegt, sonst ist es grün.

Sie können die Option **Kommunikation blockieren, die das Zertifikat verwendet** auswählen, um verschlüsselte Verbindungen zu der Site, die das nicht verifizierte Zertifikat verwendet, immer zu beenden.

Wenn das Zertifikat ungültig oder beschädigt ist, ist es entweder abgelaufen oder wurde fehlerhaft selbst signiert. In diesem Fall empfehlen wir, die Verbindung, die das Zertifikat verwendet, zu blockieren.

Verschlüsselte Netzwerkverbindung

Wenn das System für SSL-Protokollüberprüfung eingerichtet ist, werden Sie in den folgenden beiden Situationen in einem Dialogfenster aufgefordert, eine Aktion auszuwählen:

Wenn eine Website ein nicht überprüfbares oder ungültiges Zertifikat verwendet und ESET Endpoint Antivirus so konfiguriert ist, dass der Benutzer in solchen Fällen gefragt werden soll (standardmäßig „ja“ bei nicht überprüfbaren und „nein“ bei ungültigen Zertifikaten), werden Sie in einem Dialogfeld aufgefordert, die Option **Zulassen** oder **Blockieren** für die Verbindung auszuwählen. Wenn sich das Zertifikat nicht im Trusted Root Certification Authorities store (Trusted Root Certification Authorities, TRCA) befindet, wird es als nicht vertrauenswürdig eingestuft.

Wenn die **SSL-Protokollüberprüfung** auf **Interaktiver Modus** eingestellt ist, werden Sie zu jeder Website in einem Dialogfeld aufgefordert, für den Datenverkehr **Scannen** oder **Ingorieren** auszuwählen. Einige Anwendungen überprüfen, ob ihr SSL-Datenverkehr von jemandem geändert oder untersucht wurde. In diesem Fall muss ESET Endpoint Antivirus den Datenverkehr **Ignorieren**, damit die Anwendung ordnungsgemäß funktioniert.



Beispiele mit Abbildungen

Die folgenden Artikel in der ESET-Knowledgebase sind möglicherweise nur auf Englisch verfügbar:

- Zertifikatbenachrichtigungen in ESET-Produkten
- Beim Aufrufen von Webseiten wird die Meldung „Verschlüsselte Netzwerkverbindung: Nicht vertrauenswürdiges Zertifikat“ angezeigt

In beiden Fällen kann der Benutzer die ausgewählte Aktion speichern. Gespeicherte Aktionen werden in der Liste bekannter Zertifikate gespeichert.

Liste bekannter Zertifikate

Mit der **Liste bekannter Zertifikate** können Sie das Verhalten von ESET Endpoint Antivirus bei bestimmten SSL-Zertifikaten anpassen und gewählte Aktionen speichern, wenn der **Interaktive Modus** unter **SSL/TLS-Protokollfilterungsmodus** ausgewählt ist. Sie können die Liste unter **Erweiterte Einstellungen** (F5) > **Web und E-Mail** > **SSL/TLS** > **Liste bekannter Zertifikate** anzeigen und bearbeiten.

Das Fenster **Liste bekannter Zertifikate** besteht aus folgendem Inhalt:

Spalten

Name- Name des Zertifikats

Zertifikataussteller- Name des Zertifikaterstellers

Zertifikatbetreff- Das Betrefffeld enthält die Entität, die mit dem öffentlichen Schlüssel verknüpft ist, welcher im entsprechenden Feld des Betreffs gespeichert ist.

Zugriff - Wählen Sie **Zulassen** oder **Blockieren** als **Zugriffsaktion**, um die von diesem Zertifikat gesicherte Verbindung unabhängig von ihrer Vertrauenswürdigkeit zuzulassen oder zu blockieren. Wählen Sie **Autom.**, wennvertrauenswürdige Zertifikate zugelassen werden sollen und bei nicht vertrauenswürdigen nachgefragt werden soll. Wählen Sie **Nachfragen**, wenn der Benutzer immer gefragt werden soll, welche Maßnahme ergriffen werden soll.

Scannen - Wählen Sie **Scannen** oder **Ignorieren**als**Prüfungsaktion**, um die von diesem Zertifikat gesicherte Verbindung zu scannen oder zu ignorieren. Wählen Sie **Autom.**, wenn im automatischen Modus geprüft und im interaktiven Modus nachgefragt werden soll. Wählen Sie **Nachfragen**, wenn der Benutzer immer gefragt werden soll, welche Maßnahme ergriffen werden soll.

Steuerelemente

Hinzufügen - Zertifikate können manuell als Dateien mit den Endungen *.cer*, *.crt* oder *.pem* geladen werden. Klicken Sie auf **Datei** um ein lokales Zertifikat hochzuladen, oder auf **URL**, um die URL eines Online-Zertifikats anzugeben.

Bearbeiten - Wählen Sie das zu konfigurierende Zertifikat aus und klicken Sie auf **Bearbeiten**.

Löschen – Wählen Sie das zu löschende Zertifikat aus und klicken Sie auf **Löschen**.

OK/Abbrechen - Klicken Sie auf **OK**, um die Änderungen zu speichern, oder auf **Abbrechen**, um den Vorgang ohne Speichern zu beenden.

Liste der vom SSL/TLS-Filter betroffenen Anwendungen

Mit der **Liste der vom SSL/TLS-Filter betroffenen Anwendungen** können Sie das Verhalten von ESET Endpoint Antivirus für bestimmte Anwendungen anpassen und ausgewählte Aktionen speichern, wenn der **Interaktive Modus** als **Filtermodus für das SSL/TLS-Protokoll** ausgewählt ist. Sie können die Liste unter **Erweiterte Einstellungen** (F5) > **Web und E-Mail** > **SSL/TLS** > **Liste der vom SSL/TLS-Filter betroffenen Anwendungen** anzeigen und bearbeiten.

Das Fenster **Liste der vom SSL-Filter betroffenen Anwendungen** enthält die folgenden Elemente:

Spalten

Anwendung– Name der Anwendung.

Scan-Aktion–Wählen Sie **Scannen** oder **Ignorieren** aus, um die Kommunikation zu scannen oder zu ignorieren. Wählen Sie **Autom.**, wenn im automatischen Modus geprüft und im interaktiven Modus nachgefragt werden soll. Wählen Sie **Nachfragen**, wenn der Benutzer immer gefragt werden soll, welche Maßnahme ergriffen werden soll.

Steuerelemente

Hinzufügen– Gefilterte Anwendung hinzufügen.

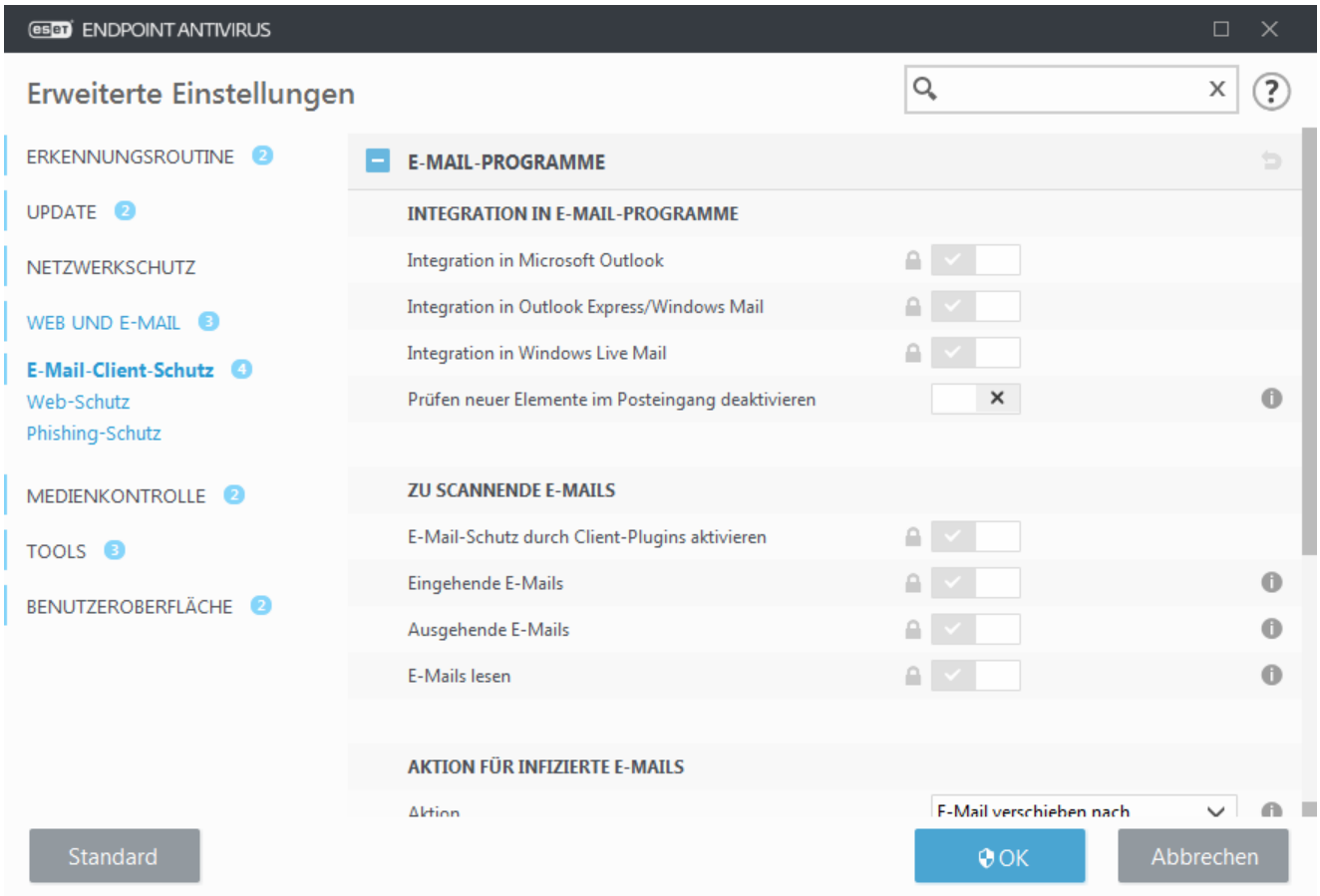
Bearbeiten– Wählen Sie das zu konfigurierende Zertifikat aus und klicken Sie auf **Bearbeiten**.

Löschen – Wählen Sie das zu löschende Zertifikat aus und klicken Sie auf **Löschen**.

OK/Abbrechen– Klicken Sie auf **OK**, um die Änderungen zu speichern, oder auf **Abbrechen**, um den Vorgang ohne Speichern zu beenden.

E-Mail-Schutz

Die Integration von ESET Endpoint Antivirus mit Ihrem E-Mail-Client verbessert den aktiven Schutz vor Schadcode in E-Mail-Nachrichten. Wenn Ihr E-Mail-Programm dies unterstützt, kann die Integration in ESET Endpoint Antivirus aktiviert werden. Mit der Integration in Ihren E-Mail-Client wird die ESET Endpoint Antivirus-Symbolleiste direkt im E-Mail-Programm angezeigt und ermöglicht einen effizienteren E-Mail-Schutz. Sie finden die Integrationseinstellungen unter **Erweiterte Einstellungen** (F5) > **Web und E-Mail** > **E-Mail-Schutz** > **E-Mail-Programme**.



Integration in E-Mail-Programme

Zu den derzeit unterstützten E-Mail-Programmen gehören Microsoft Outlook, Outlook Express, Windows Mail und Windows Live Mail. Der E-Mail-Schutz ist ein Plug-In für diese Programme. Das Plugin funktioniert unabhängig vom eingesetzten Protokoll. Wenn beim E-Mail-Client eine verschlüsselte Nachricht eingeht, wird diese entschlüsselt und an das Virenschutz-Prüfmodul weitergeleitet. Eine vollständige Liste der unterstützten E-Mail-Programme und Versionen finden Sie im entsprechenden ESET-Knowledgebase-Artikel.

Aktivieren Sie die Option **Prüfen neuer Elemente im Posteingang deaktivieren**, falls beim Abrufen von E-Mails die Systemleistung beeinträchtigt wird.

Zu scannende E-Mails

E-Mail-Schutz durch Client-Plugins aktivieren - Wenn Sie diese Funktion deaktivieren, wird der Schutz durch E-Mail-Client-Plugins deaktiviert.

Eingehende E-Mails – Wenn diese Option aktiviert ist, werden eingehende E-Mails geprüft.

Ausgehende E-Mails – Wenn diese Option aktiviert ist, werden ausgehende E-Mails geprüft.

E-Mails lesen – Wenn diese Option aktiviert ist, werden gelesene E-Mails geprüft.

> **Hinweis**
> Wir empfehlen, die Option **E-Mail-Schutz durch Client-Plugins aktivieren** aktiviert zu lassen. Selbst wenn die Integration nicht aktiviert ist oder nicht funktioniert, wird Ihre E-Mail-Kommunikation trotzdem durch die Protokollprüfung (IMAP/IMAPS und POP3/POP3S) geschützt.

Aktion für infizierte E-Mails

Keine Aktion - Infizierte Anhänge werden erkannt, aber es werden keine Aktionen für E-Mails durchgeführt.

E-Mail löschen - Es werden Hinweise zu Bedrohungen angezeigt. Betroffene E-Mails werden gelöscht.

In den Ordner „Gelöschte Objekte“ verschieben - Infizierte E-Mails werden automatisch in den Ordner „Gelöschte Objekte“ verschoben.

In Ordner verschieben (Standardaktion) - Infizierte E-Mails werden automatisch in den angegebenen Ordner verschoben.

Ordner – Geben Sie den Ordner an, in den erkannte infizierte E-Mails verschoben werden sollen.

Scan nach Signaturdatenbank-Update wiederholen - Wenn diese Option aktiviert ist, werden infizierte E-Mails nach einem Update der Erkennungsroutine erneut gescannt.

Scanergebnisse von anderen Modulen akzeptieren - Mit dieser Option akzeptiert das E-Mail-Schutzmodul Scanergebnisse von anderen Schutzmodulen, anstatt erneut zu scannen.

E-Mail-Protokolle

IMAP und POP3 sind die gängigsten Protokolle für den Empfang von E-Mails in E-Mail-Clientanwendungen. Das Internet Message Access Protocol (IMAP) ist ein weiteres Internetprotokoll für den E-Mail-Abruf. IMAP bietet einige Vorteile gegenüber POP3, z. B. können sich mehrere Clients gleichzeitig mit demselben Postfach verbinden und Informationen zum Nachrichtenstatus beibehalten, etwa ob die Nachricht gelesen, beantwortet oder gelöscht wurde. Das Schutzmodul, das diese Kontrolle bereitstellt, wird beim Systemstart automatisch initialisiert und ist anschließend im Arbeitsspeicher aktiv.

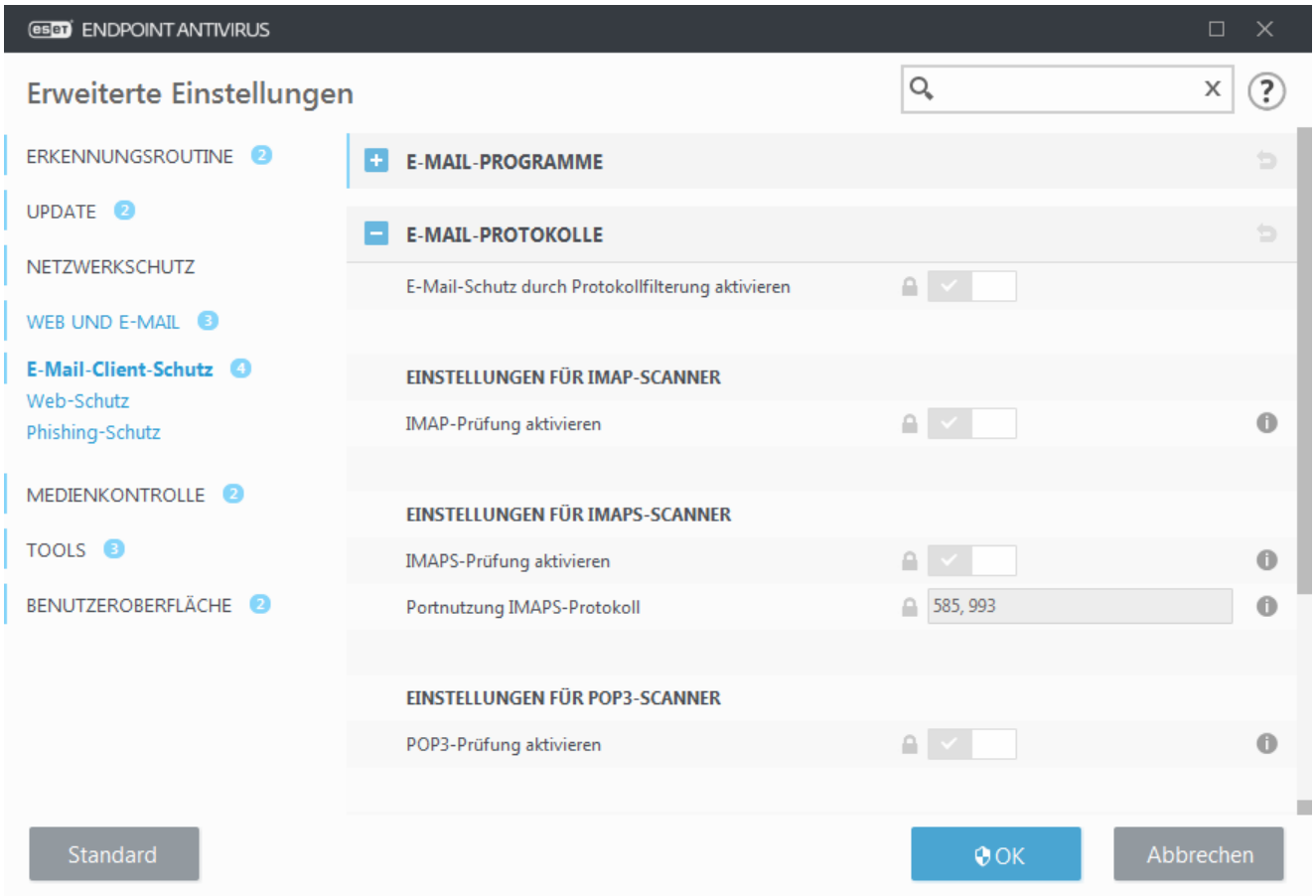
ESET Endpoint Antivirus bietet Schutz für diese Protokolle, egal welcher E-Mail-Client verwendet wird und ohne

den E-Mail-Client neu konfigurieren zu müssen. Standardmäßig wird sämtliche Kommunikation über POP3 oder IMAP gescannt, unabhängig von den standardmäßigen POP3- und IMAP-Portnummern.
Das MAPI-Protokoll wird nicht gescannt. Die Kommunikation mit dem Microsoft Exchange Server kann jedoch mit dem Integrationsmodul in E-Mail-Clients wie etwa Microsoft Outlook gescannt werden.

Wir empfehlen, die Option **E-Mail-Schutz durch Protokollfilterung aktivieren** aktiviert zu lassen**.** Sie finden die IMAP/IMAPS- und POP3/POP3S-Protokollprüfung unter Erweiterte Einstellungen > **Web und E-Mail** > **E-Mail-Client-Schutz** > **E-Mail-Protokolle**.

ESET Endpoint Antivirus unterstützt außerdem die Prüfung von IMAPS- (585, 993) und POP3S-Protokollen (995), die Daten zwischen Server und Client über einen verschlüsselten Kanal übertragen. ESET Endpoint Antivirus überwacht die Kommunikation über die Protokolle SSL (Secure Socket Layer) und TLS (Transport Layer Security). Unabhängig von der Version des Betriebssystems wird nur Datenverkehr auf Ports gescannt, die unter **Portnutzung IMAPS-/POP3S-Protokoll** definiert wurden. Weitere Kommunikationsports können bei Bedarf hinzugefügt werden. Mehrere Portnummern werden durch Kommas getrennt.

Verschlüsselter Datenverkehr wird standardmäßig gescannt. Um die Scaneinstellungen anzuzeigen, navigieren Sie zu SSL/TLS in den erweiterten Einstellungen, klicken Sie auf **Web und E-Mail** > **SSL/TLS** und aktivieren Sie die Option **SSL/TLS-Protokollfilterung aktivieren**.



E-Mail-Warnungen und Hinweise

Die Optionen für diese Funktion finden Sie unter **Erweiterte Einstellungen unter Web und E-Mail** > **E-Mail-Client-Schutz** > **Warnungen und Hinweise**.

Nach erfolgtem Scan kann ein Scan-Hinweis zu der E-Mail-Nachricht hinzugefügt werden. Sie haben folgende

Optionen: **Prüfhinweis an eingehende/gelesene E-Mails anhängen** oder **Prüfhinweis an ausgehende E-Mails anhängen**. Es kann jedoch nicht ausgeschlossen werden, dass bestimmte Bedrohungen Prüfhinweise in problematischen HTML-Nachrichten fälschen oder löschen. Prüfhinweise können zu empfangenen und gelesenen E-Mails und/oder zu gesendeten E-Mails hinzugefügt werden. Folgende Optionen stehen zur Verfügung:

- **Nie** - Es werden keine Prüfhinweise zu E-Mails hinzugefügt.
- **Wenn ein Ereignis auftritt** - Prüfhinweise werden nur an E-Mails angehängt, in denen Schadcode erkannt wurde (Standardeinstellung).
- **Für alle E-Mails beim Scannen** - Alle gescannten E-Mails werden mit Prüfhinweisen versehen.

Betreff versendeter E-Mails aktualisieren - Deaktivieren Sie dieses Kontrollkästchen, um Prüfhinweise zu den Betreffzeilen infizierter E-Mails hinzuzufügen. In Ihrem E-Mail-Programm können Sie mühelos eine Filterregel erstellen, die diesen Prüfhinweis erkennt (falls Ihr E-Mail-Programm Filterregeln unterstützt). Diese Funktion erhöht beim Empfänger auch die Glaubwürdigkeit von Nachrichten. Bei der Erkennung von eingedrungener Schadsoftware stehen wertvolle Informationen zur Bedrohungsebene der Nachricht oder des Absenders zur Verfügung.

Text, der zum Betreff der erkannten E-Mail hinzugefügt wird - Geben Sie hier den Text ein, der das Präfix in der Betreffzeile von infizierten E-Mails ersetzen soll. Mit dieser Funktion wird der Nachrichtenbetreff „Hallo“ folgendermaßen formatiert: „[Ereignis %DETECTIONNAME%] Hallo“. Die Variable %DETECTIONNAME% steht dabei für das erkannte Ereignis.

Integration mit E-Mail-Programmen

Zu den derzeit unterstützten E-Mail-Programmen gehören Microsoft Outlook, Outlook Express, Windows Mail und Windows Live Mail. Der E-Mail-Schutz ist ein Plug-In für diese Programme. Das Plugin funktioniert unabhängig vom eingesetzten Protokoll. Wenn beim E-Mail-Client eine verschlüsselte Nachricht eingeht, wird diese entschlüsselt und an das Virenschutz-Prüfmodul weitergeleitet. Eine vollständige Liste der unterstützten E-Mail-Programme und Versionen finden Sie im entsprechenden ESET-Knowledgebase-Artikel.

Microsoft Outlook-Symbolleiste

Die Sicherheitslösung für Microsoft Outlook ist ein Plug-In. Nach der Installation von ESET Endpoint Antivirus wird in Microsoft Outlook diese Symbolleiste für den Viren- und mit folgenden Schutzoptionen angezeigt:

ESET Endpoint Antivirus - Klicken Sie auf das Symbol, um das Hauptprogrammfenster von ESET Endpoint Antivirus zu öffnen.

E-Mails erneut prüfen - Ermöglicht es Ihnen, die E-Mail-Prüfung manuell zu starten. Sie können E-Mails festlegen, die geprüft werden sollen. Außerdem können Sie das erneute Prüfen empfangener E-Mails aktivieren. Weitere Informationen hierzu finden Sie unter E-Mail-Client-Schutz.

Einstellungen für Prüfung - Anzeige der Optionen für den E-Mail-Client-Schutz.

Symbolleisten für Outlook Express und Windows Mail

Für den Schutz in Outlook Express und Windows Mail wird ein Plug-In verwendet. Nach der Installation von ESET Endpoint Antivirus wird in Outlook Express bzw. Windows Mail diese Symbolleiste für den Viren- und mit folgenden Schutzoptionen angezeigt:

ESET Endpoint Antivirus - Klicken Sie auf das Symbol, um das Hauptprogrammfenster von ESET Endpoint Antivirus zu öffnen.

E-Mails erneut prüfen - Ermöglicht es Ihnen, die E-Mail-Prüfung manuell zu starten. Sie können E-Mails festlegen, die geprüft werden sollen. Außerdem können Sie das erneute Prüfen empfangener E-Mails aktivieren. Weitere Informationen hierzu finden Sie unter E-Mail-Client-Schutz.

Einstellungen für Prüfung - Anzeige der Optionen für den E-Mail-Client-Schutz.

Benutzeroberfläche

Anzeige anpassen - Die Anzeige der Symbolleiste kann für Ihr E-Mail-Programm geändert werden. Deaktivieren Sie die Option für die Anpassung der Anzeige unabhängig von den Parametern des E-Mail-Programms.

Symboltitel anzeigen - Anzeige der Beschreibung für Symbole.

Symboltitel rechts - Die Beschreibungen werden vom unteren zum seitlichen Bereich der Symbole verschoben.

Große Symbole - Anzeige großer Symbole für Menüeinstellungen.

Bestätigungsfenster

Mit diesem Hinweis wird geprüft, ob die ausgewählte Aktion wirklich durchgeführt werden soll. Dadurch sollen mögliche Fehler vermieden werden.

Darüber hinaus bietet das Fenster die Option, die Anzeige von Bestätigungsfenstern zu deaktivieren.

E-Mails erneut prüfen

Die in E-Mail-Programmen integrierte ESET Endpoint Antivirus-Symbolleiste bietet Benutzern verschiedene Optionen zum Prüfen von E-Mails. Die Option **E-Mails erneut prüfen** bietet zwei Prüfmodi:

Alle E-Mails im aktuellen Ordner - Alle E-Mails im aktuell angezeigten Ordner werden geprüft.

Nur markierte E-Mails - Nur markierte E-Mails werden geprüft.

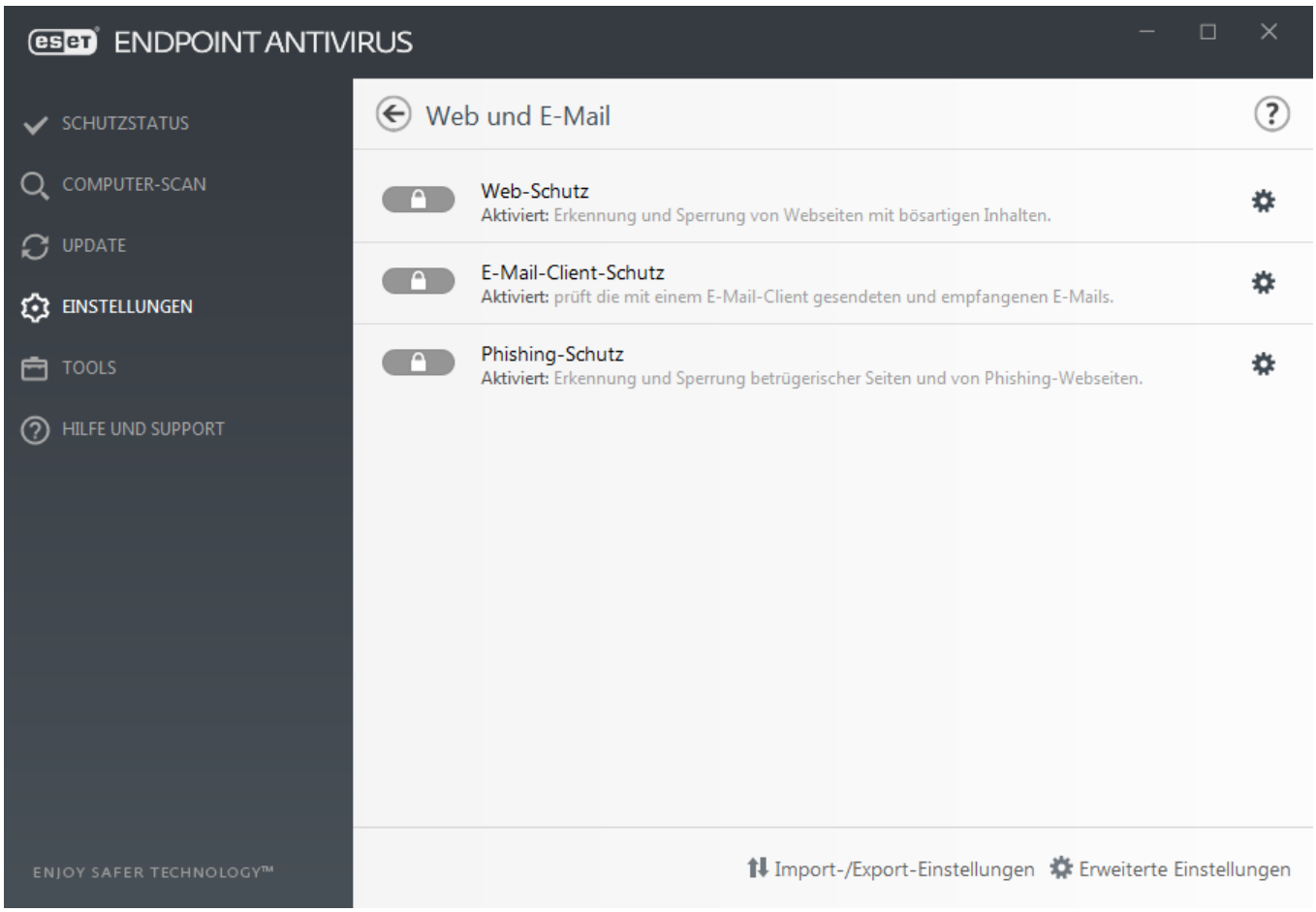
Das Kontrollkästchen **Bereits geprüfte E-Mails erneut prüfen** bietet dem Benutzer die Option einer erneuten Prüfung von bereits geprüften E-Mails.

Web-Schutz

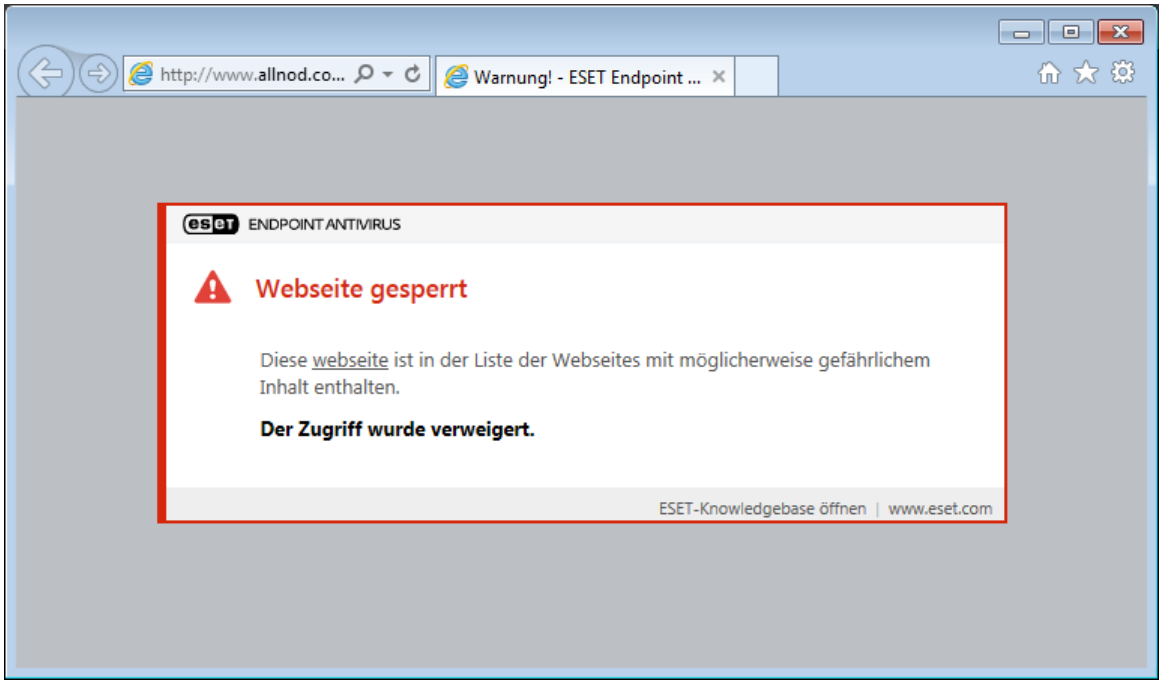
Der Internetzugang ist eine Standardfunktion von Computern. Leider ist diese technische Möglichkeit mittlerweile auch der wichtigste Weg zur Verbreitung von Schadsoftware. Der Web-Schutz besteht in der Überwachung der Kommunikation zwischen Webbrowsern und Remoteservern und entspricht den Regeln für HTTP (Hypertext Transfer Protocol) und HTTPS (verschlüsselte Kommunikation).

Der Zugriff auf Webseiten, die bekannterweise Schadcode enthalten, wird vor dem Herunterladen von Inhalt blockiert. Alle anderen Webseiten werden beim Laden vom ThreatSense-Prüfmodul geprüft und blockiert, wenn Schadcode gefunden wird. Der Web-Schutz bietet zwei Schutzebenen: Blockieren nach Negativliste und Blockieren nach Inhalt.

Wir empfehlen dringend, den Web-Schutz zu aktivieren. Sie finden diese Option im Hauptfenster von ESET Endpoint Antivirus unter **Einstellungen** > **Internet-Schutz** > **Web-Schutz**.



Der Web-Schutz zeigt die folgende Nachricht in Ihrem Browser an, wenn eine Website blockiert wird:



Illustrierte Anweisungen

Die folgenden Artikel in der ESET-Knowledgebase sind möglicherweise nur auf Englisch verfügbar:

- Entsperren einer sicheren Website auf einer einzelnen Workstation in ESET Endpoint Antivirus
- Entsperren einer sicheren Website auf einem Endpunkt mit ESET Security Management Center

---

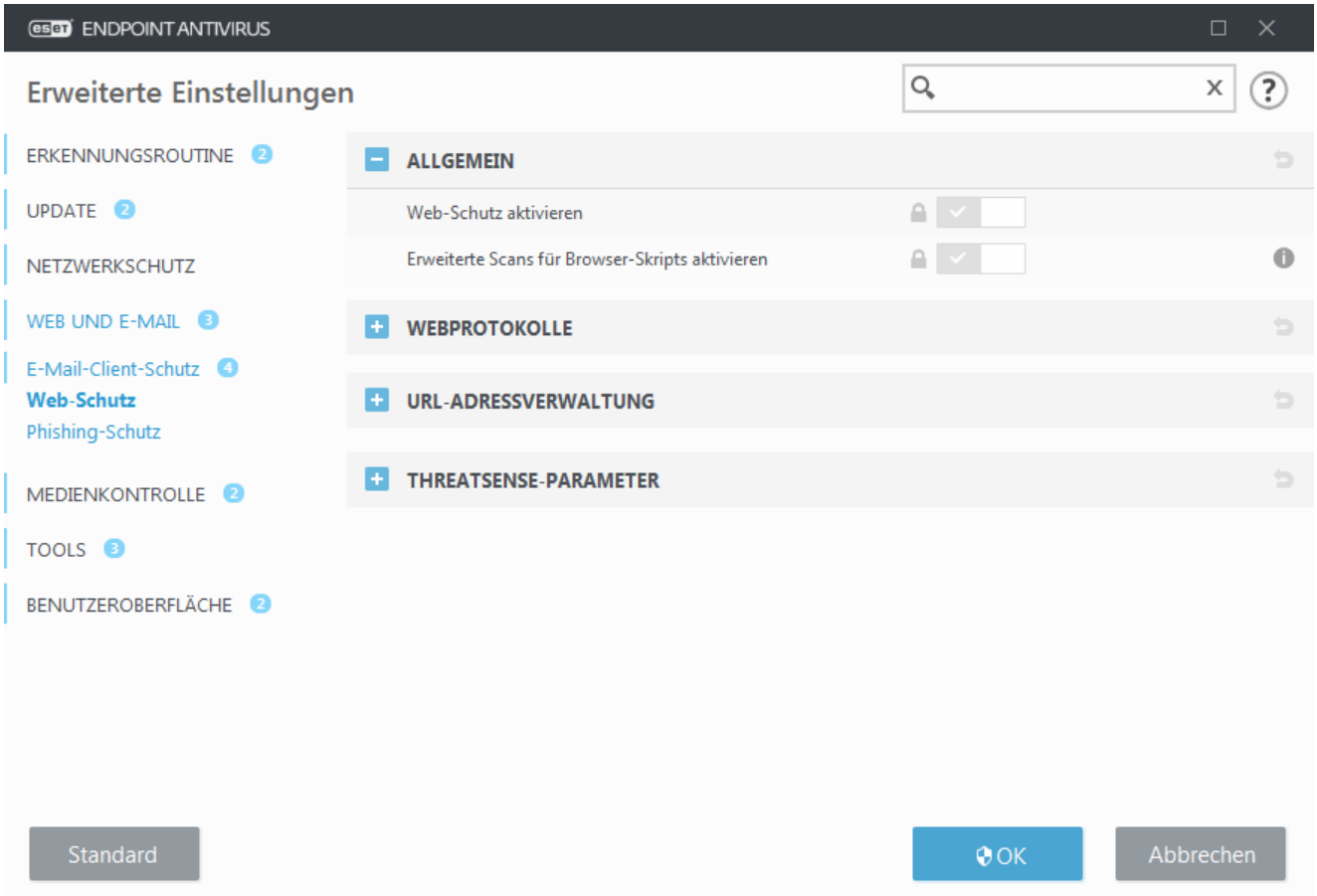
In **Erweiterte Einstellungen** (F5) > **Web und E-Mail** > **Web-Schutz** stehen die folgenden Optionen zur Verfügung

- **Einfach** - Hier können Sie diese Funktion in den erweiterten Einstellungen aktivieren oder deaktivieren.

- **Web-Protokolle** - Hier können Sie die Überwachung dieser von den meisten Internetbrowsern verwendeten Standardprotokolle konfigurieren.

- **URL-Adressverwaltung** - Hier können Sie festlegen, welche URL-Adressen blockiert, zugelassen oder vom Scannen ausgeschlossen werden sollen.

- **ThreatSense -Parameter** – In diesem Bereich finden Sie erweiterte Einstellungen für den Virenschutz. Hier können Sie Einstellungen für zu prüfende Objekte (E-Mails, Archive usw.), Erkennungsmethoden für den Web-Schutz usw. festlegen.



Erweiterte Einstellungen für den Web-Schutz

In **Erweiterte Einstellungen** (F5) > **Web und E-Mail** > **Web-Schutz** > **Einfach** stehen die folgenden Optionen zur Verfügung:

Web-Schutz aktivieren - Wenn diese Option deaktiviert ist, funktionieren Web-Schutz und Phishing-Schutz nicht.

Erweiterte Scans für Browser-Skripts aktivieren - Wenn diese Option aktiviert ist, werden alle in Webbrowsern ausgeführten JavaScript-Programme von der Erkennungsroutine gescannt.

> **Hinweis**
> Der Web-Schutz sollte unbedingt immer aktiviert sein.

Webprotokolle

ESET Endpoint Antivirus ist standardmäßig so konfiguriert, dass das von den meisten Internetbrowsern verwendete HTTP-Protokoll überwacht wird.

Einstellungen für den HTTP-Scanner

Der HTTP-Datenverkehr wird auf allen Ports für alle Anwendungen ständig überwacht.

Einstellungen für den HTTPS-Scanner

ESET Endpoint Antivirus unterstützt auch die HTTPS-Protokollprüfung. Bei der HTTPS-Kommunikation wird zur Datenübertragung zwischen Server und Client ein verschlüsselter Kanal verwendet. ESET Endpoint Antivirus überwacht die mit Hilfe der Protokolle SSL (Secure Socket Layer) und TLS (Transport Layer Security) abgewickelte Kommunikation. Unabhängig von der Version des Betriebssystems wird nur Datenverkehr an Ports (443, 0-65535) geprüft, die in **Portnutzung HTTPS-Protokoll** definiert wurden.

Verschlüsselter Datenverkehr wird standardmäßig gescannt. Um die Scaneinstellungen anzuzeigen, navigieren Sie zu SSL/TLS in den erweiterten Einstellungen, klicken Sie auf **Web und E-Mail** > **SSL/TLS** und aktivieren Sie die Option **SSL/TLS-Protokollfilterung aktivieren**.

URL-Adressverwaltung

In der URL-Adressverwaltung können Sie festlegen, welche HTTP-Adressen blockiert, zugelassen oder von den Inhalts-Scans ausgeschlossen werden sollen.

Wenn neben HTTP-Webseiten auch HTTPS-Adressen gefiltert werden sollen, muss die Option SSL/TLS-Protokollfilterung aktivieren aktiviert sein. Andernfalls werden nur die Domains besuchter HTTPS-Sites hinzugefügt, nicht aber die URL.

Auf Websites in der **Liste gesperrter Adressen** kann nicht zugegriffen werden, es sei denn, die Website ist auch in der **Liste zugelassener Adressen** enthalten. Websites, die in der **Liste der Adressen, die vom Inhaltsscan ausgeschlossen werden** aufgeführt sind, werden vor dem Zugriff nicht auf Schadcode gescannt.

Wenn alle HTTP-Adressen außer denen in der aktiven **Liste zugelassener Adressen** blockiert werden sollen, fügen Sie der aktiven **Liste blockierter Adressen** ein Sternchen (*) hinzu.

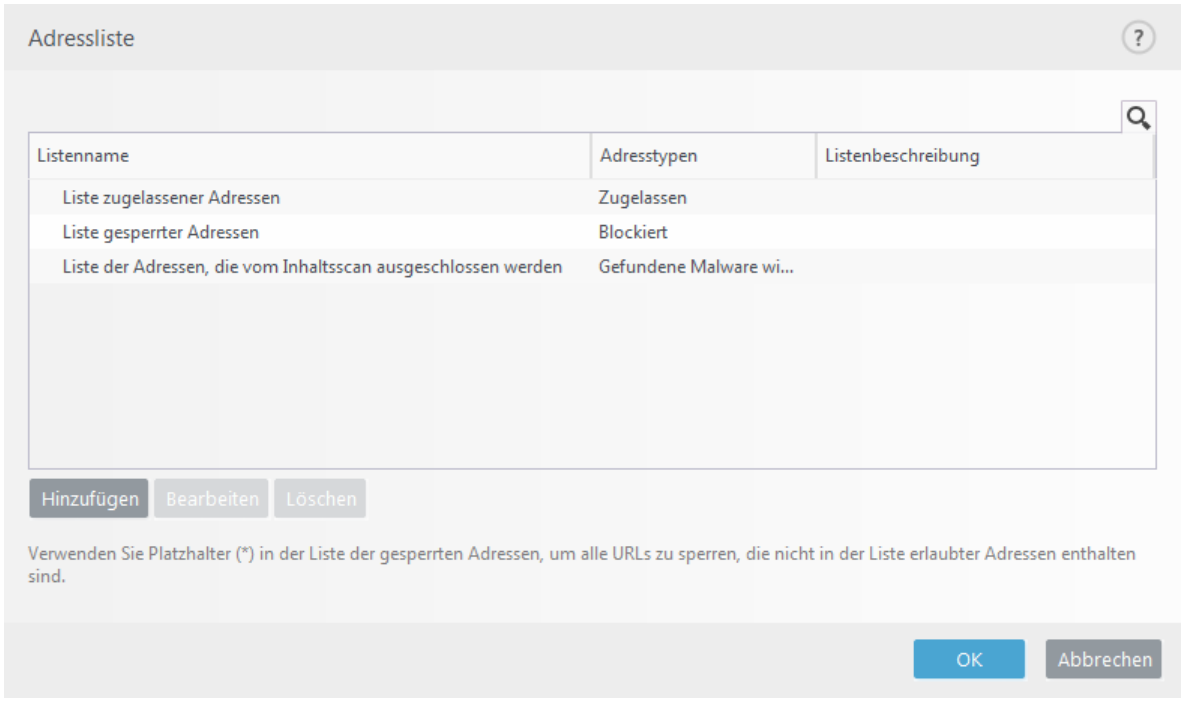
Die Sonderzeichen „*“ (Sternchen) und „?“ (Fragezeichen) können in Listen verwendet werden. Das Sternchen ersetzt eine beliebige Zeichenfolge, das Fragezeichen ein beliebiges Symbol. Die Liste der ausgeschlossenen Adressen sollten Sie mit Bedacht zusammenstellen. Geben Sie ausschließlich vertrauenswürdige und sichere Adressen an. Achten Sie darauf, dass die Zeichen „*“ und „?“ korrekt verwendet werden. Unter Maske für HTTP-Adressen/Domains hinzufügen finden Sie Informationen zur sicheren Angabe gesamter Domänen inklusive Unterdomänen. Um eine Liste zu aktivieren, wählen Sie die Option **Liste aktiv**. Wenn Sie benachrichtigt werden möchten, wenn Sie eine Adresse aus der aktuellen Liste eingeben, wählen Sie **Bei Anwendung benachrichtigen** aus.

Dateierweiterungen blockieren oder zulassen

Mit der URL-Adressverwaltung können Sie auch das Öffnen bestimmter Dateitypen beim Internetsurfen blockieren bzw. erlauben. Wenn Sie z. B. das Öffnen ausführbarer Dateien verbieten möchten, wählen Sie im Dropdownmenü die Liste aus, in der Sie diese Dateien sperren möchten, und geben Sie "**.exe" ein.

Vertrauenswürdige Domänen

Wenn die Einstellung **Web und E-Mail** > **SSL/TLS** > **Kommunikation mit vertrauenswürdigen Domains ausschließen** aktiviert ist und die Domäne als vertrauenswürdig gilt, werden keine Adressen gefiltert.



Steuerelemente

Hinzufügen – Erstellen einer neuen Liste zusätzlich zu den vordefinierten. Dies kann nützlich sein, wenn Sie verschiedene Gruppen und Adressen auf logische Art und Weise aufteilen möchten. So kann eine Liste blockierter Adressen beispielsweise Adressen aus einer externen öffentlichen Negativliste und eine zweite eigene Negativliste enthalten. Auf diese Weise lässt sich die externe Liste einfacher aktualisieren, während Ihre Liste intakt bleibt.

Bearbeiten – Bearbeiten bestehender Listen. Hiermit können Sie Adressen zu den Listen hinzufügen oder daraus entfernen.

Löschen – Löschen bestehender Listen. Es können nur Listen entfernt werden, die mit der Option **Hinzufügen** erstellt wurden; nicht Standardlisten.

URL-Adressliste

In diesem Bereich können Sie festlegen, welche HTTP-Adressen blockiert, zugelassen oder von der Prüfung ausgeschlossen werden sollen.

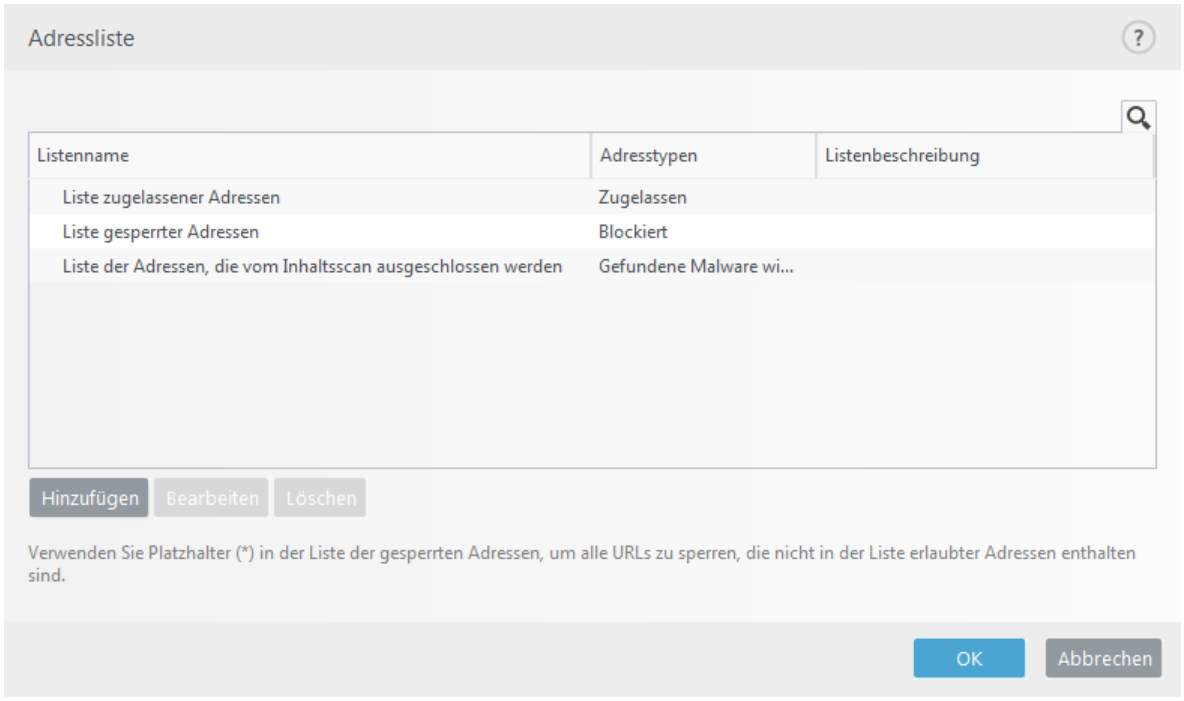
Standardmäßig stehen die drei folgenden Listen zur Verfügung:

- **Liste der Adressen, die vom Inhaltsscan ausgeschlossen werden** - Die Adressen in dieser Liste werden nicht auf Schadcode gescannt.

- **Liste zugelassener Adressen** - Wenn die Option „Nur Zugriff auf HTTP-Adressen aus der Liste zulässiger Adressen erlauben“ aktiviert ist und die Liste blockierter Adressen ein Sternchen (*) enthält, darf der Benutzer nur auf Adressen in dieser Liste zugreifen. Die Adressen in der Liste sind zugelassen, auch wenn Sie ebenfalls in der Liste blockierter Adressen enthalten sind.

- **Liste blockierter Adressen** – Auf die in dieser Liste genannten Adressen kann der Benutzer nicht zugreifen, es sei denn, die Adressen sind auch in der Liste zugelassener Adressen enthalten.

Klicken Sie auf **Hinzufügen**, um eine neue Liste zu erstellen. Klicken Sie auf **Löschen**, um ausgewählte Listen zu löschen.



Illustrierte Anweisungen

Die folgenden Artikel in der ESET-Knowledgebase sind möglicherweise nur auf Englisch verfügbar:

- Entsperren einer sicheren Website auf einer einzelnen Workstation in ESET Endpoint Antivirus
- Entsperren einer sicheren Website auf einem Endpunkt mit ESET Security Management Center

Weitere Informationen finden Sie unter URL-Adressverwaltung.

Erstellen einer neuen URL-Adressliste

In diesem Bereich können Sie festlegen, welche URL-Adressen/Masken blockiert, zugelassen oder von der Prüfung ausgeschlossen werden sollen.

Für die Erstellung einer neuen Liste stehen die folgenden Optionen zur Verfügung:

Typ der Adressliste - Es stehen drei vordefinierte Listentypen zur Verfügung:

- **Von der Prüfung ausgenommen** - Die Adressen in dieser Liste werden nicht auf Schadcode geprüft.
- **Gesperrt**- Der Benutzer darf nicht auf die Adressen in dieser Liste zugreifen.
- **Zugelassen**–Wenn Ihre Policy so konfiguriert ist, dass diese Funktion verwendet wird, wird der Platzhalterwert (*) zu dieser Liste hinzugefügt. Sie haben auch dann Zugriff auf die Adressen in dieser Liste, wenn diese Adressen ebenfalls in der blockierten Liste vorhanden sind.

Listenname - Geben Sie den Namen der Liste ein. Bei der Bearbeitung einer der drei vordefinierten Listen ist dieses Feld nicht verfügbar.

Listenbeschreibung– Geben Sie eine kurze Beschreibung für die Liste ein (optional). Dieses Feld ist nicht verfügbar, wenn Sie eine der drei vordefinierten Listen bearbeiten.

Liste aktiv–aktivieren Sie die Liste mit dem Schieberegler.

Bei Anwendung benachrichtigen – Wählen Sie den Schieberegler, falls Sie benachrichtigt werden möchten, wenn diese Liste bei der Prüfung einer von Ihnen besuchten HTTP-Site verwendet wird. So wird beispielsweise eine Benachrichtigung ausgegeben, wenn eine Website blockiert oder zugelassen wird, da sie in der Liste der blockierten oder zugelassenen Adressen enthalten ist. Die Benachrichtigung enthält den Listennamen der Liste, die die Website festlegt.

Logging-Schweregrad– Wählen Sie einen Logging-Schweregrad aus dem Dropdownmenü aus. Einträge mit Warninformationen können vom Remote Administrator gesammelt werden.

Steuerelemente

Hinzufügen - Hinzufügen einer neuen URL-Adresse zur Liste (geben Sie mehrere Werte mit einem Trennzeichen ein).

Bearbeiten - Bearbeiten einer bestehenden Adresse in der Liste. Nur bei Adressen möglich, die mit **Hinzufügen** erstellt wurden.

Entfernen – Entfernen einer bestehenden Adresse aus der Liste. Nur bei Adressen möglich, die mit **Hinzufügen** erstellt wurden.

Importieren - Importieren einer Datei mit URL-Adressen (trennen Sie die Werte mit einem Zeilenumbruch, z. B. *.txt mit der Codierung UTF-8).

Hinzufügen einer URL-Maske

Beachten Sie die Anweisungen in diesem Dialogfenster, bevor Sie die gewünschte Maske für die Adresse/Domain eingeben.

Mit ESET Endpoint Antivirus kann der Zugriff auf bestimmte Webseiten gesperrt werden, so dass der Browser deren Inhalte nicht anzeigt. Darüber hinaus können Adressen angegeben werden, die nicht geprüft werden sollen. Ist der vollständige Name des Remoteservers nicht bekannt oder soll eine ganze Gruppe von Remoteservern angegeben werden, kann eine solche Gruppe über eine so genannte Maske bestimmt werden. Für Masken können Sie die Symbole „?“ und „*“ verwenden:

- Mit „?“ können Sie ein einzelnes Zeichen ersetzen.
- Mit „*“ können Sie eine Textfolge ersetzen.

*.c?m steht beispielsweise für alle Adressen, deren erster Buchstabe „c“ ist, die auf „m“ enden und dazwischen ein unbekanntes Zeichen enthalten (.com, .cam usw.).

Die vorangestellte Sequenz „*.“ am Anfang eines Domänennamens hat eine Sonderbedeutung. Zunächst erfasst der *-Platzhalter in diesem Fall nicht den Schrägstrich ('/'). Auf diese Weise wird eine Umgehung der Maske vermieden. Die Maske **.domaene.com* erfasst z. B. nicht die URL *http://beliebigedomaene.com/pfad#.domaene.com* (dieses Suffix kann an beliebige URLs angehängt werden, ohne den Download zu beeinträchtigen). Außerdem erfasst die Sequenz „*.“ in diesem Sonderfall auch eine leere Zeichenfolge. Auf diese Weise ist es möglich, eine gesamte Domäne inklusive aller Unterdomänen mit einer einzigen Maske zu erfassen. Die Maske **.domaene.com* erfasst z. B. auch *http://domaene.com*. **domaene.com* wäre dagegen nicht korrekt, da diese Maske auch *http://anderedomaene.com* erfasst.

Phishing-Schutz

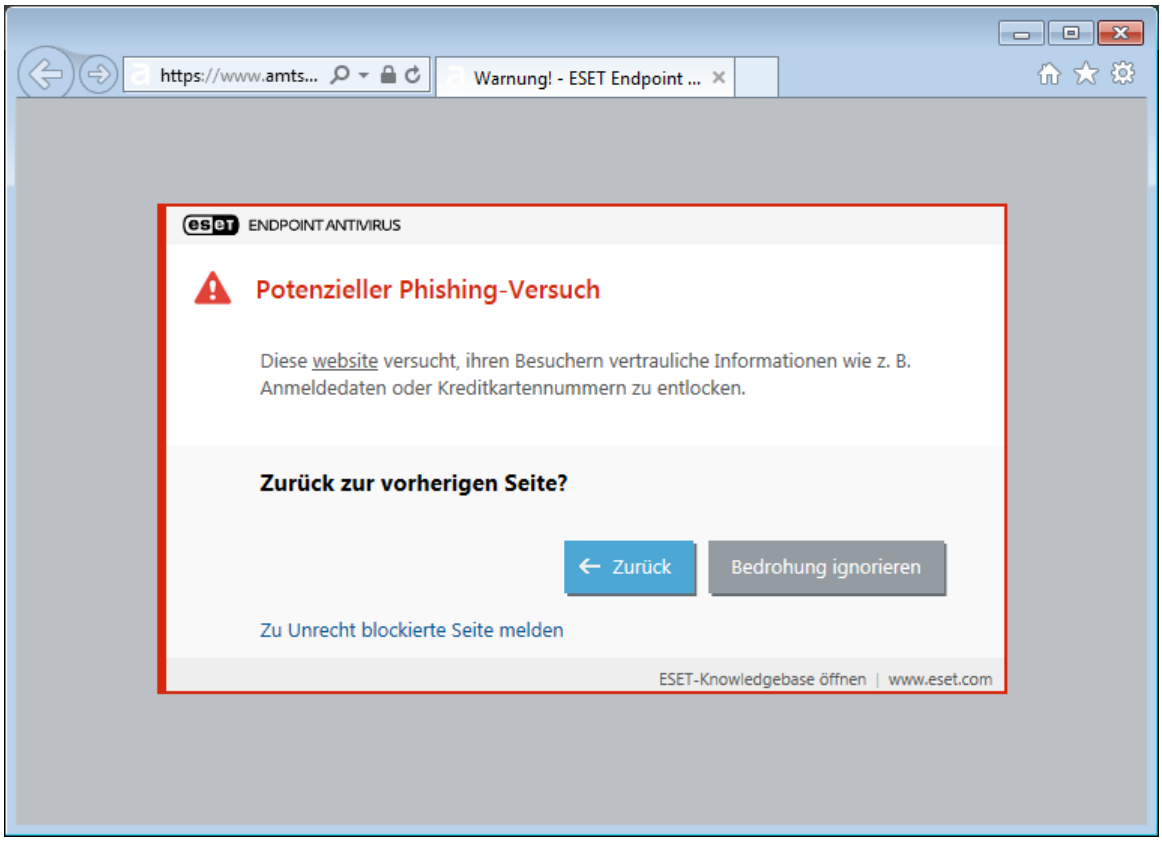
Der Begriff „Phishing“ bezeichnet eine kriminelle Vorgehensweise, die sich Techniken des Social Engineering (Manipulation von Benutzern zur Erlangung vertraulicher Informationen) zunutze macht. Phishing wird oft eingesetzt, um Zugriff auf vertrauliche Daten zu erlangen, wie Kontonummern oder PIN-Codes. Weitere Informationen zu dieser Aktivität finden Sie im Glossar. ESET Endpoint Antivirus enthält einen Phishing-Schutz: Webseiten, die dafür bekannt sind, Phishing-Inhalte zu enthalten, können gesperrt werden.

Wir empfehlen, den Phishing-Schutz in ESET Endpoint Antivirus zu aktivieren. Diese Option finden Sie im Bereich **Erweiterte Einstellungen** (F5) unter **Web und E-Mail** > **Phishing-Schutz**.

In unserem Knowledgebase-Artikel finden Sie weitere Informationen zum Phishing-Schutz von ESET Endpoint Antivirus.

Zugriff auf eine Phishing-Website

Wenn Sie auf eine erkannte Phishing-Website zugreifen, wird das folgende Dialogfenster im Webbrowser angezeigt. Wenn Sie trotzdem auf die Website zugreifen möchten, klicken Sie auf **Weiter zur Webseite** (nicht empfohlen).



Hinweis

Potenzielle Phishing-Websites, die zur Positivliste hinzugefügt wurden, werden standardmäßig nach einigen Stunden wieder von der Liste gelöscht. Verwenden Sie die URL-Adressverwaltung, um eine Website dauerhaft zuzulassen. Klicken Sie unter **Erweiterte Einstellungen** (F5) auf **Web und E-Mail** > **Web-Schutz** > **URL-Adressverwaltung** > **Adressliste**. Klicken Sie anschließend auf **Bearbeiten** und fügen Sie die Website, die Sie bearbeiten möchten, zu dieser Liste hinzu.

Melden einer Phishing-Website

Über den Link Melden können Sie eine Website mit vermutetem Phishing-Inhalt oder anderem Schadcode bei ESET melden.

> **Hinweis**
> Auf Websites, die Sie bei ESET melden, sollte mindestens eines der folgenden Kriterien zutreffen:
> - Die Website wird nicht als Bedrohung erkannt.
> - Die Website wird als Bedrohung erkannt, obwohl sie keinen Schadcode enthält. In diesem Fall können Sie einen Phishing-Fehlalarm melden.

Sie können Websites auch per E-Mail melden. Senden Sie die E-Mail an samples@eset.com. Verwenden Sie einen treffenden Text in der Betreffzeile und liefern Sie möglichst viele Informationen zur Website (wie Sie auf die Website gelangt sind, wo Sie von der Website erfahren haben usw.).

Aktualisieren des Programms

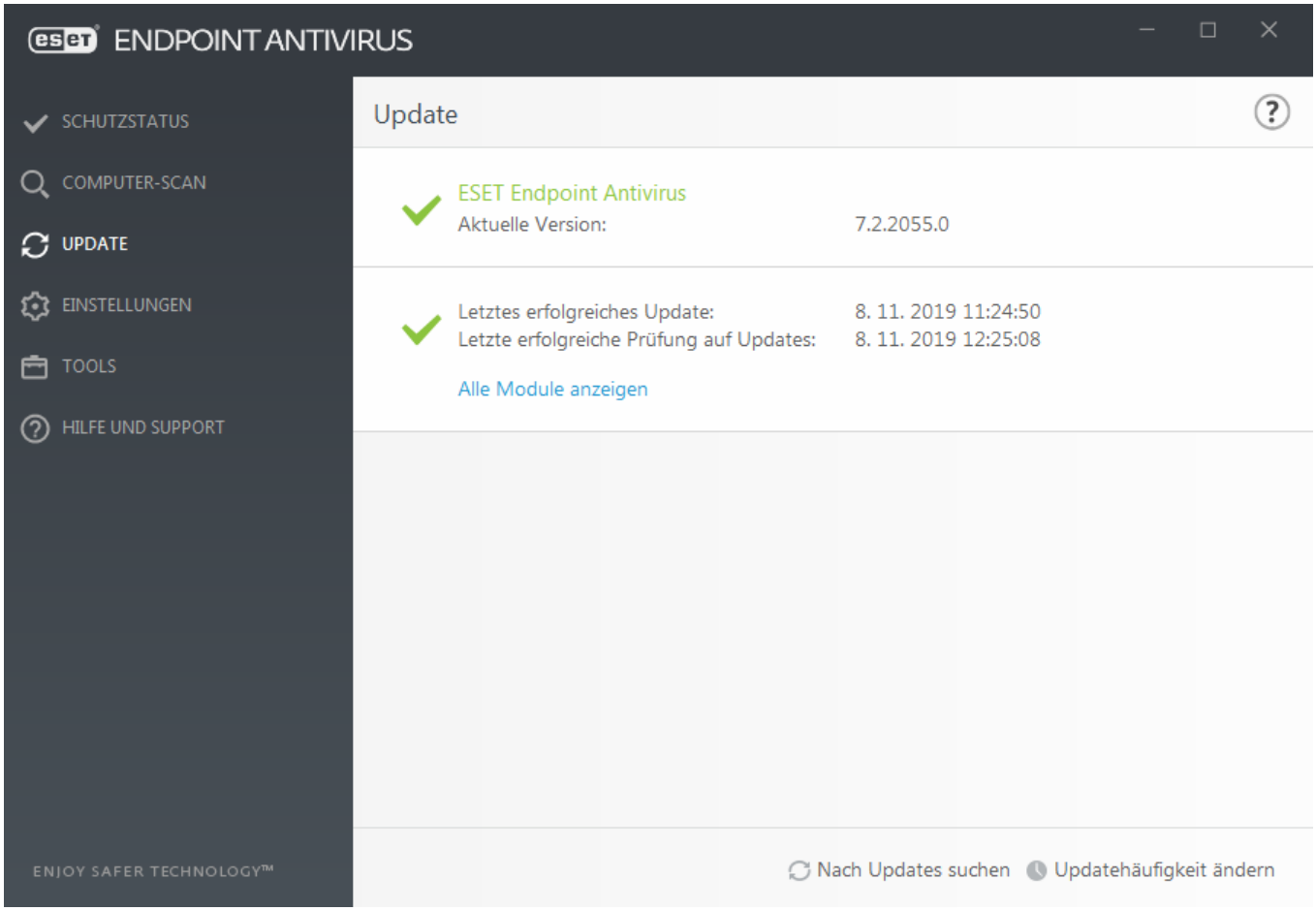
Den optimalen Schutz Ihres Computers gewährleisten Sie, indem Sie ESET Endpoint Antivirus regelmäßig aktualisieren. Das Updatemodul hält das Programm fortlaufend auf dem neuesten Stand, indem Erkennungsroutine und Systemkomponenten aktualisiert werden. Wenn das Programm aktiviert ist, werden die Updates standardmäßig automatisch durchgeführt.

Über den Punkt **Update** im Hauptprogrammfenster können Sie sich den aktuellen Update-Status anzeigen lassen. Sie sehen hier Datum und Uhrzeit des letzten Updates und können feststellen, ob ein Update erforderlich ist. Sie können auch auf den Link **Alle Module anzeigen** klicken, um eine Liste der installierten Module anzuzeigen und die Version und das Datum der letzten Aktualisierung eines bestimmten Moduls zu überprüfen.

Außerdem können Sie den Updatevorgang mit der Option **Nach Updates suchen** manuell starten. Die Updates für die Erkennungsroutine und die Programmkomponenten sind wichtige Bestandteile der Maßnahmen für einen möglichst umfassenden Schutz vor Schadcode. Seien Sie deshalb bei Konfiguration und Ausführung besonders sorgfältig. Wenn Sie Ihre Lizenzdaten noch nicht während der Installation eingegeben haben, können Sie vor dem Update auf **Produkt aktivieren** klicken, um Ihren Lizenzschlüssel einzugeben und auf die ESET-Update-Server zuzugreifen.

Wenn Sie ESET Endpoint Antivirus mit einer Offline-Lizenzdatei ohne Benutzername und Passwort aktivieren und ein Update ausführen, wird der Hinweis **Modulupdate fehlgeschlagen** in Rot angezeigt. Dies bedeutet, dass Updates nur vom Mirror heruntergeladen werden können.

> **Hinweis**
> Den Lizenzschlüssel erhalten Sie von ESET mit dem Kauf von ESET Endpoint Antivirus.



Aktuelle Version – Die Buildnummer von ESET Endpoint Antivirus.

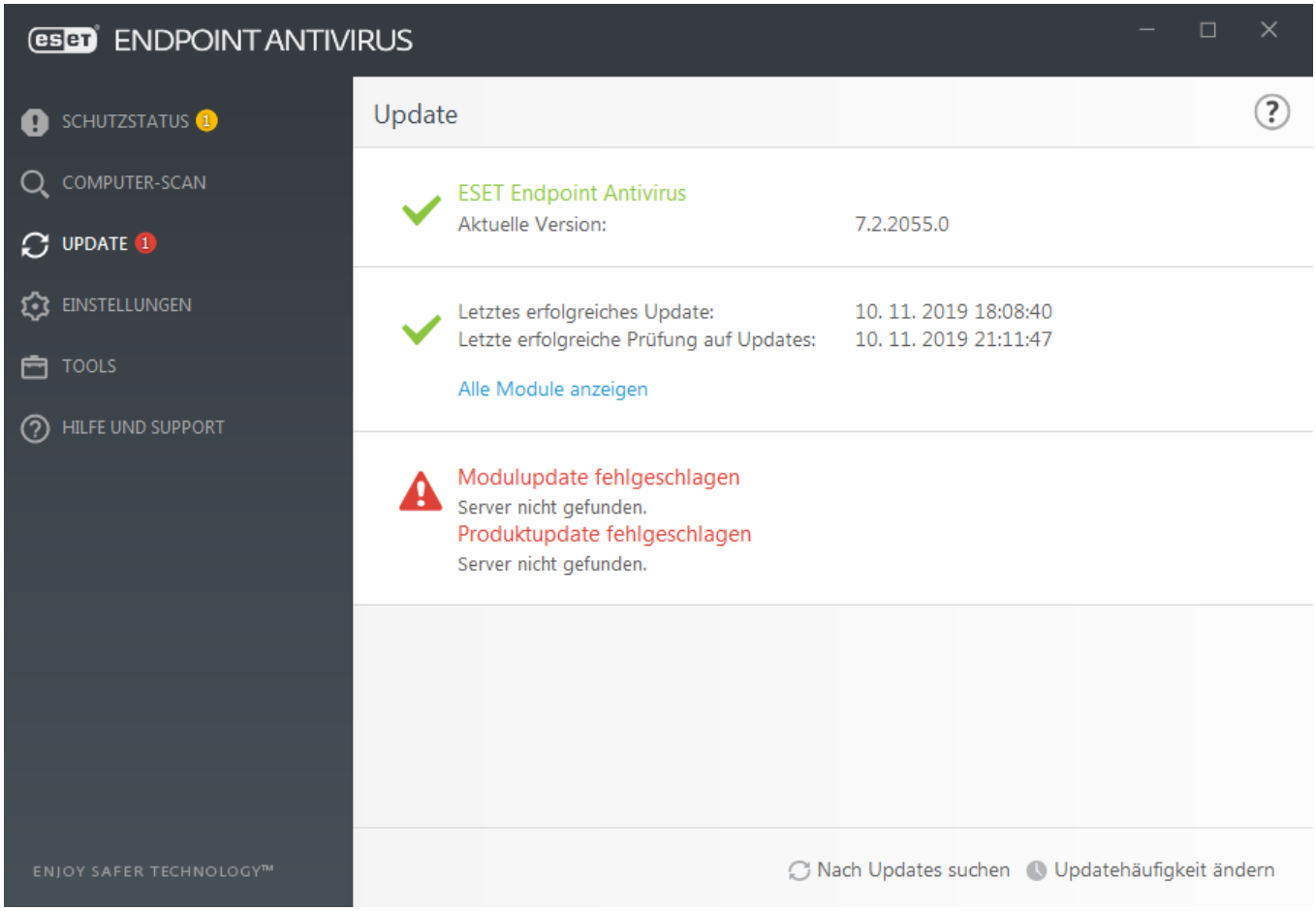
Letztes erfolgreiches Update – Datum und Uhrzeit des letzten erfolgreichen Updates. Wenn die Erkennungsroutine auf dem aktuellen Stand ist, sollte hier ein aktuelles Datum angezeigt werden.

Letzte erfolgreiche Prüfung auf Updates – Datum und Uhrzeit des letzten erfolgreichen Updateversuchs für Module.

Alle Module anzeigen – Klicken Sie auf diesen Link, um eine Liste der installierten Module anzuzeigen und die Version und das Datum der letzten Aktualisierung eines bestimmten Moduls zu überprüfen.

Update-Vorgang

Klicken Sie auf **Nach Updates suchen**, um den Download zu starten. Eine Fortschrittsanzeige und die verbleibende Zeit wird angezeigt. Um den Update-Vorgang abzubrechen, klicken Sie auf **Update abbrechen**.

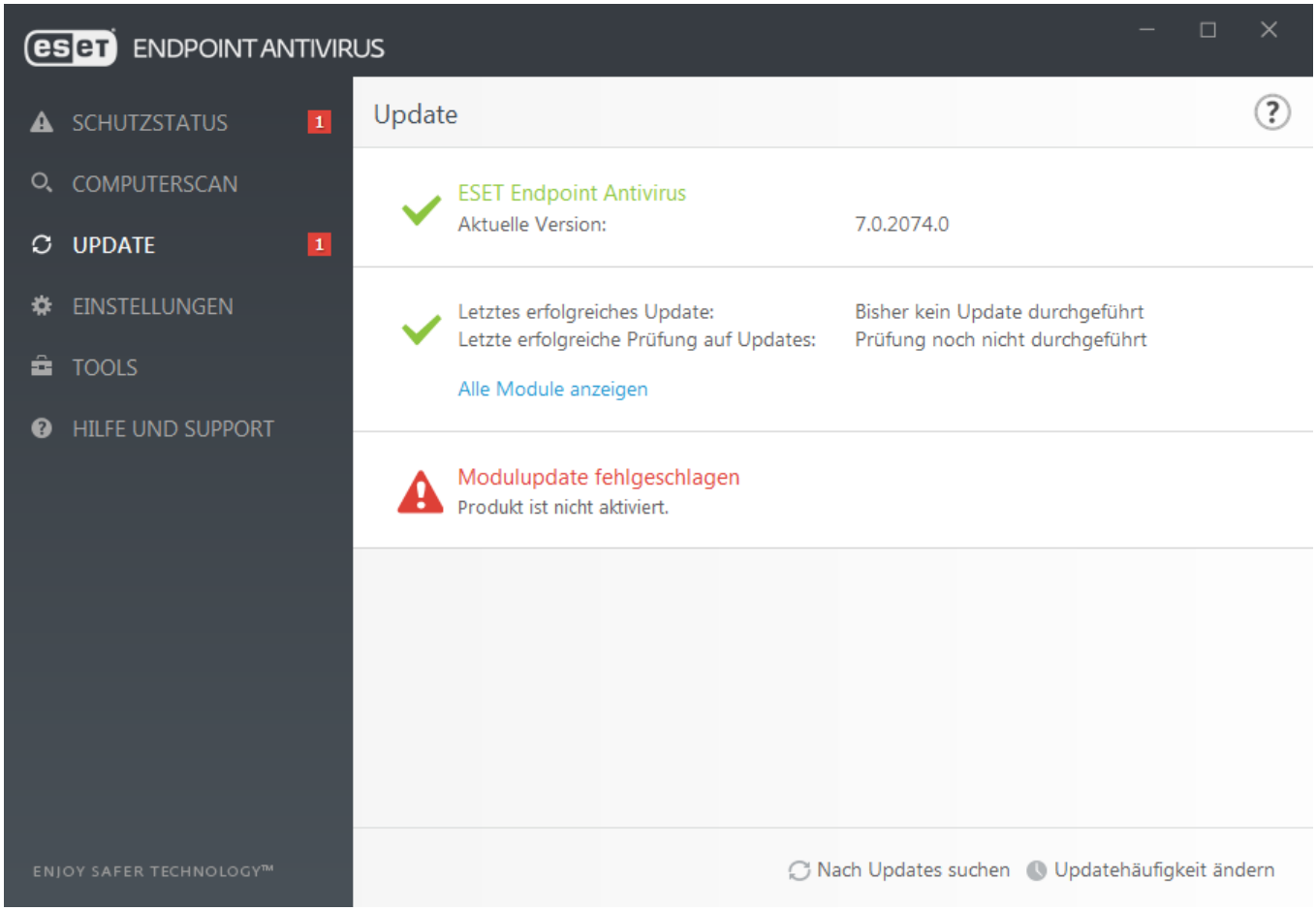


Wichtig
Normalerweise werden die Module mehrmals täglich aktualisiert. Andernfalls ist das Programm nicht auf dem neuesten Stand und anfälliger für Infektionen. Aktualisieren Sie die Module so schnell wie möglich.

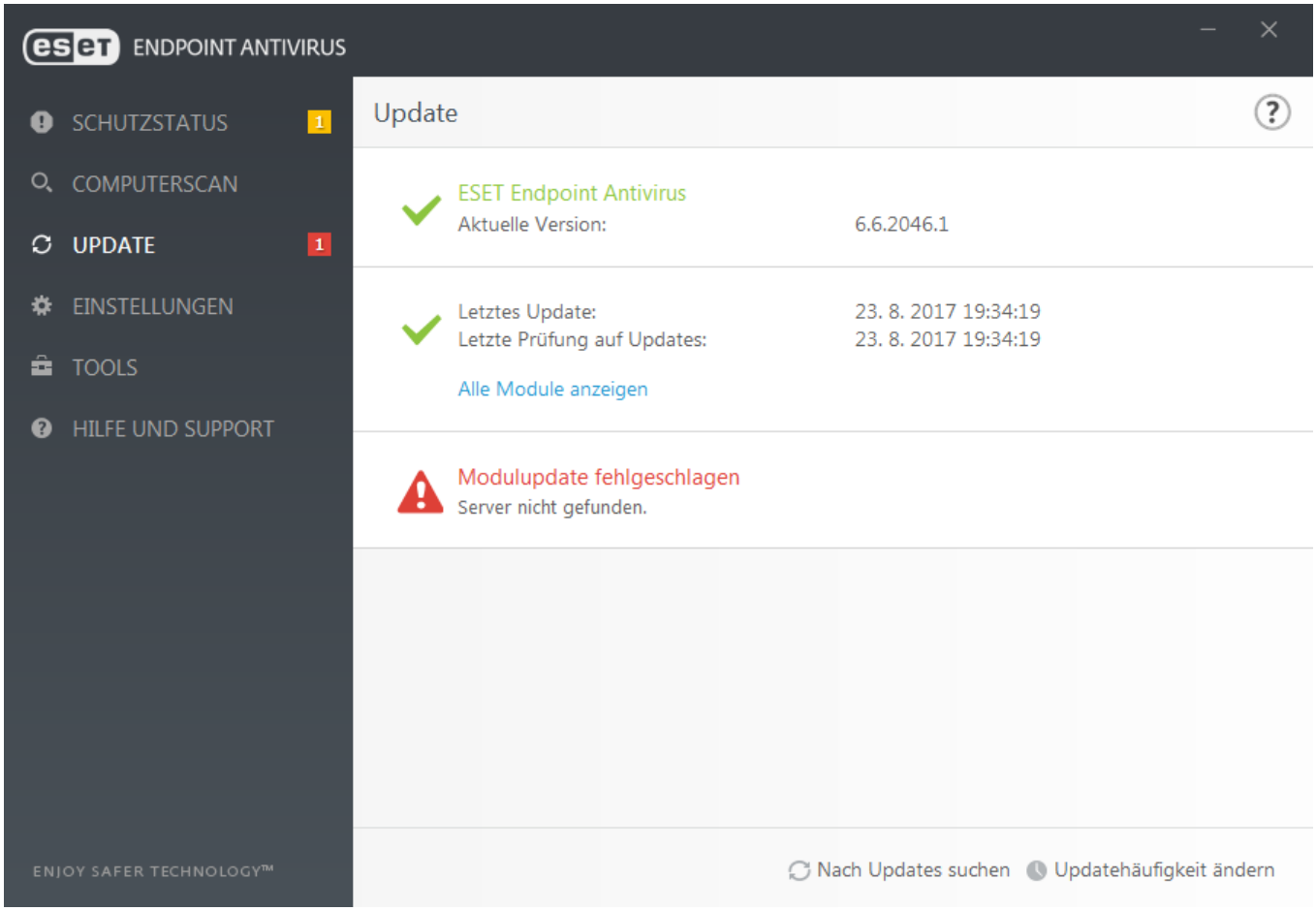
Erkennungsroutine ist veraltet – Dieser Fehler wird angezeigt, wenn die Module trotz wiederholter Versuche nicht aktualisiert werden konnten. Überprüfen Sie in diesem Fall die Update-Einstellungen. Die häufigste Fehlerursache sind falsch eingegebene Authentifizierungsdaten oder fehlerhaft konfigurierte Verbindungseinstellungen.

Der genannte Hinweis steht im Zusammenhang mit den folgenden beiden Meldungen (**Modulupdate fehlgeschlagen**) über fehlgeschlagene Updates:

1. **Ungültige Lizenz** – Der Lizenzschlüssel wurde falsch in den Update-Einstellungen eingegeben. Überprüfen Sie die richtige Eingabe der Lizenzdaten. Im Fenster „Erweiterte Einstellungen“ (klicken Sie im Hauptmenü auf **Einstellungen** und dann auf **Erweiterte Einstellungen**, oder drücken Sie F5) finden Sie zusätzliche Update-Optionen. Klicken Sie im Hauptmenü auf **Hilfe und Support** > **Lizenzen verwalten**, um einen neuen Lizenzschlüssel einzugeben.



2. **Fehler beim Herunterladen der Update-Dateien** - Ein Grund für den Fehler könnten falsche Einstellungen der Internetverbindung sein. Überprüfen Sie die Internetverbindung, z. B. indem Sie eine beliebige Internetseite im Webbrowser aufrufen. Wenn die Website nicht aufgerufen werden kann, besteht mit ziemlicher Sicherheit keine Internetverbindung. Falls dies der Fall ist, wenden Sie sich an Ihren Internetdienstanbieter.



Hinweis
Weitere Informationen finden Sie in diesem Artikel in der ESET-Knowledgebase.

Einstellungen für Updates

Die Optionen für die Update-Einstellungen finden Sie im Fenster **Erweiterte Einstellungen** (F5) unter **Update**. In diesem Bereich finden Sie Informationen zum Abruf von Updates, z. B. die Liste der Update-Server und die Anmeldedaten für diese Server.

Update-Einstellungen korrekt konfigurieren
Damit Updates fehlerfrei heruntergeladen werden können, müssen Sie alle Uptdate-Einstellungen ordnungsgemäß eingeben. Falls Sie eine Firewall verwenden, stellen Sie sicher, dass das ESET-Programm Verbindungen mit dem Internet herstellen darf (zum Beispiel HTTPS-Verbindungen).

Einfach

Das aktuell verwendete Updateprofil wird im Dropdownmenü **Standardprofil für Updates auswählen** angezeigt.

Im Abschnitt Update-Profile können Sie ein neues Profil erstellen.

Update-Benachrichtigungen konfigurieren (ehemals **Empfangene Update-Benachrichtigungen auswählen**) - Klicken Sie auf **Bearbeiten**, um auszuwählen, welche Anwendungsbenachrichtigungen angezeigt werden. Wählen

Sie aus, ob die Benachrichtigungen **auf dem Desktop angezeigt** und/oder **per E-Mail verschickt werden**.

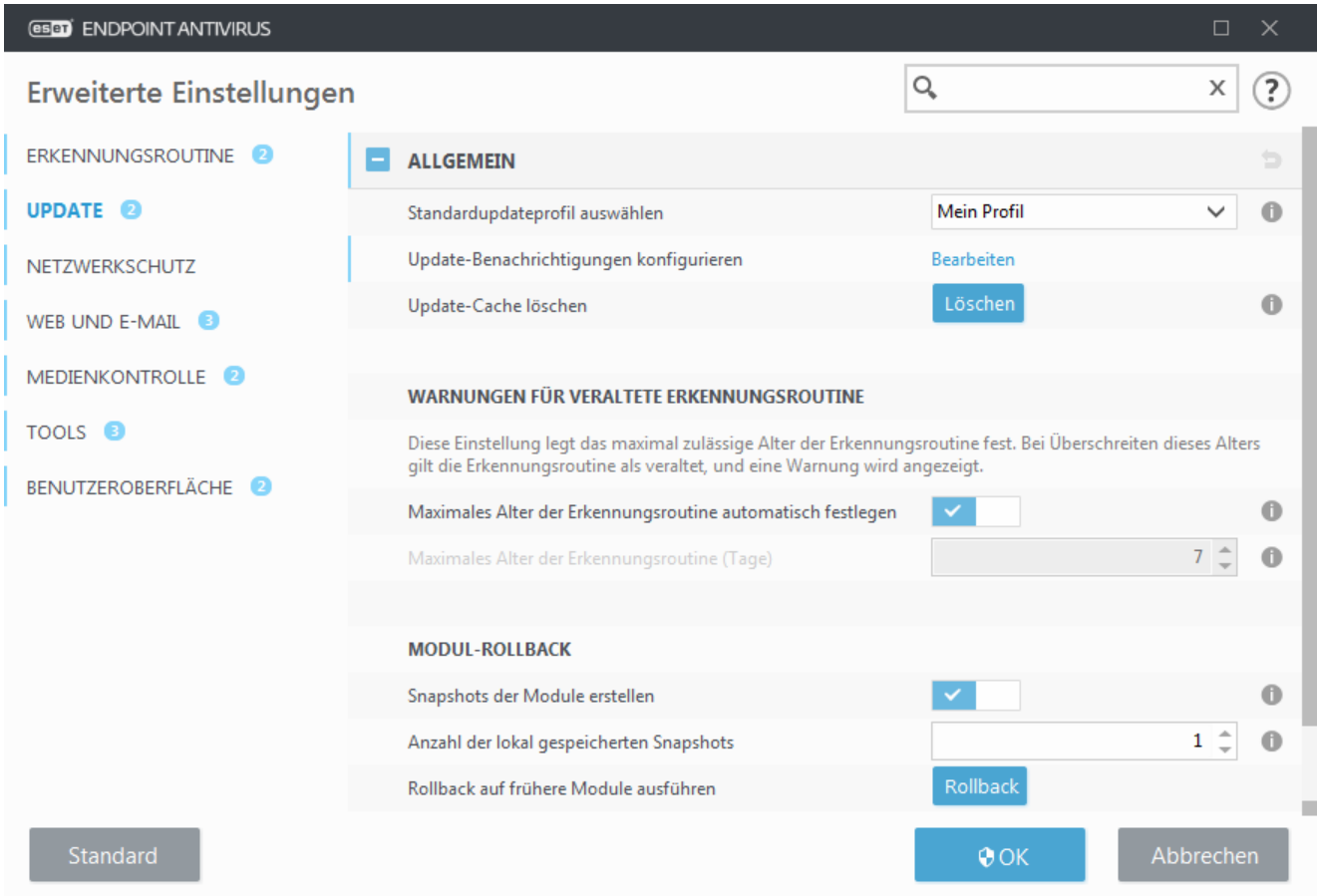
Wenn beim Download der Modulupdates Fehler auftreten, klicken Sie auf **Löschen** neben **Update-Cache löschen**, um die temporären Update-Dateien und den Cache zu löschen.

Warnungen zu veralteter Erkennungsroutine

Maximales Alter der Erkennungsroutine automatisch festlegen - Hier können Sie eine Zeitdauer in Tagen festlegen, nach der die Erkennungsroutine spätestens als veraltet gemeldet wird. Der Standardwert für **Maximales Alter der Erkennungsroutine (Tage)** ist 7.

Modul-Rollback

Wenn Sie vermuten, dass ein neues Update der Erkennungsroutine oder eines Programmmoduls beschädigt oder nicht stabil ist, können Sie einen Rollback auf die vorherige Version ausführen und Updates für einen bestimmten Zeitraum deaktivieren.



Profile

Update-Profile können für verschiedene Update-Konfigurationen und -Tasks erstellt werden. Besonders sinnvoll ist das Erstellen von Update-Profilen für mobile Benutzer, die auf regelmäßige Änderungen bei der Internetverbindung mit entsprechenden Profilen reagieren können.

Im Dropdownmenü **Zu bearbeitendes Profil auswählen** wird das aktuell ausgewählte Profil angezeigt. Standardmäßig ist hier **Mein Profil** ausgewählt.

Um ein neues Profil zu erstellen, klicken Sie neben **Profilliste** auf **Bearbeiten**. Geben Sie den **Namen des Profils**

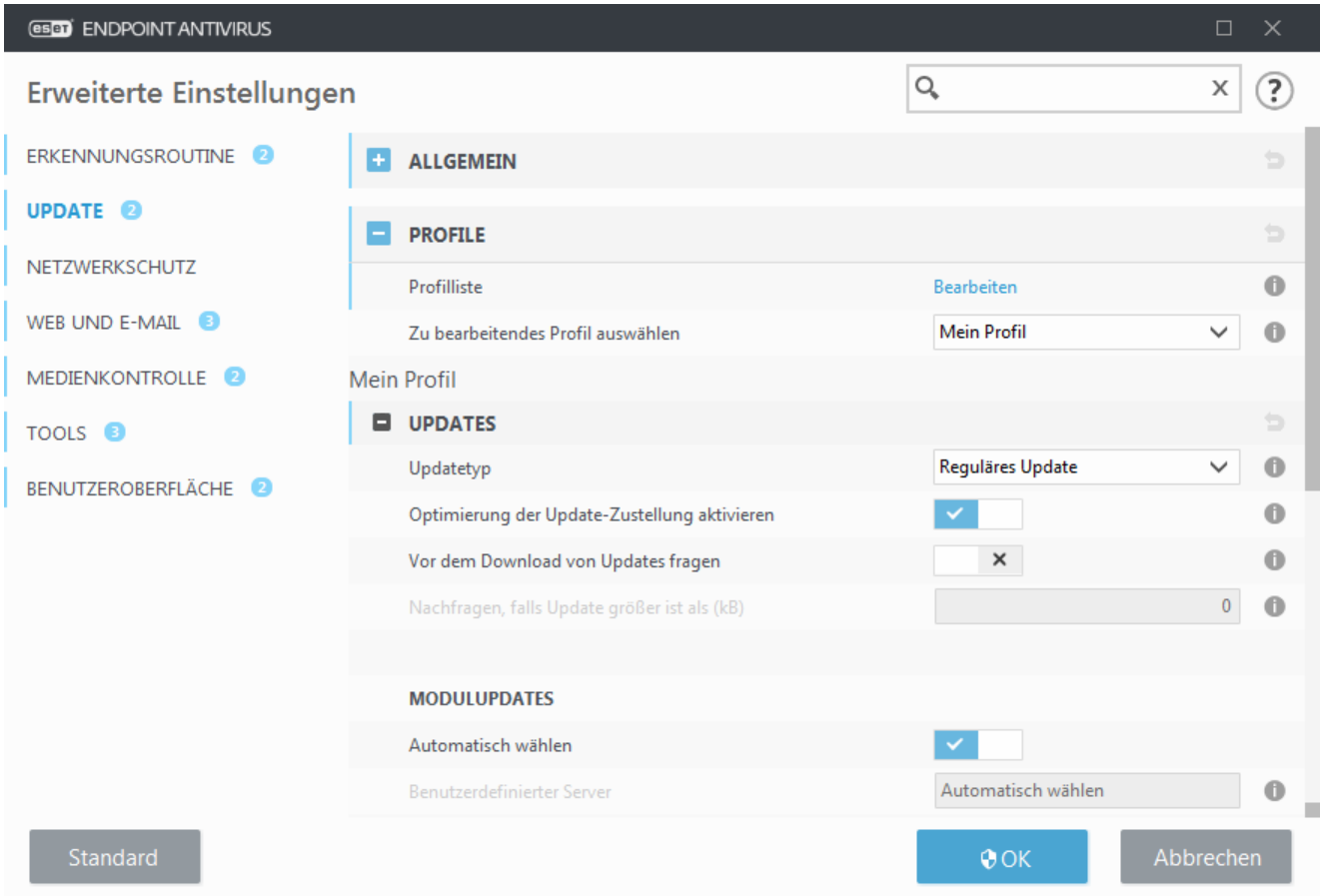
ein und klicken Sie auf **Hinzufügen**.

Updates

Standardmäßig ist der **Update-Typ** auf **Reguläres Update** eingestellt. So werden Updates automatisch von dem ESET-Server heruntergeladen, der am wenigsten belastet ist. Der Testmodus (Option **Test-Update**) stellt Updates bereit, die intern umfangreich geprüft wurden und in absehbarer Zeit allgemein verfügbar sein werden. Wenn Sie den Testmodus aktivieren, können Sie früher von den neuesten Erkennungsmethoden und Fehlerkorrekturen profitieren. Da jedoch letzte Fehler nicht ausgeschlossen werden können, sind diese Updates ausdrücklich NICHT für Rechner in Produktionsumgebungen vorgesehen, die durchgängig stabil und verfügbar laufen müssen. **Verzögerte Updates** führt Updates über besondere Update-Server aus, die neue Versionen der Signaturdatenbank mit einer Verzögerung von mindestens X Stunden zur Verfügung stellen. Die Signaturdatenbanken wurden also bereits in einer Produktionsumgebung getestet und sind daher stabil.

Optimierung der Update-Zustellung aktivieren - Wenn diese Option aktiviert ist, können Updatedateien aus dem CDN (Content Delivery Network) heruntergeladen werden. Wenn Sie diese Einstellung deaktivieren, werden Downloads unter Umständen unterbrochen oder verlangsamt, wenn die dedizierten ESET-Updateserver überlastet sind. Deaktivieren Sie diese Option, wenn eine Firewall den Zugriff auf die IP-Adressen der ESET-Updateserver einschränkt oder die CDN-Dienste nicht erreichbar sind.

Vor dem Download von Updates fragen - Das Programm zeigt eine Benachrichtigung an, und Sie können die Dateidownloads bestätigen oder ablehnen. Wenn die Größe der Update-Datei den unter **Fragen, falls Update größer ist als (KB)** festgelegten Wert überschreitet, wird eine Benachrichtigung angezeigt. Wenn Sie die Updategröße auf 0 kB festlegen, zeigt das Programm immer eine Benachrichtigung an.



Modulupdates

Die Option **Automatisch wählen** ist standardmäßig aktiviert. Die Option **Benutzerdefinierter Server** legt fest, wo die Updates gespeichert werden. Falls Sie einen ESET-Updateserver verwenden, sollten Sie die Standardoption unverändert lassen.

Aktiviert häufigere Updates für Erkennungssignaturen – Die Erkennungssignaturen werden in kürzeren Abständen aktualisiert. Das Deaktivieren dieser Einstellung kann die Erkennungsrate beeinträchtigen.

Modulupdates von Wechselmedien zulassen – Ermöglicht Updates von Wechselmedien, die das entsprechende Installationsprogramm enthalten. Mit der Option **Automatisch** wird das Update im Hintergrund ausgeführt. Wählen Sie **Immer nachfragen** aus, um Update-Dialogfelder anzuzeigen.

Wenn Sie einen lokalen HTTP-Server (auch als „Update-Mirror“ bezeichnet) verwenden, konfigurieren Sie den Server wie folgt:
http://Computername_oder_IP_Adresse:2221

Wenn Sie einen lokalen HTTP-Server mit SSL verwenden, konfigurieren Sie den Server wie folgt:
https://Computername_oder_IP_Adresse:2221

Wenn Sie einen lokalen freigegebenen Ordner verwenden, konfigurieren Sie den Server wie folgt:
\\Computername_oder_IP_Adresse\freigegebener_Ordner

> **HTTP Serverportnummer**
> Die HTTP-Serverportnummer in den oben gezeigten Beispielen hängt davon ab, auf welchem Port Ihr HTTP/HTTPS auf Verbindungen wartet.

Updates für Programmkomponenten

Wählen Sie Updates für Programmkomponenten aus.

Update-Mirror

Siehe Update-Mirror.

Update-Rollback

Wenn Sie befürchten, dass ein neues Update der Erkennungsroutine oder eines Programmmoduls beschädigt oder nicht stabil ist, können Sie einen Rollback zur vorigen Version ausführen und Updates für einen bestimmten Zeitraum deaktivieren. Hier können Sie auch zuvor für einen unbegrenzten Zeitraum deaktivierte Updates wieder aktivieren.

ESET Endpoint Antivirus erfasst Snapshots der Erkennungsroutine und der Programmmodule zur späteren Verwendung mit der Rollback-Funktion. Um Snapshots der Erkennungsroutine zu erstellen, lassen Sie das Kontrollkästchen **Snapshots der Module erstellen** aktiviert. Das Feld **Zahl der lokal gespeicherten Snapshots** legt fest, wie viele vorherige Snapshots der Erkennungsroutine gespeichert werden.

Wenn Sie auf **Rollback ausführen** (**Erweiterte Einstellungen** (F5) > **Update** > **Einfach** > **Modul-Rollback**) klicken, müssen Sie im Dropdownmenü einen Zeitraum auswählen, um festzulegen, wie lange die Updates der Erkennungsroutine und der Programmkomponenten ausgesetzt werden sollen.



Wählen Sie **bis zum Widerrufen**, um keine regelmäßigen Updates auszuführen, bis die Update-Funktion manuell wieder aktiviert wird. Das Aktivieren dieser Option ist mit einem Sicherheitsrisiko verbunden und daher nicht empfehlenswert.

Die Version der Erkennungsroutine wird auf die älteste verfügbare Version herabgestuft und als Snapshot im lokalen Dateisystem des Computers gespeichert.

> **Hinweis**
> Angenommen, die aktuellste Version der Erkennungsroutine ist 19959. Die Versionen 19958 und 19956 sind als Snapshots der Erkennungsroutine gespeichert. Die Version 19957 ist nicht verfügbar, weil der Computer beispielsweise eine Zeit lang heruntergefahren war und ein aktuelleres Update verfügbar war, bevor Version 19957 heruntergeladen wurde. Wenn Sie im Feld **Zahl der lokal gespeicherten Snapshots** den Wert 2 eingegeben haben und auf **Rollback** klicken, wird die Version 19956 der Erkennungsroutine (und Programmmodule) wiederhergestellt. Dieser Vorgang kann einige Zeit in Anspruch nehmen. Überprüfen Sie, ob die Version der Erkennungsroutine im Hauptprogrammfenster von ESET Endpoint Antivirus im Abschnitt Update herabgestuft wurde.

Updates für Programmkomponenten

Im Abschnitt **Updates für Programmkomponenten** finden Sie Optionen zum Aktualisieren der Programmkomponenten. Sie können festlegen, wie das Programm reagieren soll, wenn neue Updates für Programmkomponenten verfügbar sind.

Mit den Updates für Programmkomponenten können neue Funktionen in das Programm integriert oder bestehende Funktionen modifiziert werden. Updates für Programmkomponenten können automatisch oder nach Bestätigung durch den Benutzer gestartet werden. Nach der Installation von Updates der Programmkomponenten muss der Computer möglicherweise neu gestartet werden.

Im Dropdownmenü **Updatemodus** haben Sie drei Optionen zur Auswahl:

- **Vor Updates nachfragen** - Die Standardoption. Wenn Updates für Programmkomponenten verfügbar sind, können Sie diese bestätigen oder ablehnen.
- **Automatisch aktualisieren** - Updates für Programmkomponenten werden automatisch heruntergeladen und installiert. Unter Umständen ist ein Neustart des Computers erforderlich.
- **Nie aktualisieren** - Updates für Programmkomponenten werden nicht ausgeführt. Diese Option wird für Serverinstallationen empfohlen, da Server normalerweise nur im Rahmen geplanter Wartungsarbeiten neu gestartet werden dürfen.

Updates für Programmkomponenten werden standardmäßig von den ESET-Repositoryservern heruntergeladen. In großen oder Offlineumgebungen können Sie den Datenverkehr verteilen, um die Dateien der Programmkomponenten intern zwischenzuspeichern.

Benutzerdefinierte Server für Updates für Programmkomponenten definieren

1.Im Feld **Benutzerdefinierter Server** können Sie den Pfad zu den Updates für Programmkomponenten definieren.
Sie können einen HTTP(S)-Link, einen Pfad zu einer SMB-Netzwerkfreigabe, ein lokales Laufwerk oder ein Wechselmedium angeben. Verwenden Sie für Netzlaufwerke den UNC-Pfad anstelle des zugeordneten Laufwerksbuchstabens.

2.Lassen Sie die Felder **Benutzername** und **Passwort** leer, falls keine Authentifizierung erforderlich ist. Geben Sie hier bei Bedarf die Anmeldedaten für die HTTP-Authentifizierung bei Ihrem benutzerdefinierten Webserver ein.

3.Bestätigen Sie die Änderungen und testen Sie mit einem normalen ESET Endpoint Antivirus-Update, ob Updates für Programmkomponenten vorhanden sind.



Hinweis
Die Auswahl der geeigneten Option hängt vom jeweiligen Computer ab, auf dem die Einstellungen ausgeführt werden. Beachten Sie die unterschiedliche Funktion von Arbeitsplatzcomputern und Servern. Das automatische Neustarten eines Servers nach einem Update kann beispielsweise schwerwiegende Folgen haben.

Verbindungsoptionen

Um die Proxyserver-Einstellungen für ein bestimmtes Updateprofil zu öffnen, klicken Sie auf **Update** unter **Erweiterte Einstellungen** (F5) und dann auf **Profile** > **Updates** > **Verbindungsoptionen**.

Proxyserver

Klicken Sie auf das Dropdownmenü **Proxy-Modus** und wählen Sie eine dieser drei Optionen aus:

- Keinen Proxyserver verwenden
- Verbindung über Proxyserver
- In Systemsteuerung eingestellten Proxy verwenden

Wählen Sie die Option **Globale Proxyeinstellungen verwenden** aus, um die unter „Erweiterte Einstellungen“ (**Tools** > **Proxyserver**) festgelegte Proxyserver-Konfiguration zu übernehmen.

Mit der Option **Keinen Proxyserver verwenden** legen Sie fest, dass kein Proxyserver für Updates von ESET Endpoint Antivirus genutzt wird.

Wählen Sie die Option Verbindung über Proxyserver in den folgenden Fällen aus:

- Für Updates von ESET Endpoint Antivirus wird ein anderer Proxyserver als der unter **Einstellungen** > **Proxyserver** konfigurierte Server verwendet. In dieser Konfiguration werden die Informationen für den neuen Proxy unter **Proxyserver**-Adresse, Kommunikations-**Port** (standardmäßig 3128) sowie bei Bedarf

Benutzername und **Passwort** für den Proxyserver angegeben.
• Die Proxyserver-Einstellungen werden nicht global festgelegt, allerdings lädt ESET Endpoint Antivirus Updates über einen Proxyserver herunter.
• Ihr Computer über einen Proxyserver mit dem Internet verbunden ist. Bei der Installation werden die Einstellungen aus Internet Explorer übernommen. Falls Sie später Änderungen vornehmen (wenn Sie z. B. den Internetanbieter wechseln), müssen Sie diese Proxy-Einstellungen prüfen und ggf. anpassen. Andernfalls kann keine Verbindung zu den Update-Servern hergestellt werden.

Die Standardeinstellung für den Proxyserver ist **In Systemsteuerung eingestellten Proxy verwenden**.

Direktverbindung verwenden, wenn der Proxy nicht verfügbar ist – Der Proxy wird bei der Aktualisierung umgangen, wenn er nicht erreichbar ist.

Windows-Freigaben

Beim Aktualisieren von einem lokalen Server mit einem Windows NT-Betriebssystem ist standardmäßig eine Authentifizierung für jede Netzwerkverbindung erforderlich.

Um ein entsprechendes Konto zu konfigurieren, wählen Sie einen Eintrag im Dropdownmenü **Lokaler Benutzertyp** aus:

- **Systemkonto (Standard)**
- **Aktueller Benutzer**
- **Angegebener Benutzer**

Wählen Sie **Systemkonto (Standard)**, um das Systemkonto für die Authentifizierung zu verwenden. Normalerweise findet keine Authentifizierung statt, wenn in den Haupteinstellungen für Updates keine Anmeldedaten angegeben sind.

Wenn sich das Programm mit dem Konto des aktuell angemeldeten Benutzers anmelden soll, wählen Sie **Aktueller Benutzer**. Nachteil dieser Lösung ist, dass das Programm keine Verbindung zum Update-Server herstellen kann, wenn kein Benutzer angemeldet ist.

Wählen Sie **Folgender Benutzer**, wenn das Programm ein spezielles Benutzerkonto für die Authentifizierung verwenden soll. Nutzen Sie diese Option, wenn eine Anmeldung mit dem standardmäßigen Systemkonto nicht möglich ist. Beachten Sie, dass für das ausgewählte Benutzerkonto Zugriffsrechte auf den Ordner mit den Update-Dateien definiert sein müssen. Wenn keine Zugriffsrechte definiert sind, kann das Programm keine Updates abrufen.

Die Einstellungen **Benutzername** und **Passwort** sind optional.



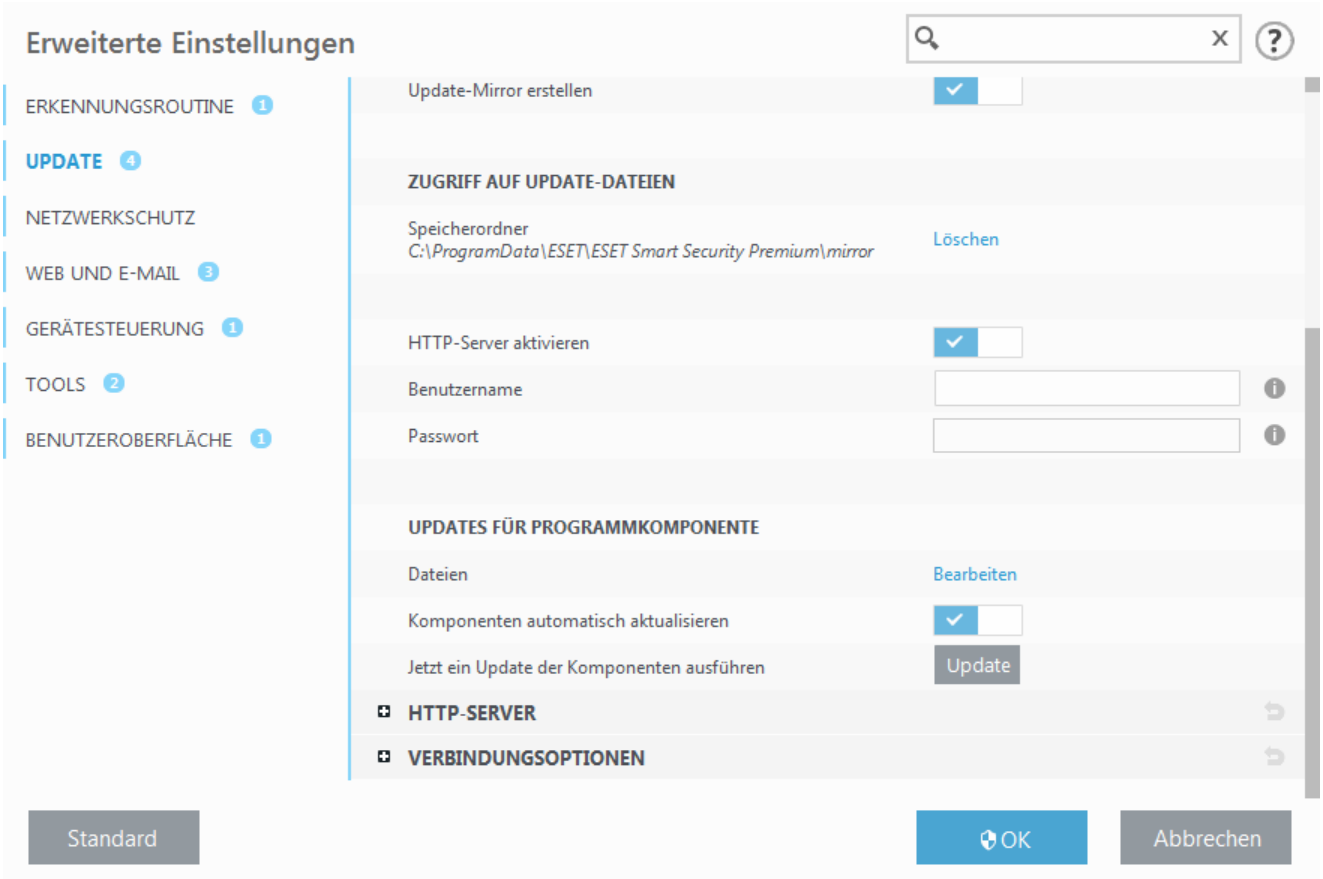
Warnung
Wenn entweder **Aktueller Benutzer** oder **Folgender Benutzer** aktiviert ist, kann ein Fehler beim Wechsel der Identität zum gewünschten Benutzer auftreten. Aus diesem Grund wird empfohlen, die LAN-Anmeldedaten in den Haupteinstellungen für Updates einzugeben. In diesen Update-Einstellungen geben Sie die Anmeldedaten wie folgt ein: *Domänenname**Benutzer* (bei einer Arbeitsgruppe geben Sie *Arbeitsgruppenname**Name* ein) und das Passwort. Bei Aktualisierung von der HTTP-Version des lokalen Servers ist keine Authentifizierung erforderlich.

Wählen Aktivieren Sie die Option **Nach Update Verbindung zum Server trennen aus, um das Trennen der Verbindung zu erzwingen**, wenn die Verbindung zum Server nach dem Abrufen von Update-Dateien aktiv bleibt.

Update-Mirror

ESET Endpoint Antivirus bietet Ihnen die Möglichkeit, Kopien der Update-Dateien zu erstellen. Diese können Sie dann zur Aktualisierung anderer Workstations im Netzwerk verwenden. Das Verwenden eines „Update-Mirrors“ - das Vorhalten von Kopien der Update-Dateien im lokalen Netzwerk - kann vorteilhaft sein, da die Dateien dann nicht von allen Arbeitsplatzcomputern einzeln über das Internet heruntergeladen werden müssen. Updates werden auf den lokalen Mirror-Server heruntergeladen und von dort an die Arbeitsstationen verteilt. Die Internetverbindung wird erheblich entlastet. Das Aktualisieren der Client-Computer von einem Update-Mirror optimiert die Lastenverteilung im Netzwerk und entlastet Internetverbindungen.

Sie finden die Konfigurationsoptionen für den lokalen Mirror-Server in den erweiterten Einstellungen unter **Update**. Drücken Sie die Taste **F5**, klicken Sie auf **Update** > **Profile und wählen Sie die** Registerkarte **Mirror** aus.



Um einen Mirror auf einem Clientcomputer zu erstellen, aktivieren Sie **Update-Mirror erstellen**. Durch Aktivieren dieser Option stehen weitere Konfigurationsoptionen für Update-Mirrors zur Verfügung, die beispielsweise die Art des Zugriffs auf Update-Dateien und den Pfad zu den Kopien der Update-Dateien betreffen.

Zugriff auf Update-Dateien

HTTP-Server aktivieren - Wenn dieses Kontrollkästchen aktiviert ist, können Update-Dateien über HTTP abgerufen werden. Hierzu sind keine Anmeldedaten erforderlich.

Die Zugriffsmethoden auf den Mirror-Server sind unter Aktualisieren über Update-Mirror ausführlich beschrieben. Es gibt zwei Grundvarianten des Zugriffs auf einen Update-Mirror: Der Ordner mit den Update-Dateien kann eine

Netzwerkfreigabe sein, oder der Zugriff auf den Update-Mirror auf einem HTTP-Server kann über Clients erfolgen.

Der für die Update-Dateien vorgesehene Ordner wird unter **Ordner zum Speichern der Update-Dateien** festgelegt. Um einen anderen Ordner auszuwählen, klicken Sie zunächst auf **Löschen**, um den vordefinierten Ordner *C:\ProgramData\ESET\ESET Endpoint Antivirus\mirror* zu löschen, und dann auf **Bearbeiten**, um nach einem lokalen oder einem Netzwerkordner zu suchen. Wenn für den angegebenen Ordner eine Authentifizierung erforderlich ist, müssen die Anmeldedaten in die Felder **Benutzername** und **Passwort** eingegeben werden. Wenn sich der Speicherordner auf einem Windows NT/2000/XP-Netzlaufwerk befindet, wird ein Benutzerkonto mit Schreibzugriff auf den Ordner benötigt. Der Benutzername muss im Format *Domäne/Benutzer* oder *Arbeitsgruppe/Benutzer* eingegeben werden. Denken Sie daran, auch die entsprechenden Passwörter einzugeben.

Updates für Programmkomponenten

Dateien - Bei der Konfiguration des Mirrors können Sie die Sprachversionen der herunterzuladenden Updates festlegen. Die ausgewählte Sprache muss vom konfigurierten Mirror-Server unterstützt werden.

Komponenten automatisch aktualisieren – Ermöglicht das Installieren von neuen Funktionen und Updates für bestehende Funktionen. Updates für Programmkomponenten können automatisch oder nach Bestätigung durch den Benutzer gestartet werden. Nach der Installation von Updates der Programmkomponenten muss der Computer möglicherweise neu gestartet werden.

Komponenten jetzt aktualisieren - Hiermit werden die Programmkomponenten auf die neueste Version aktualisiert.



HTTP-Server

Server-Port - Als Server-Port wird standardmäßig 2221 festgelegt.

Authentifizierung - Dient zur Festlegung der Authentifizierungsmethode für den Zugriff auf die Update-Dateien. Folgende Optionen stehen zur Verfügung: **Keine**, **Basis** und **NTLM**. Wählen Sie **Basic** für Base64-Verschlüsselung und einfache Authentifizierung mit Benutzername und Passwort. Bei Auswahl von **NTLM** wird eine sichere Verschlüsselungsmethode verwendet. Zur Authentifizierung wird der auf dem Computer erstellte Benutzer verwendet, der die Update-Dateien freigegeben hat. Die Standardeinstellung ist **Keine**, sodass für den Zugriff auf die Update-Dateien keine Authentifizierung erforderlich ist.

Hängen Sie die **Zertifikatskettendatei** an oder generieren Sie ein eigensigniertes Zertifikat, wenn Sie den HTTP-Server mit HTTPS (SSL)-Unterstützung ausführen möchten. Folgende **Zertifikattypen** stehen zur Verfügung: ASN, PEM und PFX. Für zusätzliche Sicherheit können Update-Dateien mit dem HTTPS-Protokoll heruntergeladen werden. Das Nachverfolgen der übertragenen Daten und Anmeldeberechtigungen ist bei der Verwendung dieses Protokolls nahezu unmöglich. Die Option **Typ des privaten Schlüssels** wird standardmäßig auf **Integriert** eingestellt (und die Option **Datei mit privatem Schlüssel** ist standardmäßig deaktiviert). Dies bedeutet, dass der private Schlüssel Bestandteil der ausgewählten Zertifikatskettendatei ist.

Hinweis
Die Felder mit den Anmeldedaten (**Benutzername** und **Passwort**) sind nur für den Zugriff auf den Proxyserver vorgesehen. Geben Sie in diesen Feldern nur Daten ein, wenn diese für den Zugriff auf den Proxyserver erforderlich sind. Beachten Sie, dass in diese Felder nicht das Passwort und der Benutzername für ESET Endpoint Antivirus eingetragen werden. Eine Eingabe ist nur dann erforderlich, wenn Sie für die Internetverbindung über den Proxyserver ein Passwort benötigen.

Aktualisieren über Update-Mirror

Es gibt zwei grundlegende Methoden zum Konfigurieren eines Mirrors. Ein Mirror ist im Grunde ein Repository, aus dem Client Update-Dateien herunterladen können. Der Ordner mit den Update-Dateien kann als Netzwerkfreigabe oder als HTTP-Server dargestellt werden.

Zugriff auf den Update-Mirror über internen HTTP-Server

Diese Variante ist die Standardeinstellung des Programms und wird automatisch verwendet. Um über den HTTP-Server auf den Update-Mirror zugreifen zu können, wechseln Sie zu **Erweiterte Einstellungen** > **Update** > **Profile** > **Mirror** und wählen Sie **Update-Mirror erstellen** aus.

Im Bereich **HTTP-Server** der Registerkarte **Update-Mirror** können Sie den **Server-Port** angeben, auf dem der HTTP-Server Anfragen empfängt, und den Typ der **Authentifizierung** festlegen, die vom HTTP-Server verwendet wird. In der Standardeinstellung ist der Server-Port **2221** angegeben. Unter **Authentifizierung** wird die Authentifizierungsmethode für den Zugriff auf die Update-Dateien festgelegt. Folgende Optionen stehen zur Verfügung: **Keine**, **Basic** und **NTLM**. Wählen Sie **Basic** für Base64-Verschlüsselung und einfache Authentifizierung mit Benutzername und Passwort. Bei Auswahl von **NTLM** wird eine sichere Verschlüsselungsmethode verwendet. Zur Authentifizierung wird der auf dem Computer erstellte Benutzer verwendet, der die Update-Dateien freigegeben hat. Die Standardeinstellung ist **Keine**, sodass für den Zugriff auf die Update-Dateien keine Authentifizierung erforderlich ist.

Warnung
Wenn Sie den Zugriff auf die Update-Dateien über einen HTTP-Server zulassen möchten, muss sich der Ordner mit den Kopien der Update-Dateien auf demselben Computer befinden wie die Instanz von ESET Endpoint Antivirus, mit der dieser Ordner erstellt wird.

SSL für HTTP-Server

Hängen Sie die **Zertifikatskettendatei** an oder generieren Sie ein eigensigniertes Zertifikat, wenn Sie den HTTP-Server mit HTTPS (SSL)-Unterstützung ausführen möchten. Folgende Zertifikattypen stehen zur Verfügung: **PEM, PFX** und **ASN**. Für zusätzliche Sicherheit können Update-Dateien mit dem HTTPS-Protokoll heruntergeladen werden. Das Nachverfolgen der übertragenen Daten und Anmeldeberechtigungen ist bei der Verwendung dieses Protokolls nahezu unmöglich. **Typ des privaten Schlüssels** ist standardmäßig auf **Integriert** festgelegt, was bedeutet, dass der private Schlüssel Bestandteil der ausgewählten Zertifikatskettendatei ist.

Hinweis
Nach mehreren erfolglosen Versuchen, die Erkennungsroutine über den Update-Mirror zu aktualisieren, wird im Update-Bereich des Hauptmenüs der Fehler **Ungültiger Benutzername und/oder ungültiges Passwort** angezeigt. Navigieren Sie in diesem Fall zu **Erweiterte Einstellungen** > **Update** > **Profile** > **Mirror** und überprüfen Sie den Benutzernamen und das Passwort. Die häufigste Ursache für diesen Fehler sind falsch eingegebene Authentifizierungsdaten.



Nach Abschluss der Konfiguration des Mirror-Servers müssen Sie den neuen Update-Server auf Clientcomputern hinzufügen. Führen Sie dazu die folgenden Schritte aus:

- **Öffnen Sie die erweiterten Einstellungen**(F5) und klicken Sie auf **Update** > **Profile** > **Einfach**.

- Deaktivieren Sie **Automatisch auswählen** und fügen Sie im Feld **Update-Server** einen neuen Server in einem der folgenden Formate hinzu:
http://IP-Adresse_Ihres_Servers:2221
https://IP_adresse_des_servers:2221 (bei Verwendung von SSL)

Zugriff auf den Update-Mirror über Systemfreigaben

Zunächst muss ein freigegebener Ordner auf einem lokalen Laufwerk oder auf einem Netzlaufwerk erstellt werden. Beachten Sie beim Erstellen des Ordners für den Update-Mirror Folgendes: Der Benutzer, der Dateien im Ordner speichert, benötigt Schreibzugriff, während die Benutzer, die ESET Endpoint Antivirus über diesen Ordner aktualisieren, eine Leseberechtigung benötigen.

Konfigurieren Sie als Nächstes den Zugriff auf den Update-Mirror im Bereich **Erweiterte Einstellungen** > **Update** > **Profile** > **Mirror**, indem Sie die Option **Dateien über integrierten HTTP-Server bereitstellen** deaktivieren. Diese Option ist in der Standardeinstellung des Programms aktiviert.

Wenn der freigegebene Ordner sich auf einem anderen Computer im Netzwerk befindet, ist für den Zugriff auf den anderen Computer eine Authentifizierung erforderlich. Um die Anmeldedaten anzugeben, öffnen Sie die **Erweiterten Einstellungen** (F5) von ESET Endpoint Antivirus und klicken Sie auf **Update** > **Profile** > **Verbindung mit LAN herstellen als**. Diese Einstellung entspricht der Einstellung für Updates, wie im Kapitel Verbindung mit LAN herstellen als beschrieben.

Um auf den Mirror-Ordner zugreifen zu können, müssen Sie diesen Vorgang mit demselben Konto ausführen, das Sie auch für die Anmeldung bei dem Computer verwenden, auf dem Sie den Mirror erstellen. Falls der Computer Teil einer Domäne ist, geben Sie den Benutzernamen im Format „Domäne\Benutzer“ an. Falls der Computer nicht Teil einer Domäne ist, verwenden Sie „IP_Adresse_Ihres_Servers\Benutzer“ bzw. „Hostname\Benutzer“.

Nach Abschluss der Konfiguration des Update-Mirrors geben Sie auf den Client-Workstations jeweils *UNC**PFAD* als Update-Server ein. Gehen Sie hierbei folgendermaßen vor:

1. Klicken Sie in ESET Endpoint Antivirus unter **Erweiterte Einstellungen** auf **Update** > **Profile** > **Updates**.

2. Deaktivieren Sie die Option **Automatisch auswählen** neben **Modul-Updates** und geben Sie einen neuen Server in das Feld**Update-Server im** Format *UNC**PFAD* ein.



Hinweis
Damit Updates fehlerfrei funktionieren, muss der Pfad zum Ordner mit den Kopien der Update-Dateien als UNC-Pfad angegeben werden. Updates über zugeordnete Netzlaufwerke können möglicherweise nicht ausgeführt werden.



Mirror mit dem Mirror-Tool erstellen
Die vom Mirror-Tool erstellte Ordnerstruktur unterscheidet sich von der Struktur des Endpunkt-Mirrors. Jeder Ordner enthält Updatedateien für eine Gruppe von Produkten. Sie müssen den vollständigen Pfad zum korrekten Ordner in den Updateeinstellungen des Produkts angeben, das den Mirror verwendet.
Um beispielsweise ESMC 7 über den Mirror zu aktualisieren, leben Sie den Update-Server wie folgt fest (je nach Stammverzeichnis Ihres HTTP-Servers):
`http://your_server_address/mirror/eset_upd/era6`

Der letzte Bereich dient der Steuerung der Programmkomponenten (PCUs). Standardmäßig werden heruntergeladene Programmkomponenten zur Kopie auf den lokalen Update-Mirror vorbereitet. Wenn die Option **Updates für Programmkomponenten** aktiviert ist, ist es nicht erforderlich, auf **Update** zu klicken, da die Dateien bei ihrer Verfügbarkeit automatisch auf den lokalen Update-Mirror kopiert werden. Weitere Informationen zu Updates von Programmkomponenten finden Sie unter Update-Modus.

Fehlerbehebung bei Problemen mit Updates über Update-Mirror

Die meisten Probleme bei Updates von einem Update-Mirror haben eine oder mehrere der folgenden Ursachen: falsche Einstellungen für den Mirror-Ordner, falsche Anmeldedaten für den Mirror-Ordner, falsche Konfiguration auf lokalen Computern, die versuchen, Update-Dateien vom Update-Mirror herunterzuladen, oder eine Kombination der angegebenen Gründe. Hier erhalten Sie einen Überblick über die am häufigsten auftretenden Probleme bei Updates von einem Update-Mirror:

ESET Endpoint Antivirus meldet einen Fehler bei der Verbindung mit dem Mirror-Server– Wahrscheinlich wird dieser Fehler durch falsche Angaben zum Update-Server (Netzwerkpfad zum Mirror-Ordner) verursacht, von dem die lokalen Computer Updates herunterladen. Um den Ordner zu überprüfen, klicken Sie auf das Windows-Menü **Start** > **Ausführen**, geben Sie den Ordnernamen ein und klicken Sie auf **OK**. Daraufhin sollte der Inhalt des Ordners angezeigt werden.

ESET Endpoint Antivirus verlangt einen Benutzernamen und ein Passwort– Es wurden wahrscheinlich falsche Anmeldedaten (Benutzername und Passwort) im Bereich „Update“ angegeben. Benutzername und Passwort werden für den Zugriff auf den Update-Server verwendet, über den das Programm aktualisiert wird. Vergewissern Sie sich, dass die Anmeldedaten korrekt und im richtigen Format eingegeben sind. Verwenden Sie das Format Domäne/Benutzername bzw. Arbeitsgruppe/Benutzername und die entsprechenden Passwörter. Auch wenn der Zugriff auf den Mirror-Server für die Gruppe „Jeder“ gestattet wurde, sollten Sie bedenken, dass deshalb nicht jedem beliebigen Benutzer der Zugriff gewährt wird. „Jeder“ umfasst keine nicht autorisierten Benutzer, sondern bedeutet, dass alle Benutzer der Domäne auf den Ordner zugreifen können. Daher müssen, auch wenn die Gruppe „Jeder“ auf den Ordner zugreifen kann, in den Update-Einstellungen ein Benutzername und ein Passwort für die Domäne eingegeben werden.

ESET Endpoint Antivirus meldet einen Fehler bei der Verbindung mit dem Mirror-Server– Der für den Zugriff auf die HTTP-Version des Update-Mirrors angegebene Port ist blockiert.

ESET Endpoint Antivirus meldet einen Fehler beim Download von Updatedateien – Dieser Fehler wird vermutlich durch falsche Angaben zum Update-Server (Netzwerkpfad zum Mirror-Ordner) verursacht, von dem die lokalen Computer Updates herunterladen.

So erstellen Sie Update-Tasks

Updates können manuell ausgeführt werden. Klicken Sie dazu im Hauptmenü auf **Update**, und wählen Sie im daraufhin angezeigten Dialogfenster die Option **Nach Updates suchen** aus.

Darüber hinaus können Sie Updates auch als geplante Tasks einrichten. Um einen geplanten Task zu konfigurieren, klicken Sie auf **Tools** > **Taskplaner**. Standardmäßig sind in ESET Endpoint Antivirus folgende Tasks aktiviert:

- **Automatische Updates in festen Zeitabständen**
- **Automatische Updates beim Herstellen von DFÜ-Verbindungen**
- **Automatische Updates beim Anmelden des Benutzers**

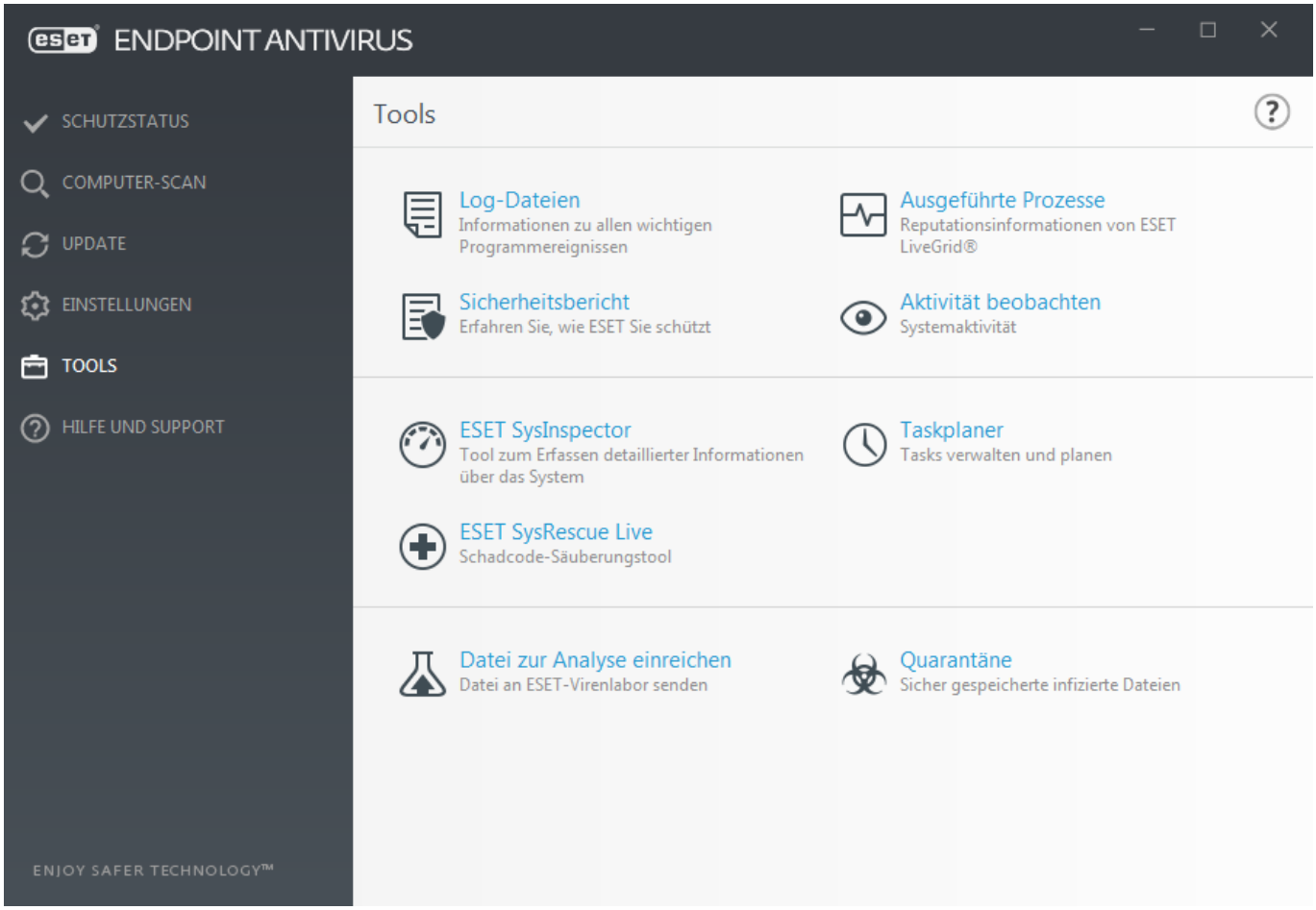
Jeder Update-Task kann bei Bedarf angepasst werden. Neben den standardmäßig ausgeführten Update-Tasks können zusätzliche Update-Tasks mit benutzerdefinierten Einstellungen erstellt werden. Weitere Informationen zum Erstellen und Konfigurieren von Update-Tasks finden Sie unter Taskplaner.

Tools

Das Menü **Tools** enthält Module, die die Verwaltung des Programms vereinfachen und zusätzliche Optionen für erfahrene Benutzer bereitstellen.

Dieser Bereich enthält die folgenden Elemente:

- Log-Dateien
- Sicherheitsbericht
- Ausgeführte Prozesse (wenn ESET LiveGrid® in ESET Endpoint Antivirus aktiviert ist)
- Aktivität beobachten
- Taskplaner
- ESET SysInspector
- ESET SysRescue Live – Leitet Sie zur ESET SysRescue Live-Seite weiter, auf der Sie das ESET SysRescue Live .iso CD/DVD-Abbild herunterladen können.
- Quarantäne
- Datei zur Analyse einreichen - Ermöglicht Ihnen, eine verdächtige Datei zur Analyse bei ESET einzureichen. Das Dialogfenster, das nach dem Klicken auf diese Option angezeigt wird, wird in diesem Abschnitt beschrieben.



Log-Dateien

Die Log-Dateien enthalten Informationen zu allen wichtigen aufgetretenen Programmereignissen und geben einen Überblick über erkannte Bedrohungen. Logs sind unabdingbar für die Systemanalyse, die Erkennung von Problemen oder Risiken sowie die Fehlerbehebung. Die Logs werden im Hintergrund ohne Eingriffe des Benutzers erstellt. Welche Informationen aufgezeichnet werden, ist abhängig von den aktuellen Einstellungen für die Mindestinformation in Logs. Textnachrichten und Logs können direkt aus ESET Endpoint Antivirus heraus angezeigt werden. Das Archivieren von Log-Dateien erfolgt ebenfalls direkt über das Programm.

Log-Dateien können über das Hauptprogrammfenster aufgerufen werden, indem Sie auf **Tools** > **Log-Dateien** klicken. Wählen Sie im Dropdown-Menü **Log** den gewünschten Log-Typ aus. Folgende Logs sind verfügbar:

- **Erkennungen** – Dieses Log enthält detaillierte Informationen über die von den ESET Endpoint Antivirus-Modulen entdeckte eingedrungene Schadsoftware, darunter der Erkennungszeitpunkt, der Name des Ereignisses, deren Ort, die ausgeführte Aktion und der Name des Benutzers, der zum jeweiligen Zeitpunkt angemeldet war. Doppelklicken Sie auf einen Log-Eintrag, um die Details in einem separaten Fenster anzuzeigen. Nicht gesäuberte Bedrohungen werden immer mit rotem Text auf hellrotem Hintergrund angezeigt. Gesäuberte Bedrohungen sowie nicht gesäuberte und potenziell unsichere oder unerwünschte Anwendungen werden mit gelbem Text auf weißem Hintergrund angezeigt.

- **Ereignisse** – Alle von ESET Endpoint Antivirus ausgeführten wichtigen Aktionen werden im Ereignis-Log aufgezeichnet. Das Ereignis-Log enthält Informationen über Ereignisse und im Programm aufgetretene Fehler. Es unterstützt Systemadministratoren und Benutzer bei der Fehlerbehebung. Die hier aufgeführten Informationen sind oftmals hilfreich, um ein im Programm aufgetretenes Problem zu beheben.

- **Computer-Scan** – Alle Prüfergebnisse werden in diesem Fenster angezeigt. Jede Zeile entspricht der Überprüfung eines einzelnen Computers. Durch Doppelklicken auf einen Eintrag können Sie Einzelheiten zu der entsprechenden Prüfung anzeigen.

- **Gesperrte Dateien** – Enthält Einträge zu Dateien, die gesperrt waren und nicht geöffnet werden konnten. Das Protokoll enthält den Grund und das Quellmodul, das die Datei gesperrt hat, sowie die Anwendung und den Benutzer, der die Datei ausgeführt hat.

- **Verschickte Dateien** – Enthält eine Aufzeichnung der Dateien, die zur Analyse an ESET LiveGrid® oder ESET Dynamic Threat Defense verschickt wurden.

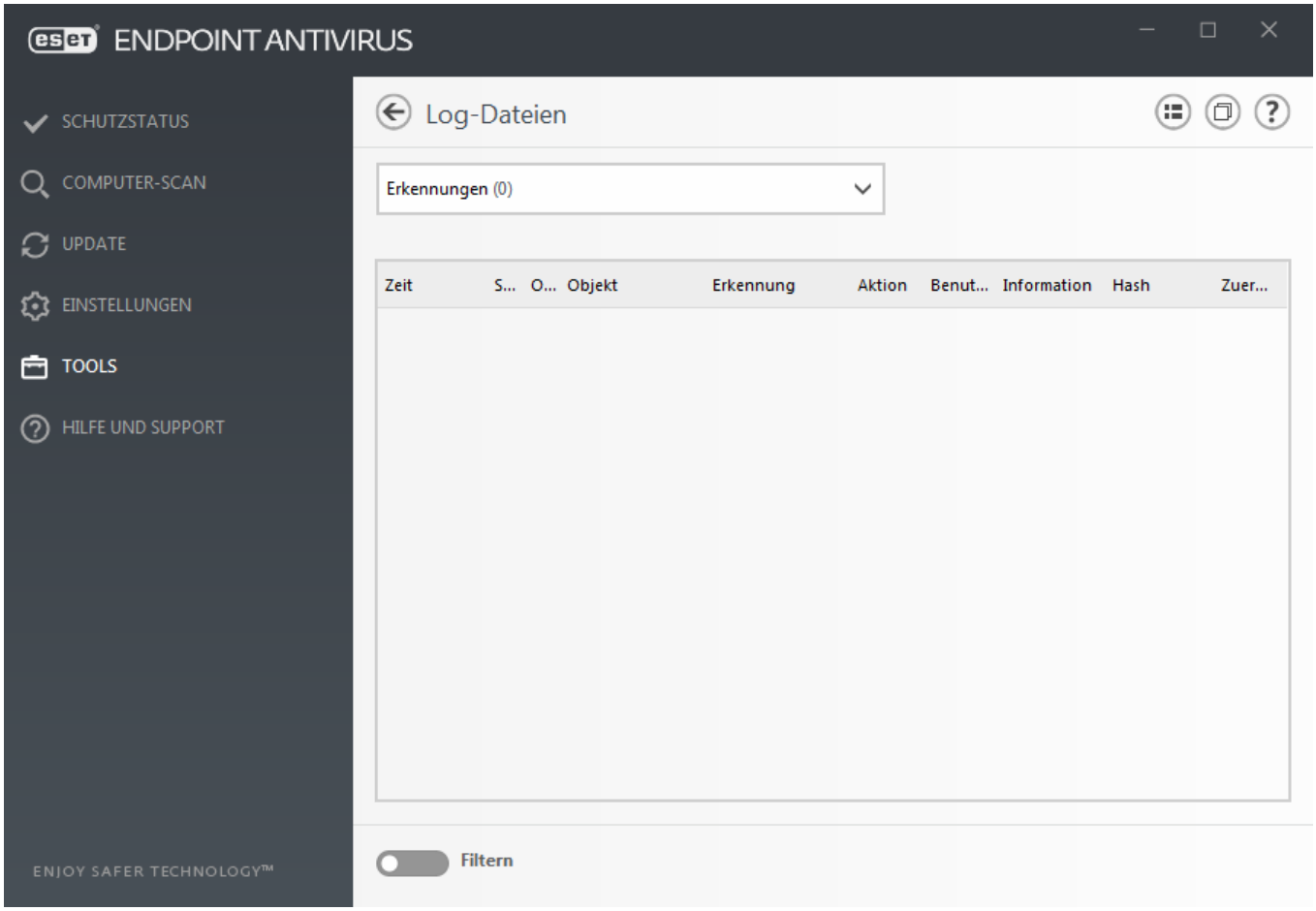
- **Audit-Logs** – Diese Logs enthalten Informationen zu Datum und Uhrzeit der Änderung, Art der Änderung, eine Beschreibung sowie eine Quelle und den Benutzer. Weitere Informationen finden Sie unter Audit-Logs.

- **HIPS** – Enthält Einträge spezifischer Regeln, die zum Aufzeichnen markiert wurden. Das Protokoll zeigt die Anwendung an, die den Vorgang angefordert hat, das Ergebnis (ob der Vorgang zugelassen oder blockiert wurde) sowie den erstellten Regelnamen.

- **Netzwerk-Schutz** – Im Firewall-Log werden alle vom Netzwerkangriffsschutz erkannten Angriffe angezeigt. Hier erhalten Sie Informationen über alle Angriffe auf Ihren Computer. In der Spalte Ereignis werden die entdeckten Angriffe angezeigt. Unter Quelle erfahren Sie mehr über den Angreifer. Die Spalte Protokoll zeigt das für den Angriff verwendete Datenübertragungsprotokoll an. Eine Analyse des Firewall-Logs hilft Ihnen dabei, Eindringversuche von Schadsoftware rechtzeitig zu erkennen, um den unerlaubten Zugriff auf Ihr System zu verhindern. Weitere Informationen zu bestimmten Netzwerkangriffen finden Sie unter IDS und erweiterte Optionen.

- **Gefilterte Websites** – Diese Liste enthält die durch den Web-Schutz gesperrten Websites. Die Logs enthalten die Uhrzeit, die URL, den Benutzer und die Anwendung, die eine Verbindung zur gegebenen Website hergestellt hat.

- **Medienkontrolle** – Enthält Datensätze zu Wechselmedien oder externen Geräten, die an den Computer angeschlossen wurden. Nur Geräte mit einer Regel für die Medienkontrolle werden in die Log-Datei aufgenommen. Wenn auf ein angeschlossenes Gerät keine Regel zutrifft, wird für das Gerät kein Log-Eintrag erstellt. Hier können Sie außerdem Details wie Gerätetyp, Seriennummer, Herstellername und Mediengröße (je nach Verfügbarkeit der Informationen) anzeigen.



Wählen Sie den Inhalt eines Logs aus und drücken Sie `Ctrl + C`**, um die Daten in die Zwischenablage zu kopieren**. Halten Sie `Ctrl + Shift` gedrückt, um mehrere Einträge auszuwählen.

Klicken Sie auf **Filtern**, um das Fenster Log-Filter zu öffnen, wo Sie die Filterkriterien definieren können.

Klicken Sie mit der rechten Maustaste auf einen Eintrag, um das Kontextmenü zu öffnen. Im Kontextmenü stehen folgende Optionen zur Verfügung:

- **Anzeigen** – Zeigt weitere detaillierte Informationen zum ausgewählten Log in einem neuen Fenster an.
- **Gleiche Datensätze filtern** - Wenn Sie diesen Filter aktivieren, werden nur Einträge desselben Typs angezeigt (Diagnose, Warnungen, ...).
- **Filter/Suchen** – Wenn Sie diese Option anklicken, können Sie im Fenster Log-Filter Filterkriterien für bestimmte Log-Einträge festlegen.
- **Filter aktivieren** – Aktiviert die Filtereinstellungen.
- **Filter deaktivieren** – Setzt alle Filtereinstellungen (wie oben beschrieben) zurück
- **Kopieren/Alles kopieren** – Kopiert die Informationen zu allen im Fenster angezeigten Einträgen
- **Löschen/Alle löschen** – Löscht die ausgewählten oder alle angezeigten Einträge; für diese Option sind Administratorrechte erforderlich
- **Exportieren...** – Exportiert Informationen zu den Einträgen im XML-Format.

- **Alle exportieren ...** – Exportiert Informationen zu allen Einträgen im XML-Format.

- **Suchen/Weitersuchen/Rückwärts suchen** – Wenn Sie diese Option anklicken, können Sie im Fenster Log-Filter Filterkriterien für bestimmte Log-Einträge festlegen.

- **Ausschluss erstellen** - Erstellen Sie einen neuen Ereignisausschluss mit einem Assistenten (Nicht verfügbar für Malware-Erkennungen).

Log-Filter

Klicken Sie auf **Filterung** unter **Tools** > **Log-Dateien**, um Filterkriterien zu definieren.

Mit dem Log-Filter finden Sie Ihre gesuchten Informationen schnell, insbesondere in großen Datenmengen. Sie können die Log-Einträge beispielsweise nach Ereignistyp, Status oder Zeitraum eingrenzen. Außerdem können Sie Log-Einträge mit bestimmten Suchoptionen filtern, um nur relevante Einträge (die Ihren Suchoptionen entsprechen) im Fenster „Log-Dateien“ anzuzeigen.

Geben Sie Ihren Suchbegriff in das Feld **Suchen nach** ein. Mit dem Dropdownmenü **In Spalten** können Sie Ihre Suche eingrenzen. Wählen Sie einen oder mehrere Einträge im Dropdownmenü **Eintragstypen** aus. Legen Sie den **Zeitraum**, aus dem Sie Einträge anzeigen möchten. Dazu haben Sie weitere Suchoptionen wie **Nur ganze Wörter** oder **Groß-/Kleinschreibung beachten** zur Auswahl.

Suchen nach

Geben Sie eine Zeichenfolge (ein Wort oder ein Teil eines Worts) ein, um nur Einträge anzuzeigen, die diese Zeichenfolge enthalten. Alle anderen Einträge werden ausgeblendet.

In Spalten

Wählen Sie aus, welche Spalten für die Suche berücksichtigt werden sollen. Sie können eine oder mehrere Spalten für die Suche markieren.

Eintragstypen

Wählen Sie einen oder mehrere Eintragstypen aus dem Dropdownmenü aus:

- **Diagnose** – Alle Meldungen höherer Stufen und alle sonstigen Informationen, die für das Beheben von Fehlern wichtig sein können, werden protokolliert.
- **Informationen** – Meldungen wie erfolgreiche Updates und alle Meldungen höherer Stufen werden protokolliert.
- **Warnungen** – Kritische Fehler und Warnungen werden protokolliert.
- **Fehler** – Fehler wie „Fehler beim Herunterladen der Datei“ und kritische Fehler werden aufgezeichnet.
- **Kritische Warnungen**– Nur kritische Warnungen (z. B. bei einem Fehler beim Start des Virenschutz-Moduls).

Zeitraum

Zeitraum - Legen Sie fest, aus welchem Zeitraum die Suchergebnisse stammen sollen:

- **Nicht angegeben** (Standard) - Kein Zeitraum angegeben, das gesamte Log wird durchsucht.
- **Gestern**
- **Letzte Woche**

- **Letzter Monat**
- **Zeitraum** - Sie können einen exakten Zeitraum (Von: und Bis:) angeben, um die Einträge aus diesem Zeitraum herauszufiltern.

Nur ganze Wörter

Aktivieren Sie dieses Kontrollkästchen, wenn Sie mit ganzen Wörtern genauere Suchergebnisse erzielen möchten.

Groß-/Kleinschreibung beachten

Aktivieren Sie diese Option, wenn die Groß- oder Kleinschreibung beim Filtern beachtet werden soll. Konfigurieren Sie Ihre Filter-/Suchoptionen und klicken Sie auf **OK**, um die gefilterten Einträge anzuzeigen oder auf **Suchen**, um die Suche zu starten. Die Log-Dateien werden ausgehend von Ihrer aktuellen Position (der hervorgehobene Eintrag) von oben nach unten durchsucht. Die Suche endet, wenn der erste übereinstimmende Eintrag gefunden wurde. Drücken Sie **F3**, um nach dem nächsten Eintrag zu suchen oder klicken Sie mit der rechten Maustaste und wählen Sie **Suchen** aus, um Ihre Suchoptionen einzugrenzen.

Log-Dateien

Die Log-Konfiguration für ESET Endpoint Antivirus können Sie aus dem Hauptprogrammfenster aufrufen. Klicken Sie auf **Einstellungen** > **Erweiterte Einstellungen** > **Tools** > **Log-Dateien**. In diesem Bereich können Sie Einstellungen für Logs festlegen. Um den Speicherbedarf zu reduzieren, werden ältere Logs automatisch gelöscht. Für Log-Dateien können die folgenden Einstellungen vorgenommen werden:

Mindestinformation in Logs - Hier können Sie festlegen, welche Ereignistypen in Logs aufgezeichnet werden sollen.

- **Diagnose**– Alle Meldungen höherer Stufen und alle sonstigen Informationen, die für das Beheben von Fehlern wichtig sein können, werden protokolliert.
- **Informationen**– Meldungen wie erfolgreiche Updates und alle Meldungen höherer Stufen werden protokolliert.
- **Warnungen**– Kritische Fehler und Warnungen werden protokolliert.
- **Fehler**– Fehler wie „Fehler beim Herunterladen der Datei“ und kritische Fehler werden aufgezeichnet.
- **Kritische Warnungen**– Nur kritische Warnungen (z. B. bei einem Fehler beim Start des Virenschutz-Moduls,, usw.) werden protokolliert.



Hinweis
Wenn Sie die Mindestinformationen in Logs auf die Stufe „**Diagnose**“ festlegen, werden alle blockierten Verbindungen aufgezeichnet.

Log-Einträge, die älter sind als die unter **Einträge automatisch löschen nach (Tage)** angegebene Anzahl an Tagen, werden automatisch gelöscht.

Log-Dateien automatisch optimieren - Diese Option defragmentiert die Log-Dateien automatisch, wenn die Prozentzahl der Fragmentierung höher ist als der unter **Wenn ungenutzte Einträge größer als (%)** angegebene

Wert.

Klicken Sie zum Defragmentieren der Log-Dateien auf **Optimieren**. Bei diesem Prozess werden alle leeren Log-Einträge gelöscht, wodurch Leistung und Log-Verarbeitung verbessert werden. Eine starke Verbesserung ist insbesondere dann erkennbar, wenn die Logs eine große Anzahl an Einträgen enthalten.

Mit der Option **Textprotokoll aktivieren** wird die Speicherung von Logs in einem anderen, von Log-Dateien getrennten Format aktiviert:

- **Zielverzeichnis** - Das Verzeichnis, in dem Log-Dateien gespeichert werden (nur für Text/CSV). Kopieren Sie den Pfad oder klicken Sie auf **Löschen**, um ein anderes Verzeichnis auszuwählen. Jeder Log-Bereich verfügt über eine eigene Datei mit einem vordefinierten Dateinamen (z. B. *virlog.txt* für den Bereich **Erkannte Bedrohungen** von Log-Dateien, wenn Logs im Nur-Text-Format gespeichert werden).

- **Typ** - Mit dem Dateiformat **Text** werden Logs in einer Textdatei gespeichert, wobei die Daten durch Tabulatorzeichen getrennt werden. Gleiches gilt für das kommagetrennte Dateiformat **CSV**. Mit der Option **Ereignis** werden die Logs im Windows-Ereignis-Log anstatt in einer Datei gespeichert (dieses kann in der Ereignisanzeige in der Systemsteuerung eingesehen werden).

- Mit der Option **Alle Log-Dateien löschen** werden alle aktuell im Dropdownmenü **Typ** ausgewählten Logs gelöscht. Eine Benachrichtigung über das erfolgreiche Löschen der Logs wird angezeigt.

Nachverfolgen von Konfigurationsänderungen im Audit-Log aktivieren - Informiert Sie über alle Konfigurationsänderungen. Weitere Informationen finden Sie unter Audit-Logs.

> **ESET Log Collector**
> Zum Zwecke der schnellen Problemlösung werden Sie von ESET möglicherweise gebeten, Logs von Ihrem Computer bereitzustellen. Mit dem ESET Log Collector können Sie die benötigten Informationen ganz einfach sammeln. Weitere Informationen zum ESET Log Collector finden Sie in diesem Artikel in der ESET Knowledgebase.

Audit-Logs

In Unternehmensumgebungen haben oft mehrere Benutzer die Berechtigung zum Konfigurieren von Endpunkten. Da Änderungen an der Produktkonfiguration dramatische Auswirkungen auf den Betrieb des Produkts haben können, müssen Administratoren nachverfolgen können, welche Benutzer welche Änderungen vorgenommen haben, um Probleme schnell identifizieren, beheben und für die Zukunft ausschließen zu können.

Das Audit-Log wurde als neues Log in ESET Endpoint Antivirus Version 7.1 eingeführt und unterstützt Sie dabei, die Problemursache zu identifizieren. Das Audit-Log überwacht Änderungen an der Konfiguration oder am Schutzstatus und erfasst Snapshots zur späteren Verwendung.

Um das **Audit-Log** zu öffnen, klicken Sie im Hauptmenü auf **Tools**, dann auf **Log-Dateien** und wählen Sie **Audit-Logs** im Dropdownmenü aus.

Das Audit-Log enthält die folgenden Informationen:

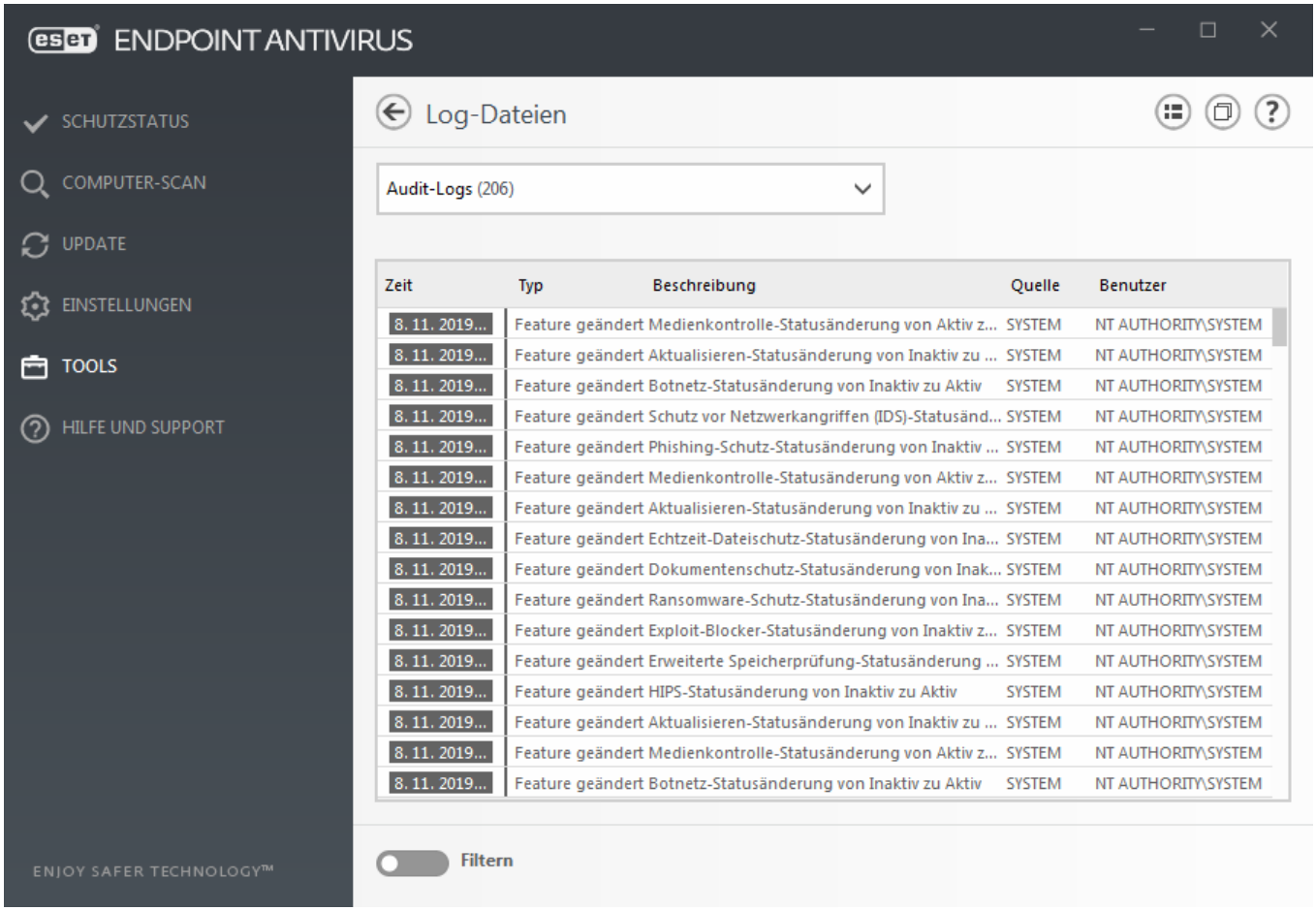
- Zeitpunkt - Wann wurde die Änderung vorgenommen?

- Typ - Welche Art von Einstellung oder Funktion wurde geändert?

• Beschreibung - Was genau wurde geändert, welcher Teil der Einstellung wurde geändert, und wie viele Einstellungen wurden geändert?

• Quelle - Woher stammte die Änderung?

• Benutzer - Wer hat die Änderung vorgenommen?



Klicken Sie im Fenster „Log-Dateien“ mit der rechten Maustaste auf einen beliebigen Audit-Logeintrag vom Typ **Einstellungen geändert** und wählen Sie **Änderungen anzeigen** im Kontextmenü aus, um ausführliche Informationen zur vorgenommenen Änderung anzuzeigen. Außerdem können Sie beliebige Einstellungsänderungen rückgängig machen, indem Sie im Kontextmenü auf **Wiederherstellen** klicken (nicht verfügbar für Produkte, die mit ESMC verwaltet werden). Wenn Sie **Alle löschen** im Kontextmenü auswählen, wird ein Log mit Informationen über diese Aktion erstellt.

Wenn die Option **Log-Dateien automatisch optimieren** unter **Erweiterte Einstellungen** > **Tools** > **Log-Dateien** aktiviert ist, werden die Audit-Logs zusammen mit den anderen Logs automatisch defragmentiert.

Wenn die Option **Einträge automatisch löschen, die älter sind als (Tage)** unter **Erweiterte Einstellungen** > **Tools** > **Log-Dateien** aktiviert ist, werden Log-Einträge, die älter als die angegebene Anzahl von Tagen sind, automatisch gelöscht.

Taskplaner

Der Taskplaner verwaltet und startet Tasks mit vordefinierter Konfiguration und voreingestellten Eigenschaften.

Um ihn zu öffnen, klicken Sie im Hauptprogrammfenster von ESET Endpoint Antivirus unter **Tools** auf **Taskplaner**.

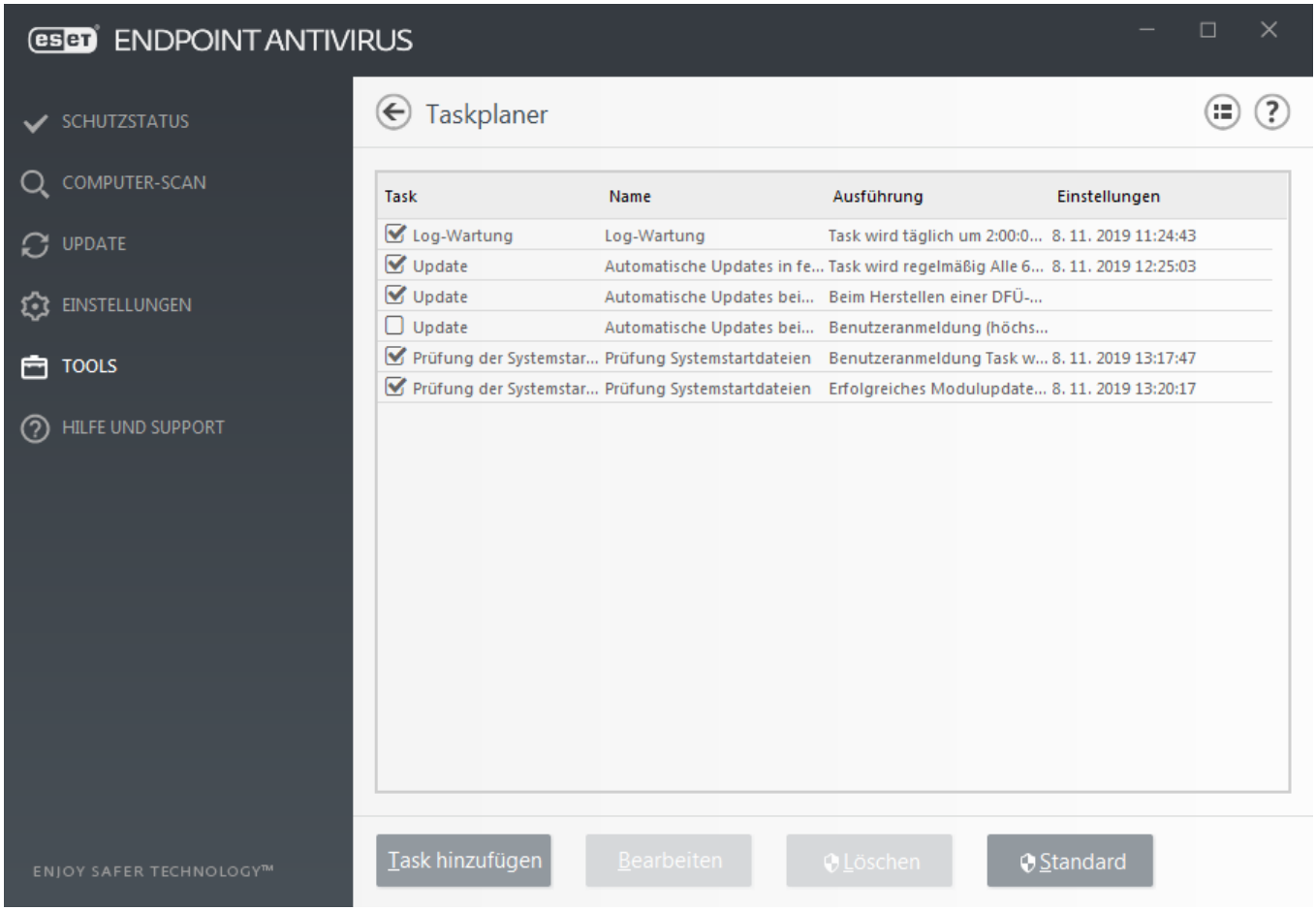
Der **Taskplaner** umfasst eine Liste aller geplanten Tasks sowie deren Konfigurationseigenschaften, inklusive des vordefinierten Datums, der Uhrzeit und des verwendeten Prüfprofils.

Er dient zur Planung der folgenden Vorgänge: Update der Erkennungsroutine, Prüftask, Prüfung Systemstartdateien und Log-Wartung. Tasks können direkt über das Fenster „Taskplaner“ hinzugefügt oder gelöscht werden. (Klicken Sie dazu unten auf **Task hinzufügen** oder **Löschen**.) Klicken Sie an einer beliebigen Stelle mit der rechten Maustaste in das Fenster „Taskplaner“, um folgende Aktionen auszuführen: Anzeigen ausführlicher Informationen, sofortige Ausführung des Vorgangs, Hinzufügen eines neuen Vorgangs und Löschen eines vorhandenen Vorgangs. Verwenden Sie die Kontrollkästchen vor den einzelnen Einträgen zum Aktivieren oder Deaktivieren der jeweiligen Vorgänge.

Standardmäßig werden im **Taskplaner** die folgenden Tasks angezeigt:

- **Log-Wartung**
- **Automatische Updates in festen Zeitabständen**
- **Automatische Updates beim Herstellen von DFÜ-Verbindungen**
- **Automatische Updates beim Anmelden des Benutzers**
- **Prüfung Systemstartdateien** (nach Benutzeranmeldung)
- **Prüfung Systemstartdateien** (nach erfolgreichem Modulupdate)

Um die Konfiguration eines vorhandenen Standardtasks oder eines benutzerdefinierten Tasks zu ändern, klicken Sie mit der rechten Maustaste auf den Task und dann auf **Bearbeiten**, oder wählen Sie den Task aus, den Sie ändern möchten, und klicken Sie auf **Bearbeiten**.



Hinzufügen eines neuen Tasks

1. Klicken Sie am unteren Fensterrand auf **Task hinzufügen**.

2. Geben Sie einen Namen für den Task ein.

3. Wählen Sie den gewünschten Task im Dropdownmenü aus:

- **Start externer Anwendung** - Planen der Ausführung einer externen Anwendung
- **Log-Wartung** - Log-Dateien enthalten auch unbenutzte leere Einträge von gelöschten Datensätzen. Dieser Task optimiert regelmäßig die Einträge in Log-Dateien.
- **Prüfung Systemstartdateien** - Prüft Dateien, die während des Systemstarts oder der Anmeldung ausgeführt werden.
- **Snapshot des Computerstatus erstellen** - Erstellt einen ESET SysInspector-Snapshot und eine genaue Risikoanalyse Ihrer Systemkomponenten (z. B. Treiber und Anwendungen).
- **On-Demand-Prüfung** - Prüft die Dateien und Ordner auf Ihrem Computer.
- **Update** – Erstellt einen Update-Task für die Aktualisierung von Erkennungsroutine und Programmmodulen.

4. Aktivieren Sie den Task mithilfe der Option **Aktivieren** (Sie können dies auch später tun, indem Sie das Kontrollkästchen in der Liste der geplanten Tasks markieren oder die Markierung daraus entfernen), klicken Sie auf **Weiter** und wählen Sie eine Zeitangabe aus:

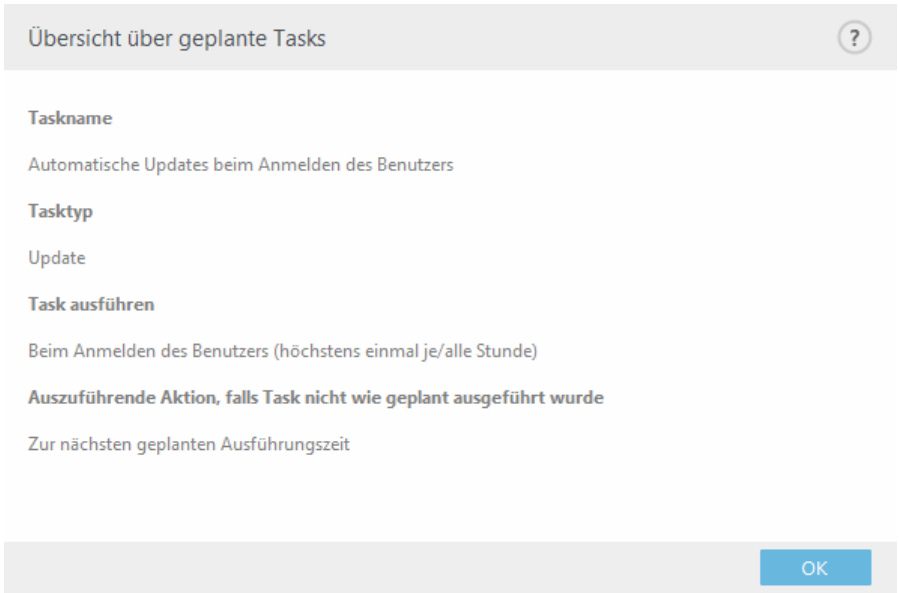
- **Einmalig** - Der Task wird nur einmalig zu einem festgelegten Zeitpunkt ausgeführt.

- **Wiederholt** - Der Task wird in dem angegebenen Zeitabstand ausgeführt.
- **Täglich** - Der Task wird wiederholt täglich zur festgelegten Uhrzeit ausgeführt.
- **Wöchentlich** - Der Task wird am festgelegten Wochentag zur angegebenen Uhrzeit ausgeführt.
- **Bei Ereignis** - Der Task wird ausgeführt, wenn ein bestimmtes Ereignis eintritt.

5. **Wählen Sie Task im Akkubetrieb überspringen**, um die Systembelastung für einen Laptop während des Akkubetriebs möglichst gering zu halten. Der angegebene Task wird zum angegeben Zeitpunkt in den Feldern **Taskausführung** ausgeführt. Wenn der Task nicht zur festgelegten Zeit ausgeführt werden konnte, können Sie einen Zeitpunkt für die nächste Ausführung angeben:

- **Zur nächsten geplanten Ausführungszeit**
- **Baldmöglichst**
- **Sofort ausführen, wenn Intervall seit letzter Ausführung überschritten** (das Intervall kann über das Feld **Zeit seit letzter Ausführung (Stunden)** festgelegt werden)

Sie können den geplanten Task durch Klicken mit der rechten Maustaste und Auswählen der Option **Task-Eigenschaften** überprüfen.



Schutzstatistiken

Um statistische Daten zu den Schutzmodulen von ESET Endpoint Antivirus in einem Diagramm anzeigen zu lassen, klicken Sie auf **Tools** > **Schutzstatistiken**. Wählen Sie im Dropdown-Menü **Statistik** das gewünschte Schutzmodul aus, um das entsprechende Diagramm und die Legende anzuzeigen. Wenn Sie mit dem Mauszeiger über einen bestimmten Punkt in der Legende fahren, werden im Diagramm nur die Daten für diesen Punkt angezeigt.

In ESET Endpoint Antivirus Version 7.1 wurde eine neue Art von Berichten eingeführt, der Sicherheitsbericht. Der Bereich „Schutzstatistiken“ ist nicht mehr verfügbar.

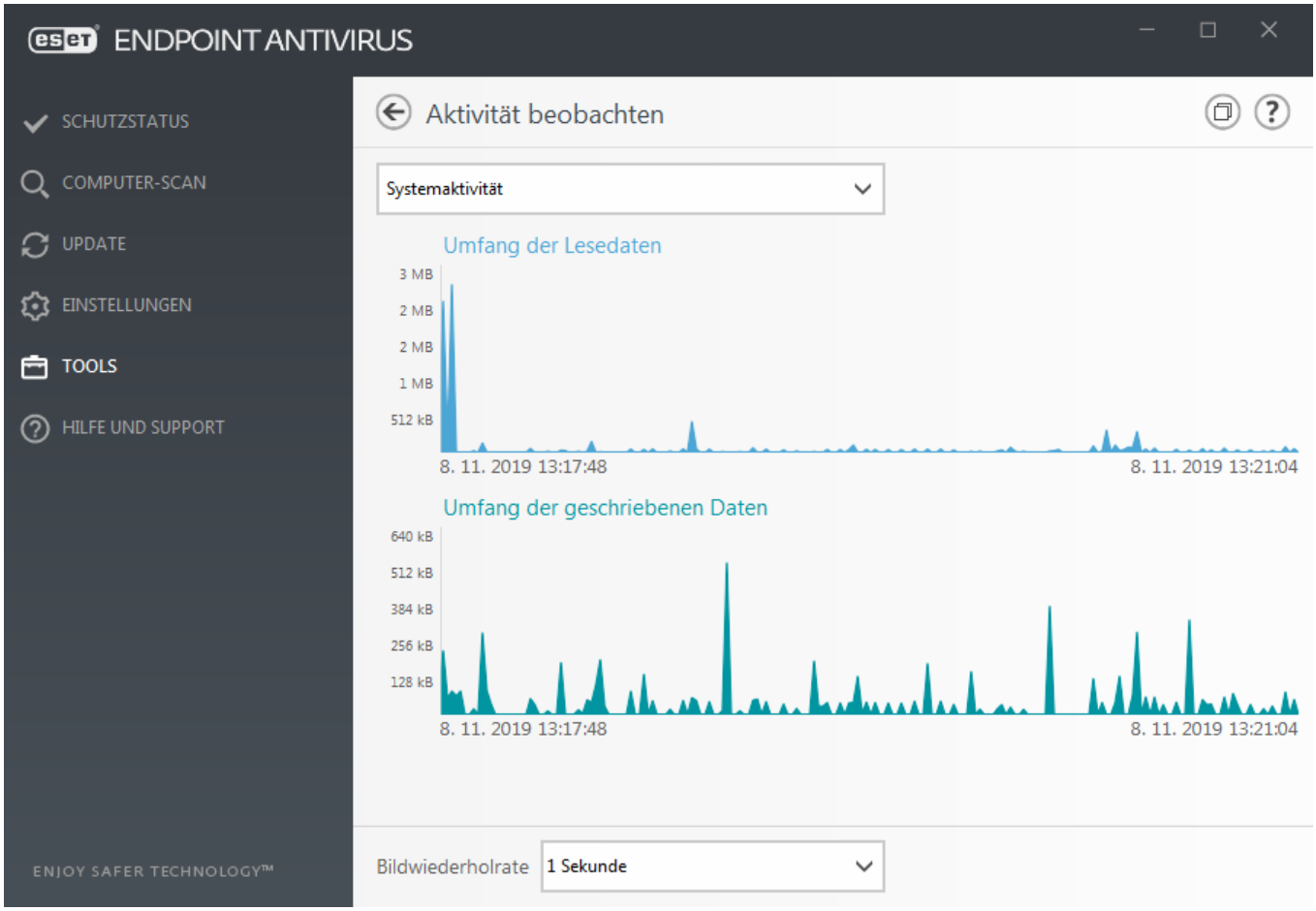
Folgende Diagramme stehen zur Auswahl:

- **Viren- und Spyware-Schutz** - Anzeige der Anzahl infizierter Objekte und gesäuberter Objekte
- **Dateischutz** - Lediglich Anzeige von Objekten, die aus dem Dateisystem gelesen oder in das Dateisystem geschrieben wurden
- **E-Mail-Client-Schutz** - Lediglich Anzeige von Objekten, die von E-Mail-Programmen gesendet oder empfangen wurden
- **Web- und Phishing-Schutz** - Lediglich Anzeige von Objekten, die von einem Webbrowser heruntergeladen wurden

Nebendem Statistik-Diagramm wird die Gesamtanzahl der geprüften, infizierten, gesäuberten und sauberen Objekte angezeigt Durch Klicken auf **Zurücksetzen** werden die Statistikdaten gelöscht; durch Klicken auf **Alle zurücksetzen** werden alle bestehenden Daten gelöscht und entfernt.

Aktivität beobachten

Um die aktuelle **Systemaktivität** als Diagramm anzuzeigen, klicken Sie auf **Tools** > **Aktivität beobachten**. Im unteren Bereich des Diagramms befindet sich eine Zeitleiste, welche die Systemaktivität in Echtzeit innerhalb des gewählten Zeitraums aufzeichnet. Um die Zeitleiste zu ändern, wählen Sie im Dropdownmenü **Bildwiederholrate** einen Wert aus.



Folgende Optionen stehen zur Verfügung:

- **Schritt: 1 Sekunde** - Das Diagramm wird jede Sekunde aktualisiert, und die Zeitleiste umfasst die letzten 10 Minuten.

- **Schritt: 1 Minute (letzte 24 Stunden)** - Das Diagramm wird jede Minute aktualisiert. Die Zeitleiste deckt die letzten 24 Stunden.

- **Schritt: 1 Stunde (letzter Monat)** - Das Diagramm wird jede Stunde aktualisiert. Die Zeitleiste deckt den letzten Monat.

- **Schritt: Schritt: 1 Stunde (ausgewählter Monat)** - Das Diagramm wird jede Stunde aktualisiert. Die Zeitleiste deckt die X letzten, ausgewählten Monate.

Die vertikale Achse im **Systemaktivitätsdiagramm** bildet die Menge an gelesenen (blau) und geschriebenen Daten (türkis) ab. Beide Werte werde in KB (Kilobyte)/MB/GB angegeben. Wenn Sie mit dem Mauszeiger über die gelesenen oder geschriebenen Daten in der Legende unterhalb des Diagramms fahren, werden im Diagramm nur die Daten für diesen Aktivitätstyp angezeigt.

ESET SysInspector

ESET SysInspector ist eine Anwendung, die Ihren Computer gründlich durchsucht und eine genaue (Risikostufen-)Analyse Ihrer Systemkomponenten erstellt. Hierzu zählen u. a. Treiber und Anwendungen, Netzwerkverbindungen oder wichtige Registrierungseinträge. Diese Informationen helfen Ihnen beim Aufspüren der Ursache für verdächtiges Systemverhalten, welches möglicherweise durch Software- oder Hardwareinkompatibilität oder eine Infektion mit Schadcode hervorgerufen wurde. Weitere Informationen finden Sie in der ESET SysInspector-Onlinehilfe.

Das Fenster „SysInspector“ zeigt folgende Informationen zu erstellten Logs an:

- **Zeit** - Zeitpunkt der Log-Erstellung.

- **Kommentar** - Eine kurze Beschreibung

- **Benutzer** - Der Name des Benutzers, der das Log erstellt hat.

- **Status** - Status bei der Log-Erstellung.

Folgende Aktionen stehen zur Verfügung:

- **Anzeigen –** Öffnet das erstellte Log. Sie können auch mit der rechten Maustaste auf die Log-Datei klicken und im Kontextmenü **Anzeigen** auswählen.

- **Vergleichen** - Vergleicht zwei vorhandene Logs.

- **Erstellen...** - Erstellen eines neuen Logs Warten Sie, bis ESET SysInspector die Erstellung abgeschlossen hat (bis der Log-Status „Erstellt“ lautet), bevor Sie versuchen, auf die Log-Datei zuzugreifen.

- **Löschen** - Löschen der ausgewählten Logs aus der Liste.

Die folgenden Einträge sind im Kontextmenü verfügbar, wenn eine oder mehrere Log-Dateien ausgewählt sind:

- **Anzeigen** - Anzeige des ausgewählten Logs in ESET SysInspector (entspricht einem Doppelklick auf einen beliebigen Eintrag)

- **Vergleichen** - Vergleicht zwei vorhandene Logs.
- **Erstellen...** - Erstellen eines neuen Logs Warten Sie, bis ESET SysInspector die Erstellung abgeschlossen hat (bis der Log-Status „Erstellt“ lautet), bevor Sie versuchen, auf die Log-Datei zuzugreifen.
- **Löschen** - Löschen des ausgewählten Logs.
- **Alle löschen** - Löschen aller Logs.
- **Exportieren** - Exportieren des Logs in eine .xml-Datei oder eine komprimierte .xml-Datei.

Cloudbasierter Schutz

ESET LiveGrid® basiert auf dem ESET ThreatSense.Net -Frühwarnsystem und arbeitet mit von ESET-Anwendern weltweit übermittelten Daten, die es an das ESET-Virenlabor sendet. ESET LiveGrid® stellt verdächtige Samples und Metadaten „aus freier Wildbahn“ bereit und gibt uns so die Möglichkeit, unmittelbar auf die Anforderungen unserer Kunden zu reagieren und sie vor den neuesten Bedrohungen zu schützen.

Sie haben drei Optionen zur Auswahl:

Option 1: ESET LiveGrid®-Reputationssystem aktivieren

Das ESET LiveGrid®-Reputationssystem arbeitet mit Cloud-basierten White- und Blacklists.

Sie können die Reputation von ausgeführten Prozessen oder Dateien direkt im Programmfenster oder im jeweiligen Kontextmenü anzeigen lassen. In ESET LiveGrid® sind außerdem weitere Informationen verfügbar.

Option 2: ESET LiveGrid®-Feedbacksystem aktivieren

Zusätzlich zum ESET LiveGrid®-Reputationssystem sammelt das ESET LiveGrid®-Feedbacksystem Daten über neue Bedrohungen, die auf Ihrem Computer erkannt wurden. Dazu können auch Samples oder Kopien der Datei gehören, in der eine Bedrohung aufgetreten ist, der Pfad zu dieser Datei, der Dateiname, Datum und Uhrzeit, der Prozess, über den die Bedrohung auf Ihrem Computer in Erscheinung getreten ist, und Informationen zum Betriebssystem Ihres Computers.

ESET Endpoint Antivirus Ist standardmäßig so konfiguriert, dass verdächtige Dateien zur genauen Analyse beim ESET-Virenlabor eingereicht werden. Dateien mit bestimmten Erweiterungen (z. B. *.doc* oder *.xls*) sind immer von der Übermittlung ausgeschlossen. Sie können andere Dateierweiterungen hinzufügen, wenn es bestimmte Dateitypen gibt, die Sie oder Ihr Unternehmen nicht übermitteln möchten.

Option 3: ESET LiveGrid® nicht aktivieren

Die Funktionalität der Software geht nicht verloren, in einigen Fällen reagiert ESET Endpoint Antivirus jedoch möglicherweise schneller auf neue Bedrohungen, wenn ESET LiveGrid® aktiviert ist.



Weitere Informationen

Weitere Informationen zu ESET LiveGrid® finden Sie im Glossar.
Beachten Sie unsere illustrierten Anweisungen auf Englisch und in verschiedenen weiteren Sprachen dazu, wie Sie ESET LiveGrid® in ESET Endpoint Antivirus aktivieren oder deaktivieren können.

Cloudbasierten Schutz in den erweiterten Einstellungen konfigurieren

Um auf die Einstellungen für ESET LiveGrid® zuzugreifen, drücken Sie **F5**, um die erweiterten Einstellungen zu öffnen und erweitern Sie den Eintrag **Erkennungsroutine** > Cloudbasierter Schutz.

An ESET LiveGrid® teilnehmen (empfohlen)– Das ESET LiveGrid®-Reputationssystem erhöht die Wirksamkeit der ESET-Sicherheitslösungen, indem es gescannte Dateien mit Positiv- und Negativlisten in einer Datenbank in der Cloud vergleicht.

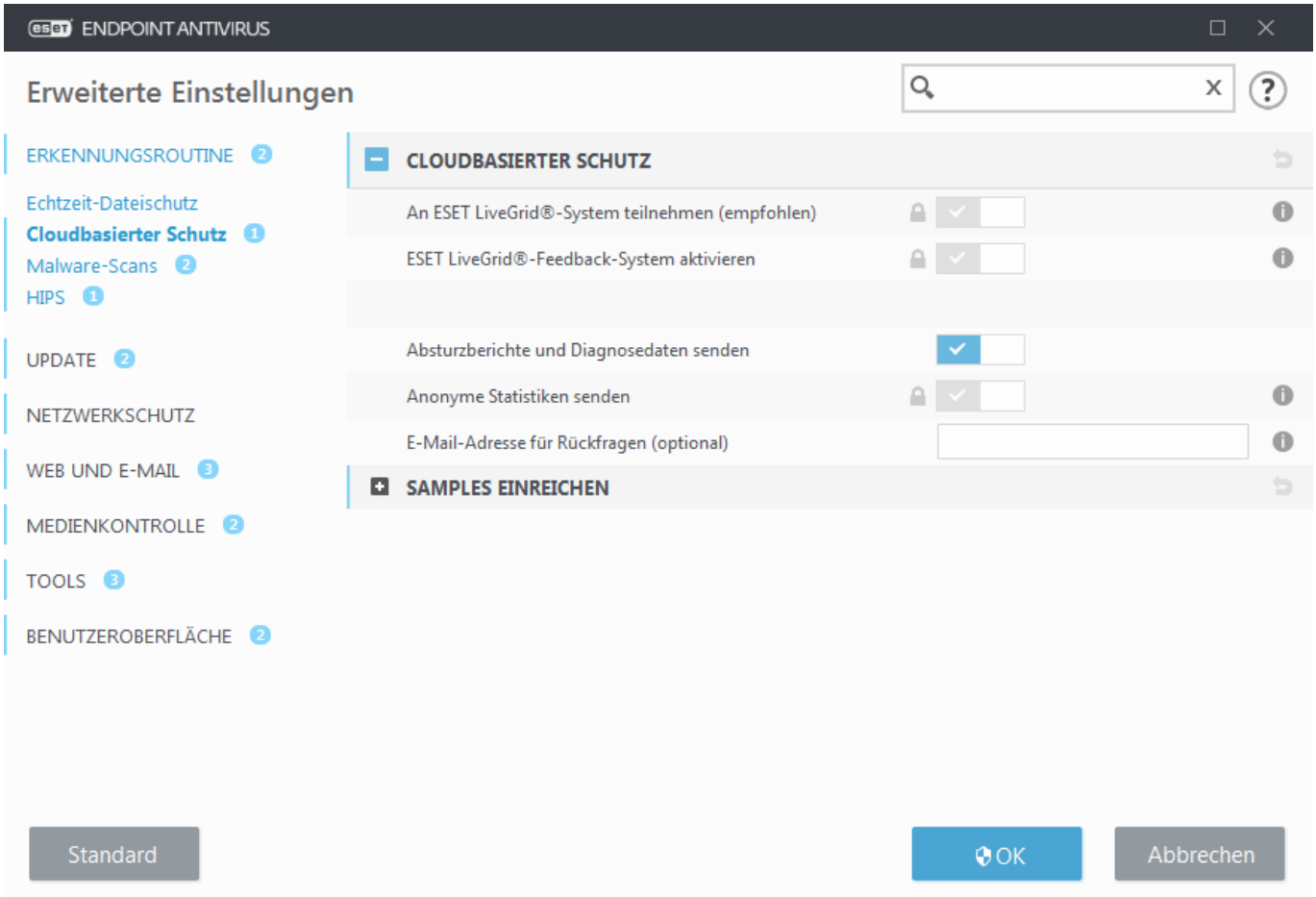
ESET LiveGrid®-Feedbacksystem aktivieren - Sendet die entsprechenden Übermittlungsdaten (siehe Abschnitt **Übermittlung von Samples** weiter unten) zusammen mit Absturzberichten und Statistiken zur weiteren Analyse an das ESET-Virenlabor.

ESET Dynamic Threat Defense aktivieren (nicht sichtbar in ESET Endpoint Antivirus) - ESET Dynamic Threat Defense ist ein kostenpflichtiger Dienst von ESET, der eine zusätzliche Schutzebene speziell zu Abwehr neuer Bedrohungen bietet. Verdächtige Dateien werden automatisch an die ESET-Cloud übermittelt, wo sie von unseren fortschrittlichen Malware-Erkennungsroutinen analysiert werden. Der Benutzer, der das Sample übermittelt hat, erhält einen Verhaltensbericht mit einer Übersicht über das Verhalten des beobachteten Samples.

Absturzberichte und Diagnosedaten senden - Sendet Diagnosedaten für ESET LiveGrid® wie etwa Absturzberichte und Speicherabbilder der Module. Wir empfehlen, diese Option aktiviert zu lassen, da ESET diese Daten verwendet, um Probleme zu diagnostizieren und die Produkte sowie den Schutz der Endbenutzer zu verbessern.

Anonyme Statistiken senden– Zulassen, dass ESET Informationen über neu erkannte Bedrohungen erfasst, wie den Bedrohungsnamen, das Datum und die Uhrzeit der Erkennung, die Erkennungsmethode und verknüpften Metadaten oder die Produktversion und -konfiguration, einschließlich Daten zum System.

E-Mail-Adresse für Rückfragen (optional) – Sie können mit den verdächtigen Dateien eine E-Mail-Adresse für Rückfragen angeben, wenn zur Analyse weitere Informationen erforderlich sind. Beachten Sie, dass Sie nur dann eine Antwort von ESET erhalten, wenn weitere Informationen von Ihnen benötigt werden.



Samples einreichen

Erkannte Samples automatisch einreichen

Wählen Sie aus, welche Arten von Samples zur Analyse an ESET übermittelt werden sollen, und um die zukünftige Erkennung zu verbessern. Sie haben die folgenden Optionen zur Auswahl:

- **Alle erkannten Samples** - Alle Objekte, die von der Erkennungsroutine erkannt wurden (inklusive potenziell unerwünschter Anwendungen, falls dies in den Scannereinstellungen aktiviert ist).
- **Alle Samples mit Ausnahme von Dokumenten** - Alle erkannten Objekte mit Ausnahme von **Dokumenten** (siehe unten).
- **Nicht übermitteln** - Erkannte Objekte werden nicht an ESET übermittelt.

Verdächtige Samples automatisch einreichen

Diese Samples werden auch dann an ESET übermittelt, wenn sie nicht von der Erkennungsroutine erkannt wurden. Beispiele sind Samples, die beinahe erkannt wurden oder die von einem der ESET Endpoint Antivirus-Schutzmodule als verdächtig oder unbekannt eingestuft wurden.

- **Ausführbare Dateien** – Dateien mit den Endungen .exe, .dll, .sys.
- **Archive** – Dateien mit den Endungen .zip, .rar, .7z, .arch, .arj, .bzip, .gzip, .ace, .arc, .cab.
- **Archive** – Dateien mit den Endungen .bat, .cmd, .hta, .js, .vbs, .ps1.

- **Archive** – Andere Dateitypen wie etwa .jar, .reg, .msi, .sfw, .lnk.

- **Mögliche Spam-E-Mails** – Senden Sie mögliche Spam-Komponenten oder ganze Spam-E-Mails mit Anhang zur weiteren Analyse an ESET. Diese Option verbessert die globale Spam-Erkennung inklusive der zukünftigen Spam-Erkennung für Sie selbst.

- **Dokumente** - Microsoft Office- oder PDF-Dokumente mit oder ohne aktiven Inhalten.

Liste aller enthaltenen Dokumentdateitypen erweitern

ACCDB, ACCDT, DOC, DOC_OLD, DOC_XML, DOCM, DOCX, DWFX, EPS, IWORK_NUMBERS, IWORK_PAGES, MDB, MPP, ODB, ODF, ODG, ODP, ODS, ODT, OLE2, OLE2_ENCRYPTED, OLE2_MACRO, OLE2_PROTECTED, ONE, ONEPKG, PDF, PPT, PPT_XML, PPTM, PPTX, PS, PSD, RTF, SYLK, THMX, VSD, VSD_XML, WPC, WPS, XLS, XLS_XML, XLSB, XLSM, XLSX, XPS

Ausschlussfilter

Mit dem Ausschlussfilter können Sie bestimmte Dateien/Ordner von der Übermittlung ausschließen. So kann es beispielsweise nützlich sein, Dateien mit vertraulichen Informationen wie Dokumente oder Tabellenkalkulationen auszuschließen. Hier eingetragene Dateien werden nicht an ESET übermittelt, auch wenn sie verdächtigen Code enthalten. Einige typische Dateitypen sind bereits in der Standardeinstellung in die Liste eingetragen (.doc usw.). Sie können weitere Dateien zur Ausschlussliste hinzufügen.

ESET Dynamic Threat Defense

Informationen zum Aktivieren des ESET Dynamic Threat Defense-Diensts auf einem Clientcomputer mit der ESMC-Web-Konsole finden Sie unter EDTD-Konfiguration für ESET Endpoint Antivirus.

Wenn Sie ESET LiveGrid® einige Zeit verwendet haben, kann es sein, dass auch nach dem Deaktivieren des Systems noch einige Datenpakete zum Senden vorliegen. Derartige Datenpakete werden auch nach der Deaktivierung noch an ESET gesendet. Nachdem alle aktuellen Informationen versendet wurden, werden keine weiteren Pakete mehr erstellt.

Ausschlussfilter für den cloudbasierten Schutz

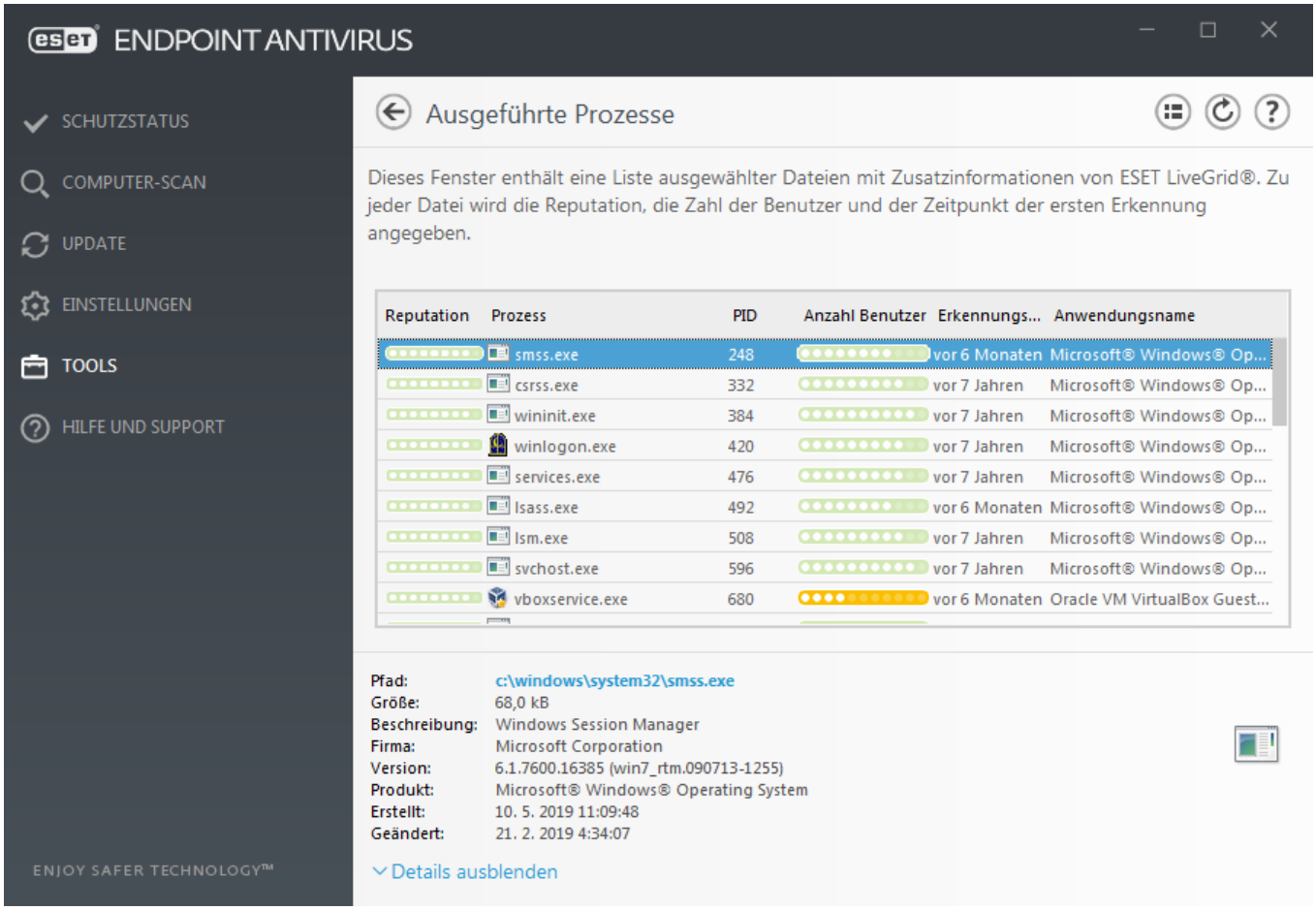
Mit dem Ausschlussfilter können Sie bestimmte Dateien/Ordner von der Sample-Übermittlung ausschließen. Hier eingetragene Dateien werden nicht an ESET übermittelt, auch wenn sie verdächtigen Code enthalten. Gängige Dateitypen (.doc usw.) sind bereits in der Standardeinstellung in die Liste eingetragen.



Hinweis
Diese Funktion eignet sich dazu, Dateien einzutragen, die eventuell vertrauliche Informationen enthalten, wie zum Beispiel Textdokumente oder Tabellen.

Ausgeführte Prozesse

Die Informationen zu ausgeführten Prozessen zeigen die auf dem Computer ausgeführten Programme und Prozesse an und stellen dem ESET-Produkt laufend aktuelle Informationen zu neuen Infiltrationen bereit. ESET Endpoint Antivirus bietet ausführliche Informationen zu ausgeführten Prozessen, um den Benutzern den Schutz der ESET LiveGrid®-Technologie zu bieten.



Reputation – Um Objekten wie Dateien, Prozessen, Registrierungsschlüsseln usw. eine Risikostufe zuzuordnen, verwenden ESET Endpoint Antivirus und die ESET LiveGrid®-Technologie einen Satz heuristischer Regeln, mit denen die Merkmale des Objekts untersucht werden, um anschließend nach entsprechender Gewichtung das Potenzial für schädliche Aktivitäten abzuschätzen. Basierend auf dieser Heuristik wird Objekten eine Reputationsstufe von 9 – Beste Reputation (grün) bis 0 – Schlechteste Reputation (rot) zugewiesen.

Prozess - Zeigt den Namen des Programms oder Prozesses an, das/der derzeit auf dem Computer ausgeführt wird. Sie können alle auf Ihrem Computer ausgeführten Prozesse auch über den Windows-Taskmanager anzeigen. Öffnen Sie den Taskmanager, indem Sie mit der rechten Maustaste auf einen leeren Bereich auf der Taskleiste und dann auf „Taskmanager“ klicken oder indem Sie **Strg**+**Umschalt**+**Esc** auf Ihrer Tastatur drücken.

PID - Stellt eine ID der in Windows-Betriebssystemen ausgeführten Prozessen dar.

> **Hinweis**
> Bekannte Anwendungen, die als grün markiert sind, sind in jedem Fall sauber (Positivliste) und werden von der Prüfung ausgenommen. Dadurch wird die Geschwindigkeit der On-Demand-Prüfung bzw. des Echtzeit-Dateischutzes auf Ihrem Computer verbessert.

Anzahl Benutzer - Die Anzahl der Benutzer, die eine bestimmte Anwendung verwenden. Diese Informationen werden von der ESET LiveGrid®-Technologie gesammelt.

Erkennungszeitpunkt - Zeitspanne seit der Erkennung der Anwendung durch die ESET LiveGrid®-Technologie.

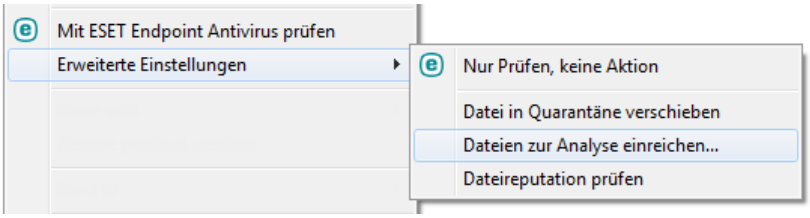
> **Hinweis**
> Wenn eine Anwendung als Unbekannt (orange) eingestuft wurde, muss es sich nicht zwangsläufig um Schadsoftware handeln. In der Regel ist es einfach eine neuere Anwendung. Wenn Sie sich bei einer Datei unsicher sind, können Sie diese über die Funktion Dateien zur Analyse einreichen an ESET einreichen. Wenn sich herausstellt, dass die Datei Schadcode enthält, wird deren Erkennung in einem der nächsten Updates der Erkennungsroutine hinzugefügt.

Anwendungsname - Der Name eines Programms oder Prozesses.

Wenn Sie unten auf eine Anwendung klicken, werden unten im Fenster die folgenden Informationen angezeigt:

- **Pfad** - Speicherort einer Anwendung auf Ihrem Computer.
- **Größe** - Dateigröße entweder in KB (Kilobyte) oder MB (Megabyte).
- **Beschreibung** - Dateieigenschaften auf Basis der Beschreibung des Betriebssystems.
- **Firma** - Name des Herstellers oder des Anwendungsprozesses.
- **Version** - Information vom Herausgeber der Anwendung.
- **Produkt** - Name der Anwendung und/oder Firmenname.
- **Erstellt** - Datum und Uhrzeit der Erstellung einer Anwendung.
- **Geändert** - Datum und Uhrzeit der Erstellung einer Anwendung.

> **Hinweis**
> Der Reputations-Check kann auch auf Dateien angewendet werden, die nicht als Programme/Prozesse ausgeführt werden. Markieren Sie die Dateien, die Sie überprüfen möchten, klicken Sie mit der rechten Maustaste darauf und wählen Sie aus dem Kontextmenü **Erweiterte Einstellungen** > **Dateireputation mit ESET LiveGrid® überprüfen**.



Sicherheitsbericht

Diese Funktion enthält eine Übersicht über die Statistiken für die folgenden Kategorien:

Blockierte Webseiten - Die Anzahl der blockierten Webseiten (URL in Negativliste für eventuell unerwünschte Anwendung, Phishing, gehackter Router, IP oder Zertifikat).

Infizierte E-Mail-Objekte erkannt - Die Anzahl der erkannten infizierten E-Mail-Objekte.

Potenziell unerwünschte Anwendungen erkannt – Die Anzahl der Potenziell unerwünschte Anwendungen (PUA).

Überprüfte Dokumente – Die Anzahl der gescannten Dokumentobjekte.

Gescannte Apps – Die Anzahl der gescannten ausführbaren Objekte.

Sonstige gescannte Objekte – Die Anzahl der sonstigen gescannten Objekte.

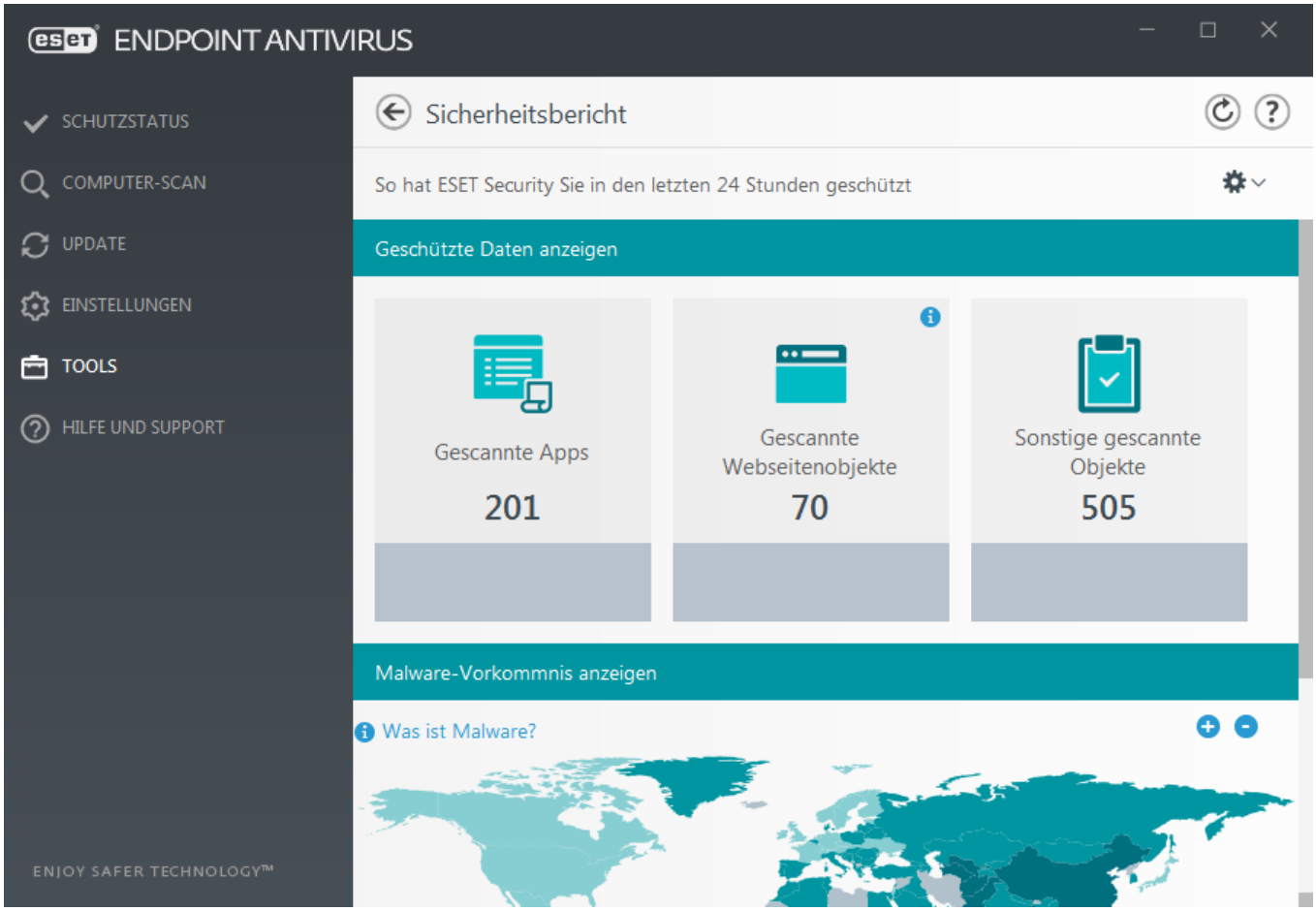
Gescannte Webseitenobjekte – Die Anzahl der gescannten Webseitenobjekte.

Gescannte E-Mail-Objekte – Die Anzahl der gescannten E-Mail-Objekte.

Diese Kategorien werden vom höchsten zum niedrigsten numerischen Wert geordnet. Kategorien mit Nullwert werden nicht angezeigt. Klicken Sie auf „**Mehr anzeigen**“, um ausgeblendete Kategorien zu erweitern und anzuzeigen.

Unter den Kategorien wird die aktuelle Virenlage mit einer Weltkarte angezeigt. Das Vorhandensein von Viren in einzelnen Ländern wird farblich markiert (dunklere Farben bedeuten höhere Zahlen). Länder ohne Daten sind ausgegraut. Bewegen Sie die Maus über ein Land, um Daten für das jeweilige Land anzuzeigen. Wählen Sie einen Kontinent aus, um automatisch zu zoomen.

Über das Zahnrad in der oberen rechten Ecke können Sie **Benachrichtigungen für Sicherheitsberichte aktivieren/deaktivieren** oder auswählen, ob die Daten für die letzten 30 Tage oder seit der Produktaktivierung angezeigt werden sollen. Falls ESET Endpoint Antivirus vor weniger als 30 Tagen installiert wurde, können Sie nur die Anzahl der Tage seit der Installation auswählen. Der Zeitraum von 30 Tagen ist standardmäßig vorausgewählt.



Mit **Daten zurücksetzen** können Sie alle Statistiken löschen und die vorhandenen Daten für den Sicherheitsbericht zurücksetzen. Diese Aktion muss bestätigt werden, es sei denn, Sie haben die Option **Vor dem Zurücksetzen von Statistiken nachfragen** unter **Erweiterte Einstellungen** > **Benutzeroberfläche** > **Warnungen und Hinweisfenster** > **Bestätigungsnachrichten** deaktiviert.

ESET SysRescue Live

ESET SysRescue Live ist ein kostenloses Hilfsprogramm, mit dem Sie eine bootfähige Rettungs-CD/DVD bzw. ein USB-Laufwerk erstellen können. Anschließend können Sie infizierte Computer mit Ihrem Rettungsmedium starten, um sie nach Malware zu scannen und infizierte Dateien zu säubern.

ESET SysRescue Live bietet den wichtigen Vorteil, dass die Software unabhängig vom Betriebssystem auf dem jeweiligen Rechner ausgeführt werden kann, aber trotzdem direkten Zugriff auf die Festplatte und das gesamte Dateisystem hat. Auf diese Weise lassen sich auch Bedrohungen entfernen, bei denen dies normalerweise (bei laufendem Betriebssystem usw.) nicht möglich wäre.

- Onlinehilfe für ESET SysRescue Live

Proben zur Analyse einreichen

Wenn Sie eine Datei mit verdächtigen Verhaltensweisen auf Ihrem Computer oder eine verdächtige Webseite im Internet finden, können Sie sie zur Analyse an das ESET-Virenlabor senden.

Bevor Sie Sample an ESET übermitteln

Übermitteln Sie die Probe nur, wenn sie mindestens eines der folgenden Kriterien erfüllt:
- Ihr ESET-Produkt erkennt die Probe überhaupt nicht
- Die Probe wird fälschlicherweise als Bedrohung erkannt
- Wir akzeptieren keine persönlichen Dateien, die Sie gerne von ESET auf Malware gescannt hätten, als Sample. Das ESET-Virenlabor führt keine On-Demand-Scans für unsere Benutzer durch.
- Formulieren Sie eine aussagekräftige Betreffzeile und geben Sie möglichst viele Informationen zu der eingesandten Datei an (z. B. einen Screenshot oder die Website, von der Sie die Datei heruntergeladen haben).

Sie können Samples (Dateien oder Webseiten) auf die folgenden Arten zur Analyse an ESET übermitteln:

1. Verwenden Sie das Dialogfeld zum Einreichen von Samples unter **Tools** > **Probe zur Analyse einreichen**.

2. Sie können Dateien auch per E-Mail einsenden. Komprimieren Sie in diesem Fall die Datei(en) mit WinRAR/ZIP, verschlüsseln Sie das Archiv mit dem Passwort „infected“ und senden Sie es an samples@eset.com.

3. Spam oder Fehlalarm melden, beachten Sie bitte unseren Artikel in der ESET-Knowledgebase.

Wählen Sie unter **Probe für die Analyse auswählen** im Dropdownmenü **Grund für Einreichen der Probe** die Beschreibung aus, die am besten auf Ihre Mitteilung zutrifft:

- **Verdächtige Datei**
- **Verdächtige Website** **(eine Website, die mit Schadsoftware infiziert ist)**
- **Fehlalarm Datei** (als Bedrohung erkannte Datei, die jedoch nicht infiziert ist)
- **Fehlalarm Webseite**
- **Sonstige**

Datei/Webseite– Der Pfad zu der Datei oder Webseite, die eingesandt werden soll.

E-Mail-Adresse für Rückfragen – Diese E-Mail-Adresse wird zusammen mit verdächtigen Dateien an ESET übermittelt. Möglicherweise wird ESET über diese Adresse Kontakt mit Ihnen aufnehmen, wenn zusätzliche Angaben für die Dateianalyse benötigt werden. Diese Angabe ist freiwillig. Wählen Sie **Anonym übermitteln** aus, falls Sie dieses Feld nicht ausfüllen möchten.

Sie erhalten möglicherweise keine Antwort von ESET

Sie erhalten nur eine Antwort von ESET, wenn wir weitere Informationen von Ihnen benötigen, da täglich mehrere Zehntausend Dateien auf unseren Servern eingehen und wir nicht jede Meldung individuell beantworten können.
Wenn sich herausstellt, dass die Datei bzw. Webseite Schadcode enthält, werden entsprechende Erkennungsfunktionen in einem zukünftigen ESET-Update berücksichtigt.

Probe für die Analyse auswählen - Verdächtige Datei

Beobachtete Anzeichen und Symptome einer Malware-Infektion– Beschreiben Sie, wie sich die verdächtige Datei auf Ihrem Computer verhält.

Herkunft der Datei (URL oder Hersteller)– Bitte geben Sie an, woher die Datei stammt (Quelle) und wie Sie sie entdeckt haben.

Hinweise und Zusatzangaben– Hier können Sie zusätzliche Informationen oder eine Beschreibung eingeben, die die Identifizierung und Auswertung der verdächtigen Datei erleichtern.

> **Hinweis**
> Das erste Feld –**Beobachtete Anzeichen und Symptome einer Malware-Infektion** – muss stets ausgefüllt werden, Zusatzangaben helfen dem Virenlabor jedoch erheblich bei der Identifizierung und Probenauswertung.

Probe für die Analyse auswählen - Verdächtige Webseite

Bitte wählen Sie eine der folgenden Optionen aus der Auswahlliste **Was stimmt mit de Webseite nicht** aus:

- **Infiziert** – Eine Webseite, die Viren oder sonstige Schadsoftware enthält, die auf verschiedenen Wegen verbreitet werden.
- **Phishing**–Oft eingesetzt, um Zugriff auf vertrauliche Daten zu erlangen, wie Kontonummern oder PIN-Codes. Nähere Informationen zu dieser Angriffsart finden Sie im Glossar.
- **Betrug** – Eine betrügerische Webseite, insbesondere zum Erreichen schneller Profite.
- Wählen Sie **Sonstige** aus, wenn keine der vorherigen Optionen für die Webseite zutrifft, die Sie übermitteln werden.

Hinweise und Zusatzangaben– Hier können Sie zusätzliche Informationen oder eine Beschreibung eingeben, die die Analyse der verdächtigen Webseite erleichtern.

Probe für die Analyse auswählen - Fehlalarm Datei

Wenn eine Datei als eingedrungene Schadsoftware erkannt wird, tatsächlich aber nicht infiziert ist, bitten wir Sie, diese Datei an uns einzureichen, um unseren Viren- und Spyware-Schutz zu verbessern und andere Benutzer zu schützen. Fehlalarme können auftreten, wenn das Muster einer Datei einem Muster entspricht, das in einer Malware Scan Engine gespeichert ist.

Name und Version der Anwendung– Bezeichnung und Version des Programms (z. B. Nummer, Aliasname oder Programmname).

Herkunft der Datei (URL oder Hersteller)– Bitte geben Sie an, woher die Datei stammt (Quelle) und wie Sie sie entdeckt haben.

Zweck der Anwendung– Eine allgemeine Beschreibung der Anwendung, die Art der Anwendung (z. B. Browser, Media-Player usw.) und ihre Funktion.

Hinweise und Zusatzangaben– Hier können Sie zusätzliche Informationen oder eine Beschreibung eingeben, die die Auswertung der verdächtigen Datei erleichtern.

> **Hinweis**
> Die ersten drei Angaben sind notwendig, um legitime Anwendungen zu identifizieren und von Schadcode zu unterscheiden. Zusatzangaben helfen dem Virenlabor erheblich bei der Identifizierung einer Bedrohung und der Auswertung von Sample.

Probe für die Analyse auswählen - Fehlalarm Webseite

Wenn eine Webseite als infiziert, Betrug oder Phishing erkannt wird, dies jedoch nicht ist, bitten wir Sie, diese Webseite an uns einzureichen. Fehlalarme können auftreten, wenn das Muster einer Datei einem Muster entspricht, das in einer Erkennungsroutine gespeichert ist. Reichen Sie diese Webseite bitte an uns ein, um unseren Viren- und Spyware-Schutz zu verbessern und andere Benutzer zu schützen.

Hinweise und Zusatzangaben– Hier können Sie zusätzliche Informationen oder eine Beschreibung eingeben, die die Auswertung der verdächtigen Datei erleichtern.

Probe für die Analyse auswählen - Sonstiges

Verwenden Sie diese Auswahlmöglichkeit, wenn die Datei keine **Verdächtige Datei** und kein **Fehlalarm** ist.

Grund für das Einsenden der Datei– Geben Sie eine genaue Beschreibung und den Grund für das Einreichen der Datei ein.

Benachrichtigungen

Optionen für die Kommunikation von Ereignissen vom ESET Endpoint Antivirus zum Benutzer finden Sie unter **Erweiterte Einstellungen (F5)** > **Tools** > **Benachrichtigungen**. In diesem Konfigurationsfenster können Sie die folgenden Benachrichtigungsarten definieren:

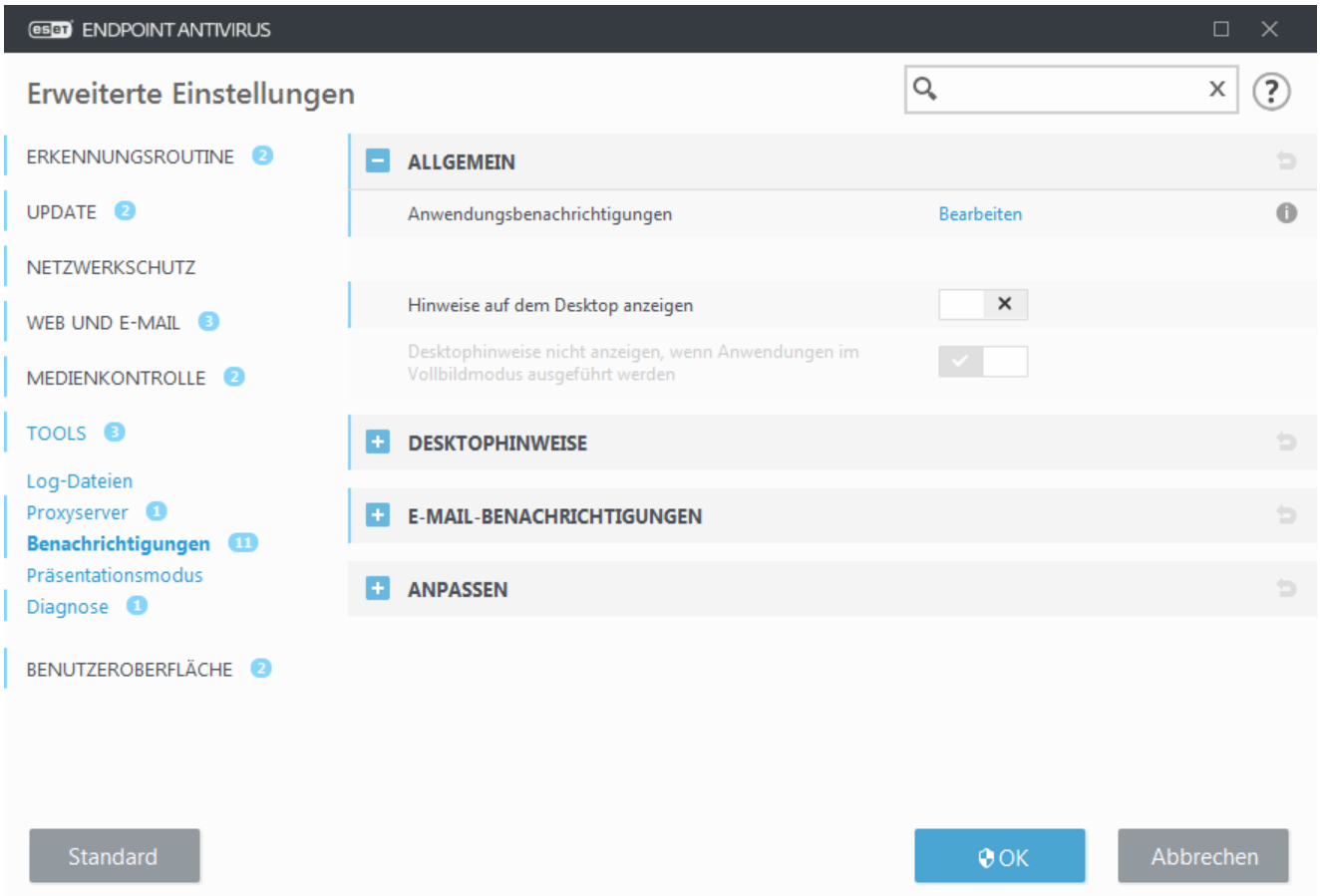
- Anwendungsbenachrichtigungen – Werden direkt im Hauptprogrammfenster angezeigt.
- Desktophinweise – Desktophinweise werden als kleines Popupfenster neben der Systemtaskleiste angezeigt.
- E-Mail-Benachrichtigungen – E-Mail-Benachrichtigungen werden an die angegebene E-Mail-Adresse verschickt.
- Anpassen der Benachrichtigungen – Fügen Sie beispielsweise eine benutzerdefinierte Nachricht zu einem Desktophinweis hinzu.

Mit den Schaltern im Bereich **Einfach** können Sie die folgenden Optionen anpassen:

Schalter	Standard	Beschreibung

Benachrichtigungen auf dem Desktop anzeigen	☑	Deaktivieren Sie diese Option, um die Popupbenachrichtigungen neben der Systemtaskleiste auszublenden. Wir empfehlen jedoch, diese Option aktiviert zu lassen, um über neue Ereignisse informiert zu werden.
Desktophinweise nicht anzeigen, wenn ...	☑	Lassen Sie **Desktophinweise nicht anzeigen, wenn Anwendungen im Vollbildmodus ausgeführt werden** aktiviert, um alle nicht interaktiven Benachrichtigungen zu unterdrücken.
Benachrichtigungen für Sicherheitsbericht anzeigen	☐	Aktivieren Sie diese Option, um eine Benachrichtigung zu erhalten, wenn eine neue Version eines Sicherheitsberichts generiert wird.
Benachrichtigungen über erfolgreiche Updates anzeigen	☐	Aktualisieren Sie diese Option, um eine Benachrichtigung zu erhalten, wenn das Produkt seine Komponenten und die Module der Erkennungsroutine aktualisiert.
Ereignisbenachrichtigungen per E-Mail versenden	☐	Aktivieren Sie diese Option, um E-Mail-Benachrichtigungen zu erhalten.

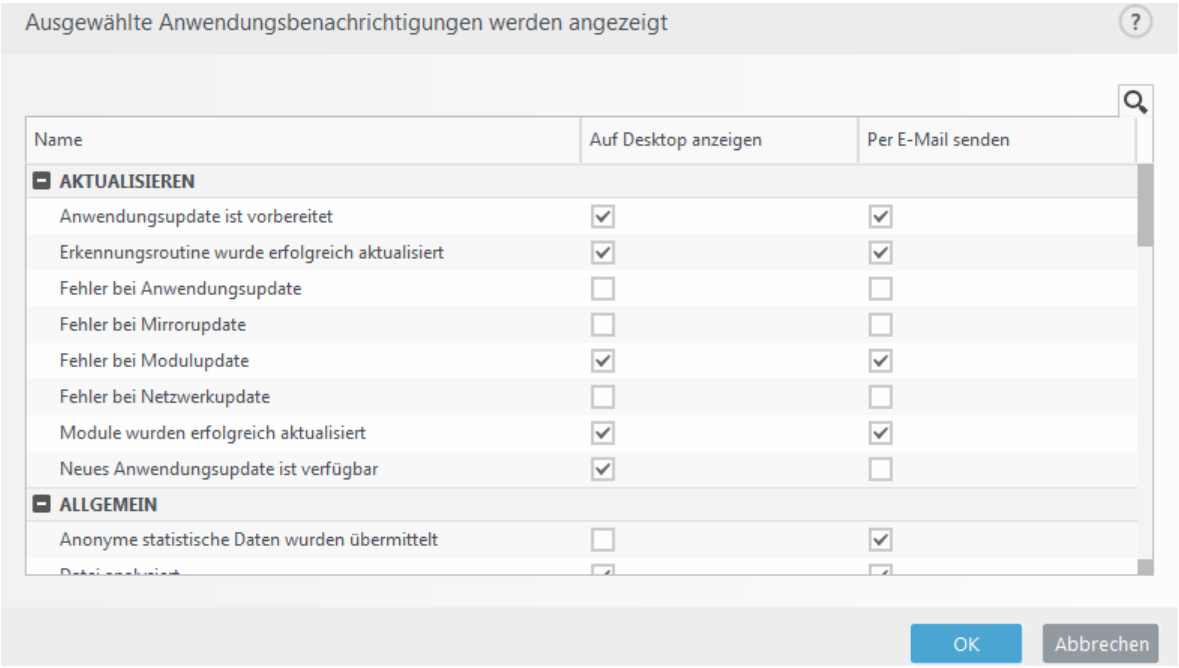
Um einzelne Anwendungsbenachrichtigungen zu aktivieren oder zu deaktivieren, klicken Sie auf **Bearbeiten** neben **Anwendungsbenachrichtigungen**.



Anwendungsbenachrichtigungen

Um die Sichtbarkeit von Anwendungsbenachrichtigungen (unten rechts auf dem Bildschirm) anzupassen, navigieren Sie zu **Tools** > **Benachrichtigungen** > **Einfach** > **Anwendungsbenachrichtigungen** in den erweiterten Einstellungen von ESET Endpoint Antivirus.

Die Liste der Benachrichtigungen ist in drei Spalten unterteilt. Die Namen der Benachrichtigungen sind in der ersten Spalte nach Kategorien sortiert. Mit den Kontrollkästchen in den Spalten **Auf Desktop anzeigen** und **Per E-Mail senden** können Sie festlegen, welche Benachrichtigungen das Produkt für neue Anwendungsereignisse generiert.



Allgemeine Einstellungen für Desktophinweise, wie etwa die Anzeigedauer für Benachrichtigungen und der Mindestinformationsumfang, können Sie unter **Erweiterte Einstellungen** > **Tools** > **Benachrichtigungen** > Desktophinweise anpassen.

Weitere Optionen wie das Format von E-Mail-Benachrichtigungen und SMTP-Servereinstellungen können Sie unter **Erweiterte Einstellungen** > **Tools** > **Benachrichtigungen** > E-Mail-Benachrichtigungen anpassen.

Desktophinweise

Desktophinweise werden als kleines Popupfenster neben der Systemtaskleiste angezeigt. Diese Hinweise verblassen standardmäßig nach 10 Sekunden langsam. Auf diese Weise kommuniziert ESET Endpoint Antivirus mit den Benutzern und benachrichtigt sie über erfolgreiche Produktupdates, neue verbundene Geräte, abgeschlossene Viren-Scans oder neue gefundene Bedrohungen.

Im Bereich **Desktophinweise** können Sie das Verhalten dieser Popupbenachrichtigungen mit den folgenden Attributen anpassen:

Dauer – Legt fest, wie lange die Benachrichtigung sichtbar ist. Dieser Wert muss im Bereich von 3 bis 30 Sekunden liegen.

Transparenz – Legt die Transparenz der Benachrichtigung als Prozentwert fest. Der unterstützte Bereich reicht von 0 (keine Transparenz) bis 80 (sehr hohe Transparenz).

Mindestinformationen anzuzeigender Ereignisse – Wählen Sie im Dropdownmenü den niedrigsten Schweregrad der anzuzeigenden Benachrichtigungen aus:

- **Diagnose**– Alle Meldungen höherer Stufen und alle sonstigen Informationen, die für das Beheben von Fehlern wichtig sein können, werden protokolliert.

• **Informationen**– Informationsmeldungen, wie nicht standardmäßige Netzwerkereignisse und erfolgreiche Updates, sowie alle Meldungen höherer Stufen werden protokolliert.

• **Warnungen**– Schwerwiegende Fehler und Warnmeldungen werden aufgezeichnet (z. B. Anti-Stealth wird nicht ordnungsgemäß ausgeführt oder bei einem Update ist ein Fehler aufgetreten).

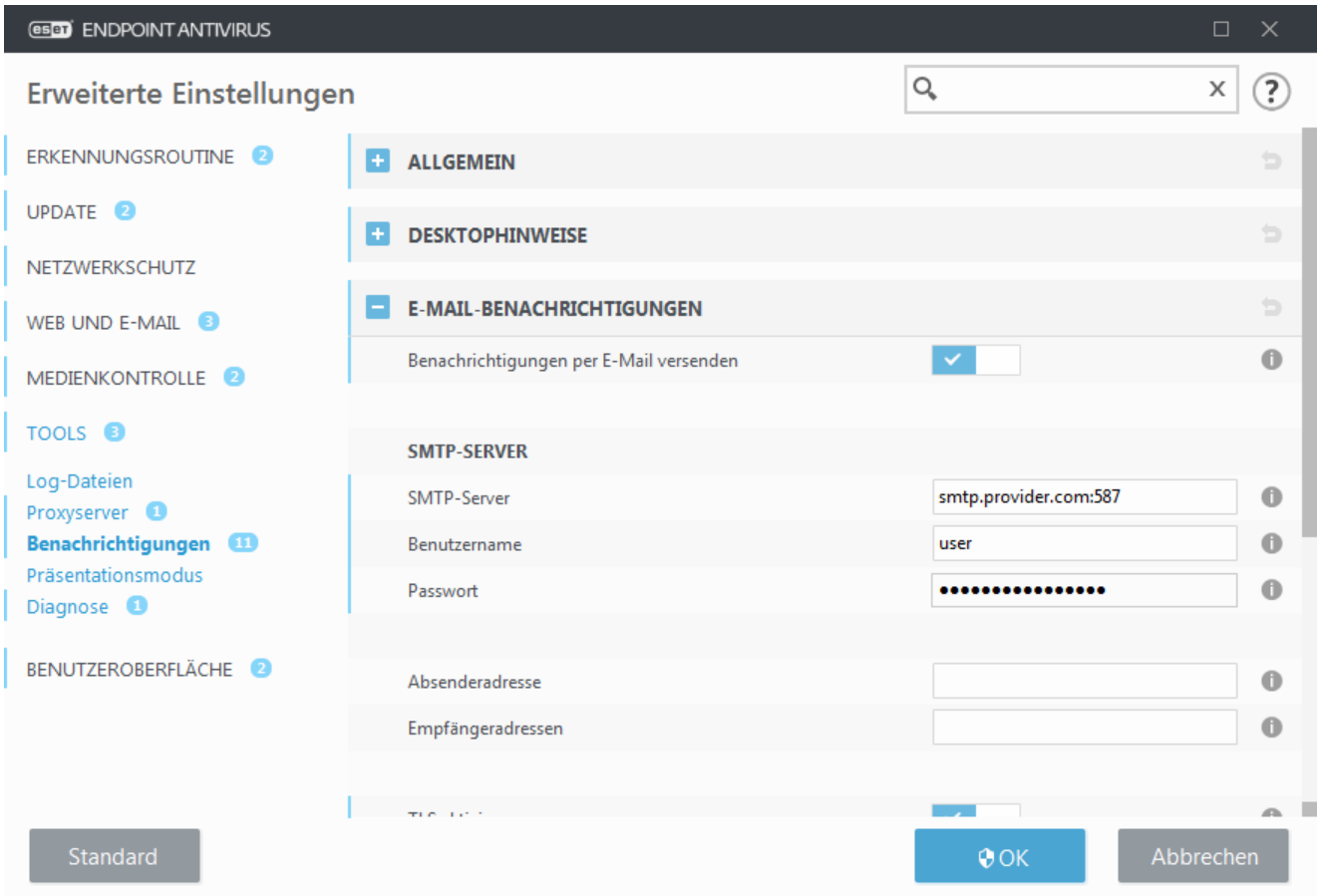
• **Fehler**– Fehler (z. B. Dokumentschutz nicht gestartet) und schwerwiegende Fehler werden aufgezeichnet.

• **Kritische Warnungen**– Nur kritische Fehler werden aufgezeichnet, z. B. Fehler beim Starten des Virenschutz-Moduls oder ein infiziertes System.

Auf Mehrbenutzersystemen Hinweise auf dem Bildschirm des folgenden Benutzers ausgeben – Geben Sie die kompletten Kontonamen der Benutzer ein, die Desktophinweise erhalten sollen, z. B. falls Sie Ihren Computer neben dem Administratorkonto auch mit einem anderen Benutzerkonto verwenden und weiterhin über neue Produktereignisse informiert werden möchten.

E-Mail-Benachrichtigungen

ESET Endpoint Antivirus kann automatisch Ereignismeldungen senden, wenn ein Ereignis mit dem ausgewählten Informationsumfang auftritt. Aktivieren Sie **Ereignismeldungen per E-Mail versenden** im Bereich **Einfach**, damit Ereignismeldungen versendet werden.



SMTP-Server

SMTP-Server–Der SMTP-Server, über den Benachrichtigungen verschickt werden (z. B. *smtp.Anbieter.com:587*, der Standardport ist 25).

Hinweis
ESET Endpoint Antivirus unterstützt keine SMTP-Server mit TLS-Verschlüsselung.

Benutzername und **Passwort**–Falls für den SMTP-Server Zugangsdaten zur Authentifizierung erforderlich sind, geben Sie hier einen gültigen Benutzernamen und das Passwort ein.

Absenderadresse–Dieses Feld enthält die Adresse, die in Ereignismeldungen als Absender verzeichnet sein soll.

Empfängeradresse–Dieses Feld enthält die Empfängeradresse, die in Ereignismeldungen als Empfänger verzeichnet sein soll. Geben Sie mehrere E-Mail-Adressen durch ein Semikolon ";" voneinander getrennt an.

TLS aktivieren– Hiermit werden von der TLS-Verschlüsselung unterstützte Warnungen und Hinweismeldungen versendet.

E-Mail-Einstellungen

Im Dropdownmenü **Informationsumfang der Meldungen** können Sie festlegen, für welchen anfänglichen Schweregrad Benachrichtigungen gesendet werden sollen.

- **Diagnose**– Alle Meldungen höherer Stufen und alle sonstigen Informationen, die für das Beheben von Fehlern wichtig sein können, werden protokolliert.
- **Informationen**– Informationsmeldungen, wie nicht standardmäßige Netzwerkereignisse und erfolgreiche Updates, sowie alle Meldungen höherer Stufen werden protokolliert.
- **Warnungen**– Schwerwiegende Fehler und Warnmeldungen werden aufgezeichnet (z. B. Anti-Stealth wird nicht ordnungsgemäß ausgeführt oder bei einem Update ist ein Fehler aufgetreten).
- **Fehler**– Fehler (z. B. Dokumentschutz nicht gestartet) und schwerwiegende Fehler werden aufgezeichnet.
- **Kritische Warnungen**– Nur kritische Fehler werden aufgezeichnet, z. B. Fehler beim Starten des Virenschutz-Moduls oder ein infiziertes System.

Jede Benachrichtigung in einer getrennten E-Mail senden – Wenn diese Option aktiviert ist, erhält der Empfänger für jede einzelne Benachrichtigung eine separate E-Mail. Dies kann dazu führen, dass innerhalb kurzer Zeit eine große Anzahl E-Mails empfangen werden.

Intervall bis zum Senden neuer Benachrichtigungs-E-Mails (Min.)– Intervall in Minuten, nach dem neue Benachrichtigungen per E-Mail gesendet werden. Wenn der Wert auf „0“ festgelegt wird, werden die Benachrichtigungen sofort gesendet.

Format von Meldungen

Ereignismeldungen werden als E-Mails oder LAN-Nachrichten (Windows-Messaging-Dienst) an Remotebenutzer oder Systemadministratoren weitergeleitet. Das Standard-Nachrichtenformat ist für die meisten Einsatzfälle ausreichend. Sie können das Format der Meldungen bei Ereignissen jedoch auch anpassen.

Format der Meldungen bei Ereignissen - Format der Meldungen bei auf Remotecomputern angezeigten Ereignissen.

Format der Meldungen bei Bedrohungen – Warnungen und Benachrichtigungen besitzen ein vordefiniertes Standardformat. Dieses Format sollte nicht geändert werden. Unter bestimmten Umständen (etwa, wenn Sie ein automatisiertes E-Mail-Verarbeitungssystem verwenden) ist es jedoch möglicherweise erforderlich, das Meldungsformat zu ändern.

Zeichensatz - Konvertiert eine E-Mail-Nachricht in den ANSI-Zeichensatz gemäß der Windows-Regionseinstellungen (z. B. windows-1250, Unicode (UTF-8), ACSII 7-bit oder Japanisch (ISO-2022-JP)). Dabei wird beispielsweise "á" in "a" geändert, und unbekannte Zeichen in "?").

Quoted-Printable-Kodierung verwenden – Die E-Mail-Nachrichtenquelle wird in das Quoted-Printable-Format (QP) konvertiert, das ASCII-Zeichen verwendet und besondere regionale Zeichen in der E-Mail korrekt im 8-Bit-Format überträgt (áéíóú).

Schlüsselwörter (durch %-Zeichen abgetrennte Zeichenfolgen) in der Meldung werden durch entsprechende Informationen ersetzt. Folgende Schlüsselwörter sind verfügbar:

- **%TimeStamp%** – Datum und Uhrzeit des Ereignisses
- **%Scanner%** – betroffenes Modul
- **%ComputerName%** – Name des Computers, auf dem die Warnmeldung aufgetreten ist
- **%ProgramName%** – Programm, das die Warnung erzeugt hat
- **%InfectedObject%** – Name der infizierten Datei, Nachricht usw.
- **%VirusName%** – Angabe des Infektionsverursachers
- **%Action%** – bei der Infiltration durchgeführte Aktion
- **%ErrorDescription%** – Beschreibung eines nicht durch einen Virus ausgelösten Ereignisses

Die Schlüsselwörter **%InfectedObject%** und **%VirusName%** werden nur in Warnmeldungen bei Bedrohungen verwendet, **%ErrorDescription%** nur in Ereignismeldungen.

Anpassen der Benachrichtigungen

In diesem Fenster können Sie die Benachrichtigungen anpassen.

Standardbenachrichtigung - Eine Standardnachricht, die in der Fußzeile von Benachrichtigungen angezeigt wird.

Bedrohungen

Wenn die Option **Warnhinweise für Bedrohungen nicht automatisch schließen** aktiviert ist, werden Warnhinweise auf dem Bildschirm angezeigt, bis diese manuell geschlossen werden.

Deaktivieren Sie die Option **Standardnachricht verwenden** und geben Sie eine eigene Nachricht unter **Bedrohungsbenachrichtigung** ein, um diese eigene Nachricht zu verwenden.

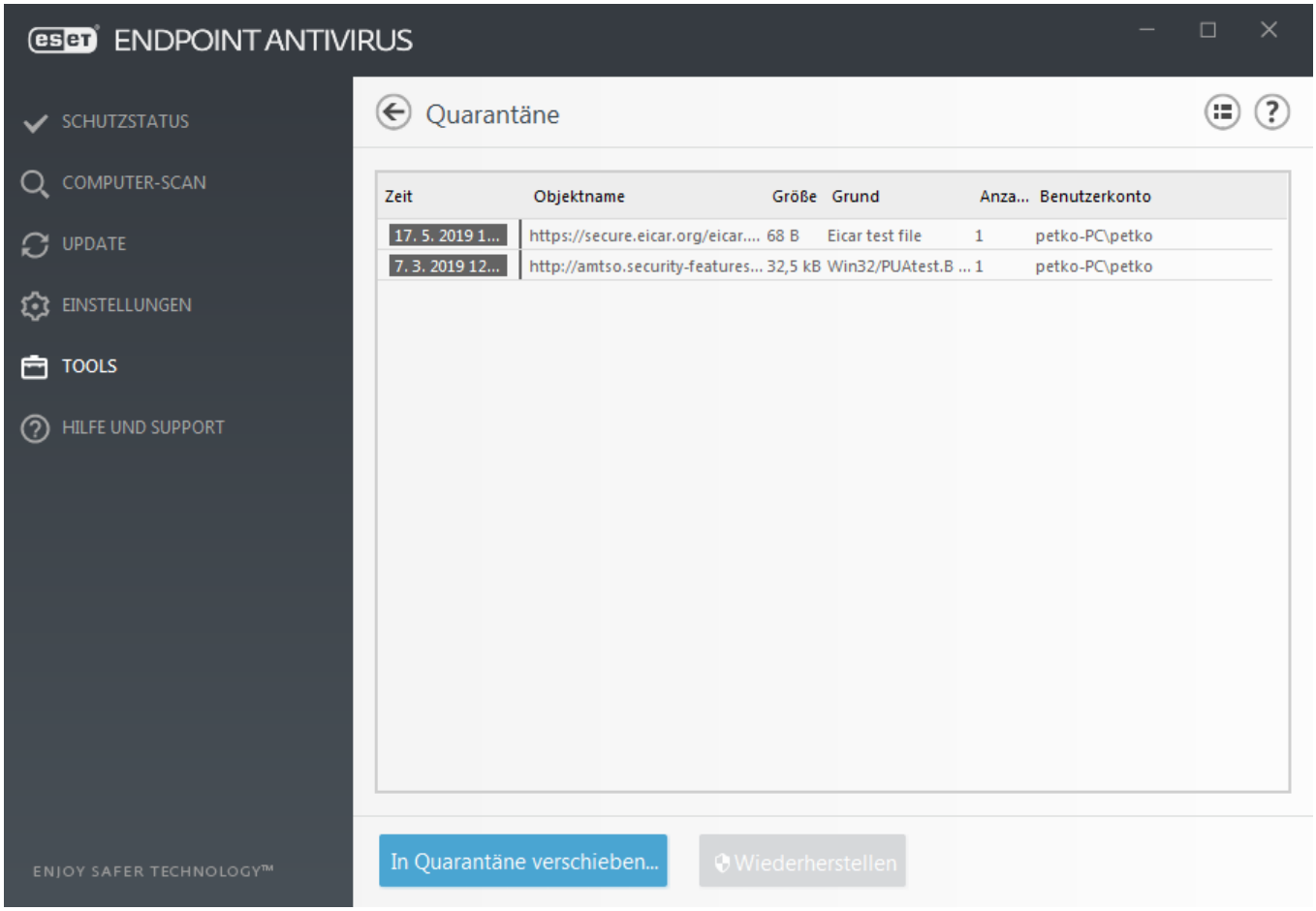
Quarantäne

Die Hauptfunktion der Quarantäne ist die sichere Verwahrung infizierter Dateien. Dateien sollten in die Quarantäne verschoben werden, wenn sie nicht gesäubert werden können, wenn es nicht sicher oder ratsam ist, sie zu löschen, oder wenn sie von ESET Endpoint Antivirus fälschlicherweise erkannt worden sind.

Sie finden die Quarantäne im Hauptprogrammfenster von ESET Endpoint Antivirus unter **Tools** > **Quarantäne**.

Sie können beliebige Dateien per Ziehen und Ablegen manuell in die Quarantäne verschieben, indem Sie die Datei anklicken, den Mauszeiger mit gedrückter Maustaste in den markierten Bereich ziehen und anschließend

loslassen. Anschließend wird die Anwendung in den Vordergrund verschoben. Verwenden Sie diese Vorgehensweise, wenn sich eine Datei verdächtig verhält, aber nicht vom Virenschutz-Scanner erkannt wird. Quarantäne-Dateien können zur Analyse an das ESET-Virenlabor übermittelt werden.



Die Dateien im Quarantäneordner können in einer Tabelle angezeigt werden, die Datum und Uhrzeit der Quarantäne, den Pfad zum ursprünglichen Speicherort der infizierten Datei, ihre Größe in Byte, einen Grund (z. B. Objekt hinzugefügt durch Benutzer) und die Anzahl der Ereignisse enthält.

Quarantäne für Dateien

ESET Endpoint Antivirus verschiebt gelöschte Dateien automatisch in den Quarantäneordner (sofern diese Option nicht im Warnfenster deaktiviert wurde). Auf Wunsch können Sie beliebige verdächtige Dateien manuell in die Quarantäne verschieben, indem Sie auf **In Quarantäne verschieben** klicken. Die Datei wird aus ihrem ursprünglichen Speicherort entfernt. Diese Aktion ist auch im Kontextmenü verfügbar: Klicken Sie mit der rechten Maustaste in das Fenster **Quarantäne** und wählen Sie **Datei in Quarantäne verschieben** aus.

Wiederherstellen aus der Quarantäne

Dateien aus der Quarantäne können auch an ihrem ursprünglichen Speicherort wiederhergestellt werden. Um eine Datei aus der Quarantäne wiederherzustellen, klicken Sie mit der rechten Maustaste in das Quarantänefenster und wählen Sie im Kontextmenü **Wiederherstellen** aus. Wenn eine Datei als Eventuell unerwünschte Anwendung gekennzeichnet ist, wird die Funktion **Wiederherstellen und von Prüfungen ausschließen** verfügbar. Das Kontextmenü enthält außerdem die Option **Wiederherstellen nach ...**, mit der Dateien an einem anderen als ihrem ursprünglichen Speicherort wiederhergestellt werden können.

Löschen aus der Quarantäne - Klicken Sie mit der rechten Maustaste auf ein Element und wählen Sie **Aus**

Quarantäne löschen aus. Alternativ können Sie das zu löschende Element auswählen und auf der Tastatur die Entf-Taste drücken. Sie können auch mehrere Einträge gleichzeitig auswählen und gesammelt löschen.

> **Hinweis**
> Wenn versehentlich eine harmlose Datei in die Quarantäne versetzt wurde, schließen Sie die Datei nach der Wiederherstellung vom Scan aus und senden Sie sie an den ESET-Support.

Einreichen einer Datei aus der Quarantäne

Wenn Sie eine verdächtige, nicht vom Programm erkannte Datei in die Quarantäne verschoben haben oder wenn eine Datei fälschlich als infiziert eingestuft wurde und infolgedessen in den Quarantäneordner verschoben wurde, senden Sie die Datei zur Analyse an ESET. Um eine Datei zu senden, die in der Quarantäne gespeichert ist, klicken Sie mit der rechten Maustaste darauf und wählen im angezeigten Kontextmenü die Option **Datei zur Analyse einreichen**.

Einstellungen für Proxyserver

In großen LAN-Netzwerken wird die Verbindung zum Internet häufig über Proxyserver vermittelt. In einer solchen Konfiguration müssen die folgenden Einstellungen definiert werden. Wenn die Einstellungen nicht vorgenommen werden, ist es möglicherweise nicht möglich, automatisch Updates über das Internet zu beziehen. Die Proxyserver-Einstellungen in ESET Endpoint Antivirus sind über zwei verschiedene Bereiche der erweiterten Einstellungen verfügbar.

Die Einstellungen für den Proxyserver können zum einen in **Erweiterte Einstellungen** unter **Tools** > **Proxyserver** konfiguriert werden. So legen Sie die allgemeinen Proxyserver-Einstellungen für alle Funktionen von ESET Endpoint Antivirus fest. Diese Parameter werden von allen Modulen verwendet, die eine Verbindung zum Internet benötigen.

Um die Proxyserver-Einstellungen für diese Ebene festzulegen, aktivieren Sie die Option **Proxyserver verwenden** und geben im Feld **Proxyserver** die entsprechende Adresse zusammen mit dem **Port** des Proxyservers ein.

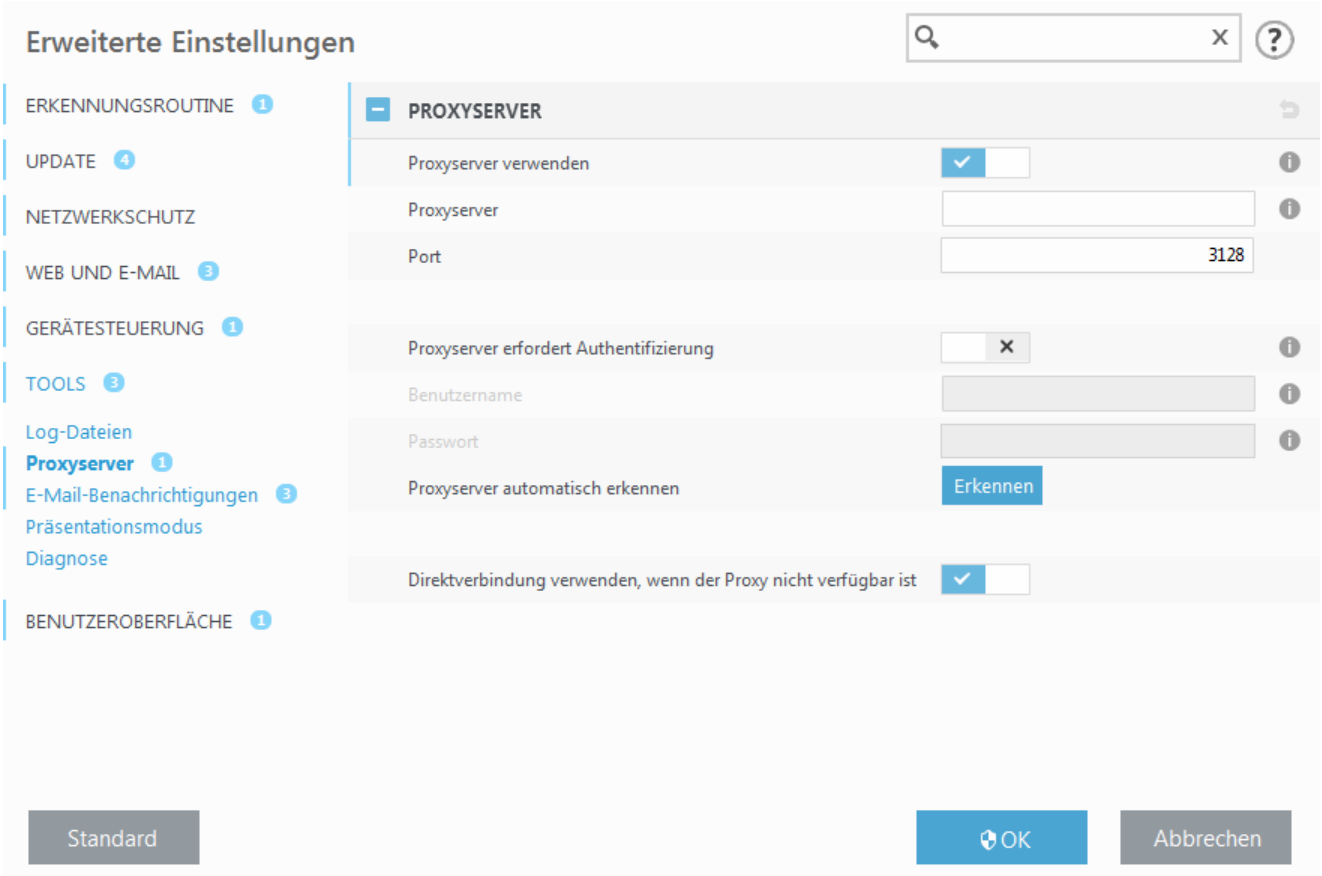
Wenn der Proxyserver eine Authentifizierung benötigt, aktivieren Sie **Proxyserver erfordert Authentifizierung** und geben einen gültigen **Benutzernamen** sowie das entsprechende **Passwort** ein. Klicken Sie auf **Proxyserver automatisch erkennen**, wenn die Einstellungen des Proxyservers automatisch erkannt und ausgefüllt werden sollen. Die in den Internetoptionen für Internet Explorer oder Google Chrome festgelegten Einstellungen werden kopiert.

> **Hinweis**
> Sie müssen den Benutzernamen und das Passwort manuell in den Einstellungen für den **Proxyserver** eingeben.

Direktverbindung verwenden, wenn Proxy nicht verfügbar ist – Wenn ESET Endpoint Antivirus für die Verwendung eines Proxys konfiguriert ist und der Proxy nicht erreichbar ist, umgeht ESET Endpoint Antivirus den Proxy und kommuniziert direkt mit ESET-Servern.

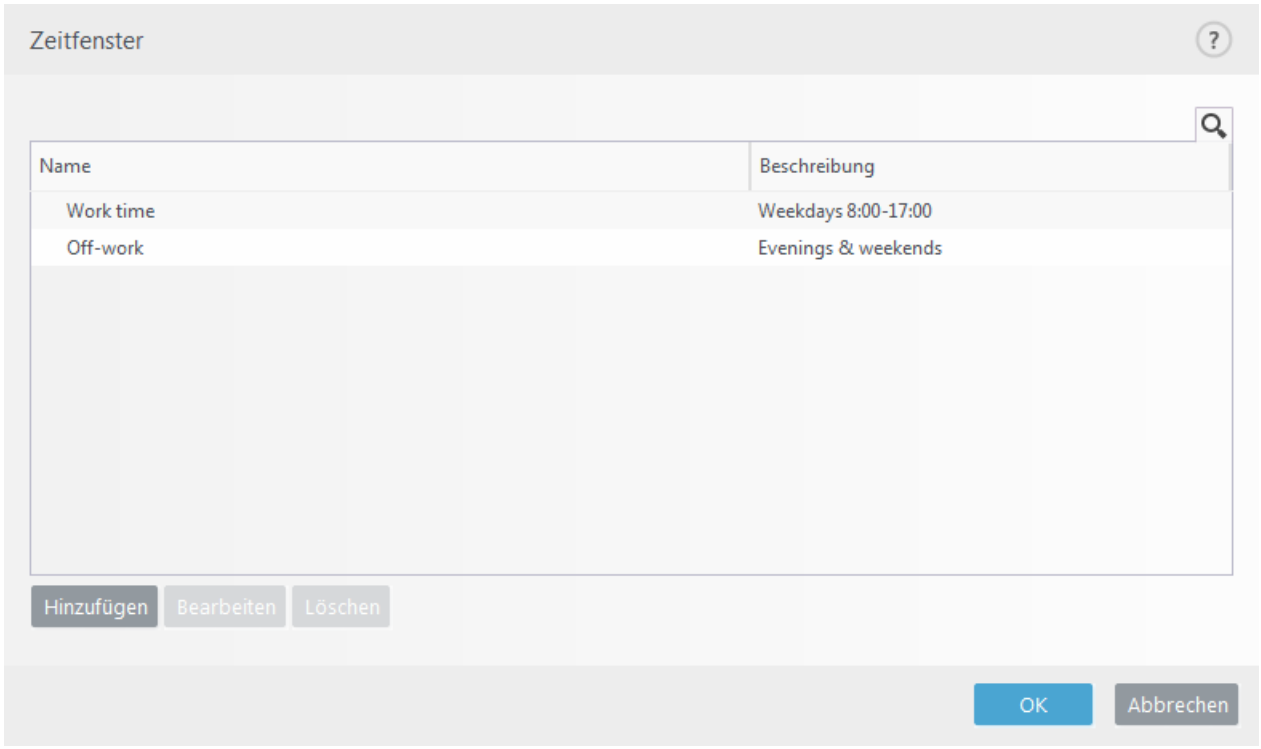
Die Proxyserver-Einstellungen können auch in den erweiterten Einstellungen für Updates festgelegt werden (**Erweiterte Einstellungen** > **Update** > **Profile** > **Update** > **Verbindungsoptionen**, Option **Verbindung über Proxyserver** im Dropdown-Menü **Proxy-Modus**). Die Einstellungen gelten dann für das entsprechende Update-

Profil. Diese Methode empfiehlt sich für Laptops, da diese die Updates der Erkennungsroutine oft von Remotestandorten beziehen. Weitere Informationen zu diesen Einstellungen finden Sie unter Erweiterte Einstellungen für Updates.



Zeitfenster

Sie können Zeitfenster erstellen und anschließend zu Regeln für die **Medienkontrolle**. Sie finden die Einstellungen für **Zeitfenster** unter **Erweiterte Einstellungen** > **Tools**. Dort können Sie häufig verwendete Zeitfenster (z. B. Arbeitszeit, Wochenende usw.) konfigurieren und wiederverwenden, ohne für jede Regel neue Zeitfenster zu definieren. Zeitfenster können für jeden passenden Regeltyp verwendet werden, der zeitbasierte Kontrollen unterstützt.



Gehen Sie wie folgt vor, um ein Zeitfenster zu erstellen:

1. Klicken Sie auf **Bearbeiten** > **Hinzufügen.**
2. Geben Sie einen Namen und eine **Beschreibung** für das Zeitfenster ein und klicken Sie auf **Hinzufügen**.
3. Geben Sie den Tag und die Start- und Endzeit für das Zeitfenster ein oder wählen Sie **Ganzer Tag** aus.
4. Klicken Sie auf **OK**, um Ihre Eingaben zu bestätigen.

Jedes Zeitfenster kann mit einem oder mehreren Zeitintervallen zu unterschiedlichen Wochentagen und Uhrzeiten definiert werden. Nach der Erstellung werden die Zeitfenster im Dropdownmenü **Anwendungszeitraum** im Fenster Regel-Editor für die Medienkontrollewird.

Microsoft Windows Update

Die Windows Update-Funktion ist ein wichtiger Bestandteil des Schutzes vor bösartiger Software. Aus diesem Grund ist es essenziell, dass Sie verfügbare Microsoft Windows-Updates sofort installieren. Entsprechend der von Ihnen festgelegten Richtlinien benachrichtigt Sie ESET Endpoint Antivirus über fehlende Updates. Folgende Richtlinien sind verfügbar:

- **Keine Updates** - Es werden keine Updates zum Download angeboten.
- **Optionale Updates** - Updates mit beliebiger Priorität werden zum Download angeboten.
- **Empfohlene Updates** - Updates mit normaler Priorität und höher werden zum Download angeboten.
- **Wichtige Updates** - Updates mit hoher Priorität und kritische Updates werden zum Download angeboten.
- **Kritische Updates** - Nur kritische Updates werden zum Download angeboten.

Klicken Sie auf **OK**, um die Änderungen zu speichern. Das Fenster „System-Updates“ wird nach erfolgter Statusverifizierung durch den Update-Server angezeigt. Dementsprechend stehen die aktualisierten Systemdaten möglicherweise nicht unmittelbar nach Speicherung der Änderungen zur Verfügung.

Lizenzintervall überprüfen

ESET Endpoint Antivirus muss sich automatisch mit den ESET-Servern verbinden. Sie können diese Einstellung unter **Erweiterte Einstellungen (F5)** > **Tools** > **Lizenz** anpassen. Standardmäßig ist die **Intervallprüfung** auf **Automatisch** festgelegt, und der ESET-Lizenzserver überprüft das Produkt mehrmals pro Stunde. Bei erhöhtem Netzwerkdatenverkehr können Sie diese Einstellung auf **Eingeschränkt** festlegen, um den Mehraufwand zu reduzieren. Wenn Sie die Option **Eingeschränkt** auswählen, überprüft ESET Endpoint Antivirus den Lizenzserver nur einmal pro Tag oder wenn der Computer neu gestartet wird.



Wichtig

Wenn Sie unter **Intervallprüfung** die Option **Eingeschränkt** auswählen, kann es bis zu einen Tag dauern, bis Ihre in ESET Business Account /ESET MSP Administrator vorgenommenen Änderungen in die ESET Endpoint Antivirus-Einstellungen übernommen werden.

Benutzeroberfläche

Im Abschnitt **Benutzeroberfläche** können Sie das Verhalten der grafischen Benutzeroberfläche (GUI) des Programms konfigurieren.

Mit dem Tool Elemente der Benutzeroberfläche können Sie die Darstellung und die Effekte des Programms ändern.

Um die maximale Sicherheit Ihrer Sicherheitssoftware zu gewährleisten, können Sie unbefugte Änderungen mit dem Tool Einstellungen für den Zugriff verhindern.

Konfigurieren Sie Warnungen und Hinweisfenster sowie Benachrichtigungen, um festzulegen, wie Warnungen für Ereignisse und Systemhinweise angezeigt werden sollen. Sie können diese Funktion an Ihre Anforderungen anpassen.

Wenn Sie festlegen, dass bestimmte Hinweise nicht angezeigt werden sollen, werden diese in die Liste **Elemente der Benutzeroberfläche** > **Anwendungsstatus** aufgenommen. Hier können Sie den Status anzeigen und festlegen, welche Benachrichtigungen angezeigt werden sollen.

Das Integration in Kontextmenüs wird angezeigt, wenn Sie mit der rechten Maustaste auf das gewünschte Element klicken. Mit diesem Tool können ESET Endpoint Antivirus-Steuerelemente in das Kontextmenü integriert werden.

Der Präsentationsmodus ist für Benutzer geeignet, die ohne störende Popup-Fenster, geplante Tasks und alles, was die Prozessorlast und Arbeitsspeicherbelegung steigern könnte, mit einer Anwendung arbeiten möchten.

Siehe auch Minimieren der ESET Endpoint Antivirus-Benutzeroberfläche (hilfreich für verwaltete Umgebungen).

Elemente der Benutzeroberfläche

Über die Konfigurationsoptionen für die Benutzeroberfläche von ESET Endpoint Antivirus können Sie die Arbeitsumgebung an Ihre Anforderungen anpassen. Zugriff auf diese Optionen erhalten Sie unter **Benutzeroberfläche** > **Elemente der Benutzeroberfläche** in den erweiterten Einstellungen von ESET Endpoint Antivirus.

Im Bereich **Elemente der Benutzeroberfläche** können Sie die Arbeitsumgebung anpassen. Wenn Sie auf das Dropdown-Menü **Startmodus** klicken, werden die folgenden Startmodi für die grafische Benutzeroberfläche (GUI) zur Auswahl angezeigt:

Vollständig - Die komplette Benutzeroberfläche wird angezeigt.

Minimal - Die grafische Benutzeroberfläche wird ausgeführt, aber dem Benutzer werden nur Benachrichtigungen angezeigt.

Manuell - Die grafische Benutzeroberfläche wird bei der Anmeldung nicht automatisch gestartet und kann von allen Benutzern manuell gestartet werden.

Still - Es werden keine Benachrichtigungen oder Hinweise angezeigt. Die grafische Benutzeroberfläche kann nur vom Administrator gestartet werden. Dieser Modus kann in verwalteten Umgebungen nützlich sein, um die Systemressourcen zu schonen.

> **Hinweis**
> Wenn Sie den minimalen GUI-Startmodus ausgewählt haben und der Computer neu gestartet wird, werden nur Benachrichtigungen angezeigt, jedoch nicht die grafische Benutzeroberfläche. Um wieder die vollständige grafische Benutzeroberfläche anzuzeigen, führen Sie die GUI über das Startmenü unter **Alle Programme** > **ESET** > ESET Endpoint Antivirus als Administrator aus. Sie können dies auch über ESET Security Management Center mit einer Policy bewerkstelligen.

Wenn ESET Endpoint Antivirus ohne Anzeige des Startbilds gestartet werden soll, deaktivieren Sie die Option **Startbild anzeigen**.

Wenn ESET Endpoint Antivirus bei wichtigen Ereignissen wie z. B. der Erkennung einer Bedrohung oder wenn eine Prüfung abgeschlossen wird, einen Warnton ausgeben soll, aktivieren Sie die Option **Hinweistöne wiedergeben**.

In Kontextmenü integrieren - ESET Endpoint Antivirus kann in das Kontextmenü integriert werden.

Status

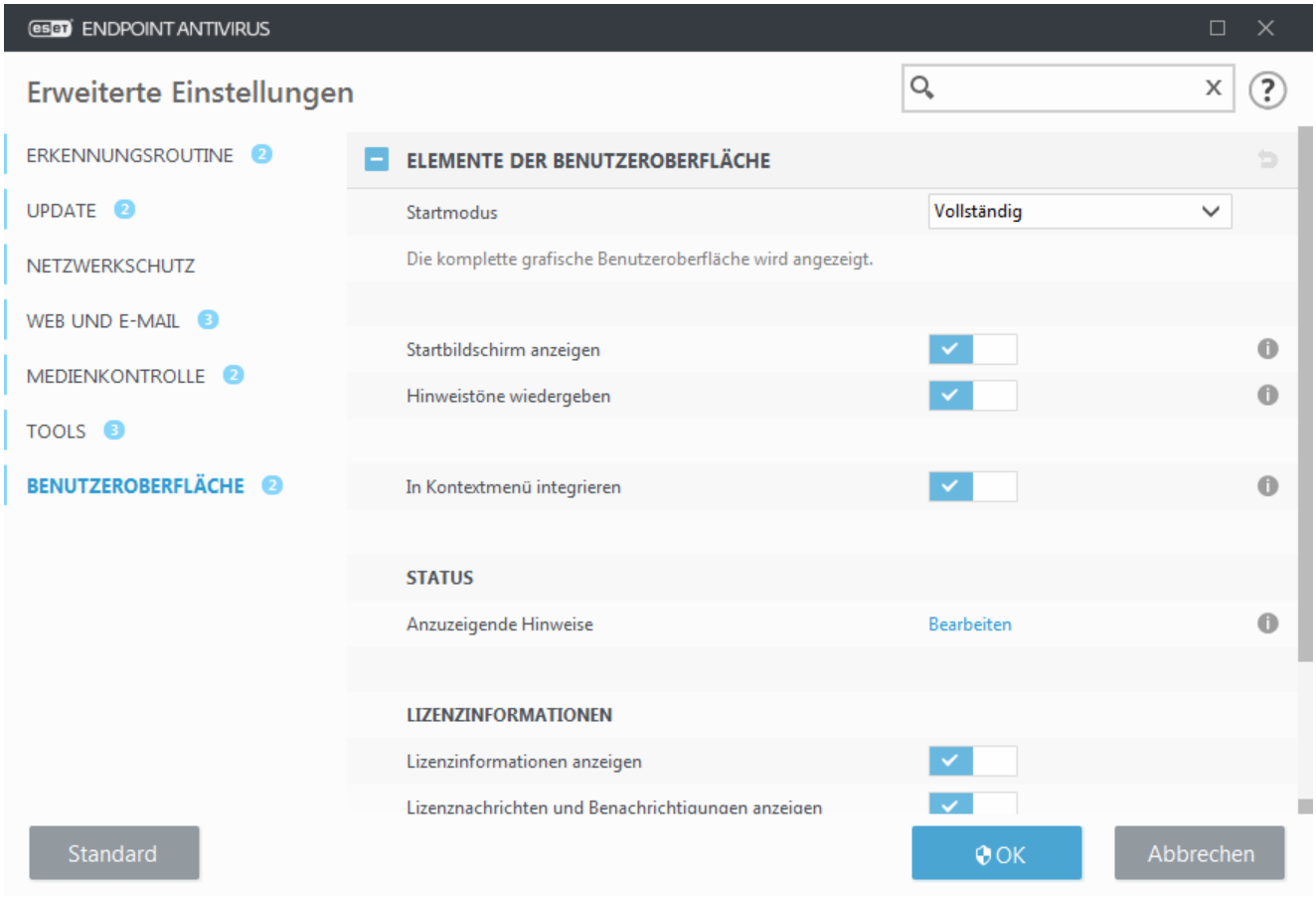
Anwendungsstatus - Klicken Sie auf **Bearbeiten**, um Status, die im Hauptmenü im Bereich **Schutzstatus** angezeigt werden, zu verwalten (zu deaktivieren).

Lizenzinformationen

Lizenzinformationen anzeigen - Wenn diese Option deaktiviert ist, wird das Ablaufdatum der Lizenz in den Bildschirmen **Schutzstatus** und **Hilfe und Support** nicht angezeigt.

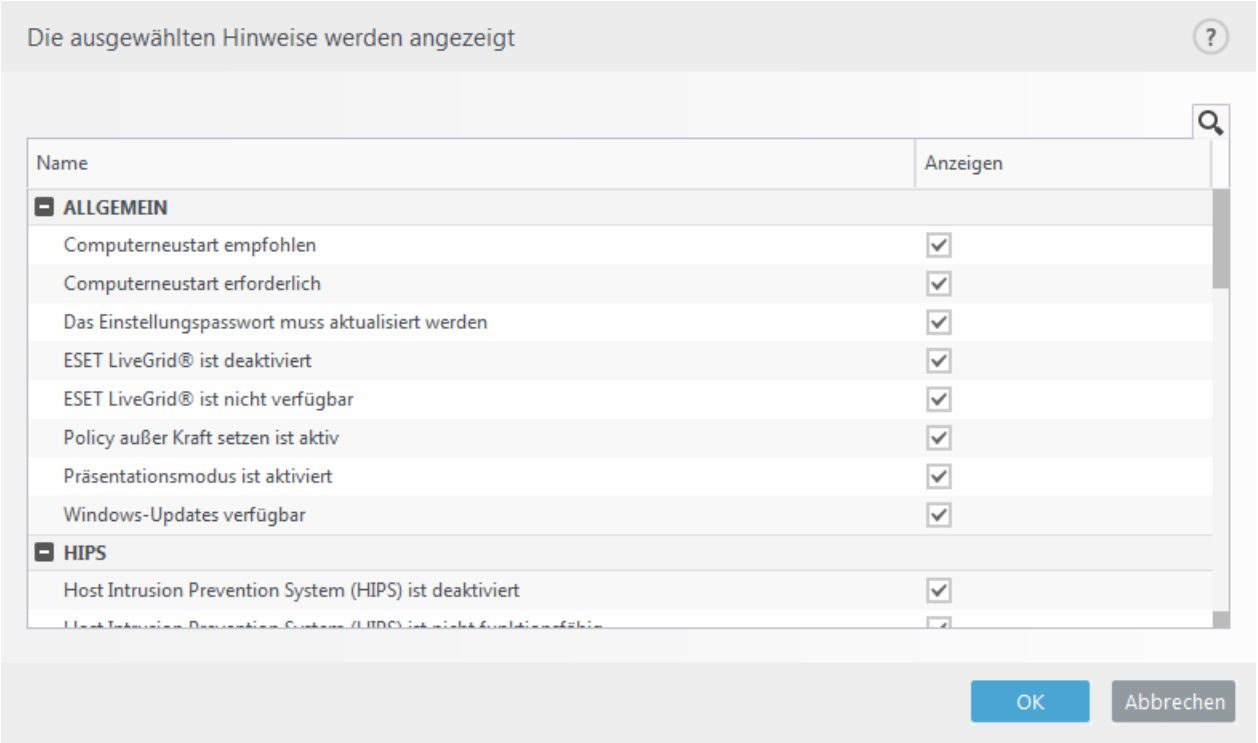
Lizenzinformationen und Benachrichtigungen anzeigen - Wenn diese Option deaktiviert ist, werden nur beim Ablauf der Lizenz Benachrichtigungen angezeigt.

> **Hinweis**
> Die Lizenzinformationen werden für ESET Endpoint Antivirus-Installationen, die über eine MSP-Lizenz aktiviert wurden, zwar übernommen, können jedoch nicht abgerufen werden.



Anzuzeigende Hinweise

Um den produktinternen Status im ersten Bereich von ESET Endpoint Antivirus anzupassen, navigieren Sie zu **Benutzeroberfläche** > **Elemente der Benutzeroberfläche** > **Anzuzeigende Hinweise** in den erweiterten Einstellungen von ESET Endpoint Antivirus.



Wählen Sie aus, welche Anwendungs-Statusmeldungen angezeigt werden sollen. Hier können Sie beispielsweise den Viren- und Spyware-Schutz anhalten oder den Präsentationsmodus aktivieren. Wenn Ihr Produkt nicht aktiviert oder Ihre Lizenz abgelaufen ist, wird ebenfalls eine Anwendungs-Statusmeldung angezeigt. Diese Einstellung kann mit ESET Security Management Center-Policies geändert werden.

Einstellungen für den Zugriff

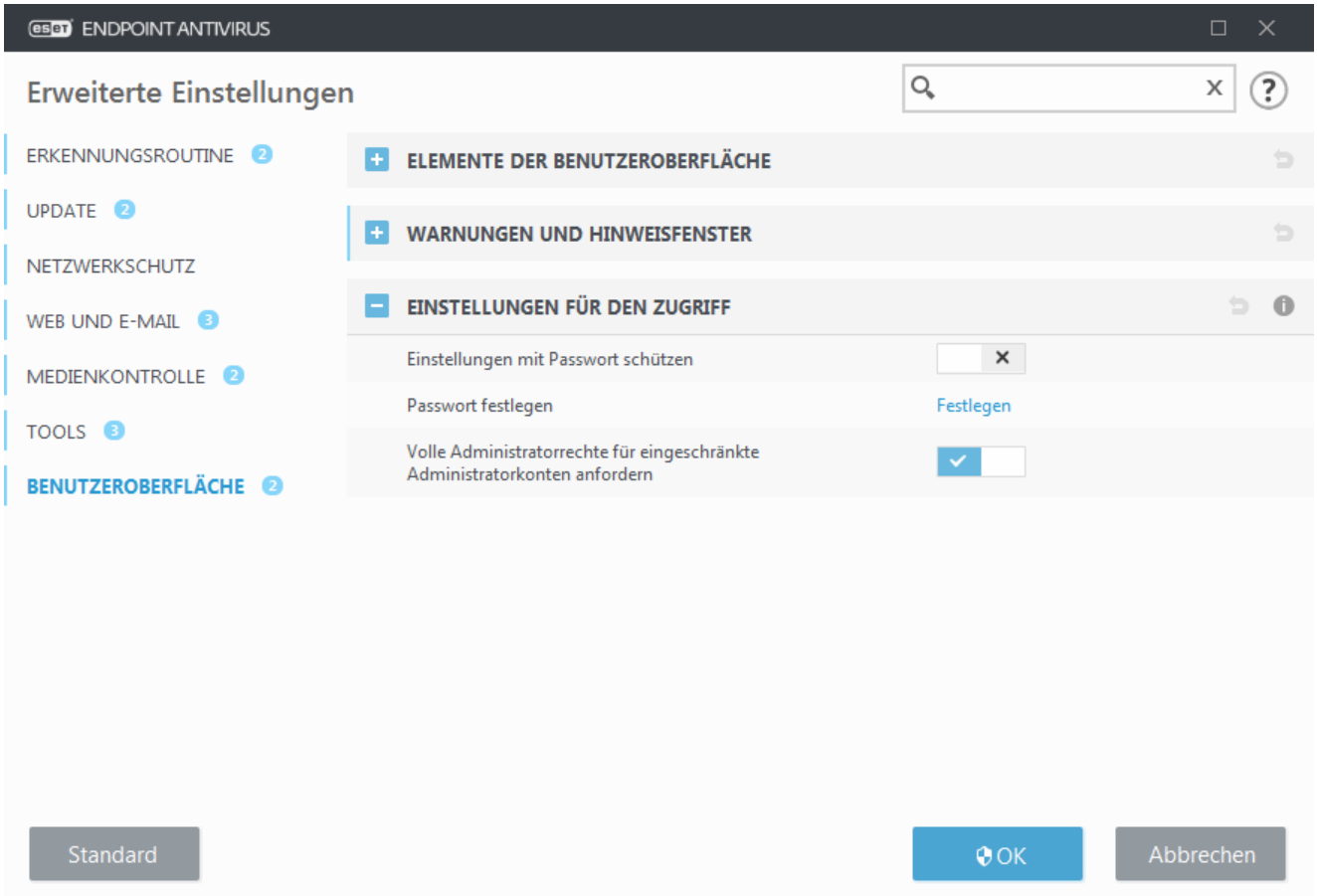
Maßgeblich für einen wirksamen Schutz Ihres Systems ist die ordnungsgemäße Konfiguration von ESET Endpoint Antivirus. Bei unbedachten Änderungen können wichtige Daten verlorengehen. Um unberechtigte Änderungen zu verhindern, können Sie die Einstellungen von ESET Endpoint Antivirus mit einem Passwort schützen.

Verwaltete Umgebungen

Administratoren können eine Policy erstellen, um die Einstellungen für ESET Endpoint Antivirus auf verbundenen Clientcomputern mit einem Passwort zu schützen. Informationen zum Erstellen einer neuen Policy finden Sie unter Passwortgeschützte Einstellungen.

Nicht verwaltet

Die Konfigurationseinstellungen für den Passwortschutz befinden sich in den **erweiterten Einstellungen** (F5) unter **Benutzeroberfläche** > **Einstellungen für den Zugriff**.



Einstellungen mit Passwort schützen - Legt fest, ob ein Passwortschutz angewendet wird. Durch Klicken hierauf wird das Passwortfenster geöffnet.

Klicken Sie auf **Festlegen**, um ein Passwort für den Schutz der Einstellungen festzulegen oder um es zu ändern.

Volle Administratorrechte für eingeschränkte Administratorkonten anfordern - Lassen Sie diese Option aktiviert, damit Benutzer ohne Administratorrechte zur Eingabe eines Administratorbenutzernamens und -passworts aufgefordert werden, wenn sie bestimmte Systemeinstellungen ändern möchten (ähnlich der Benutzerkontensteuerung/UAC in Windows Vista). Dazu gehört das Deaktivieren von Schutzmodulen.

Nur für Windows XP:

Administratorrechte anfordern (Systeme ohne UAC-Support) - Aktivieren Sie diese Option, damit ESET Endpoint Antivirus zur Eingabe des Administratornachweises auffordert.

Passwort für erweiterte Einstellungen

Zum Schutz der Einstellungsparameter von ESET Endpoint Antivirus vor unbefugten Änderungen müssen Sie ein neues Passwort festlegen.

Verwaltete Umgebungen

Administratoren können eine Policy erstellen, um die Einstellungen für ESET Endpoint Antivirus auf verbundenen Clientcomputern mit einem Passwort zu schützen. Informationen zum Erstellen einer neuen Policy finden Sie unter Passwortgeschützte Einstellungen.

Nicht verwaltet

So ändern Sie ein vorhandenes Passwort:

1. Geben Sie Ihr altes Passwort in das Feld **Altes Passwort** ein.
2. Geben Sie Ihr neues Passwort in die Felder **Neues Passwort** und **Passwort bestätigen** ein.
3. Klicken Sie auf **OK**.

Dieses Passwort ist für alle zukünftigen Änderungen an ESET Endpoint Antivirus erforderlich.

Falls Sie Ihr Passwort vergessen haben, können Sie den Zugang zu den erweiterten Einstellungen wiederherstellen.

- Wiederherstellen mit der Methode „Passwort wiederherstellen“ (Version 7.1 und höher)
- Wiederherstellen mit dem ESET-Tool zum Entsperren (Version 7.0 und niedriger)

Klicken Sie hier, falls Sie Ihren von ESET ausgestellten Lizenzschlüssel, das Ablaufdatum Ihrer Lizenz oder andere Lizenzinformationen für ESET Endpoint Antivirus vergessen haben.

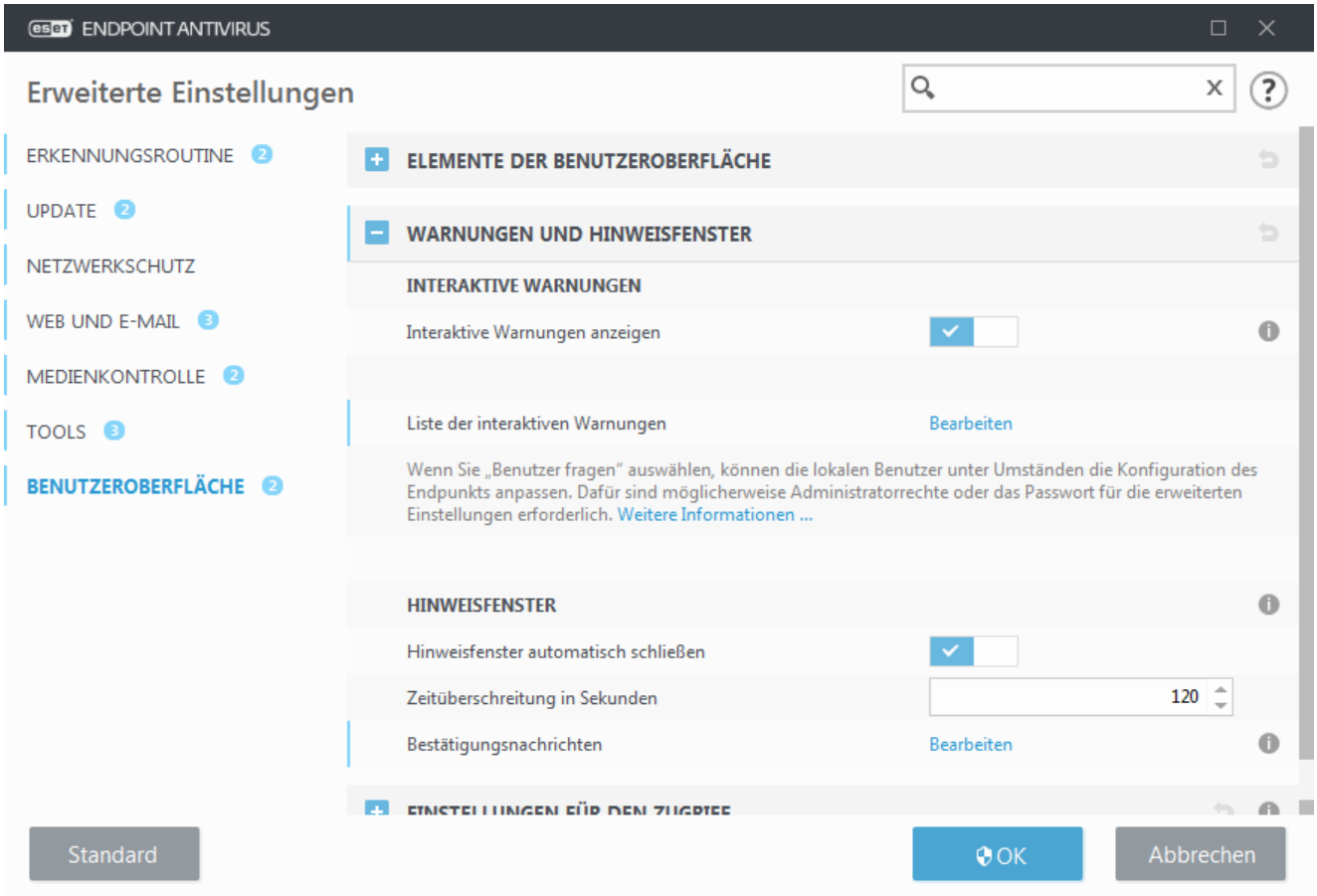
Warnungen und Hinweisfenster



Suchen Sie nach Informationen zu allgemeinen Warnungen und Hinweisen?

- Bedrohung gefunden
- Adresse wurde blockiert
- Produkt nicht aktiviert
- Kostenloses Upgrade verfügbar
- Update-Daten sind nicht konsistent
- So beheben Sie das Problem „Modulupdate fehlgeschlagen“
- „Datei beschädigt“ oder „Datei konnte nicht umbenannt werden“
- Website-Zertifikat widerrufen
- Bedrohnung für das Netzwerk blockiert

Im Abschnitt **Warnungen und Hinweisfenster** (ehemals **Warnungen und Benachrichtigungen**) unter **Benutzeroberfläche** können Sie festlegen, wie ESET Endpoint Antivirus Ereignisse verarbeitet, wenn eine Entscheidung von einem Benutzer erforderlich ist (z. B. potenzielle Phishing-Websites).



Interaktive Warnungen

Interaktive Warnfenster werden angezeigt, wenn ein Ereignis gefunden wurde oder wenn ein Eingreifen des Benutzers erforderlich ist.

Interaktive Warnungen anzeigen

ESET Endpoint Antivirus Version 7.2 und höher:

- Für nicht verwaltete Benutzer empfehlen wir, die Standardeinstellung für diese Option (aktiviert) zu übernehmen.
- Verwaltete Benutzer können diese Einstellung aktiviert lassen und eine vordefinierte Aktion für die Benutzer in der Liste der interaktiven Warnungen auswählen.

Wenn Sie **Interaktive Warnungen anzeigen** deaktivieren, werden alle Warnmeldungen und browserinternen Dialoge ausgeblendet, und eine vordefinierte Standardaktion wird automatisch ausgewählt (potenzielle Phishing-Websites werden beispielsweise blockiert).

ESET Endpoint Antivirus Version 7.1 und niedriger:

Diese Einstellung heißt **Warnungen anzeigen**, und es ist nicht möglich, vordefinierte Aktionen für bestimmte interaktive Warnmeldungen anzupassen.

Desktophinweise

Hinweise auf dem Desktop und Sprechblasen dienen ausschließlich zu Informationszwecken; Eingaben des Benutzers sind nicht erforderlich. Der Abschnitt **Desktophinweise** befindet sich jetzt unter **Tools** >

Benachrichtigungen in den erweiterten Einstellungen (Version 7.1 und höher).

Hinweisfenster

Wenn Popup-Fenster nach einer bestimmten Zeit automatisch geschlossen werden sollen, aktivieren Sie die Option **Fenster mit Hinweisen schließen**. Die Hinweise werden nach Ablauf der festgelegten Zeit automatisch geschlossen, sofern sie nicht bereits vom Benutzer geschlossen wurden.

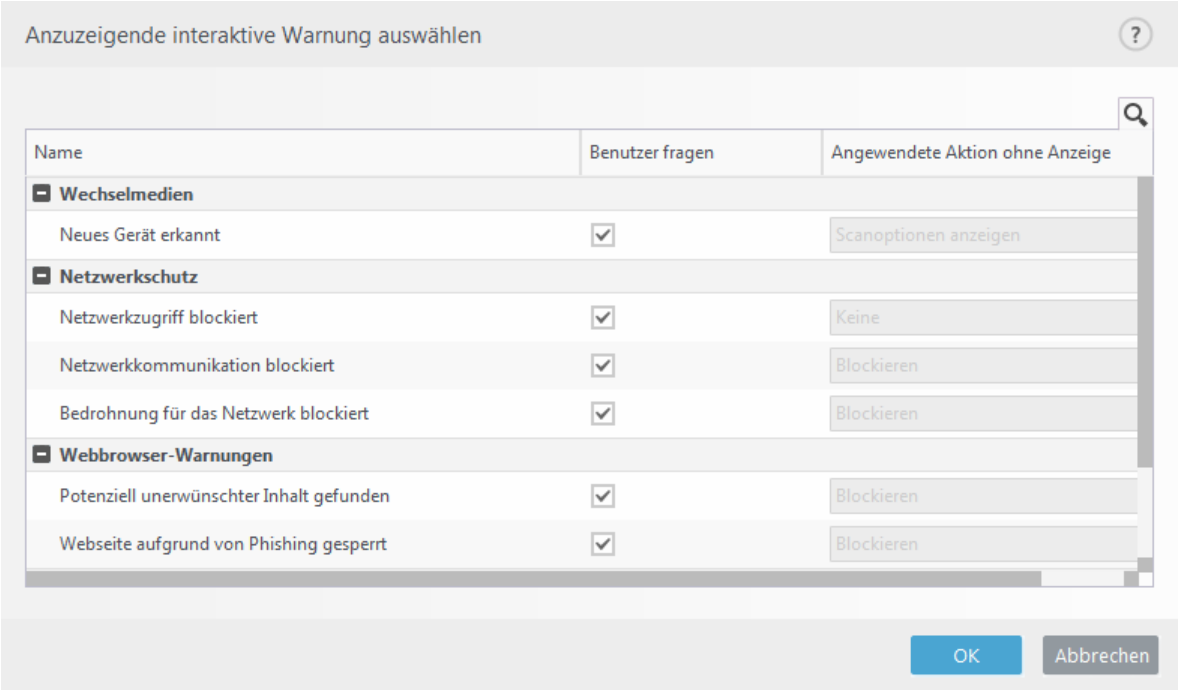
Bestätigungsmeldungen– Zeigt eine Liste von Bestätigungsmeldungen an, die Sie zur Anzeige oder zur Nicht-Anzeige auswählen können.

Interaktive Warnungen

Dieser Abschnitt beschreibt verschiedene interaktive Warnmeldungen, die in ESET Endpoint Antivirus angezeigt werden, bevor eine Aktion ausgeführt wird.

Um das Verhalten für konfigurierbare interaktive Warnungen anzupassen, navigieren Sie zu **Benutzeroberfläche** > **Warnungen und Hinweisfenster** > **Liste der interaktiven Warnungen** in den erweiterten Einstellungen von ESET Endpoint Antivirus, und klicken Sie auf **Bearbeiten**.

Zweck
Nützlich für verwaltete Umgebungen, in denen ein Administrator die Aktion **Benutzer fragen** generell auswählen und eine vordefinierte Aktion festlegen kann, wenn interaktive Warnmeldungen angezeigt werden.
Siehe auch produktinterner Anwendungsstatus.



Die folgenden Hilfeseiten enthalten Hinweise zu bestimmten interaktiven Warnmeldungen:

Wechselmedien

- Neues Gerät erkannt

Netzwerk-Schutz

- Netzwerkzugriff blockiert wird angezeigt, wenn der Clienttask **Computer vom Netzwerk isolieren** auf dieser Arbeitsstation in ESMC ausgelöst wird.
- Netzwerkkommunikation blockiert
- Bedrohnung für das Netzwerk blockiert

Webbrowser-Warnungen

- Potenziell unerwünschter Inhalt gefunden
- Webseite aufgrund von Phishing gesperrt

Computer

Wenn eine dieser Warnungen vorhanden ist, wird die Benutzeroberfläche in Orange angezeigt:

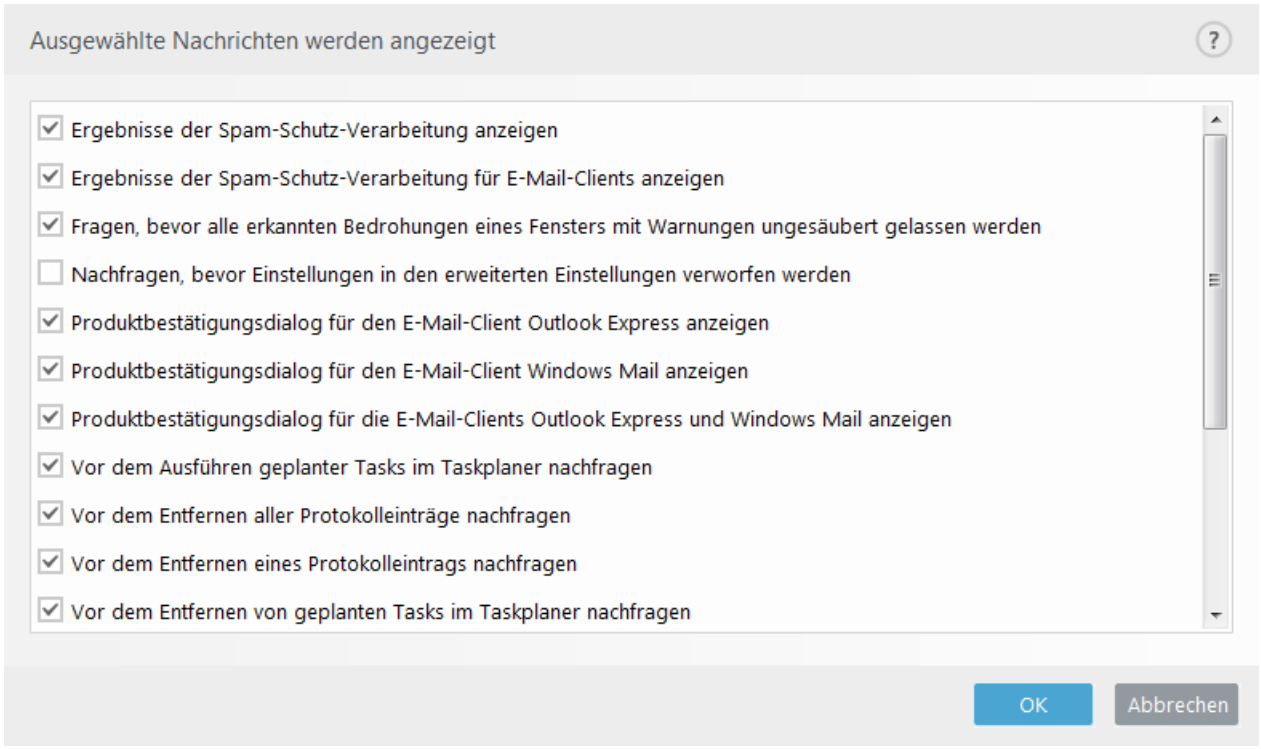
- Computer neu starten (erforderlich)
- Computer neu starten (empfohlen)



Einschränkungen
Das Verhalten der interaktiven Warnungen für Erkennungsroutine, HIPS oder Firewall kann in dieser speziellen Funktion separat konfiguriert werden, daher zählen diese Warnungen nicht zu den interaktiven Warnungen.

Bestätigungsnachrichten

Um die Bestätigungsnachrichten anzupassen, navigieren Sie zu **Benutzeroberfläche** > **Warnungen und Hinweisfenster** > **Bestätigungsnachrichten** in den erweiterten Einstellungen von ESET Endpoint Antivirus, und klicken Sie auf **Bearbeiten**.



In diesem Dialogfeld werden Bestätigungsmeldungen angezeigt, die von ESET Endpoint Antivirus vor der Durchführung von Aktionen angezeigt werden. Aktivieren oder deaktivieren Sie die gewünschten Bestätigungsmeldungen, indem Sie das jeweilige Kontrollkästchen markieren oder die Markierung daraus entfernen.

Erweiterte Einstellungen-Konfliktfehler

Dieser Fehler kann auftreten, wenn eine Komponente (z.B. HIPS) und der Benutzer gleichzeitig die Regeln im interaktiven oder Trainingsmodus erstellen.

Wichtig
Wir empfehlen, für den Filtermodus die Standardeinstellung **Automatischer Modus** zu wählen, wenn Sie Ihre eigenen Regeln erstellen möchten. Erfahren Sie mehr über HIPS und die HIPS-Filtermodi.

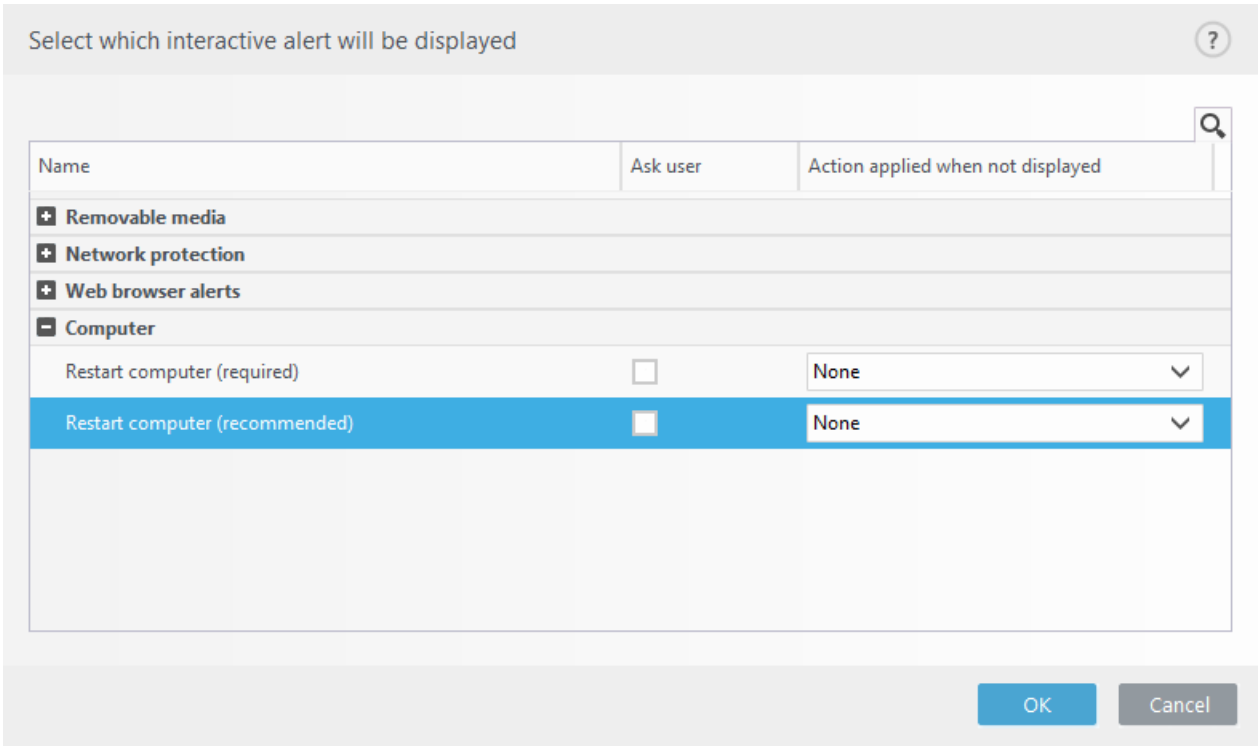
Neustart erforderlich

Wenn Endpunktgeräte die gelbe Warnung „Neustart erforderlich“ empfangen, können Sie die Anzeige der Warnungen deaktivieren.

Gehen Sie wie folgt vor, um die Warnung „Neustart erforderlich“ oder „Neustart empfohlen zu deaktivieren:

1. Drücken Sie die Taste **F5**, um die erweiterten Einstellungen zu öffnen, und erweitern Sie den Abschnitt **Warnungen und Hinweisfenster**.

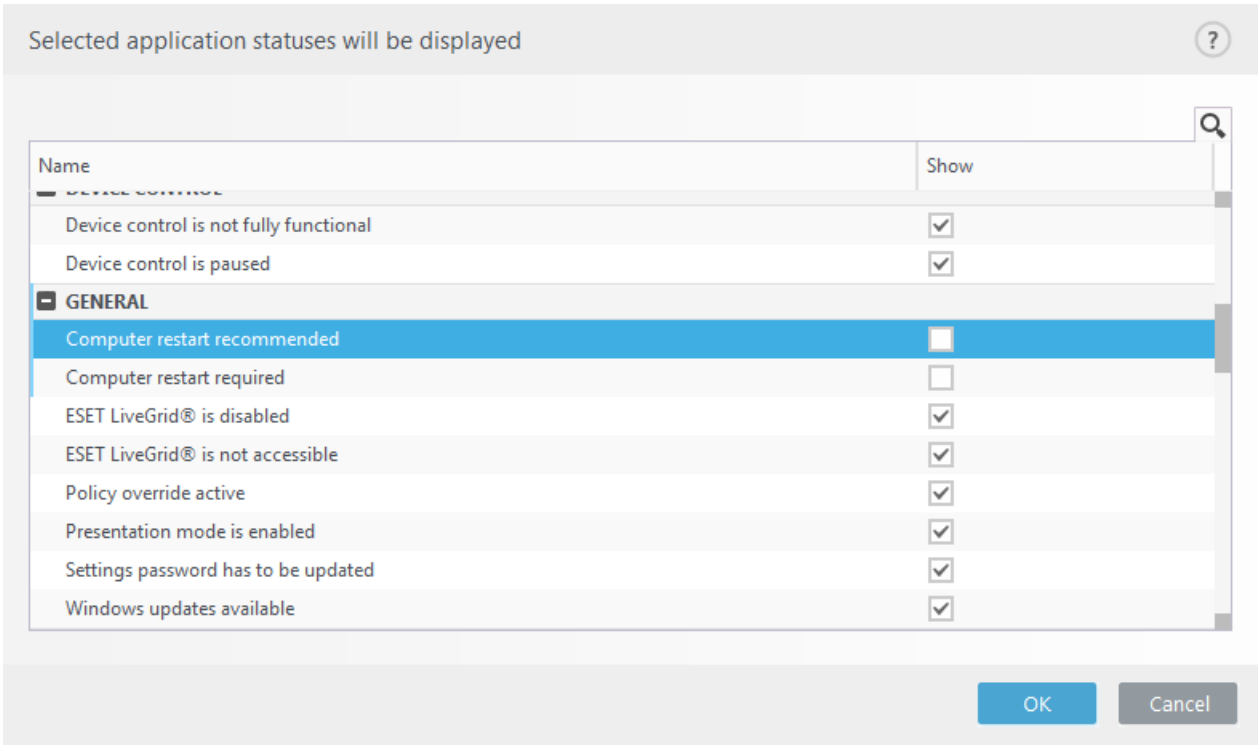
2. Klicken Sie auf **Bearbeiten** neben der **Liste der interaktiven Warnungen**. Deaktivieren Sie im Abschnitt **Computer** die Kontrollkästchen neben **Computer neu starten (erforderlich)** und **Computer neu starten (empfohlen)**.



3.Klicken Sie auf **OK**, um Ihre Änderungen in beiden geöffneten Fenstern zu speichern.

4.Anschließend werden die Warnungen nicht mehr auf dem Endpunktcomputer angezeigt.

5.(optional) Um den Anwendungsstatus im Hauptprogrammfenster von ESET Endpoint Antivirus zu deaktivieren, deaktivieren Sie im Fenster Anwendungsstatus die Kontrollkästchen neben **Computerneustart erforderlich** und **Computerneustart empfohlen**.



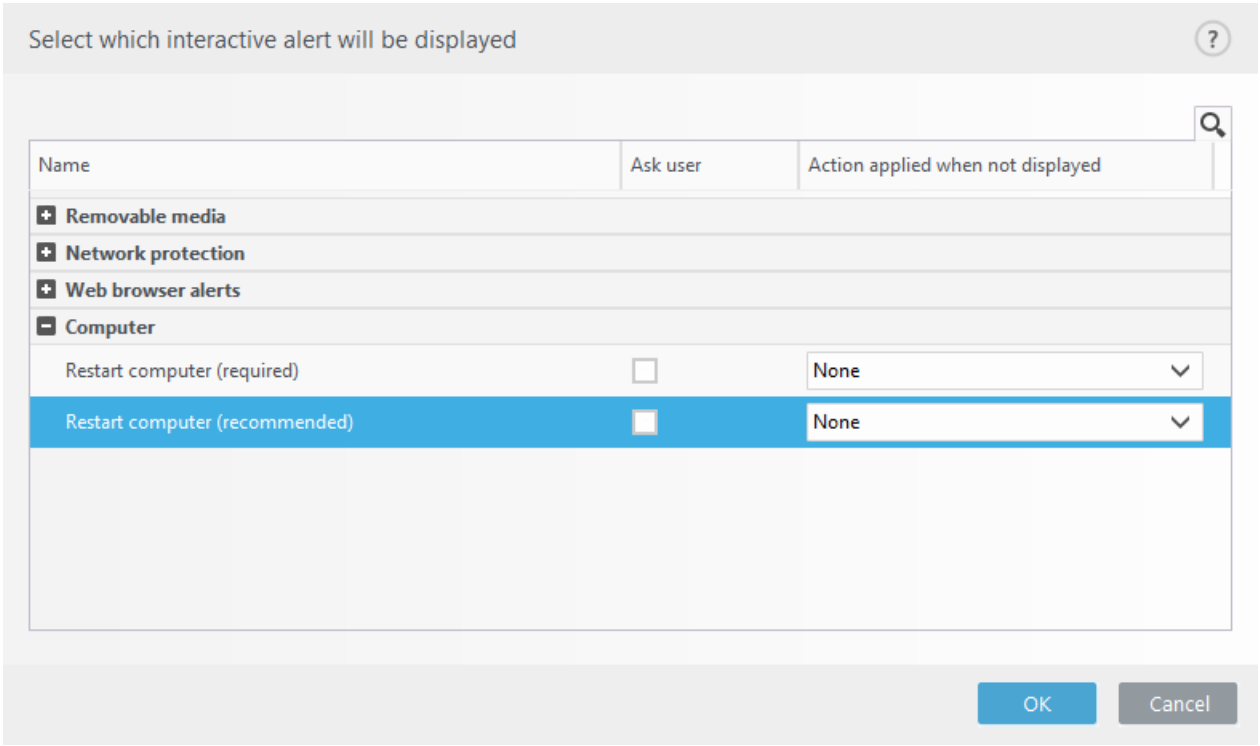
Neustart empfohlen

Wenn Endpunktgeräte die gelbe Warnung „Neustart empfohlen“ empfangen, können Sie die Anzeige der Warnungen deaktivieren.

Gehen Sie wie folgt vor, um die Warnung „Neustart erforderlich“ oder „Neustart empfohlen zu deaktivieren:

1.Drücken Sie die Taste **F5**, um die erweiterten Einstellungen zu öffnen, und erweitern Sie den Abschnitt **Warnungen und Hinweisfenster**.

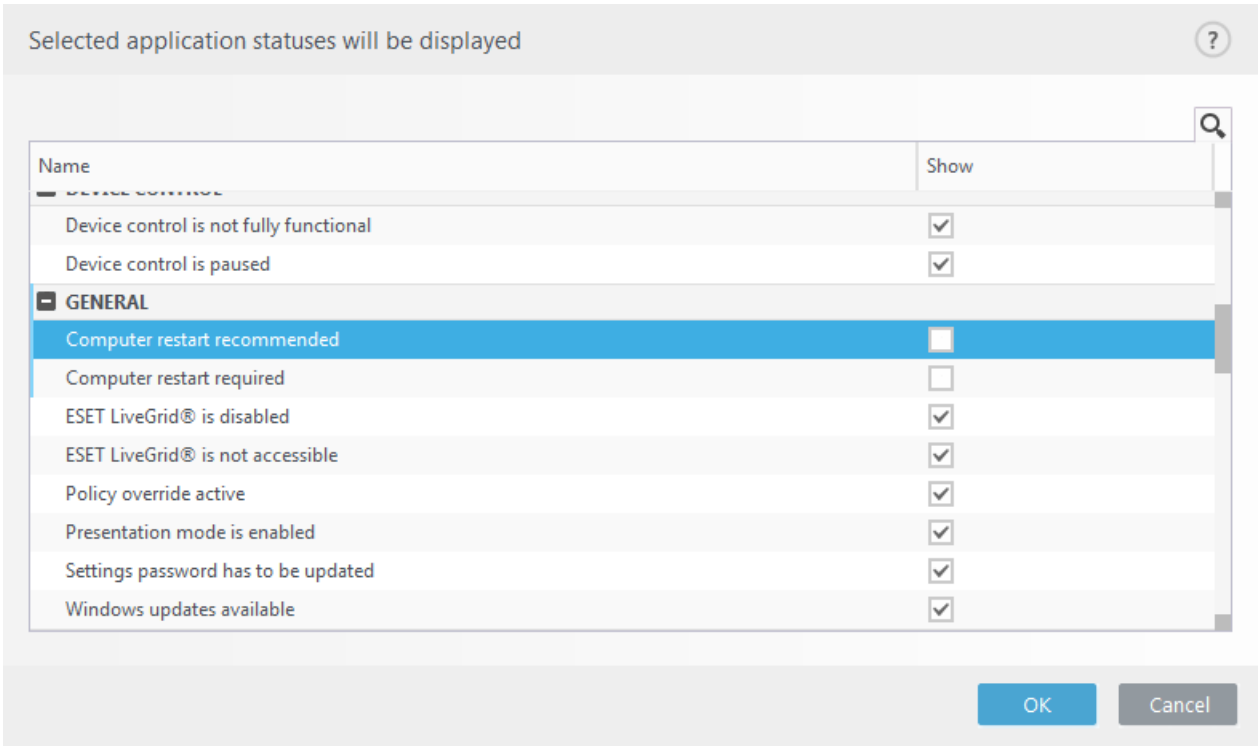
2.Klicken Sie auf **Bearbeiten** neben der **Liste der interaktiven Warnungen**. Deaktivieren Sie im Abschnitt **Computer** die Kontrollkästchen neben **Computer neu starten (erforderlich)** und **Computer neu starten (empfohlen)**.



3.Klicken Sie auf **OK**, um Ihre Änderungen in beiden geöffneten Fenstern zu speichern.

4.Anschließend werden die Warnungen nicht mehr auf dem Endpunktcomputer angezeigt.

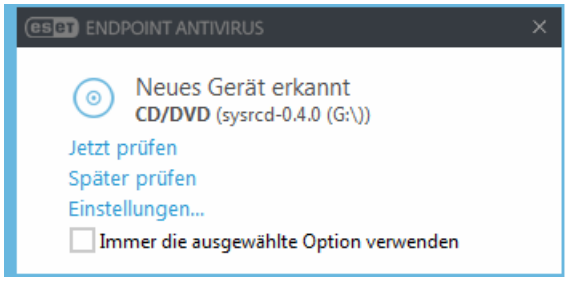
5.(optional) Um den Anwendungsstatus im Hauptprogrammfenster von ESET Endpoint Antivirus zu deaktivieren, deaktivieren Sie im Fenster Anwendungsstatus die Kontrollkästchen neben **Computerneustart erforderlich** und **Computerneustart empfohlen**.



Wechselmedien

ESET Endpoint Antivirus bietet automatische Scan-Methoden für Wechselmedien (CD/DVD/USB/...) beim Einlegen in den Computer. Dies ist sinnvoll, wenn Administratoren verhindern möchten, dass die Benutzer Wechselmedien mit unerwünschten Inhalten verwenden.

Wenn die Option **Scanoptionen anzeigen** in ESET Endpoint Antivirus aktiviert ist und ein Wechselmedium eingelegt wird, wird der folgende Dialog angezeigt:



Optionen für dieses Dialogfeld:

- **Jetzt scannen** - Dies löst den Wechselmedienscan aus.
- **Später scannen** - Der Wechselmedienscan wird auf einen späteren Zeitpunkt verschoben.
- **Einstellungen** - Öffnet die **erweiterten Einstellungen**.
- **Immer die ausgewählte Option verwenden** - Wenn diese Option aktiviert ist, wird bei jedem Einlegen eines Wechselmediums die gleiche Aktion ausgeführt.

Zusätzlich bietet ESET Endpoint Antivirus die Funktion der Medienkontrolle, mit der Sie Regeln für die Nutzung externer Geräte mit einem bestimmten Computer festlegen können. Weitere Informationen zur Medienkontrolle finden Sie im Abschnitt Medienkontrolle.

ESET Endpoint Antivirus 7.2 und höher

Sie finden die Einstellungen für den Wechselmedien-Scan in den Erweiterten Einstellungen (**F5**) unter **Benutzeroberfläche** > **Warnungen und Hinweisfenster** > **Interaktive Warnungen** > **Liste der interaktiven Warnungen** > **Bearbeiten** > **Neues Gerät erkannt**.

Falls **Benutzer fragen** nicht ausgewählt ist, wählen Sie die gewünschte Aktion beim Einlegen von Wechselmedien in einen Computer aus:

- **Nicht scannen** - Es wird keine Aktion ausgeführt, und das Fenster **Neues Gerät erkannt** wird nicht geöffnet.
- **Automatischer Gerätescan** - Ein On-Demand-Scan des eingelegten Wechselmediums wird durchgeführt.
- **Scanoptionen anzeigen** - Öffnet die Einstellungen für **Interaktive Warnungen**.

ESET Endpoint Antivirus 7.1 und niedriger

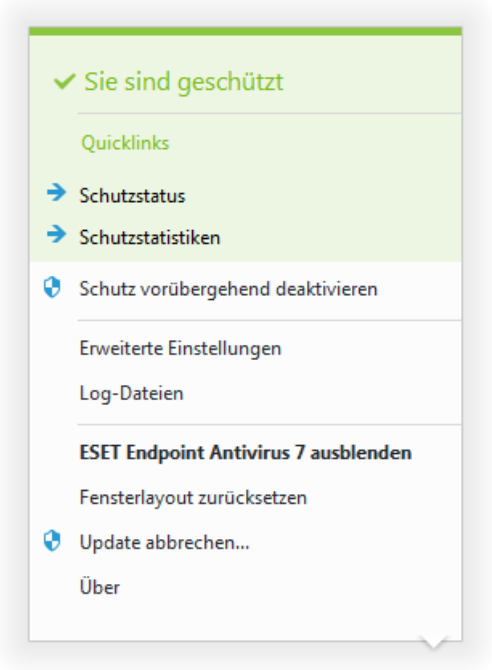
Sie finden die Einstellungen für den Wechselmedien-Scan unter Erweiterte Einstellungen (**F5**) > **Erkennungsroutine** > **Malware-Scans** > **Wechselmedien**.

Aktion nach Einlegen von Wechselmedien - Wählen Sie die Aktion, die standardmäßig ausgeführt werden soll, wenn ein Wechselmedium in den Computer eingelegt wird (CD/DVD/USB). Wählen Sie die gewünschte Aktion nach Einlegen von Wechselmedien aus:

- **Nicht scannen** - Es wird keine Aktion ausgeführt, und das Fenster **Neues Gerät erkannt** wird nicht geöffnet.
- **Automatischer Gerätescan** - Ein On-Demand-Scan des eingelegten Wechselmediums wird durchgeführt.
- **Scanoptionen anzeigen** - Öffnet die Einstellungen für **Wechselmedien**.

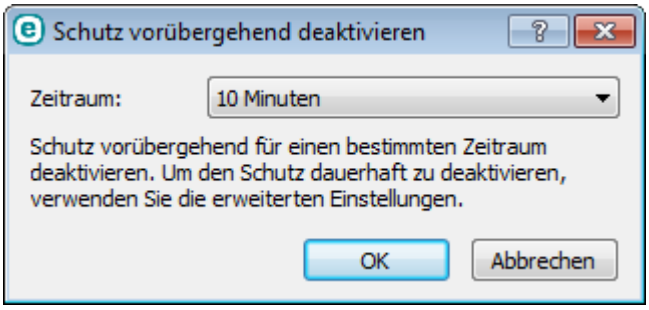
Symbol im Infobereich der Taskleiste

Einige der wichtigsten Einstellungsoptionen und -funktionen können durch Klicken mit der rechten Maustaste auf das Symbol im Infobereich der Taskleiste geöffnet werden.



Schutz vorübergehend deaktivieren - Zeigt ein Dialogfenster an, in dem Sie bestätigen müssen, dass die Erkennungsroutine deaktiviert werden soll, die Dateivorgänge sowie die Internet- und E-Mail-Kommunikation überwacht und Sie vor Angriffen schützt.

Im Dropdown-Menü **Zeitraum** können Sie festlegen, für wie lange der Schutz deaktiviert sein soll.



Erweiterte Einstellungen - Öffnet die Baumstruktur **Erweiterte Einstellungen**. Zugriff auf die erweiterten Einstellungen erhalten Sie auch durch Drücken der Taste F5 oder über **Einstellungen** > **Erweiterte Einstellungen**.

Log-Dateien - Log-Dateien enthalten Informationen zu allen wichtigen aufgetretenen Programmereignissen und geben einen Überblick über erkannte Ereignisse.

ESET Endpoint Antivirus öffnen – Öffnet das Hauptprogrammfenster von ESET Endpoint Antivirus über das Symbol im Infobereich der Taskleiste.

Fensterlayout zurücksetzen - Stellt die standardmäßige Fenstergröße und die Standardposition von ESET Endpoint Antivirus auf dem Bildschirm wieder her.

Nach Updates suchen ... – Beginnt mit der Aktualisierung der Programmmodule, um den Schutz vor Schadcode zu gewährleisten.

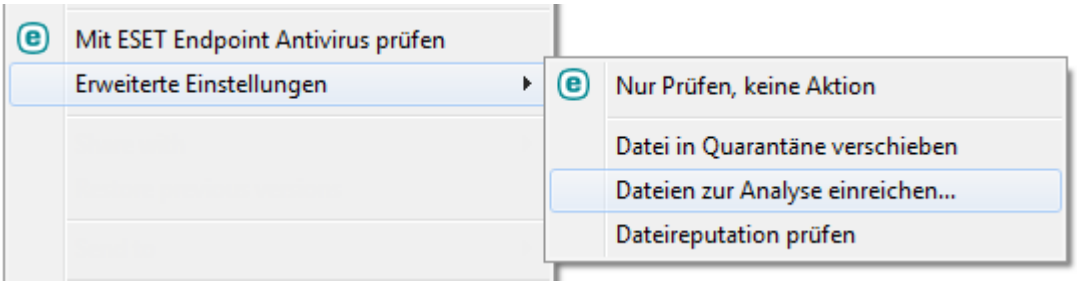
Über - Bietet Systeminformationen zur installierten Version von ESET Endpoint Antivirus und zu den installierten Programmmodulen und zeigt das Ablaufdatum der Lizenz an. Informationen zum Betriebssystem und zu den Systemressourcen befinden sich unten auf der Seite.

Kontextmenü

Das Kontextmenü wird angezeigt, wenn Sie mit der rechten Maustaste auf ein Element (eine Datei) klicken. Das Menü enthält alle Optionen, die auf das Objekt angewendet werden können.

Bestimmte Steuerungselemente von ESET Endpoint Antivirus können in das Kontextmenü integriert werden. Die Einstellungsoptionen für diese Funktion sind unter „Erweiterte Einstellungen“ in **Benutzeroberfläche** > **Elemente der Benutzeroberfläche** verfügbar.

In Kontextmenü integrieren - ESET Endpoint Antivirus kann in das Kontextmenü integriert werden.



Hilfe und Support

ESET Endpoint Antivirus enthält Tools für die Fehlerbehebung und Support-Informationen, die Ihnen bei der Lösung von möglichen Problemen behilflich sind.

Hilfe

ESET-Knowledgebase durchsuchen – Die ESET-Knowledgebase enthält Antworten auf die am häufigsten gestellten Fragen sowie Lösungsvorschläge für zahlreiche Problemstellungen. Die Knowledgebase wird regelmäßig von den ESET-Supportmitarbeitern aktualisiert und ist daher hervorragend für die Lösung verschiedenster Probleme geeignet.

Hilfe öffnen - Mit diesem Link öffnen Sie die ESET Endpoint Antivirus-Hilfeseiten.

Schnelle Lösung finden – Klicken Sie auf diesen Link, um Lösungen für die häufigsten Probleme zu finden. Lesen Sie diesen Abschnitt, bevor Sie sich an den technischen Support wenden.

Technischer Support

Supportanfrage senden – Wenn Sie Ihr Problem nicht lösen konnten, können Sie sich über das Formular auf der ESET-Website schnell mit dem technischen Support in Verbindung setzen.

Details für den technischen Support – Wenn Sie dazu aufgefordert werden, können Sie Informationen für den ESET-Support kopieren und senden (z. B. Produktname, Version, Betriebssystem und Prozessortyp).

Support-Tools

Virenenzyklopädie – Öffnet die ESET-Virenenzyklopädie mit Informationen zu den Gefahren und Symptomen verschiedener Infiltrationsarten.

Verlauf der Erkennungsroutine – Öffnet den ESET-Virusradar, der Informationen zu den Versionen der ESET-Erkennungsroutine enthält (bisher auch als „Signaturdatenbank“ bezeichnet).

ESET Log Collector – Öffnet den Artikel in der ESET-Knowledgebase, in dem Sie das ESET Log Collector-Dienstprogramm herunterladen können. Diese Anwendung sammelt automatisch Informationen und Log-Dateien von einem Computer und ermöglicht somit eine schnellere Problemlösung. Weitere Informationen finden Sie online im ESET Log Collector-Benutzerhandbuch.

Spezielles ESET-Säuberungsprogramm – Entfernungstools für bekannte Schadsoftware-Infektionen. Weitere Informationen finden Sie in diesem Artikel in der ESET-Knowledgebase.

Produkt- und Lizenzinformationen

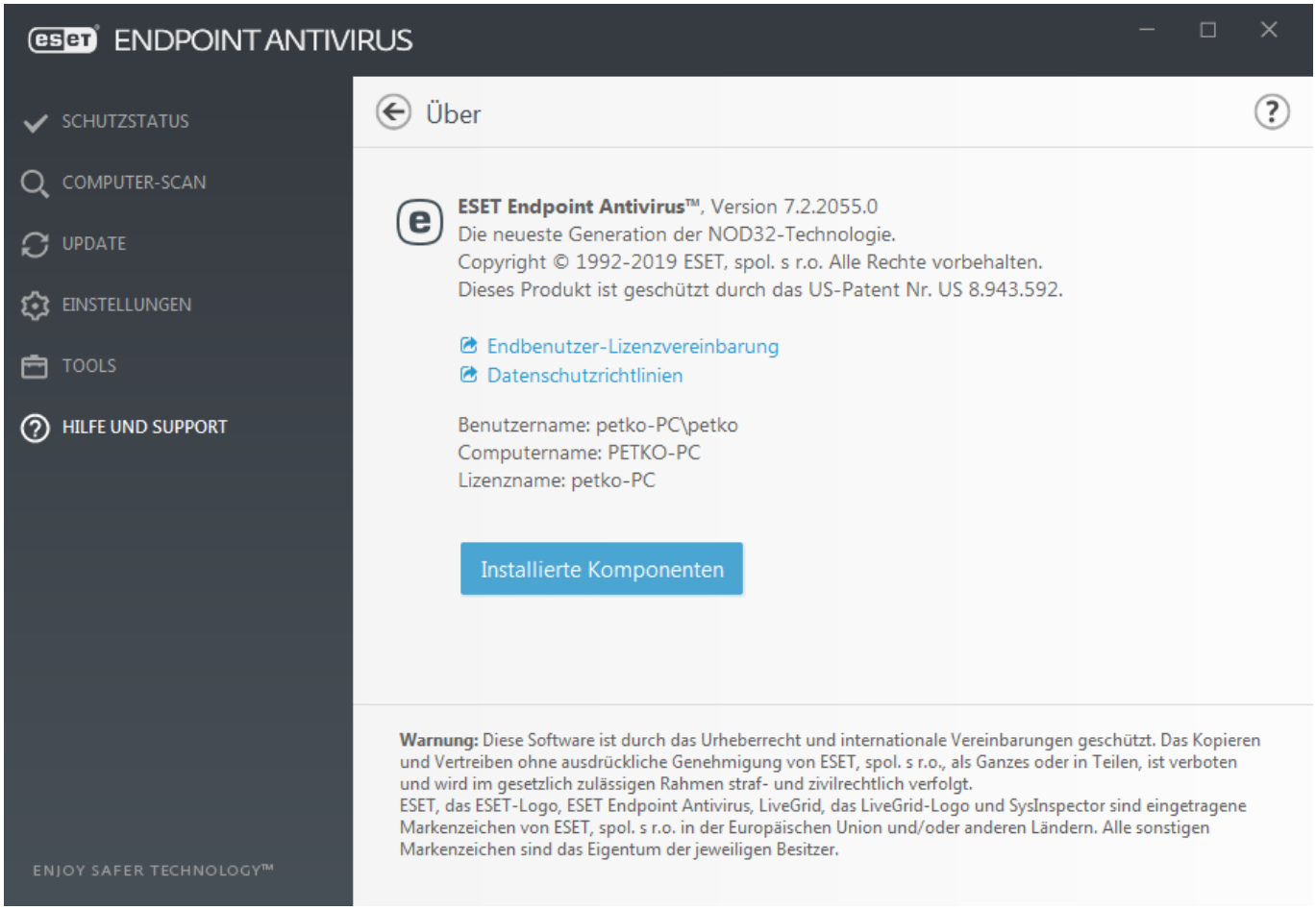
Über ESET Endpoint Antivirus – Informationen zu Ihrer Kopie von ESET Endpoint Antivirus.

Produkt aktivieren/Lizenz ändern – Klicken Sie hier, um das Aktivierungsfenster zu öffnen und Ihr Produkt zu aktivieren.

Info zu ESET Endpoint Antivirus

Dieses Fenster enthält Details über die installierte Version von ESET Endpoint Antivirus, Ihr Betriebssystem und die Systemressourcen.

Klicken Sie auf **Installierte Komponenten**, um Informationen zur Liste der installierten Programmmodule anzuzeigen. Klicken Sie auf **Kopieren**, um Informationen zu den Modulen in die Zwischenablage zu kopieren. Dies kann bei der Fehlerbehebung oder für Supportanfragen hilfreich sein.



Systemkonfigurationsdaten senden

Um möglichst schnell und effizient helfen zu können, benötigt der ESET-Support Informationen zur Konfiguration von ESET Endpoint Antivirus, detaillierte Systeminformationen, Informationen zu ausgeführten Prozessen (ESET SysInspector-Log-Datei) und Registrierungsdaten. ESET nutzt diese Daten ausschließlich zum Bereitstellen technischer Unterstützung für den Kunden.

Wenn Sie das Webformular absenden, werden Ihre Systemkonfigurationsdaten an ESET übermittelt. Wählen Sie **Diese Informationen immer senden** aus, wenn Sie diese Aktion für den Prozess speichern möchten. Um das Formular zu übermitteln, ohne Ihre Daten zu senden, klicken Sie auf **Keine Daten senden**. In diesem Fall können Sie den ESET-Support über das Online-Supportformular erreichen.

Sie finden diese Einstellung auch unter **Erweiterte Einstellungen** > **Tools** > **Diagnose** > **Technischer Support**.

> **Hinweis**
> Wenn Sie Systemdaten einreichen möchten, müssen Sie das Webformular ausfüllen und einreichen. Andernfalls wird kein Ticket erstellt und die Systemdaten werden nicht übermittelt.

Profilmanager

Der Profilmanager wird an zwei Stellen in ESET Endpoint Antivirus verwendet: in den Bereichen **On-Demand-Scan** und **Update**.

On-Demand-Prüfung

Ihre bevorzugten Einstellungen können für zukünftige Prüfungen gespeichert werden. Wir empfehlen Ihnen, für jede regelmäßig durchgeführte Prüfung ein eigenes Profil zu erstellen (mit verschiedenen zu prüfenden Objekten, Prüfmethoden und anderen Parametern).

Um ein neues Profil zu erstellen, öffnen Sie das Fenster mit den erweiterten Einstellungen (F5) und klicken auf **Antivirus** > **On-Demand-Prüfung** und anschließend auf **Bearbeiten** neben der **Profilliste**. Daraufhin wird das Dropdownmenü **Updateprofil** geöffnet, das die vorhandenen Prüfprofile enthält. Eine Beschreibung der einzelnen Prüfeinstellungen finden Sie im Abschnitt Einstellungen für ThreatSense. So können Sie ein Prüfprofil erstellen, das auf Ihre Anforderungen zugeschnitten ist.



Hinweis

Nehmen wir an, Sie möchten Ihr eigenes Prüfprofil erstellen. Die Option **Computerprüfung** eignet sich in gewissem Maße, aber Sie möchten keine laufzeitkkomprimierten Dateien oder potenziell unsichere Anwendungen prüfen. Außerdem möchten Sie die Option **Immer versuchen, automatisch zu entfernen** anwenden. Geben Sie den Namen des neuen Profils im **Profilmanager** ein und klicken Sie auf **Hinzufügen**. Wählen Sie das neue Profil im Dropdownmenü **Ausgewähltes Profil** aus, passen Sie die restlichen Parameter nach Ihren Anforderungen an und klicken Sie auf **OK**, um das neue Profil zu speichern.

Update

Mit dem Profil-Editor unter „Einstellungen für Updates“ können Benutzer neue Update-Profile erstellen. Das Erstellen und Verwenden eigener benutzerdefinierter Profile (d. h. anderer Profile als das standardmäßige **Mein Profil**) ist nur sinnvoll, wenn Ihr Computer auf mehrere Verbindungsarten zurückgreifen muss, um eine Verbindung zu den Update-Servern herzustellen.

Nehmen wir als Beispiel einen Laptop, dessen Updates normalerweise über einen lokalen Server (einen sogenannten Mirror) im lokalen Netzwerk erfolgen, der aber seine Updates direkt von den ESET-Update-Servern bezieht, wenn keine Verbindung zum lokalen Netzwerk hergestellt werden kann (z. B. auf einer Geschäftsreise). Dieser Laptop kann zwei Profile haben: das erste Profil für die Verbindung zum lokalen Server, das zweite Profil für die Verbindung zu den ESET-Servern. Sobald diese Profile eingerichtet sind, wählen Sie **Tools** > **Taskplaner** und bearbeiten Sie die Update-Task-Einstellungen. Legen Sie eines der Profile als primäres Profil fest, das andere als sekundäres Profil.

Updateprofil - Das momentan verwendete Update-Profil. Um es zu ändern, wählen Sie ein Profil aus dem Dropdown-Menü aus.

Profilliste - Hier können Sie neue Update-Profile erstellen oder vorhanden Update-Profile entfernen.

Tastaturbefehle

Zur besseren Navigation in ESET Endpoint Antivirus stehen die folgenden Tastaturbefehle zur Verfügung:

Tastaturbefehle	Ausgeführte Aktion
F1	öffnet die Hilfeseiten
F5	öffnet die erweiterten Einstellungen

Up/Down	Navigation in der Software durch Elemente
TAB	bewegt den Cursor in einem Fenster
Esc	schließt das aktive Dialogfenster
Ctrl+U	Zeigt Informationen zur ESET-Lizenz und zu Ihrem Computer an (Details für den technischen Support)
Ctrl+R	Setzt Fenstergröße und Fensterposition des Produktfensters auf dem Bildschirm zurück

Diagnose

Mit der Diagnose können Speicherabbilddateien von ESET-Prozessen erstellt werden (z. B. ekrn). Im Falle eines Absturzes einer Anwendung wird eine Speicherabbilddatei erstellt. Diese hilft Entwicklern bei der Erkennung und Korrektur verschiedener ESET Endpoint Antivirus Probleme.

Klicken Sie auf das Dropdown-Menü neben **Typ des Speicherabbilds** und wählen Sie dieser drei Optionen aus:

- Mit**Deaktivieren** wird diese Funktion deaktiviert.

- **Mini** (standard) – Protokolliert die kleinste Menge an Daten, die helfen könnten, die Ursache für den Absturz der Anwendung herauszufinden. Diese Art Dumpdatei kann nützlich sein, wenn beschränkter Speicherplatz verfügbar ist. Da jedoch die enthaltene Datenmenge ebenfalls begrenzt ist, könnten Fehler, die nicht direkt von dem Thread ausgelöst wurden, der zum Absturzzeitpunkt ausgeführt wurde, bei einer Dateianalyse unentdeckt bleiben.

- **Vollständig** – Zeichnet den gesamten Inhalt des Arbeitsspeichers auf, wenn die Anwendung unerwartet beendet wird. Ein vollständiges Speicherabbild kann auch Daten von Prozessen enthalten, die ausgeführt wurden, als das Speicherabbild geschrieben wurde.

Zielverzeichnis– Verzeichnis, in dem die Speicherabbilddatei während des Absturzes erstellt wird.

Diagnoseverzeichnis öffnen – Klicken Sie auf **Öffnen**, um dieses Verzeichnis in einem neuen Fenster von *Windows Explorer* zu öffnen.

Diagnoseabbild erstellen – Klicken Sie auf **Erstellen**, um ein Diagnoseabbild im **Zielverzeichnis** zu erstellen.

Erweitertes Logging

Erweitertes Logging für die Medienkontrolle aktivieren – Alle Ereignisse aufzeichnen, die in der Medienkontrolle auftreten. Diese Aufzeichnungen helfen Entwicklern bei der Behebung von Problemen mit der Medienkontrolle.

Erweitertes Kernel-Logging aktivieren – Alle Ereignisse im ESET-Kernel aufzeichnen (ekrn), um Diagnose und Fehlerbehebung zu erleichtern (verfügbar in Version 7.2 und höher).

Erweitertes Logging für Lizenzierung aktivieren – Sämtliche Produktkommunikation zwischen ESET-Aktivierung und ESET Business Account Servern aufzeichnen.

Erweitertes Logging für den Netzwerk-Schutz aktivieren – Alle Daten, die die Firewall durchlaufen, im PCAP-Format aufzeichnen. Diese Aufzeichnungen helfen Entwicklern bei der Behebung von Problemen mit der Firewall.

Erweitertes Betriebssystem-Logging aktivieren – Zusätzliche Informationen zum Betriebssystem wie ausgeführte Prozesse, CPU-Aktivität und Laufwerksoperationen werden erfasst. Mit diesen Informationen können die

Entwickler Probleme im Zusammenhang mit dem ESET-Produkt auf Ihrem Betriebssystem verstehen und beheben.

Erweitertes Logging für Protokollfilterung aktivieren – Alle Daten, die die Protokollfilterung durchlaufen, im PCAP-Format aufzeichnen. Diese Aufzeichnungen helfen Entwicklern bei der Behebung von Problemen mit der Protokollfilterung.

Erweitertes Logging für Scanner aktivieren – Probleme aufzeichnen, die beim Scannen von Dateien und Ordnern mit Computer-Scans oder mit dem Echtzeit-Dateischutz auftreten (verfügbar ab Version 7.2).

Erweitertes Logging für Update-Modul aktivieren – Alle Ereignisse aufzeichnen, die während des Updates auftreten. Diese Aufzeichnungen helfen Entwicklern bei der Behebung von Problemen mit dem Update-Modul.

Erweitertes Logging für die Web-Kontrolle aktivieren – Alle Ereignisse aufzeichnen, die in der Kindersicherung auftreten. Diese Aufzeichnungen helfen Entwicklern bei der Behebung von Problemen mit der Kindersicherung.

Speicherort der Log-Dateien

Betriebssystem	Verzeichnis der Log-Dateien
Windows Vista und höher	C:\ProgramData\ESET\ESET Endpoint Antivirus\Diagnostics\
Ältere Versionen von Windows	C:\Documents and Settings\All Users\...

Befehlszeilenscanner

Das Virenschutz-Modul von ESET Endpoint Antivirus kann über die Kommandozeile gestartet werden, entweder manuell (mit dem Befehl „ecls“) oder über eine Batch-Datei („.bat“). Syntax zum Starten der Prüfung aus der Befehlszeile:

```
ecls [OPTIONS..] FILES..
```

Folgende Parameter und Switches stehen zur Verfügung, um die manuelle Prüfung über die Befehlszeile auszuführen:

Methoden

/base-dir=ORDNER	Module laden aus ORDNER
/quar-dir=ORDNER	Quarantäne-ORDNER
/exclude=MASKE	Dateien, die mit der MASKE übereinstimmen, von Prüfungen ausschließen
/subdir	Unterordner scannen (Standard)
/no-subdir	Unterordner nicht scannen
/max-subdir-level=STUFE	Maximale Suchtiefe von Unterordnern bei Scans
/symlink	Symbolischen Links folgen (Standardeinstellung)
/no-symlink	Symbolischen Links nicht folgen
/ads	ADS prüfen (Standard)
/no-ads	ADS nicht scannen
/log-file=DATEI	Ausgabe in DATEI protokollieren
/log-rewrite	Ausgabedatei überschreiben (Standardeinstellung: Anhängen)

/log-console	Ausgabe in Konsole protokollieren (Standard)
/no-log-console	Ausgabe nicht in Konsole protokollieren
/log-all	Saubere Dateien auch in Log aufnehmen
/no-log-all	Saubere Dateien nicht in Log aufnehmen (Standardeinstellung)
/aind	Aktivitätsanzeige anzeigen
/auto	Alle lokalen Laufwerke scannen und automatisch säubern

Einstellungen für Prüfungen

/files	Dateien scannen (Standard)
/no-files	Dateien nicht scannen
/memory	Speicher scannen
/boots	Bootsektoren scannen
/no-boots	Bootsektoren nicht scannen (Standard)
/arch	Archive scannen (empfohlen)
/no-arch	Archive nicht scannen
/max-obj-size=GRÖSSE	Nur Dateien scannen, die kleiner als GRÖSSE Megabyte sind (Standard: 0 = unbegrenzt)
/max-arch-level=TIEFE	Maximale Verschachtelungstiefe von Archiven bei Scans
/scan-timeout=LIMIT	Archive maximal MAXIMALE PRÜFDAUER Sekunden scannen
/max-arch-size=GRÖSSE	Nur Dateien in Archiven scannen, die kleiner als SIZE sind (Standard: 0 = unbegrenzt)
/max-sfx-size=GRÖSSE	Nur Dateien in selbstentpackenden Archiven scannen, die kleiner als GRÖSSE Megabyte sind (Standard: 0 = unbegrenzt)
/mail	E-Mails scannen (Standard)
/no-mail	E-Mails nicht scannen
/mailbox	Postfächer scannen (Standard)
/no-mailbox	Postfächer nicht scannen
/sfx	Selbstentpackende Archive scannen (Standard)
/no-sfx	Selbstentpackende Archive nicht scannen
/rtp	Laufzeitkomprimierte Dateien scannen (Standard)
/no-rtp	Laufzeitkomprimierte Dateien nicht scannen
/unsafe	nach potenziell unsicheren Anwendungen scannen
/no-unsafe	nicht nach potenziell unsicheren Anwendungen scannen (Standard)
/unwanted	nach evtl. unerwünschten Anwendungen scannen
/no-unwanted	nicht nach evtl. unerwünschte Anwendungen scannen (Standard)
/suspicious	nach verdächtigen Anwendungen scannen (Standard)
/no-suspicious	nicht nach verdächtigen Anwendungen scannen
/pattern	Signaturdatenbank verwenden (Standard)
/no-pattern	Signaturdatenbank nicht verwenden
/heur	Heuristik aktivieren (Standard)
/no-heur	Heuristik deaktivieren
/adv-heur	Advanced Heuristik aktivieren (Standard)
/no-adv-heur	Advanced Heuristik deaktivieren
/ext-exclude=ERWEITERUNGEN	DATEIERWEITERUNGEN (Trennzeichen Doppelpunkt) nicht scannen

/clean-mode=MODUS	Säuberungs-MODUS für infizierte Objekte verwenden Folgende Optionen stehen zur Verfügung: • none – Es wird keine automatische Säuberung ausgeführt. • standard (standardmäßige Einstellung) – „ecls.exe“ versucht, infizierte Dateien automatisch zu säubern oder zu löschen. • strict – „ecls.exe“ versucht, infizierte Dateien ohne Benutzereingriff automatisch zu säubern oder zu löschen (Sie werden nicht aufgefordert, das Löschen von Dateien zu bestätigen). • rigorous – „ecls.exe“ löscht Dateien ohne vorherigen Säuberungsversuch unabhängig von der Art der Datei. • delete – „ecls.exe“ löscht Dateien ohne vorherigen Säuberungsversuch, lässt dabei jedoch wichtige Dateien wie Windows-Systemdateien aus.
/quarantine	Infizierte Dateien in die Quarantäne kopieren (ergänzt die beim Säubern ausgeführte Aktion)
/no-quarantine	Infizierte Dateien nicht in die Quarantäne kopieren

Allgemeine Optionen

/help	Hilfe anzeigen und beenden
/version	Versionsinformationen anzeigen und beenden
/preserve-time	Datum für „Geändert am“ beibehalten

Exitcodes

0	Keine Bedrohungen gefunden
1	Bedrohungen gefunden und entfernt
10	Einige Dateien konnten nicht geprüft werden (evtl. Bedrohungen)
50	Bedrohung gefunden
100	Fehler



Hinweis
Exitcodes größer 100 bedeuten, dass die Datei nicht geprüft wurde und daher infiziert sein kann.

ESET CMD

Diese Funktion aktiviert erweiterte ecmd-Befehle. Sie können Einstellungen über die Befehlszeile (ecmd.exe) importieren und exportieren. Bisher konnten Einstellungen nur über die Benutzeroberfläche importiert und exportiert werden. Die ESET Endpoint Antivirus-Konfiguration kann in eine.*xml*-Datei exportiert werden.

Wenn Sie ESET CMD aktiviert haben, stehen zwei Autorisierungsmethoden zur Verfügung:

- **Keine** – keine Autorisierung. Diese Methode sollte nicht verwendet werden, da andernfalls beliebige unsignierte Konfigurationen importiert werden können, was ein Sicherheitsrisiko darstellt.

- **Passwort für die erweiterten Einstellungen** – Wenn Sie eine Konfiguration aus einer.*xml*-Datei importieren, benötigen Sie ein Passwort und müssen die Datei zunächst signieren (siehe „Signieren von .*xml*-Konfigurationsdateien“ weiter unten). Sie müssen das unter Einstellungen für den Zugriff festgelegte Passwort

eingeben, um eine neue Konfiguration importieren zu können. Wenn Sie diese Einstellungen nicht festgelegt haben, das Passwort nicht übereinstimmt oder die *.xml*-Konfigurationsdatei nicht signiert ist, wird die Konfiguration nicht importiert.

Nachdem Sie ESET CMD aktiviert haben, können Sie ESET Endpoint Antivirus-Konfigurationen über die Befehlszeile importieren und exportieren. Sie können diesen Vorgang manuell ausführen oder ein Skript für die Automatisierung erstellen.

Wichtig
Sie müssen die erweiterten ecmd-Befehle entweder mit Administratorberechtigungen oder in einer Windows-Befehlszeile (cmd) mit der Option **Als Administrator ausführen** verwenden. Andernfalls erhalten Sie die Nachricht **Error executing command.** Außerdem muss der ausgewählte Zielordner beim Exportieren vorhanden sein. Der Befehl zum Exportieren funktioniert auch, wenn die ESET CMD-Einstellung deaktiviert ist.

Hinweis
Die erweiterten ecmd-Befehle können nur lokal ausgeführt werden. Der Client-Task **Befehl ausführen** in ESMC funktioniert mit diesen Befehlen nicht.

Beispiel
Befehl zum Exportieren von Einstellungen:
```
ecmd /getcfg c:\config\settings.xml
```

Befehl zum Importieren von Einstellungen:
```
ecmd /setcfg c:\config\settings.xml
```

Signieren einer *.xml*-Konfigurationsdatei:

1. Laden Sie das ausführbare XmlSignTool herunter.
2. Öffnen Sie eine Windows-Eingabeaufforderung (cmd) mit der Option **Als Administrator ausführen**.
3. Navigieren Sie zum Speicherort der Datei `xmlsigntool.exe`
4. Führen Sie den Befehl zum Signieren der *.xml*-Konfigurationsdatei mit der folgenden Syntax aus:
```
xmlsigntool /version 1|2 <xml_file_path>
```

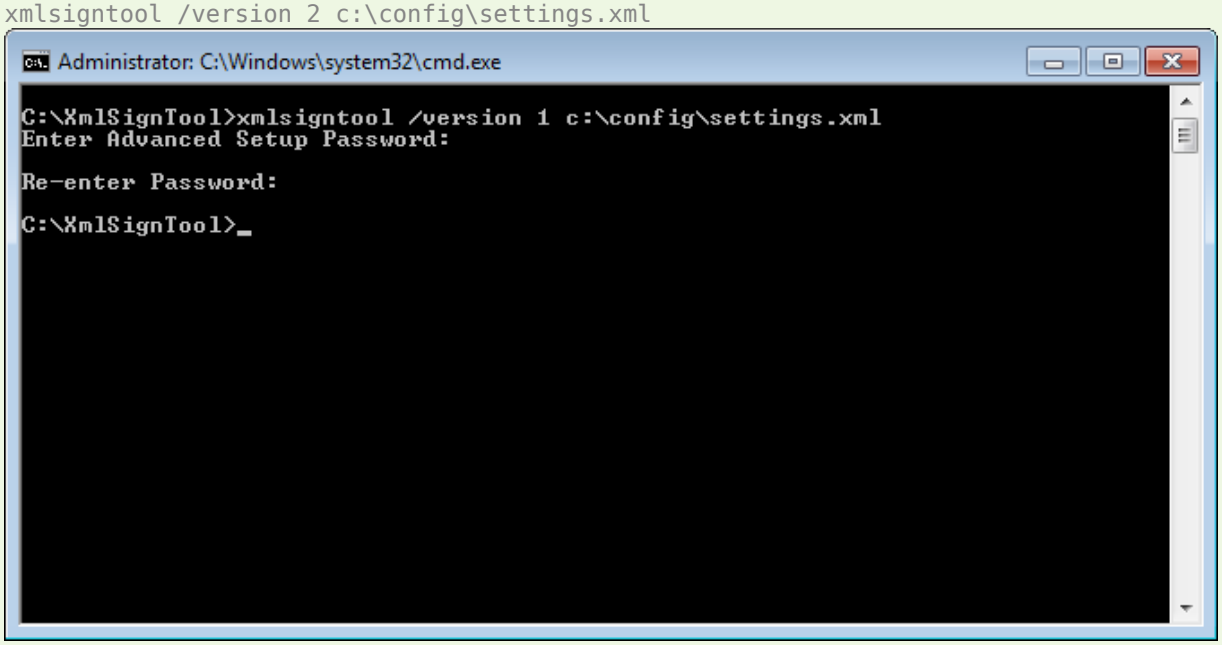
Wichtig
Der Wert des Parameters `/version` hängt von Ihrer Version von ESET Endpoint Antivirus ab. Verwenden Sie `/version 2` für Version 7 und neuere Versionen.

5. Geben Sie das Passwort für die erweiterten Einstellungen ein und bestätigen Sie es, wenn Sie vom XmlSignTool dazu aufgefordert werden. Ihre *.xml*-Konfigurationsdatei ist jetzt signiert und kann in einer anderen Instanz von ESET Endpoint Antivirus mit ESET CMD und der Passwortautorisierungsmethode importiert werden.

Beispiel

Befehl zum Signieren einer exportierten Konfigurationsdatei:

```
xmlsigntool /version 2 c:\config\settings.xml
```



HINWEIS

Wenn sich das Passwort für die erweiterten Einstellungen geändert hat und Sie eine Konfiguration importieren möchten, die mit dem alten Passwort signiert wurde, können Sie die *.xml*-Konfigurationsdatei mit Ihrem aktuellen Passwort erneut signieren. Auf diese Weise können Sie eine ältere Konfigurationsdatei wiederverwenden, ohne sie vor dem Importieren auf einem anderen Computer mit ESET Endpoint Antivirus erneut zu exportieren.

Warnung

ESET CMD sollte nicht ohne Autorisierung aktiviert werden, da andernfalls unsignierte Konfigurationen importiert werden können. Legen Sie das Passwort unter **Erweiterte Einstellungen** > **Benutzeroberfläche** > **Einstellungen für den Zugriff** fest, um Ihr System vor unbefugten Änderungen zu schützen.

Liste der ecmd-Befehle

Sie können einzelne Sicherheitsfunktionen mit dem ESMC Client-Task „Befehl ausführen“ aktivieren und vorübergehend deaktivieren. Diese Befehle überschreiben keine Policy-Einstellungen, und alle deaktivierten Einstellungen werden nach Beendigung des Befehls oder nach einem Neustart des Geräts auf den Originalzustand zurückgesetzt. Um diese Funktion zu verwenden, geben Sie die auszuführende Befehlszeile in das Feld mit dem entsprechenden Namen ein.

Hier finden Sie eine Liste der Befehle für die einzelnen Sicherheitsfunktionen:

Sicherheitsfunktion	Befehl zur vorübergehenden Deaktivierung	Befehl zum Aktivieren
Echtzeit-Dateischutz	ecmd /setfeature onaccess pause	ecmd /setfeature onaccess enable
Dokumentenschutz	ecmd /setfeature document pause	ecmd /setfeature document enable
Medienkontrolle	ecmd /setfeature devcontrol pause	ecmd /setfeature devcontrol enable

Präsentationsmodus	ecmd /setfeature presentation pause	ecmd /setfeature presentation enable
Anti-Stealth-Technologie	ecmd /setfeature antistealth pause	ecmd /setfeature antistealth enable
Personal Firewall	ecmd /setfeature firewall pause	ecmd /setfeature firewall enable
Netzwerkangriffsschutz (IDS)	ecmd /setfeature ids pause	ecmd /setfeature ids enable
Botnet-Erkennung	ecmd /setfeature botnet pause	ecmd /setfeature botnet enable
Web-Kontrolle	ecmd /setfeature webcontrol pause	ecmd /setfeature webcontrol enable
Web-Schutz	ecmd /setfeature webaccess pause	ecmd /setfeature webaccess enable
E-Mail-Client-Schutz	ecmd /setfeature email pause	ecmd /setfeature email enable
Spam-Schutz	ecmd /setfeature antispam pause	ecmd /setfeature antispam enable
Phishing-Schutz	ecmd /setfeature antiphishing pause	ecmd /setfeature antiphishing enable

Leerlauferkennung

Die Erkennung des Ruhezustands kann im Bereich **Erweiterte Einstellungen** unter **Erkennungsroutine** > **Schadsoftware-Scans** > **Scannen im Leerlaufbetrieb** > **Leerlauferkennung** konfiguriert werden. Unter diesen Einstellungen können folgende Auslöser für das Scannen im Leerlaufbetrieb festgelegt werden:

- Aktivierung des Bildschirmschoners
- Sperren des Computers
- Abmelden eines Benutzers

Aktivieren bzw. deaktivieren Sie die Auslöser für die Prüfung im Ruhezustand über die entsprechenden Kontrollkästchen.

Import-/Export-Einstellungen

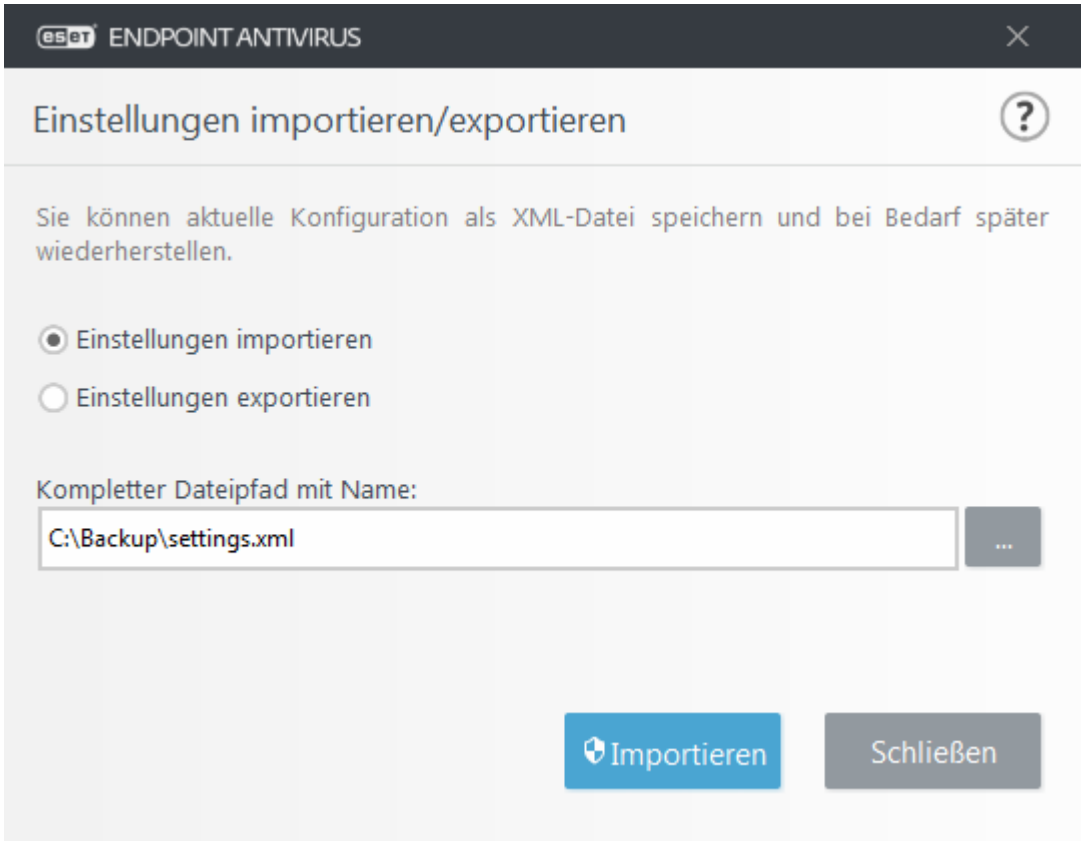
Über das Menü **Einstellungen** können Sie die XML-Datei mit Ihrer benutzerdefinierten Konfiguration von ESET Endpoint Antivirus importieren und exportieren.

Das Importieren und Exportieren der Konfigurationsdatei ist hilfreich, wenn Sie zur späteren Verwendung eine Sicherung der aktuellen Konfiguration von ESET Endpoint Antivirus erstellen möchten. Die Exportfunktion bietet sich auch für Benutzer an, die ihre bevorzugte Konfiguration auf mehreren Systemen verwenden möchten. Um die Einstellungen zu übernehmen, wird einfach eine Datei mit der Endung .xml importiert.

Die Schritte zum Importieren einer Konfiguration sind sehr einfach. Klicken Sie im Hauptprogrammfenster auf **Einstellungen** > **Einstellungen importieren/exportieren**, und wählen Sie die Option **Einstellungen importieren** aus. Geben Sie den Namen der Konfigurationsdatei ein oder klicken Sie auf **Durchsuchen**, um die Konfigurationsdatei zu suchen, die Sie importieren möchten.

Der Export einer Konfiguration verläuft sehr ähnlich. Klicken Sie im Hauptprogrammfenster auf **Einstellungen** > **Einstellungen importieren/exportieren**. Wählen Sie **Einstellungen exportieren** und geben Sie den Namen der Konfigurationsdatei (z. B. *export.xml*) ein. Suchen Sie mithilfe des Browsers einen Speicherort auf Ihrem Computer aus, an dem Sie die Konfigurationsdatei speichern möchten.

Hinweis
Beim Exportieren der Einstellungen kann ein Fehler auftreten, wenn Sie über unzureichende Berechtigungen für das angegebene Verzeichnis verfügen.



Alle Standardeinstellungen wiederherstellen

Klicken Sie auf **Standard** in den erweiterten Einstellungen (F5), um die Programmeinstellungen für alle Module auf die Standardwerte nach einer neuen Installation zurückzusetzen.

Siehe auch Import-/Export-Einstellungen.

Alle Einstellungen in aktuellem Bereich zurücksetzen

Klicken Sie auf den gebogenen Pfeil ⍰, um alle Einstellungen im aktuellen Abschnitt auf die von ESET definierten Standardeinstellungen zurückzusetzen.

Beachten Sie, dass alle vorgenommenen Änderungen nach dem Klicken auf **Auf Standard zurücksetzen** verloren gehen.

Inhalte von Tabellen zurücksetzen - Wenn diese Option aktiviert ist, gehen manuell oder automatisch hinzugefügte Regeln, Tasks oder Profile verloren.

Siehe auch Import-/Export-Einstellungen.

Fehler beim Speichern der Konfiguration

Diese Fehlermeldung weist darauf hin, dass die Einstellungen aufgrund eines Fehlers nicht ordnungsgemäß gespeichert wurden.

Dies bedeutet normalerweise, dass der Benutzer, der versucht hat, die Programmparameter zu ändern:

- nicht genügend Zugriffsrechte oder nicht die erforderlichen Betriebssystemprivilegien hat, um Konfigurationsdateien und die Systemregistrierung zu bearbeiten.
  > Um die gewünschten Änderungen vornehmen zu können, muss ein Systemadministrator angemeldet sein.

- vor kurzem den Lernmodus in HIPS oder in der Firewall aktiviert hat und versucht hat, Änderungen in den erweiterten Einstellungen vorzunehmen.
  > Um die Konfiguration zu speichern und den Konfigurationskonflikt zu vermeiden, schließen Sie die erweiterten Einstellungen ohne zu speichern und versuchen Sie erneut, die gewünschten Änderungen vorzunehmen.

Eine weitere mögliche Problemursache liegt darin, dass das Programm nicht mehr richtig funktioniert oder beschädigt ist und daher neu installiert werden muss.

Remoteüberwachung und -Verwaltung

Remoteüberwachung und -verwaltung (RMM) ist der Prozess der Beaufsichtigung und Überwachung von Softwaresystemen mit einem lokal installierten Agenten, auf den über einen Management-Dienstanbieter zugegriffen werden kann.

ERMM - ESET-Plugin für RMM

- Die Standardinstallation von ESET Endpoint Antivirus enthält die Datei `ermm.exe` in der Endpunktanwendung im folgenden Verzeichnis:
  C:\Program Files\ESET\ESET Security\ermm.exe

- `ermm.exe` ist ein Kommandozeilentool, mit dem Sie Endpunktprodukte verwalten und mit beliebigen RMM-Plugins kommunizieren können.

- `ermm.exe` tauscht Daten mit dem RMM-Plugin aus, das mit dem RMM Agent kommuniziert, der wiederum mit einem RMM-Server verbunden ist. Das ESET RMM Tool ist standardmäßig deaktiviert.

Weitere Ressourcen

- ERMM-Kommandozeile

- Liste der ERMM JSON-Befehle

- Aktivieren der Remoteüberwachung und -verwaltungESET Endpoint Antivirus

ESET Direct Endpoint Management-Plugins für externe RMM-Lösungen

Der RMM-Server wird als Dienst auf einem externen Server ausgeführt. Weitere Informationen finden Sie online in den folgenden ESET Direct Endpoint Management-Anleitungen:

- ESET Direct Endpoint Management Plugin für ConnectWise Automate
- ESET Direct Endpoint Management Plugin für DattoRMM
- ESET Direct Endpoint Management für Solarwinds N-Central
- ESET Direct Endpoint Management für NinjaRMM

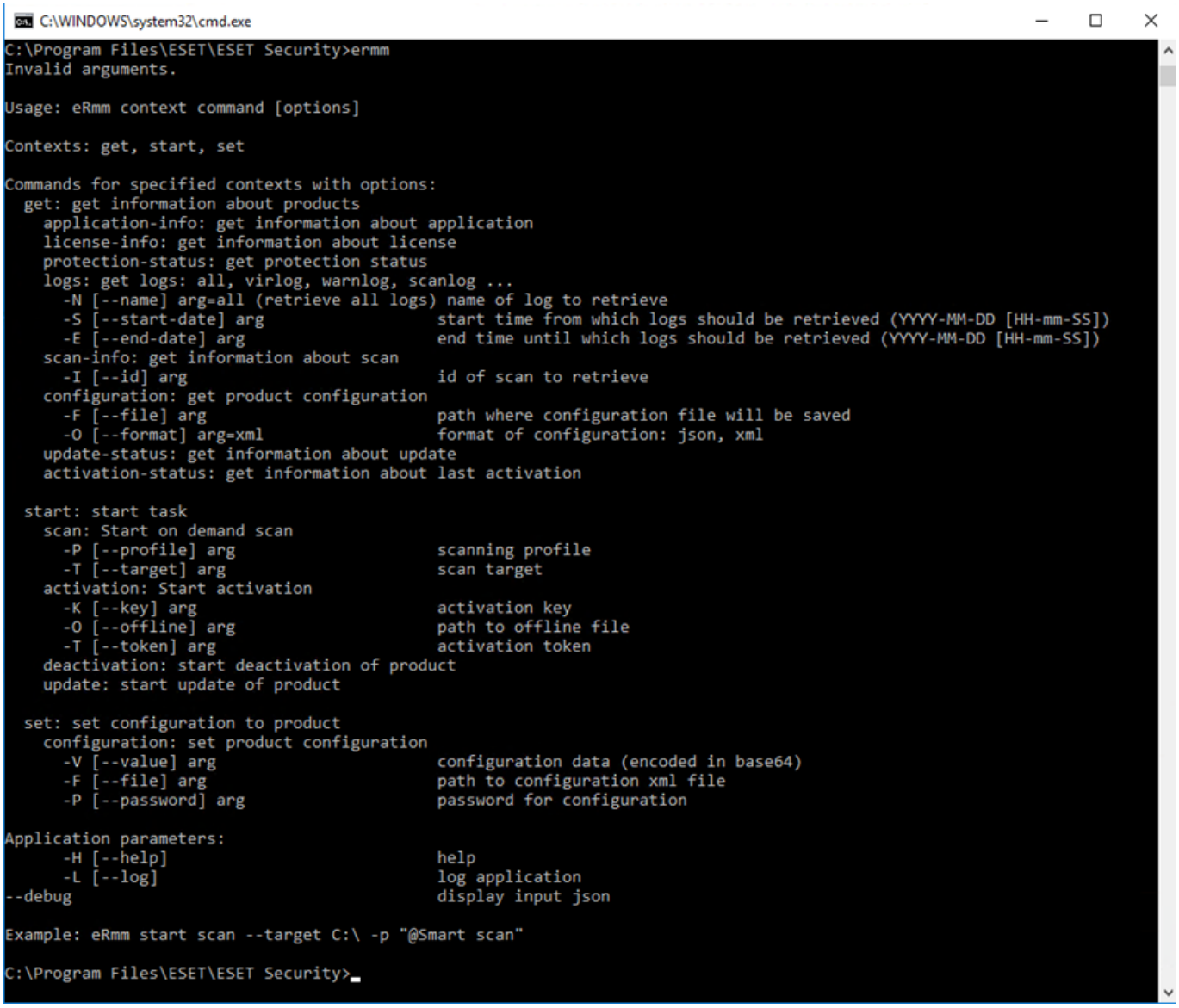
ERMM-Kommandozeile

Remote monitoring management is run using the command line interface. The default ESET Endpoint Antivirus installation contains the file ermm.exe located in the Endpoint application within the directory *c:\Program Files\ESET\ESET Security*.

Run the Command Prompt (cmd.exe) as an Administrator and navigate to the mentioned path. (To open Command Prompt, press Windows button + R on your keyboard, type a cmd.exe into the Run window and press Enter.)

The command syntax is: `ermm context command [options]`

Also note that the log parameters are case sensitive.



ermm.exe uses three basic contexts: Get, Start and Set. In the table below you can find examples of commands syntax. Click the link in the Command column to see the further options, parameters, and usage examples. After successful execution of command, the output part (result) will be displayed. To see an input part, add parameter `--debug` at the of the command.

Context	Command	Description
get		**Get information about products**
	Anwendungsinformationen	Get information about product
	Lizenzinformationen	Get information about license
	Schutzstatus	Get protection status
	Logs	Get logs
	Prüfungsinformationen	Get information about running scan
	Konfiguration	Get product configuration
	Updatestatus	Get information about update

Context	Command	Description
	Aktivierungsstatus	Get information about last activation
start		**Start task**
	Prüfung	Start on demand scan
	Aktivierung	Start activation of product
	Deaktivierung	Start deactivation of product
	Update	Start update of product
set		**Set options for product**
	Konfiguration	Set configuration to product

In the output result of every command, the first information displayed is result ID. To understand better the result information, check the table of IDs below.

Error ID	Error	Description
0	Success	
1	Command node not present	"Command" node not present in input json
2	Command not supported	Particular command is not supported
3	General error executing the command	Error during execution of command
4	Task already running	Requested task is already running and has not been started
5	Invalid parameter for command	Bad user input
6	Command not executed because it's disabled	RMM isn't enabled in advanced settings or isn't started as an administrator

Liste der ERMM JSON-Befehle

- Schutzstatus abrufen
- Anwendungsinformationen abrufen
- Lizenzinformationen abrufen
- Logs abrufen
- Aktivierungsstatus abrufen
- Prüfungsinformationen abrufen
- Konfiguration abrufen
- Updatestatus abrufen
- Prüfung starten
- Aktivierung starten

- Deaktivierung starten
- Update starten
- Konfiguration festlegen

Schutzstatus abrufen

Get the list of application statuses and the global application status

Command line

```
ermm.exe get protection-status
```

Parameters

None

Example

call

```
{
 "command":"get_protection_status",
 "id":1,
 "version":"1"
}
```

result

```
{
 "id":1,
 "result":{
  "statuses":[{
    "id":"EkrnNotActivated",
    "status":2,
    "priority":768,
    "description":"Product not activated"
   }],
  "status":2,
  "description":"Security alert"
 },
 "error":null
}
```

Anwendungsinformationen abrufen

Get information about the installed application

Command line

```
ermm.exe get application-info
```

Parameters

None

Example

call

```
{
 "command":"get_application_info",
 "id":1,
 "version":"1"
}
```

result

```
{
  "id":1,
  "result":{
   "description":"ESET Endpoint Antivirus",
   "version":"6.6.2018.0",
   "product":"eea",
   "lang_id":1033,
   "modules":[{
    "id":"SCANNER32",
    "description":"Detection engine",
    "version":"15117",
    "date":"2017-03-20"
   },{
    "id":"PEGASUS32",
    "description":"Rapid Response module",
    "version":"9734",
    "date":"2017-03-20"
   },{
    "id":"LOADER32",
    "description":"Update module",
    "version":"1009",
    "date":"2016-12-05"
   },{
    "id":"PERSEUS32",
    "description":"Antivirus and antispyware scanner module",
    "version":"1513",
    "date":"2017-03-06"
   },{
    "id":"ADVHEUR32",
    "description":"Advanced heuristics module",
    "version":"1176",
    "date":"2017-01-16"
   },{
    "id":"ARCHIVER32",
    "description":"Archive support module",
    "version":"1261",
    "date":"2017-02-22"
   },{
    "id":"CLEANER32",
    "description":"Cleaner module",
    "version":"1132",
    "date":"2017-03-15"
   },{
    "id":"ANTISTEALTH32",
    "description":"Anti-Stealth support module",
    "version":"1106",
    "date":"2016-10-17"
   },{
    "id":"SYSTEMSTATUS32",
    "description":"ESET SysInspector module",
    "version":"1266",
    "date":"2016-12-22"
   },{
    "id":"TRANSLATOR32",
    "description":"Translation support module",
    "version":"1588B",
    "date":"2017-03-01"
   },{
    "id":"HIPS32",
    "description":"HIPS support module",
    "version":"1267",
    "date":"2017-02-16"
   },{
    "id":"PROTOSCAN32",
    "description":"Internet protection module",
    "version":"1300",
    "date":"2017-03-03"
   },{
    "id":"DBLITE32",
    "description":"Database module",
    "version":"1088",
    "date":"2017-01-05"
   },{
    "id":"CONFENG32",
    "description":"Configuration module (33)",
    "version":"1496B",
    "date":"2017-03-17"
   },{
    "id":"IRIS32",
    "description":"LiveGrid communication module",
    "version":"1022",
    "date":"2016-04-01"
   },{
    "id":"SAURON32",
    "description":"Rootkit detection and cleaning module",
    "version":"1006",
    "date":"2016-07-15"
   },{
    "id":"SSL32",
    "description":"Cryptographic protocol support module",
    "version":"1009",
    "date":"2016-12-02"
   }
  },
  "error":null
 }
}
```

Lizenzinformationen abrufen

Get information about the license of the product

Command line

```
ermm.exe get license-info
```

Parameters

None

Example

call

```
{
 "command":"get_license_info",
 "id":1,
 "version":"1"
}
```

result

```
{
 "id":1,
 "result":{
  "type":"NFR",
  "expiration_date":"2020-12-31",
  "expiration_state":"ok",
  "public_id":"3XX-7ED-7XF",
  "seat_id":"6f726793-ae95-4e04-8ac3-e6a20bc620bf",
  "seat_name":"M"
 },
 "error":null
}
```

Logs abrufen

Get logs of the product

Command line

```
ermm.exe get logs --name warnlog --start-date "2017-04-04 06-00-00" --end-
date "2017-04-04 12-00-00"
```

Parameters

Name	Value
name	{ all, virlog, warnlog, scanlog, blocked, hipslog, urllog, devctrllog } : log to retrieve
start-date	start date from which logs should be retrieved (YYYY-MM-DD [HH-mm-SS])
end-date	end time until which logs should be retrieved (YYYY-MM-DD [HH-mm-SS])

Example

call


```
{
 "command":"get_logs",
 "id":1,
 "version":"1",
 "params":{
  "name":"warnlog",
  "start_date":"2017-04-04 06-00-00",
  "end_date":"2017-04-04 12-00-00"
 }
}
```


result


```
{
 "id":1,
 "result":{
  "warnlog":{
   "display_name":"Events",
   "logs":[{
    "Time":"2017-04-04 06-05-59",
    "Severity":"Info",
    "PluginId":"ESET Kernel",
    "Code":"Malware database was successfully updated to version 15198 (20170404).",
    "UserData":""
   },{
    "Time":"2017-04-04 11-12-59",
    "Severity":"Info",
    "PluginId":"ESET Kernel",
    "Code":"Malware database was successfully updated to version 15199 (20170404).",
    "UserData":""
   }]
  }
 },
 "error":null
}
```

Aktivierungsstatus abrufen

Get information about the last activation. Result of status can be { success, error }

Command line

```
ermm.exe get activation-status
```

Parameters

None

Example

call

```
{
 "command":"get_activation_status",
 "id":1,
 "version":"1"
}
```

result

```
{
 "id":1,
 "result":{
  "status":"success"
 },
 "error":null
}
```

Prüfungsinformationen abrufen

Get information about running scan.

Command line

```
ermm.exe get scan-info
```

Parameters

None

Example

call


```
{
 "command":"get_scan_info",
 "id":1,
 "version":"1"
}
```


result


```
{
 "id":1,
 "result":{
  "scan-info":{
 "scans":[{
  "scan_id":65536,
  "timestamp":272,
  "state":"finished",
  "pause_scheduled_allowed":false,
  "pause_time_remain":0,
  "start_time":"2017-06-20T12:20:33Z",
  "elapsed_tickcount":328,
  "exit_code":0,
  "progress_filename":"Operating memory",
  "progress_arch_filename":"",
  "total_object_count":268,
  "infected_object_count":0,
  "cleaned_object_count":0,
  "log_timestamp":268,
  "log_count":0,
  "log_path":"C:\\ProgramData\\ESET\\ESET Security\\Logs\\eScan\\ndl31494.dat",
  "username":"test-PC\\test",
  "process_id":3616,
  "thread_id":3992,
  "task_type":2
 }],
 "pause_scheduled_active":false
}
 },
 "error":null
}
```


Konfiguration abrufen

Get the product configuration. Result of status may be { success, error }

Command line

```
ermm.exe get configuration --file C:\tmp\conf.xml --format xml
```

Parameters

Name	Value
file	the path where the configuration file will be saved
format	format of configuration: json, xml. Default format is xml

Example

call

```
{
 "command":"get_configuration",
 "id":1,
 "version":"1",
 "params":{
  "format":"xml",
  "file":"C:\\tmp\\conf.xml"
 }
}
```

result

```
{
 "id":1,
 "result":{
  "configuration":"PD94bWwgdmVyc2lvbj0iMS4w=="
 },
 "error":null
}
```

Updatestatus abrufen

Get information about the update. Result of status may be { success, error }

Command line

```
ermm.exe get update-status
```

Parameters

None

Example

call

```
{
 "command":"get_update_status",
 "id":1,
 "version":"1"
}
```

result

```
{
 "id":1,
 "result":{
  "last_update_time":"2017-06-20 13-21-37",
  "last_update_result":"error",
  "last_successful_update_time":"2017-06-20 11-21-45"
 },
 "error":null
}
```

Prüfung starten

Start scan with the product

Command line

```
ermm.exe start scan --profile "profile name" --target "path"
```

Parameters

Name	Value

profile	Profile name of On-demand computer scan defined in product
target	Path to be scanned

Example

call

```
{
 "command":"start_scan",
 "id":1,
 "version":"1",
 "params":{
  "profile":"Smart scan",
  "target":"c:\\"
 }
}
```

result

```
{
 "id":1,
 "result":{
  "task_id":458752
 },
 "error":null
}
```

Aktivierung starten

Start activation of product

Command line

```
ermm.exe start activation --key "activation key" | --
offline "path to offline file" | --token "activation token"
```

Parameters

Name	Value
key	Activation key
offline	Path to offline file
token	Activation token

Example

call

```
{
 "command":"start_activation",
 "id":1,
 "version":"1",
 "params":{
  "key":"XXXX-XXXX-XXXX-XXXX-XXXX"
 }
}
```

result

```
{
 "id":1,
 "result":{
 },
 "error":null
}
```

Deaktivierung starten

Start deactivation of the product

Command line

```
ermm.exe start deactivation
```

Parameters

None

Example

call

```
{
 "command":"start_deactivation",
 "id":1,
 "version":"1"
}
```

result

```
{
 "id":1,
 "result":{
 },
 "error":null
}
```

Update starten

Start update of the product. Only one update may be running in the product so in case the update is already running, "Task already running" error code is returned

Command line

```
ermm.exe start update
```

Parameters

None

Example

call

```
{
 "command":"start_update",
 "id":1,
 "version":"1"
}
```

result

```
{
 "id":1,
 "result":{
 },
  "error":{
   "id":4,
   "text":"Task already running."
  }
}
```

Konfiguration festlegen

Set configuration to the product. Result of status may be { success, error }

Command line

```
ermm.exe set configuration --file C:\tmp\conf.xml --format xml --password pass
```

Parameters

Name	Value
file	the path where the configuration file will be saved
password	password for configuration
value	configuration data from the argument (encoded in base64)

Example

call

```
{
 "command":"set_configuration",
 "id":1,
 "version":"1",
 "params":{
  "format":"xml",
  "file":"C:\\tmp\\conf.xml",
  "password": "pass"
 }
}
```

result

```
{
 "id":1,
 "result":{
 },
 "error":null
}
```

Häufig gestellte Fragen

In diesem Kapitel werden einige der häufigsten Fragen und Probleme behandelt. Klicken Sie auf eine Themenüberschrift, um Hilfestellung bei der Lösung Ihres Problems zu erhalten:

- So aktualisieren Sie ESET Endpoint Antivirus
- So aktivieren Sie ESET Endpoint Antivirus
- So aktivieren Sie das neue Produkt mithilfe der aktuellen Anmeldedaten
- So entfernen Sie einen Virus von Ihrem PC
- So erstellen Sie eine neue Aufgabe im Taskplaner
- So planen Sie eine wöchentliche Computerprüfung
- So verbinden Sie Ihr Produkt mit ESET Security Management Center

– Verwenden des Override-Modus
- Anwenden einer empfohlenen Policy für ESET Endpoint Antivirus

- So konfigurieren Sie einen Mirror
- Wie aktualisiere ich auf Windows 10 mit ESET Endpoint Antivirus
- Aktivieren der Remoteüberwachung und -verwaltung
- Download bestimmter Dateitypen aus dem Internet blockieren
- Minimieren der ESET Endpoint Antivirus-Benutzeroberfläche

Wenn Ihr Problem nicht in der oben aufgeführten Liste der Hilfeseiten aufgeführt ist, suchen Sie es auf den ESET Endpoint Antivirus-Hilfeseiten über ein Schlagwort oder eine Formulierung, das/die Ihr Problem beschreibt.

Wenn Sie die Antwort auf Ihr Problem/Ihre Frage nicht in den Hilfeseiten finden können, besuchen Sie die ESET Knowledgebase, wo Sie Antworten auf häufig gestellte Fragen und gängige Probleme finden.

- Bewährte Methoden für den Schutz gegen Ransomware (Filecoder)
- Häufig gestellte Fragen zu ESET Endpoint Security und ESET Endpoint Antivirus 7
- Welche Adressen und Ports muss ich an meiner Firewall eines Drittanbieters öffnen, damit mein ESET-Produkt vollständig funktioniert?

Falls erforderlich, können Sie sich mit Ihren Fragen und Problemen auch direkt an die Online-Supportzentrale wenden. Den Link zum Online-Kontaktformular finden Sie im Hauptprogrammfenster im Bereich **Hilfe und Support**.

So aktualisieren Sie ESET Endpoint Antivirus

Die Aktualisierung von ESET Endpoint Antivirus kann manuell oder automatisch erfolgen. Klicken Sie im Bereich **Update** auf **Jetzt aktualisieren**, um eine Aktualisierung zu starten.

Bei der Standardinstallation wird stündlich ein automatisches Update ausgeführt. Sie können dieses Intervall unter **Tools** > **Taskplaner** ändern. (Weitere Informationen zum Taskplaner finden Sie hier.)

So aktivieren Sie ESET Endpoint Antivirus

Nach Abschluss der Installation werden Sie aufgefordert, Ihr Produkt zu aktivieren.

Sie können Ihr Produkt auf verschiedene Arten aktivieren. Die Verfügbarkeit einer bestimmten Aktivierungsmöglichkeit im Aktivierungsfenster hängt vom Land und von der Vertriebsart (ESET-Webseite, .msi- oder .exe-Installationsprogramm usw.) ab.

Sie können Ihre Kopie von ESET Endpoint Antivirus direkt im Programm aktivieren. Klicken Sie hierfür auf das Symbol im Infobereich der Taskleiste und wählen Sie **Produktlizenz aktivieren** aus dem Menü. Sie können das Produkt auch im Hauptmenü unter **Hilfe und Support** > **Produkt aktivieren** oder **Schutzstatus** > **Produkt aktivieren** aktivieren.

Sie können ESET Endpoint Antivirus mit einer der folgenden Methoden aktivieren:

- **Lizenzschlüssel** - Eine eindeutige Zeichenfolge im Format XXXX-XXXX-XXXX-XXXX-XXXX zur Identifizierung des Lizenzinhabers und der Aktivierung der Lizenz.

- **ESET Business Account** - Ein im ESET Business Account-Portal erstelltes Konto mit Anmeldedaten (E-Mail-Adresse und Passwort). Mit dieser Methode können Sie mehrere Lizenzen von einem Standort aus verwalten.

- **Offline-Lizenz** - Eine automatisch erzeugte Datei, die zum Zwecke der Bereitstellung von Lizenzinformationen in das ESET-Produkt übertragen wird. Wenn Ihnen eine Lizenz das Herunterladen einer Offline-Lizenzdatei (.lf) erlaubt, können Sie hiermit die Offline-Aktivierung vornehmen. Die Anzahl der Offline-Lizenzen wird von der Gesamtanzahl der verfügbaren Lizenzen abgezogen. Weitere Informationen zum Generieren einer Offline-Datei finden Sie im ESET Business Account-Benutzerhandbuch.

Klicken Sie auf **Später aktivieren**, wenn der Computer Teil eines verwalteten Netzwerks ist und der Administrator die Aktivierung remote über ESET Security Management Center ausführt. Wählen Sie diese Option nur, wenn der Client später aktiviert werden soll.

Wenn Sie einen Benutzernamen und ein Passwort für ein älteres ESET-Produkt haben und nicht wissen, wie Sie ESET Endpoint Antivirus aktivieren können, klicken Sie auf Legacy-Anmeldeinformationen zu einem Lizenzschlüssel konvertieren.

Fehler bei Produktaktivierung?

Sie können Ihre Produktlizenz jederzeit ändern. Klicken Sie dazu im Hauptprogrammfenster auf **Hilfe und Support** > **Lizenz ändern**. Dort sehen Sie die öffentliche Lizenz-ID, die Ihre Lizenz gegenüber dem ESET-Support identifiziert. Ihr Benutzername, unter dem der Computer registriert ist, befindet sich im Bereich **Über**, den Sie per Rechtsklick auf das Symbol im Infobereich der Taskleiste erreichen.

> **Hinweis**
> ESET Security Management Center kann Clientcomputer unbeaufsichtigt mit Lizenzen aktivieren, die vom Administrator bereitgestellt wurden. Weitere Informationen hierzu finden Sie in der ESET Security Management Center-Onlinehilfe.

Anmelden bei ESET Business Account

Das Sicherheitsadministratorkonto wird im ESET Business Account-Portal mit Ihrer **E-Mail-Adresse** und Ihrem **Passwort** erstellt. Dieses Konto kann die Berechtigungen sämtlicher Plätze anzeigen. Mit einem Sicherheitsadministratorkonto können Sie mehrere Lizenzen verwalten. Wenn Sie noch kein Sicherheitsadministratorkonto haben, klicken Sie auf **Konto erstellen**. Daraufhin werden Sie zum ESET Business Account-Portal weitergeleitet, wo Sie sich mit Ihren Daten anmelden können.

Falls Sie Ihr Passwort vergessen haben, klicken Sie auf **Ich habe mein Passwort vergessen**. Daraufhin werden Sie zum ESET Business Account-Portal weitergeleitet. Geben Sie Ihre E-Mail-Adresse ein und klicken Sie zur Bestätigung auf **Anmelden**. Daraufhin erhalten Sie eine Nachricht mit Anweisungen zum Zurücksetzen Ihres Passworts.

Aktivieren von neueren ESET-Endpunktprodukten mit veralteten Lizenzdaten

Wenn Sie bereits über einen Benutzernamen und ein Passwort verfügen und einen Lizenzschlüssel wünschen, lassen Sie Ihre Anmeldetdaten im ESET Business Account-Portal in einen neuen Lizenzschlüssel konvertieren.

So entfernen Sie einen Virus von Ihrem PC

Wenn Ihr Computer die Symptome einer Infektion mit Schadsoftware aufweist, beispielsweise langsamer reagiert oder oft hängt, sollten Sie folgendermaßen vorgehen:

1. Klicken Sie im Hauptfenster auf **Computer prüfen**.

2. Klicken Sie auf **Smart-Prüfung**, um die Systemprüfung zu starten.

3. Nachdem die Prüfung abgeschlossen ist, überprüfen Sie die Anzahl der geprüften, infizierten und wiederhergestellten Dateien im Log.

4. Wenn Sie nur einen Teil Ihrer Festplatte prüfen möchten, klicken Sie auf **Benutzerdefinierte Prüfung** und wählen Sie dann die Ziele aus, die auf Viren geprüft werden sollen.

Weitere Informationen finden Sie in diesem regelmäßig aktualisierten ESET-Knowledgebase-Artikel.

So erstellen Sie eine neue Aufgabe im Taskplaner

Zum Erstellen eines neuen Tasks unter **Tools** > **Taskplaner** klicken Sie auf **Task hinzufügen** oder klicken mit der rechten Maustaste und wählen im Kontextmenü die Option **Hinzufügen** aus. Es gibt fünf Arten von Tasks:

- **Start externer Anwendung** - Planen der Ausführung einer externen Anwendung

- **Log-Wartung** - Log-Dateien enthalten auch unbenutzte leere Einträge von gelöschten Datensätzen. Dieser Task optimiert regelmäßig die Einträge in Log-Dateien.

- **Prüfung Systemstartdateien** - Prüft Dateien, die während des Systemstarts oder der Anmeldung ausgeführt werden.

- **Snapshot des Computerstatus erstellen** - Erstellt einen ESET SysInspector-Snapshot und eine genaue (Risikostufen-)Analyse Ihrer Systemkomponenten (z. B. Treiber und Anwendungen).

- **On-Demand-Prüfung** - Prüft die Dateien und Ordner auf Ihrem Computer.

- **Update** – Erstellt einen Update-Task zur Aktualisierung der Module.

Da **Update**-Tasks zu den meistverwendeten Tasks gehören, wird im Folgenden das Hinzufügen eines neuen Update-Tasks beschrieben.

Wählen Sie in der Liste **Geplanter Task** den Task **Update**. Geben Sie den Namen des Tasks in das Feld **Taskname** ein und klicken Sie auf **Weiter**. Wählen Sie das gewünschte Ausführungsintervall. Folgende Optionen stehen zur Verfügung: **Einmalig**, **Wiederholt**, **Täglich**, **Wöchentlich** und **Bei Ereignis. Wählen Sie Task im Akkubetrieb überspringen** aus, um die Systembelastung für einen Laptop während des Akkubetriebs möglichst gering zu halten. Der angegebene Task wird zum angegeben Zeitpunkt in den Feldern **Taskausführung** ausgeführt. Im nächsten Schritt können Sie eine Aktion festlegen für den Fall, dass der Task zur geplanten Zeit nicht ausgeführt oder abgeschlossen werden kann. Folgende Optionen stehen zur Verfügung:

- **Zur nächsten geplanten Ausführungszeit**

- **Baldmöglichst**

- **Sofort ausführen, wenn Intervall seit letzter Ausführung überschritten** (das Intervall kann über das Feld **Zeit seit letzter Ausführung** festgelegt werden)

Anschließend wird ein Fenster mit einer vollständigen Zusammenfassung des aktuellen Tasks angezeigt. Klicken Sie auf **Fertig stellen**, wenn Sie Ihre Änderungen abgeschlossen haben.

Es wird ein Dialogfenster angezeigt, in dem Sie die Profile für den Task auswählen können. Hier können Sie das primäre und das alternative Profil festlegen. Das alternative Profil wird verwendet, wenn der Task mit dem primären Profil nicht abgeschlossen werden kann. Bestätigen Sie Ihre Auswahl mit **Fertig stellen**. Der neue Task wird zur Liste der aktuellen Tasks hinzugefügt.

So planen Sie eine wöchentliche Computerprüfung

Um einen regelmäßigen Task zu planen, öffnen Sie das Hauptprogrammfenster und klicken Sie auf **Tools** > **Taskplaner**. Hier finden Sie einen kurzen Überblick zum Planen eines Tasks, der Ihre lokalen Laufwerke einmal pro Woche scannt. Weitere Informationen finden Sie in unserem Knowledgebase-Artikel.

So planen Sie eine regelmäßige Prüfung:

1. Klicken Sie im Hauptfenster des Taskplaners auf **Hinzufügen**.

2. Wählen Sie im Dropdown-Menü die Option **On-Demand-Prüfung**.

3. Geben Sie einen Namen für den Task an, und wählen Sie **Wöchentlich** unter **Ausführungsintervall** aus.

4. Wählen Sie Tag und Uhrzeit für die Ausführung aus.

5. Wählen Sie **Ausführung zum nächstmöglichen Zeitpunkt** aus, um den Task später auszuführen, falls die geplante Ausführung aus irgendeinem Grund nicht stattfindet (z. B. weil der Computer ausgeschaltet ist).

6. Überprüfen Sie die Zusammenfassung zum geplanten Task, und klicken Sie auf **Fertig stellen**.

7. Wählen Sie im Dropdown-Menü **Zu prüfende Objekte** die Option **Lokale Laufwerke** aus.

8. Klicken Sie auf **Fertig stellen**, um den Task zu übernehmen.

So verbinden Sie ESET Endpoint Antivirus mit ESET Security Management Center

Wenn Sie ESET Endpoint Antivirus auf Ihrem Computer installiert haben und sich mit ESET Security Management Center verbinden möchten, muss der ESET Management Agent ebenfalls auf Ihrer Client-Workstation installiert sein. Der Agent ist ein grundlegender Bestandteil aller Clientlösungen, die mit dem ESMC Server kommunizieren.

- ESET Management Agent auf Client-Workstations installieren oder bereitstellen

Siehe auch:

- Dokumentation für remote verwaltete Endpunkte
- Verwenden des Override-Modus
- Anwenden einer empfohlenen Policy für ESET Endpoint Antivirus

Verwenden des Override-Modus

Benutzer mit installierten ESET Endpoint-Produkten (Version 6.5 und neuere Versionen) für Windows können die Override Funktion nutzen. Mit dem Override-Modus können Benutzer auf der Ebene des Clientcomputers die Einstellungen für das installierte ESET-Produkt ändern, selbst wenn diese Einstellungen durch eine Policy festgelegt wurden. Der Override-Modus kann für bestimmte AD-Benutzer aktiviert oder mit einem Passwort geschützt werden. Diese Funktion kann nur für maximal vier Stunden aktiviert werden.



Warnung

- Der Override-Modus kann nach der Aktivierung nicht in der ESMC-Web-Konsole beendet werden. Der Override-Modus wird nach Ablauf der festgelegten Frist automatisch deaktiviert oder kann auf dem Clientcomputer deaktiviert werden.
- Der Benutzer, der den Override-Modus verwendet, benötigt auch Windows-Administratorrechte. Andernfalls können die Änderungen an den Einstellungen von ESET Endpoint Antivirus nicht gespeichert werden.
- Die Active Directory-Gruppenauthentifizierung wird für ESET Endpoint Antivirus 7.0.2100.4 und neuere Versionen unterstützt.

So aktivieren Sie den **Override-Modus**:

1. Navigieren Sie zu **Policies** > **Neue Policy**.

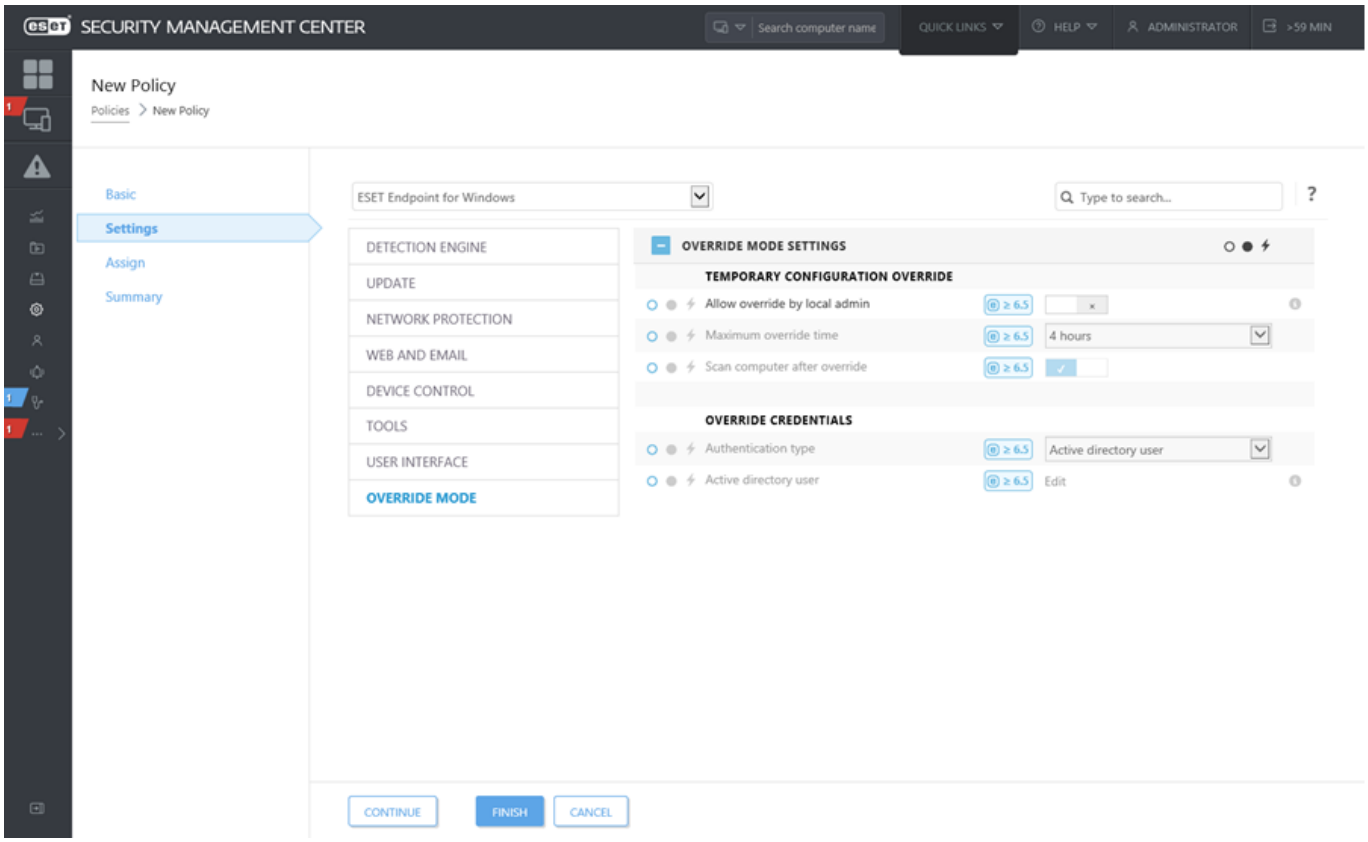
2. Geben Sie im Bereich **Einfach** einen **Namen** und eine **Beschreibung** für die Policy ein.

3. Wählen Sie im Bereich **Einstellungen** die Option **ESET Endpoint für Windows** aus.

4. Klicken Sie auf **Override-Modus** und konfigurieren Sie die Regeln für den Override-Modus.

5. Wählen Sie im Bereich **Zuweisen** den Computer oder die Computergruppe aus, auf die diese Policy angewendet werden soll.

6. Überprüfen Sie Ihre Einstellungen im Bereich **Zusammenfassung** und klicken Sie auf **Fertig stellen**, um die Policy zu übernehmen.



Beispiel

Wenn *John* ein Problem mit den Endpunkteinstellungen hat, weil diese wichtige Funktionen oder den Internetzugriff auf seinem Computer blockieren, kann der Administrator *John* erlauben, die vorhandene Endpunkt-Policy außer Kraft zu setzen und die Einstellungen auf seinem Computer manuell anzupassen. Anschließend kann ESMC diese neuen Einstellungen anfordern, damit der Administrator eine neue Policy mit diesen Einstellungen erstellen kann.
Führen Sie dazu die folgenden Schritte aus:
1. Navigieren Sie zu **Policies** > **Neue Policy**.
2. Füllen Sie die Felder **Name** und **Beschreibung** aus. Wählen Sie im Bereich **Einstellungen** die Option **ESET Endpoint für Windows** aus.
3. Klicken Sie auf **Override-Modus**, aktivieren Sie den Override-Modus für eine Stunde und wählen Sie *John* als AD-Benutzer aus.
4. Weisen Sie die Policy zu *Johns Computer* zu und klicken Sie auf **Fertig stellen**, um die Policy zu speichern.
5. *John* muss den **Override-Modus** auf seinem ESET-Endpunkt aktivieren und die Einstellungen auf seinem Computer manuell bearbeiten.
6. Navigieren Sie in der ESMC-Web-Konsole zu **Computer**, wählen Sie *Johns Computer* aus und klicken Sie auf **Details anzeigen**.
7. Klicken Sie im Bereich **Konfiguration** auf **Konfiguration anfordern**, um einen Client-Task zu planen, der die Konfiguration schnellstmöglich vom Client-Task abruft.
8. Nach kurzer Zeit wird die Konfiguration angezeigt. Klicken Sie auf das Produkt, dessen Einstellungen Sie speichern möchten, und dann auf **Konfiguration öffnen**.
9. Überprüfen Sie die Einstellungen und klicken Sie auf **In Richtlinie umwandeln**.
10. Füllen Sie die Felder **Name** und **Beschreibung** aus.
11. Im Bereich **Einstellungen** können Sie die Einstellungen bei Bedarf anpassen.
12. Im Bereich **Zuweisen** können Sie diese Policy zu *Johns Computer* (oder anderen Computern) zuweisen.
13. Klicken Sie auf **Fertig stellen**, um die Einstellungen zu speichern.
14. Vergessen Sie nicht, die Override-Policy zu entfernen, wenn Sie diese nicht mehr benötigen.

Anwenden einer empfohlenen Policy für ESET Endpoint Antivirus

Nachdem Sie ESET Endpoint Antivirus mit ESET Security Management Center verbunden haben, sollten Sie entweder eine empfohlene oder eine benutzerdefinierte Policy anwenden.

Für ESET Endpoint Antivirus sind mehrere integrierte Policies verfügbar:

Policy	Beschreibung
Antivirus - ausgewogen	Empfohlene Sicherheitskonfiguration für die meisten Umgebungen.
Antivirus - maximale Sicherheit	Einsatz von Machine Learning, tiefer Verhaltensinspektion und SSL-Filterung. Die Erkennung potenziell unsicherer, unerwünschter und verdächtiger Anwendungen ist betroffen.
Cloudbasiertes Reputations- und Feedbacksystem	Aktiviert das cloudbasierte ESET LiveGrid®-Reputations- und Feedbacksystem, um die Erkennung neuester Bedrohungen zu verbessern und um bösartige oder unbekannte potenzielle Bedrohungen zur weiteren Analyse zu teilen.
Medienkontrolle - maximale Sicherheit	Alle Geräte sind gesperrt. Wenn ein Gerät verbunden werden soll, muss es von einem Administrator zugelassen werden.

Medienkontrolle - nur schreibgeschützt	Nur Lesezugriff auf Geräte möglich. Alle Geräte sind schreibgeschützt.
Firewall - Sämtlichen Datenverkehr mit Ausnahme von ESMC- und EEI-Verbindungen blockieren	Sämtlichen Datenverkehr blockieren, mit Ausnahme von Verbindungen zu ESET Security Management Center und zum ESET Enterprise Inspector Server (nur ESET Endpoint Security).
Logging - komplettes Diagnose-Logging	Das Template gewährleistet, dass der Administrator bei Bedarf alle Logs zur Verfügung hat. Alles wird mit minimaler Ausführlichkeit in die Logs aufgenommen, einschließlich HIPS- und Threatsense-Parameter und Firewall. Die Logs werden nach 90 Tagen automatisch gelöscht.
Logging - nur wichtige Ereignisse protokollieren	Die Policy gewährleistet, dass Warnungen, Fehler und kritische Ereignisse in den Log aufgenommen werden. Die Logs werden automatisch nach 90 Tagen gelöscht.
Sichtbarkeit - ausgewogen	Standardeinstellung für die Sichtbarkeit. Status und Benachrichtigungen sind aktiviert.
Sichtbarkeit - unsichtbarer Modus	Benachrichtigungen, Warnungen, grafische Benutzeroberfläche und Integration in das Kontextmenü sind deaktiviert. egui.exe wird nicht ausgeführt. Nur für die Verwaltung über den ESET PROTECT Cloud geeignet.
Sichtbarkeit - reduzierte Interaktion mit Benutzer	Status deaktiviert, Benachrichtigungen deaktiviert, grafische Benutzeroberfläche präsentiert.

Gehen Sie wie folgt vor, um die Policy mit dem Namen **Antivirus - maximale Sicherheit** festzulegen, die mehr als 50 empfohlene Einstellungen für ESET Endpoint Antivirus auf Ihren Workstations vorschreibt:

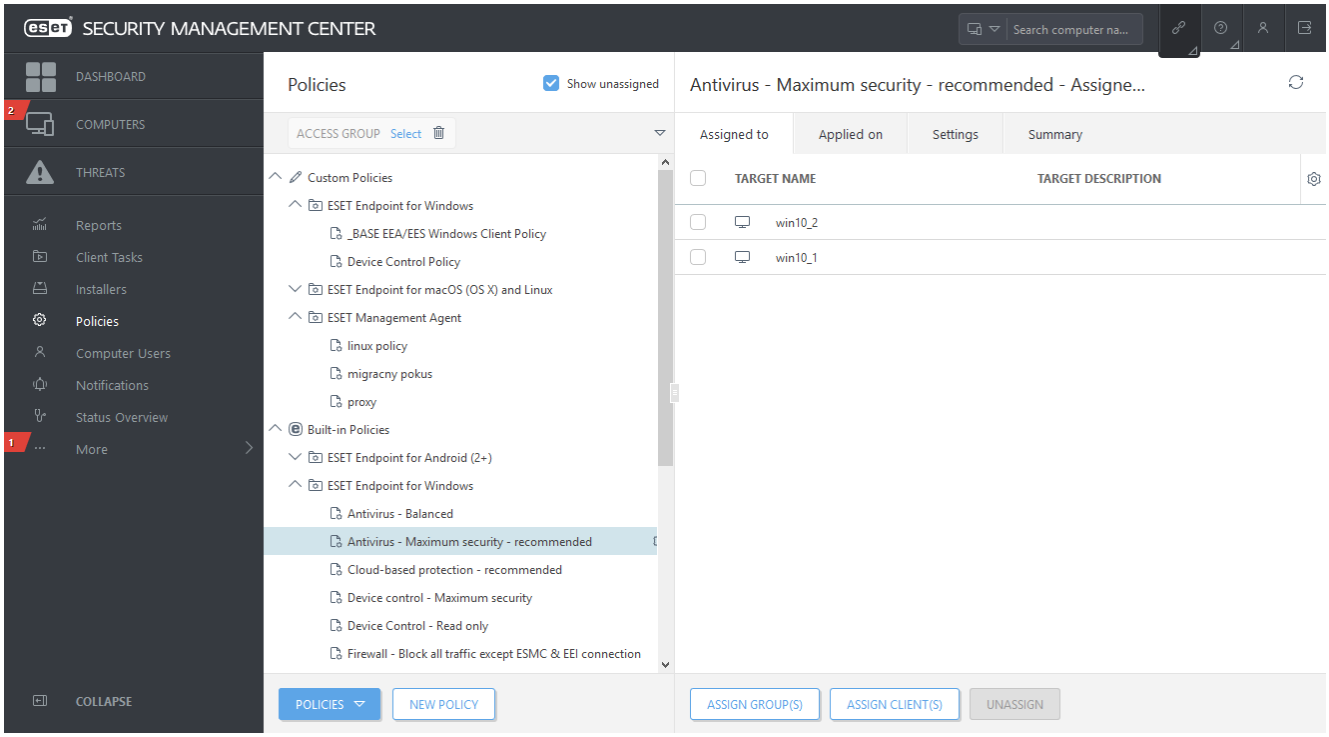
> **Illustrierte Anweisungen**
> Die folgenden Artikel in der ESET-Knowledgebase sind möglicherweise nur auf Englisch verfügbar:
> - Anwenden einer empfohlenen oder vordefinierten Policy für ESET Endpoint Antivirus mit ESMC

1. Öffnen Sie die ESMC-Web-Konsole.

2. Navigieren Sie zu **Policies** und erweitern Sie den Eintrag **Integrierte Policies** > **ESET Endpoint für Windows**.

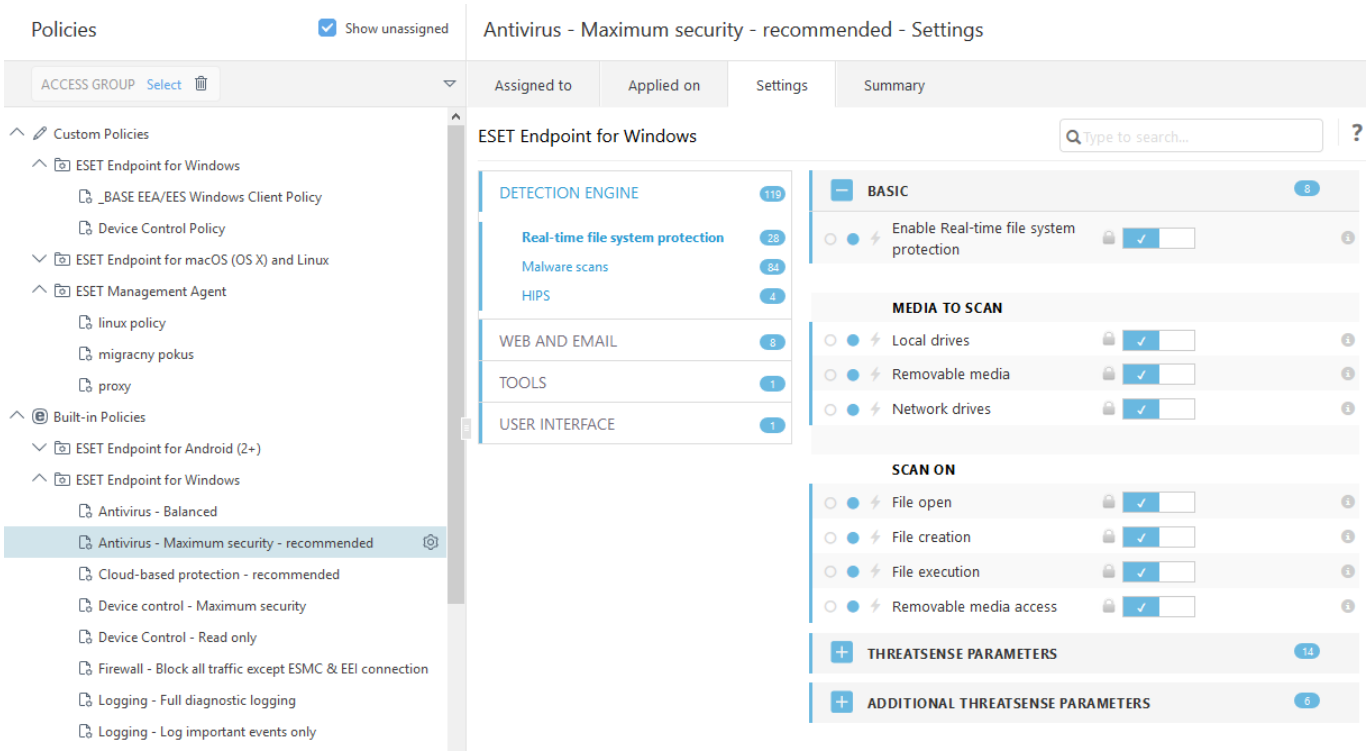
3. Klicken Sie auf **Antivirus - maximale Sicherheit - empfohlen**.

4. Klicken Sie in der Registerkarte **Zugewiesen zu** auf **Client(s) zuweisen** oder auf **Gruppe(n) zuweisen** und wählen Sie die Computer aus, für die Sie diese Policy anwenden möchten.



Um anzuzeigen, welche Einstellungen für diese Policy gelten, klicken Sie auf die Registerkarte **Einstellungen** und erweitern Sie die Struktur „Erweiterte Einstellungen“.

- Der blaue Punkt bedeutet, dass eine Einstellung für diese Policy geändert wurde
- Die Zahl im blauen Rahmen zeigt an, wie viele Einstellungen für diese Policy geändert wurden
- Weitere Infos zu ESMC-Policies



So konfigurieren Sie einen Mirror

ESET Endpoint Antivirus kann so konfiguriert werden, dass Kopien der Updatedateien für die Erkennungsroutine gespeichert und Updates an andere Workstations verteilt werden, auf denen ESET Endpoint Security oder ESET Endpoint Antivirus ausgeführt wird.

Konfigurieren von ESET Endpoint Antivirus als Mirror-Server für die Bereitstellung von Updates über einen internen HTTP-Server

1. Drücken Sie **F5**, um die erweiterten Einstellungen zu öffnen, und erweitern Sie den Eintrag **Update** > **Profile** > **Update-Mirror**.

2. Erweitern Sie den Eintrag **Updates** und vergewissern Sie sich, dass die Option **Automatisch wählen** unter **Modulupdates** aktiviert ist.

3. Erweitern Sie **Update-Mirror** und aktivieren Sie die Optionen **Update-Mirror erstellen** und **HTTP-Server aktivieren**.

Weitere Informationen finden Sie unter Update-Mirror.

Konfigurieren eines Mirror-Servers für die Bereitstellung von Updates über einen freigegebenen Netzwerkordner

1. Erstellen Sie einen freigegebenen Netzwerkordner auf einem lokalen oder einem Netzwerkgerät. Dieser Ordner muss für alle Benutzer, die ESET-Sicherheitslösungen verwenden, lesbar sein, und für das lokale Systemkonto beschreibbar sein.

2. Aktivieren Sie die Option **Update-Mirror erstellen** unter **Erweiterte Einstellungen** > **Update** > **Profile** > **Update-Mirror**.

3. Wählen Sie einen passenden **Speicherordner**, indem Sie auf **Löschen** und dann auf **Bearbeiten** klicken. Navigieren Sie zum erstellten freigegebenen Ordner und wählen Sie ihn aus.



Hinweis
Wenn Sie keine Modul-Updates über den internen HTTP-Server bereitstellen möchten, deaktivieren Sie die Option **Update-Mirror erstellen**.

Wie aktualisiere ich auf Windows 10 mit ESET Endpoint Antivirus



Warnung
Wir empfehlen dringend, Ihr ESET-Produkt zu aktualisieren und anschließend die aktuellen Modulupdates herunterzuladen, bevor Sie auf Windows 10 aktualisieren. Auf diese Weise sind Sie optimal geschützt, und Ihre Programmeinstellungen und Lizenzinformationen bleiben bei der Aktualisierung auf Windows 10 erhalten.

Version 7.x:

Klicken Sie unten auf den entsprechenden Link, um vor der Aktualisierung auf Windows 10 die neueste Version herunterzuladen und zu installieren:

ESET Endpoint Security 7 32-Bit herunterladen ESET Endpoint Antivirus 7 32-Bit herunterladen

ESET Endpoint Security 7 64-Bit herunterladen ESET Endpoint Antivirus 7 64-Bit herunterladen

Version 5.x:



Wichtig

Für die Version 5 der ESET Endpoint-Produkte gilt momentan der einfache Support. Dies bedeutet, dass die Builds nicht mehr öffentlich zum Download angeboten werden. Wir empfehlen dringend, ein Upgrade auf die neueste Version der ESET Endpoint-Produkte durchzuführen. Falls Sie Zugriff auf die MSI-Installationsprogramme brauchen, wenden Sie sich an den technischen ESET-Support, um weitere Hilfe zu erhalten.

Versionen in anderen Sprachen:

Wenn Sie nach einer Version Ihres ESET-Endpoint-Produkts in einer anderen Sprache suchen, besuchen Sie unsere Download-Seite.

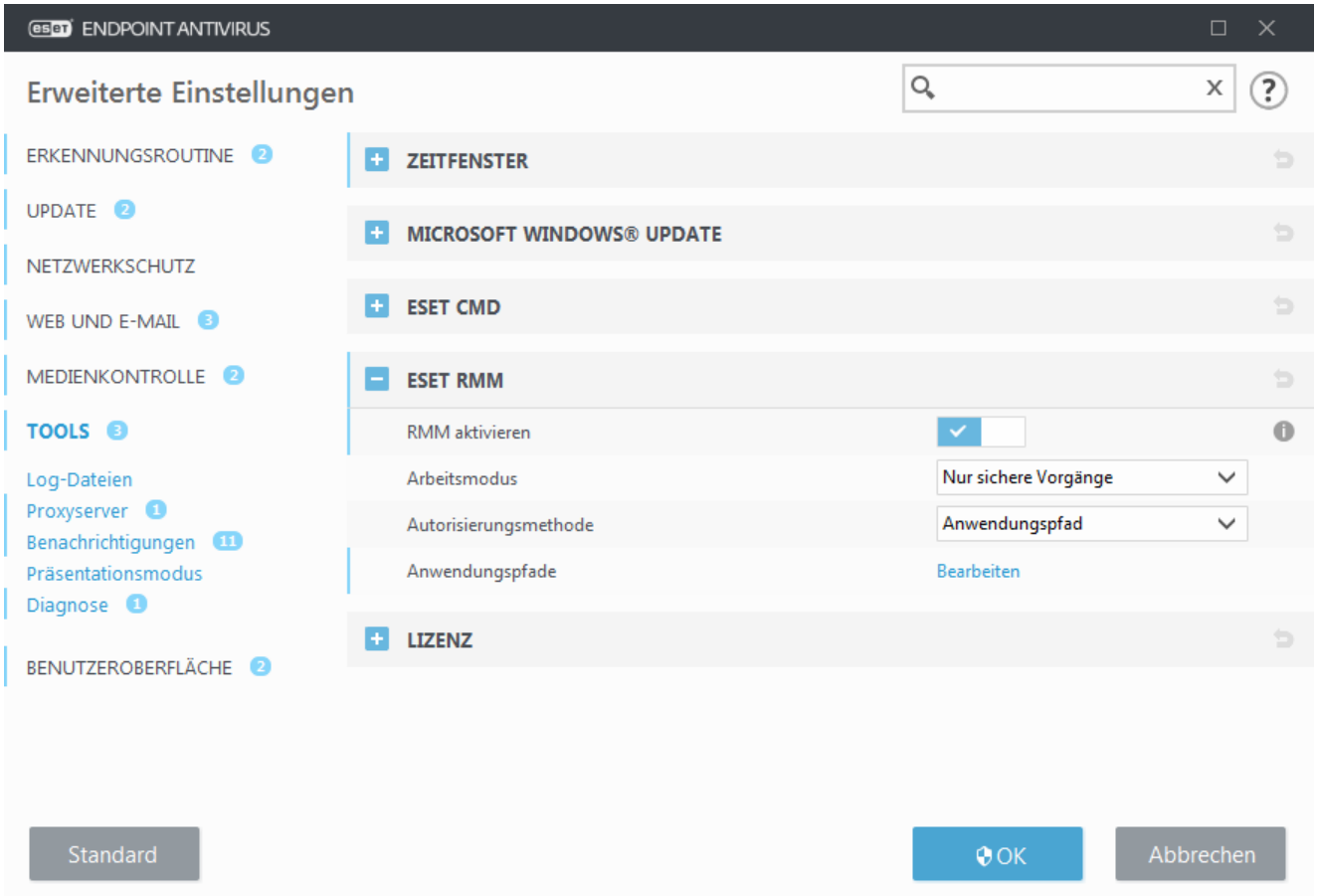


Hinweis

Weitere Informationen zur Kompatibilität von ESET-Unternehmensprodukten mit Windows 10.

Aktivieren der Remoteüberwachung und -verwaltung

Remoteüberwachung und -verwaltung (RMM) ist der Prozess der Beaufsichtigung und Überwachung von Softwaresystemen (z.B. auf Desktops, Servern und Mobilgeräten) mit einem lokal installierten Agenten, auf den über einen Management-Dienstanbieter zugegriffen wird. ESET Endpoint Antivirus kann ab Version 6.6.2028.0 per RMM verwaltet werden.



ESET RMM ist standardmäßig deaktiviert. Wenn Sie ESET RMM aktivieren möchten, drücken Sie **F5**, umauf die Erweiterten Einstellungen zuzugreifen, klicken Sie auf **Tools**, erweitern Sie **ESET RMM** und aktivieren Sie das Kontrollkästchen neben **RMM aktivieren**.

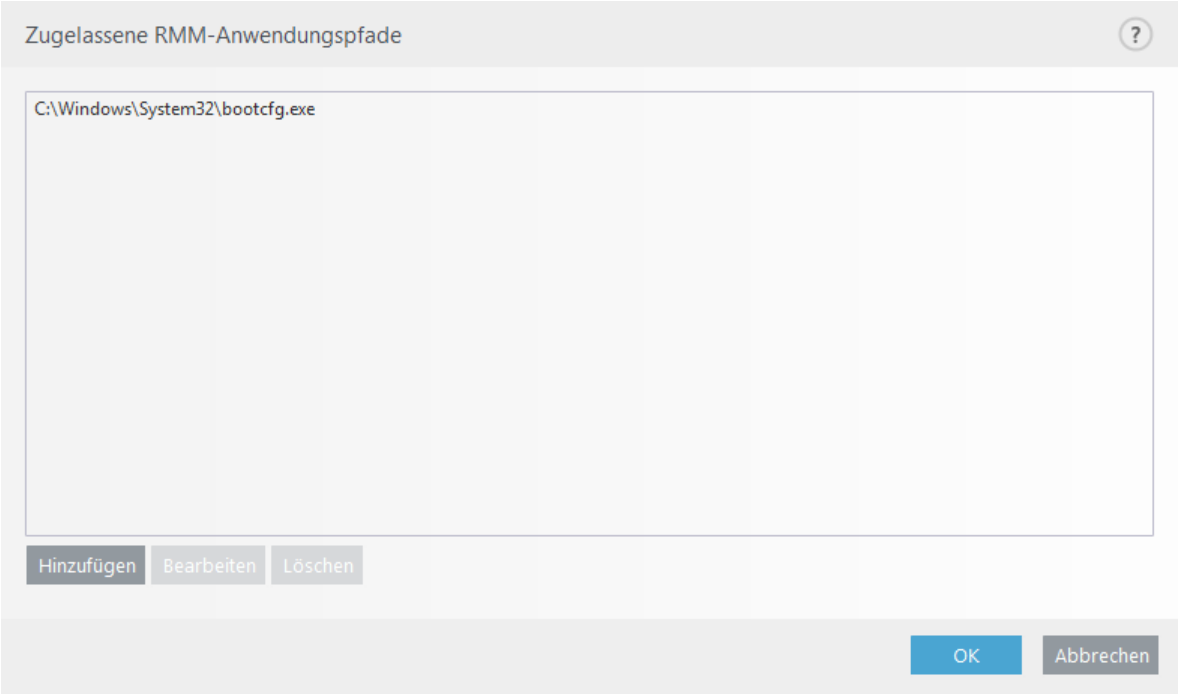
Arbeitsmodus – Wählen Sie **Nur sichere Vorgänge** aus, um die RMM-Schnittstelle für sichere und schreibgeschützte Vorgänge zu aktivieren. Wählen Sie **Alle Vorgänge** aus, falls Sie die RMM-Schnittstelle für alle Vorgänge aktivieren möchten.

Operation	Nur sichere Vorgänge	Alle Vorgänge
Anwendungsinformationen abrufen	✔	✔
Konfiguration abrufen	✔	✔
Lizenzinformationen abrufen	✔	✔
Logs abrufen	✔	✔
Schutzstatus abrufen	✔	✔
Updatestatus abrufen	✔	✔
Konfiguration festlegen		✔
Aktivierung starten		✔
Prüfung starten	✔	✔
Update starten	✔	✔

Autorisierungsmethode– Legen Sie die RMM-Autorisierungsmethode fest. Wenn Sie Autorisierung verwenden möchten, wählen Sie **Anwendungspfad** aus der Liste aus, wenn nicht, wählen Sie **Keine** aus.

Warnung
RMM sollte immer Autorisierung verwenden, um zu verhindern, dass Schadsoftware den ESET Endpoint-Schutz deaktivieren oder umgehen kann.

Anwendungspfade – Eine bestimmte Anwendung, die RMM ausführen darf. Wenn Sie **Anwendungspfad** als Autorisierungsmethode ausgewählt haben, klicken Sie auf **Bearbeiten**, um das Konfigurationsfenster **Zugelassene RMM-Anwendungspfade** zu öffnen.



Hinzufügen– Erstellen Sie einen neuen zugelassenen RMM-Anwendungspfad. Geben Sie den Pfad ein oder klicken Sie auf die Schaltfläche **…**, um eine Programmdatei auszuwählen.

Bearbeiten– Ändern Sie einen vorhandenen zugelassenen Pfad. Verwenden Sie **Bearbeiten**, wenn der Speicherort der Programmdatei in einen anderen Ordner verlegt wurde.

Löschen – Löschen Sie einen vorhandenen zugelassenen Pfad.

Bei der Standardinstallation von ESET Endpoint Antivirus ist die Datei ermm.exe im Endpunkt-Anwendungsverzeichnis enthalten (Standardpfad C*:\Program Files\ESET\ESET Security*). ermm.exe tauscht Daten mit RMM Plugin aus, das mit RMM Agent kommuniziert, das mit einem RMM Server verbunden ist.

- ermm.exe – von ESET entwickeltes Kommandozeilen-Dienstprogramm für die Verwaltung von Endpunkt-Produkten und die Kommunikation mit einem beliebigen RMM Plugin.

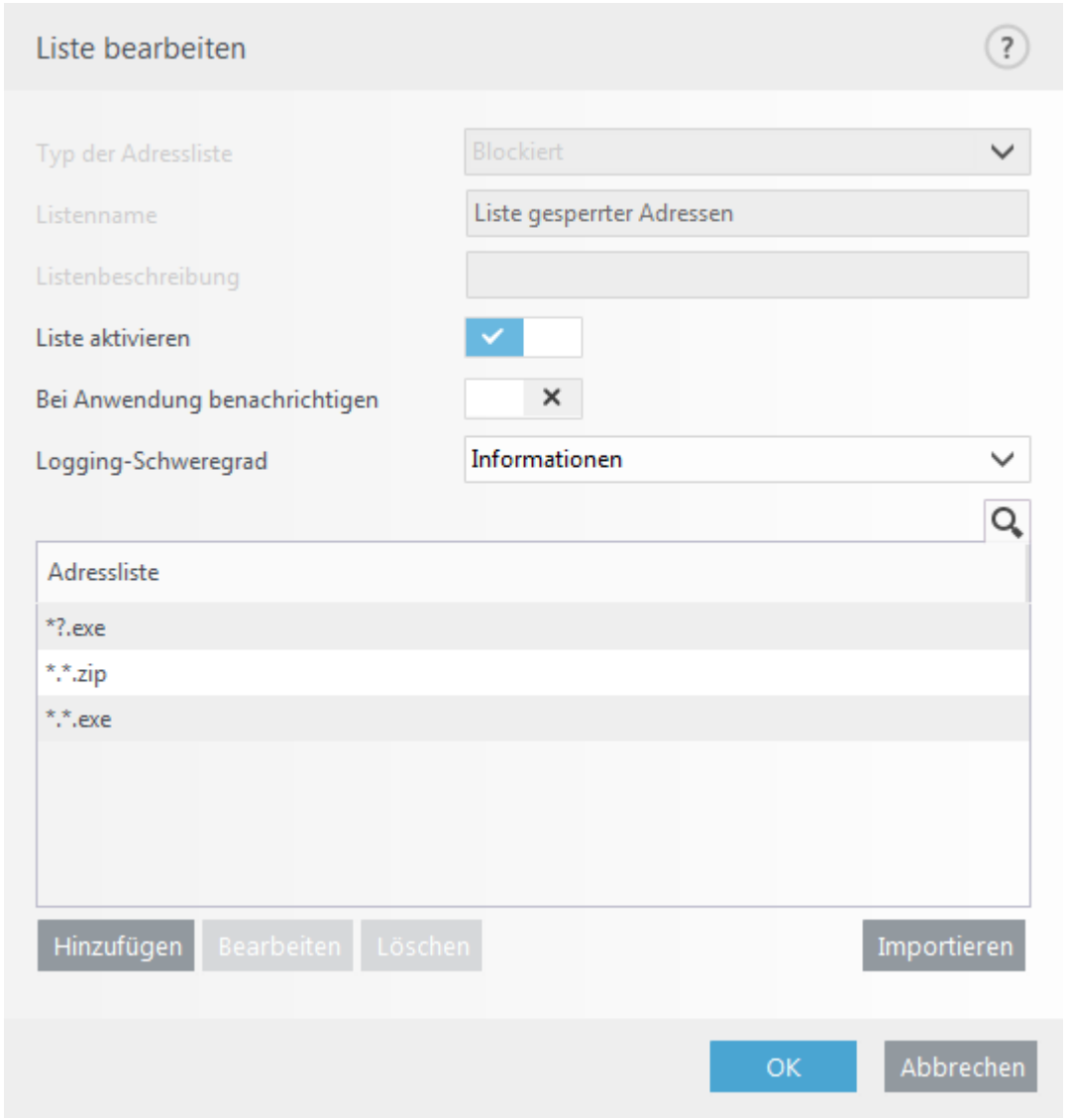
- RMM Plugin ist eine Drittanbieter-Anwendung, die lokal auf Endpoint Windows-Systemen läuft. Das Plugin wurde für die Kommunikation mit einem speziellen RMM Agent (wie z.B. ausschließlich Kaseya) und ermm.exe entwickelt.

- RMM Plugin ist eine Drittanbieter-Anwendung (z.B. von Kaseya), die lokal auf Endpoint Windows-Systemen läuft. Der Agent kommuniziert mit RMM Plugin und RMM Server.

Download bestimmter Dateitypen aus dem Internet blockieren

Falls Sie den Download bestimmter Dateitypen (z. B. exe, pdf oder zip) aus dem Internet verbieten möchten, können Sie unter URL-Adressverwaltung eine Kombination von Platzhaltern eingeben. Drücken Sie die Taste F5, um die erweiterten Einstellungen zu öffnen. Klicken Sie auf Web und E-Mail > Web-Schutz und erweitern Sie die URL-Adressverwaltung. Klicken Sie neben der Adressliste auf „Bearbeiten“.

Wählen Sie in der Adressliste entweder „Liste blockierter Adressen“ aus und klicken Sie auf Bearbeiten, oder klicken Sie auf „Hinzufügen“, um eine neue Liste zu erstellen. Daraufhin wird ein neues Fenster geöffnet. Falls Sie eine neue Liste erstellen, wählen Sie „Blockiert“ im Dropdownmenü „Typ der Adressliste“ aus, und geben Sie einen Namen für die Liste ein. Falls Sie beim Zugriff auf einen Dateityp aus der aktuellen Liste benachrichtigt werden möchten, wählen Sie den Schieberegler „Bei Anwendung benachrichtigen“ aus. Wählen Sie einen Schweregrad für die Protokollierung im Dropdownmenü aus. Remote Administrator kann Einträge mit dem Schweregrad „Warnung“ erfassen.



Klicken Sie auf „Hinzufügen“, um eine Maske für Dateitypen anzugeben, die Sie vom Download ausschließen möchten. Geben Sie die vollständige URL ein, um den Download einer bestimmten Datei von einer bestimmten Webseite zu blockieren, z. B. http://beispiel.com/datei.exe. Mit Hilfe von Platzhaltern können Sie Gruppen von Dateien ausschließen. Dabei steht ein Fragezeichen (?) für genau ein beliebiges Zeichen, ein Sternchen (*) steht

für beliebig viele Zeichen oder „kein Zeichen“. Die Maske „*/*.zip“ schließt beispielsweise alle zip-komprimierten Dateien vom Download aus.

Sie können den Download bestimmter Dateitypen mit dieser Methode nur blockieren, wenn die Dateierweiterung in der Datei-URL enthalten ist. Wenn die Website Download-URLs verwendet, zum Beispiel *www.example.com/download.php?fileid=42*, dann wird die Datei unter diesem Link trotzdem heruntergeladen, auch wenn sie eine von Ihnen blockierte Erweiterung hat.

Minimieren der ESET Endpoint Antivirus-Benutzeroberfläche

Für die Remoteverwaltung können Sie eine vordefinierte Sichtbarkeits-Policy verwenden.

Führen Sie die Schritte andernfalls manuell aus:

1. Drücken Sie **F5**, um die erweiterten Einstellungen zu öffnen, und erweitern Sie **Benutzeroberfläche** > **Elemente der Benutzeroberfläche**.

2. Legen Sie unter **Startmodus** den gewünschten Wert fest. Weitere Informationen zu Startmodi.

3. Deaktivieren Sie die Optionen **Startbildschirm anzeigen** und **Hinweistöne wiedergeben**.

4. Konfigurieren Sie Benachrichtigungen.

5. Konfigurieren Sie Anzuzeigende Hinweise.

6. Konfigurieren Sie Bestätigungsnachrichten.

7. Konfigurieren Sie Warnungen und Hinweisfenster.

Endbenutzer-Lizenzvereinbarung

WICHTIG: Vor dem Herunterladen, Installieren, Kopieren oder Verwenden des Produkts lesen Sie bitte die folgenden Nutzungsbedingungen. **DURCH DAS HERUNTERLADEN, INSTALLIEREN, KOPIEREN ODER VERWENDEN DER SOFTWARE ERKLÄREN SIE SICH MIT DEN NUTZUNGSBEDINGUNGEN EINVERSTANDEN UND AKZEPTIEREN DIE DATENSCHUTZERKLÄRUNG.**

Endbenutzer-Lizenzvereinbarung

Diese Endbenutzer-Lizenzvereinbarung (die "Vereinbarung") zwischen ESET, spol. s r. o., mit Sitz in Einsteinova 24, 851 01 Bratislava, Slovak Republic, Handelsregistereintrag 3586/B in der Rubrik Sro beim Amtsgericht Bratislava I, Firmennummer 31333532, (im Folgenden "ESET" oder "Anbieter") und Ihnen, einer natürlichen oder juristischen Person ("Sie" oder der "Endbenutzer"), berechtigt Sie zur Nutzung der in Abschnitt 1 dieser Vereinbarung definierten Software. Die in Abschnitt 1 dieser Vereinbarung definierte Software darf unter den im Folgenden aufgeführten Bedingungen auf einem Datenträger gespeichert, per E-Mail versendet, aus dem Internet oder von Servern des Anbieters heruntergeladen oder auf andere Weise beschafft werden.

DIESES DOKUMENT IST KEIN KAUFVERTRAG, SONDERN EINE VEREINBARUNG ÜBER DIE RECHTE DES ENDBENUTZERS. Der Anbieter bleibt Eigentümer des Exemplars der Software und, soweit vorhanden, des

physischen Mediums, auf dem die Software für den Verkauf vorliegt, sowie aller Kopien der Software, zu deren Erstellung der Endbenutzer unter den Bedingungen dieser Vereinbarung berechtigt ist.

Durch Klicken auf die Schaltfläche "Ich stimme zu" oder "Ich stimme zu...“ beim Installieren, Herunterladen, Kopieren oder Verwenden der Software erklären Sie sich mit den Bestimmungen und Bedingungen dieser Vereinbarung einverstanden. Wenn Sie mit einer der Bestimmungen dieser Vereinbarung nicht einverstanden sind, klicken Sie auf die Schaltfläche "Ablehnen" oder "Ich stimme nicht zu". Brechen Sie den Download oder die Installation der Software ab, vernichten oder geben Sie die Software, das Installationsmedium, die zugehörige Dokumentation und den Erwerbsnachweis an den Anbieter oder an dem Ort, an dem Sie die Software erworben haben, zurück.

MIT DER NUTZUNG DER SOFTWARE ZEIGEN SIE AN, DASS SIE DIESE VEREINBARUNG GELESEN UND VERSTANDEN HABEN UND DASS SIE DIESER VEREINBARUNG ZUGESTIMMT HABEN.

1. **Software**. Mit "Software" wird in dieser Vereinbarung bezeichnet: (i) das mit dieser Vereinbarung ausgelieferte Computerprogramm und all dessen Komponenten; (ii) alle Inhalte der Disks, CD-ROMs, DVDs, E-Mails und Anlagen oder sonstiger Medien, denen diese Vereinbarung beigefügt ist, einschließlich der Objektcodeform der Software, die auf einem Datenträger, in einer E-Mail oder durch Herunterladen im Internet bereitgestellt wurde; (iii) alle verwandten erklärenden Schriftdokumente und andere Dokumentationen in Bezug auf die Software, insbesondere Beschreibungen der Software und ihrer Spezifikationen, jede Beschreibung der Softwareeigenschaften oder -funktionen, Beschreibungen der Betriebsumgebung, in der die Software verwendet wird, Anweisungen zu Installation und zum Einsatz der Software ("Dokumentation"); (iv) Kopien der Software, Patches für mögliche Softwarefehler, Hinzufügungen zur Software, Erweiterungen der Software, geänderte Versionen und Aktualisierungen der Softwarebestandteile, sofern zutreffend, deren Nutzung der Anbieter gemäß Artikel 3 dieser Vereinbarung gewährt. Die Software wird ausschließlich in Form von ausführbarem Objektcode ausgeliefert.

2. **Installation, Computer und ein Lizenzschlüssel**. Die auf einem Datenträger bereitgestellte, per E-Mail verschickte, aus dem Internet oder von den Servern des Anbieters heruntergeladene oder auf anderem Weg beschaffte Software muss installiert werden. Sie müssen die Software auf einem korrekt konfigurierten Computer installieren, der die in der Dokumentation genannten Mindestvoraussetzungen erfüllt. Die Installationsmethode ist in der Dokumentation beschrieben. Auf dem Computer, auf dem Sie die Software installieren, darf kein Computerprogramm und keine Hardware vorhanden sein, die sich negativ auf die Software auswirken könnte. Die Bezeichnung "Computer" erstreckt sich auf Hardware inklusive, jedoch nicht ausschließlich, Personal Computer, Laptops, Arbeitsstationen, Palmtop-Computer, Smartphones, tragbare elektronische Geräte oder andere elektronische Geräte, für die die Software entwickelt wurde und auf denen die Software installiert und/oder eingesetzt wird. Der Begriff "Lizenzschlüssel" bezeichnet die eindeutige Abfolge von Symbolen, Buchstaben und Zahlen, die dem Endbenutzer bereitgestellt wird, um die legale Nutzung der Software in der jeweiligen Version bzw. die Verlängerung der Lizenz gemäß dieser Vereinbarung zu ermöglichen.

3. **Lizenz**. Unter der Voraussetzung, dass Sie dieser Vereinbarung zugestimmt haben und sämtliche darin enthaltenen Bestimmungen einhalten, gewährt Ihnen der Anbieter die folgenden Rechte (die "Lizenz"):

a) **Installation und Nutzung**. Sie erhalten das nicht exklusive und nicht übertragbare Recht, die Software auf der Festplatte eines Computers oder einem ähnlichen Medium zur dauerhaften Datenspeicherung zu installieren, die Software im Arbeitsspeicher eines Computers zu speichern und die Software auf Computern zu implementieren, zu speichern und anzuzeigen.

b) **Anzahl der Lizenzen.** Das Nutzungsrecht für die Software ist durch die Anzahl der Endbenutzer beschränkt. Unter einem "Endbenutzer" ist Folgendes zu verstehen: (i) die Installation der Software auf einem Computer; wenn der Umfang einer Lizenz sich nach der Anzahl von Postfächern richtet, ist ein Endbenutzer (ii) ein Computerbenutzer, der E-Mail über ein E-Mail-Programm empfängt. Wenn das E-Mail-Programm E-Mail

empfängt und diese anschließend automatisch an mehrere Benutzer weiterleitet, richtet sich die Anzahl der Endbenutzer nach der tatsächlichen Anzahl von Benutzern, an die auf diesem Weg E-Mail-Nachrichten gesendet werden. Wenn ein Mailserver die Funktion eines E-Mail-Gateways ausführt, entspricht die Zahl der Endbenutzer der Anzahl von Mailservern, für die dieses Gateway Dienste bereitstellt. Wenn mehrere E-Mail-Adressen (z. B. durch Aliasnamen) von einem Benutzer verwendet werden und nur ein Benutzer über diese Adressen E-Mail empfängt, während auf Clientseite keine E-Mail-Nachrichten automatisch an mehrere Benutzer verteilt werden, ist nur eine Lizenz für einen Computer erforderlich. Die gleichzeitige Nutzung derselben Lizenz auf mehreren Computern ist untersagt. Der Endbenutzer darf den Lizenzschlüssel für die Software nur in dem Umfang eingeben, für den er die entsprechende Anzahl von Lizenzen zur Nutzung der Software vom Anbieter erworben hat. Der Lizenzschlüssel ist vertraulich, und die Lizenz darf nicht mit Drittparteien geteilt oder von Drittparteien genutzt werden, sofern dies nicht in dieser Vereinbarung oder vom Anbieter erlaubt wurde. Benachrichtigen Sie den Anbieter unverzüglich, falls Ihr Lizenzschlüssel kompromittiert wurde.

c) **Business Edition.** Für die Verwendung der Software auf E-Mail-Servern, E-Mail-Relays, E-Mail- oder Internet-Gateways ist die Business Edition der Software erforderlich.

d) **Laufzeit der Lizenz.** Ihr Nutzungsrecht für die Software ist zeitlich beschränkt.

e) **OEM-Software.** OEM-Software darf ausschließlich auf dem Computer genutzt werden, mit dem Sie sie erhalten haben. Eine Übertragung auf einen anderen Computer ist nicht gestattet.

f) **Nicht für den Wiederverkauf bestimmte Software und Testversionen.** Nicht für den Wiederverkauf („not for resale“, NFR) oder als Testversion bereitgestellte Software darf nicht veräußert, sondern ausschließlich zum Vorführen oder Testen der Softwarefunktionen verwendet werden.

g) **Ablauf und Kündigung der Lizenz**. Die Lizenz läuft automatisch zum Ende des jeweiligen Lizenzzeitraums aus. Sollten Sie eine Ihrer Pflichten aus dieser Vereinbarung verletzen, ist der Anbieter berechtigt, diese außerordentlich zu kündigen und, ggf. auf dem Rechtsweg, etwaige weitere Ansprüche geltend zu machen. Bei Ablauf oder Kündigung der Lizenz müssen Sie die Software und ggf. alle Sicherungskopien sofort löschen, zerstören oder auf eigene Kosten an ESET oder das Geschäft zurückgeben, in dem Sie die Software erworben haben. Nach Ablauf oder Kündigung der Lizenz ist der Anbieter berechtigt, das Recht des Endbenutzers zur Nutzung der Softwarefunktionen zurückzuziehen, für die eine Verbindung zu Servern des Anbieters oder zu Servern von Drittanbietern erforderlich ist.

4. **Funktionen mit Datenerfassung und Anforderungen an die Internetverbindung.** Für den korrekten Betrieb benötigt die Software eine Internetverbindung und muss in der Lage sein, sich in regelmäßigen Abständen mit den Servern des Anbieters, Servern einer Drittpartei und entsprechenden Datenerfassungen gemäß der Datenschutzrichtlinie zu verbinden. Die Verbindung mit dem Internet und den entsprechenden Datenerfassungen ist für die folgenden Funktionen der Software erforderlich:

a) **Software-Updates.** Der Anbieter hat das Recht, von Zeit zu Zeit Aktualisierungen für die Software („Updates“) bereitzustellen, ist hierzu jedoch nicht verpflichtet. Diese Funktion ist in den Standardeinstellungen der Software aktiviert. Die Updates werden also automatisch installiert, sofern der Endbenutzer dies nicht deaktiviert hat. Zur Bereitstellung von Aktualisierungen muss die Echtheit der Lizenz überprüft werden. Dazu gehören Informationen über den Computer und/oder die Plattform, auf der die Software installiert wurde, in Übereinstimmung mit der Datenschutzrichtlinie.

b) **Weiterleitung von eingedrungener Schadsoftware und anderen Informationen an den Anbieter**. Die Software enthält Funktionen zur Erfassung neuer Computerviren und anderer schädlicher Computerprogramme sowie von verdächtigen, problematischen, potenziell unsicheren Objekten wie Dateien, URLs, IP-Pakete und Ethernet-Rahmen (im Folgenden "Infiltrationen"). Diese Daten werden zusammen mit Informationen über den Installationsprozess und die Plattform, auf der die Software installiert ist, oder anderen Informationen über

Betrieb und Funktionsweise der Software (im Folgenden "Informationen") an den Anbieter übertragen. Die Informationen und die Infiltrationen können Daten über den Endbenutzer oder andere Benutzer des Computers enthalten, auf dem die Software installiert ist (inklusive zufällig oder unbeabsichtigt erfasste personenbezogene Daten), sowie von eingedrungener Schadsoftware betroffene Dateien mit den entsprechenden Metadaten.

Die folgenden Funktionen der Software können Informationen und Infiltrationen sammeln:

i. Das LiveGrid Reputationssystem sammelt und sendet Einweg-Hashes im Zusammenhang mit eingedrungener Schadsoftware an den Anbieter. Diese Funktion ist in den Standardeinstellungen der Software aktiviert.

ii. Das LiveGrid-Reputationssystem erfasst Infiltrationen und überträgt diese zusammen mit den entsprechenden Metadaten und anderen Informationen an den Anbieter. Diese Funktion kann vom Endbenutzer bei der Installation der Software aktiviert werden.

Der Anbieter verwendet die erhaltenen Informationen und Infiltrationen ausschließlich zur Analyse und Erforschung der Infiltrationen, zur Verbesserung der Software und zur Überprüfung der Echtheit von Lizenzen und unternimmt angemessene Anstrengungen, um die erhaltenen Infiltrationen und Informationen zu schützen. Wenn diese Softwarefunktion aktiviert wird, darf der Anbieter gemäß der Datenschutzrichtlinie und gemäß geltender Gesetze Infiltrationen und Informationen erfassen und verarbeiten. Sie können diese Funktionen jederzeit deaktivieren.

Für die in dieser Vereinbarung festgelegten Zwecke werden Daten gesammelt, verarbeitet und gespeichert, mit denen der Anbieter Sie gemäß der Datenschutzrichtlinie identifizieren kann. Für die in dieser Vereinbarung festgelegten Zwecke werden Daten gesammelt, verarbeitet und gespeichert, mit denen der Anbieter Sie gemäß der Datenschutzrichtlinie identifizieren kann. Sie stimmen zu, dass der Anbieter mit eigenen Mitteln überprüfen darf, ob Sie die Software in Übereinstimmung mit den Bestimmungen dieser Vereinbarung nutzen. Sie erkennen an, dass es für die in dieser Vereinbarung festgelegten Zwecke erforderlich ist, dass Ihre Daten zwischen der Software und den Computersystemen des Anbieters bzw. denen seiner Geschäftspartner im Rahmen des Distributions- und Verteilungsnetzwerks des Anbietersübertragen werden, um die Funktionstüchtigkeit der Software und die Genehmigung zu deren Nutzung sowie die Rechte des Anbieters zu schützen.

Mit Abschluss dieser Vereinbarung willigen Sie zudem in die Übertragung, Verarbeitung und Speicherung Ihrer personenbezogenen Daten durch den Anbieter bzw. seine Geschäftspartner ein, soweit eine solche Nutzung zur Abrechnung und zur Erfüllung dieser Vereinbarung und zum Übertragen von Benachrichtigungen auf Ihren Computer erforderlich ist. Sie stimmen dem Empfang von Benachrichtigungen und Nachrichten zu, inklusive, jedoch nicht ausschließlich, Marketinginformationen.

Details zur Privatsphäre, zum Schutz persönlicher Daten und zu Ihren Rechten als betroffene Person finden Sie in der Datenschutzrichtlinie auf der Webseite des Anbieters oder direkt beim Installationsprozess. Sie finden diese Informationen außerdem im Hilfebereich der Software.

5. **Ausübung der Rechte des Endbenutzers**. Sie müssen Ihre Rechte als Endbenutzer selbst oder gegebenenfalls über Ihre Angestellten ausüben. Sie dürfen die Software ausschließlich zur Gewährleistung der Arbeitsfähigkeit und zum Schutz der Computer verwenden, für die Sie eine Lizenz erworben haben.

6. **Beschränkungen der Rechte.** Es ist untersagt, die Software zu kopieren, zu verbreiten oder aufzuteilen. Außerdem dürfen keine abgeleiteten Versionen erstellt werden. Für die Nutzung der Software gelten die folgenden Einschränkungen:

(a) Sie dürfen eine Kopie der Software auf einem Medium zur dauerhaften Speicherung als Sicherungskopie erstellen, vorausgesetzt die Sicherungskopien werden nicht auf einem anderen Computer installiert oder verwendet. Das Erstellen jeder weiteren Kopie der Software verstößt gegen diese Vereinbarung.

(b) Jegliche von den Bestimmungen dieser Vereinbarung abweichende Nutzung, Modifikation, Übersetzung oder Reproduktion der Software sowie die Einräumung von Rechten zur Nutzung der Software oder von Kopien der Software ist untersagt.

(c) Die Software darf nicht an andere Personen verkauft, sublizenziert oder vermietet werden. Ebenso darf die Software nicht von einer anderen Person gemietet, einer anderen Person ausgeliehen oder zur gewerbsmäßigen Erbringung von Dienstleistungen verwendet werden.

(d) Der Quellcode der Software darf nicht durch Reverse-Engineering analysiert, dekompiliert oder disassembliert oder auf andere Weise beschafft werden, soweit eine solche Beschränkung nicht ausdrücklich gesetzlichen Bestimmungen widerspricht.

(e) Sie verpflichten sich, die Software nur in Übereinstimmung mit allen am Verwendungsort geltenden gesetzlichen Bestimmungen zu verwenden, insbesondere gemäß den Beschränkungen, die sich aus dem Urheberrecht und anderen Rechten an geistigem Eigentum ergeben.

(f) Sie verpflichten sich, die Software und ihre Funktionen nur so zu nutzen, dass der Zugriff anderer Endbenutzer auf die betreffenden Dienste nicht eingeschränkt wird. Der Anbieter behält sich das Recht vor, den Leistungsumfang gegenüber einzelnen Endbenutzern einzuschränken, damit die Dienste von möglichst vielen Endbenutzern verwendet werden können. Dies kann auch bedeuten, dass die Nutzung beliebiger Softwarefunktionen vollständig gesperrt wird und dass Daten sowie Informationen im Zusammenhang mit bestimmten Funktionen der Software von den Servern des Anbieters bzw. Dritter gelöscht werden.

(g) Sie verpflichten sich hiermit, keine Aktivitäten im Zusammenhang mit dem Lizenzschlüssel auszuführen, die den Bestimmungen dieser Vereinbarung widersprechen oder die dazu führen, dass der Lizenzschlüssel an unbefugte Personen weitergegeben wird, z. B. durch die Übertragung von benutzten oder nicht benutzten Lizenzschlüsseln in jeglicher Form oder die nicht autorisierte Verteilung von duplizierten oder generierten Lizenzschlüsseln oder die Nutzung der Software im Zusammenhang mit einem Lizenzschlüssel, der aus einer anderen Quelle als direkt vom Anbieter beschafft wurde.

7. **Urheberrecht**. Die Software und alle Rechte einschließlich des Rechtstitels und der geistigen Eigentumsrechte daran sind Eigentum von ESET und/oder seiner Lizenzgeber. Sie unterliegen dem Schutz der Bestimmungen internationaler Abkommen und aller sonstigen geltenden Gesetze des Landes, in dem die Software verwendet wird. Die Struktur, die Aufteilung und der Code der Software sind Geschäftsgeheimnisse und vertrauliche Informationen von ESET und/oder seiner Lizenzgeber. Die Software darf nicht kopiert werden, wobei lediglich die in Abschnitt 6(a) angegebene Ausnahme gilt. Alle gemäß dieser Vereinbarung zulässigen Kopien müssen dieselben Urheberrechts- und Eigentümerhinweise wie die ursprüngliche Software enthalten. Wenn Sie in Verstoß gegen die Bestimmungen dieser Vereinbarung Quellcode durch Reverse-Engineering analysieren, dekompilieren oder disassemblieren oder versuchen, sich den Quellcode auf andere Weise zu beschaffen, gehen automatisch sämtliche dadurch gewonnenen Informationen unwiderruflich und unmittelbar in das Eigentum des Anbieters über. Weiterhin ist der Anbieter in diesem Fall berechtigt, etwaige weitere Ansprüche aus Ihrem Verstoß gegen diese Vereinbarung geltend zu machen.

8. **Rechtevorbehalt**. Mit Ausnahme der Rechte, die Ihnen als Endbenutzer der Software in dieser Vereinbarung ausdrücklich gewährt werden, behält sich der Anbieter alle Rechte an der Software vor.

9. **Versionen in verschiedenen Sprachen/auf mehreren Datenträgern, mehrere Exemplare**. Wenn die Software mehrere Plattformen oder Sprachen unterstützt, oder wenn Sie mehrere Exemplare der Software erhalten haben, darf die Software nur auf derjenigen Anzahl von Computern und nur in den Versionen verwendet werden, für die Sie eine Lizenz erworben haben. Es dürfen keine Versionen oder Kopien der Software, die von Ihnen nicht verwendet werden, an andere Personen verkauft, vermietet, sublizenziert, verliehen oder auf diese übertragen werden.

10. **Beginn und Gültigkeitsdauer der Vereinbarung**. Diese Vereinbarung tritt an dem Tag in Kraft, an dem Sie sich mit ihren Bestimmungen einverstanden erklären. Sie können diese Vereinbarung jederzeit kündigen, indem Sie die Software, alle Sicherungskopien und, falls vorhanden, alle vom Anbieter oder seinen Geschäftspartnern zur Verfügung gestellten zugehörigen Materialien dauerhaft löschen, sie zerstören bzw. auf eigene Kosten zurückgeben. Unabhängig von der Gültigkeitsdauer dieser Vereinbarung und der Art und Weise ihres Ablaufs bzw. ihrer Kündigung behalten die Bestimmungen der Abschnitte 7, 8, 11, 13, 19 und 21 auf unbegrenzte Zeit ihre Gültigkeit.

11. **AUSDRÜCKLICHE ERKLÄRUNGEN DES ENDBENUTZERS**. ALS ENDBENUTZER ERKENNEN SIE AN, DASS DIE SOFTWARE IM JEWEILIGEN IST-ZUSTAND UND OHNE JEGLICHE AUSDRÜCKLICHE ODER KONKLUDENTE GEWÄHRLEISTUNG BEREITGESTELLT WIRD, SOWEIT DIES IM RAHMEN DER GELTENDEN GESETZE ZULÄSSIG IST. WEDER DER ANBIETER NOCH SEINE LIZENZGEBER ODER DIE RECHTEINHABER GEWÄHREN AUSDRÜCKLICHE ODER KONKLUDENTE ZUSICHERUNGEN ODER GEWÄHRLEISTUNGEN, INSBESONDERE KEINE ZUSICHERUNGEN HINSICHTLICH DER MARKTGÄNGIGKEIT, DER EIGNUNG FÜR EINEN BESTIMMTEN ZWECK ODER DER NICHTVERLETZUNG VON PATENTEN, URHEBER- UND MARKENRECHTEN ODER SONSTIGEN RECHTEN DRITTER. ES BESTEHT VON SEITEN DES ANBIETERS ODER DRITTER KEINERLEI GEWÄHRLEISTUNG, DASS DIE IN DER SOFTWARE ENTHALTENEN FUNKTIONEN IHREN ANFORDERUNGEN ENTSPRECHEN ODER DASS DIE SOFTWARE STÖRUNGS- UND FEHLERFREI AUSGEFÜHRT WIRD. SIE ÜBERNEHMEN DIE VOLLE VERANTWORTUNG UND DAS VOLLE RISIKO HINSICHTLICH DER AUSWAHL DER SOFTWARE ZUM ERREICHEN DER VON IHNEN BEABSICHTIGTEN ERGEBNISSE SOWIE FÜR INSTALLATION UND NUTZUNG DER SOFTWARE UND DEN MIT DIESER ERZIELTEN ERGEBNISSEN.

12.**Keine weiteren Verpflichtungen**. Aus dieser Vereinbarung ergeben sich für den Anbieter und seine Lizenzgeber keine weiteren Verpflichtungen außer den explizit aufgeführten.

13. **HAFTUNGSAUSSCHLUSS**. SOWEIT IM RAHMEN DER GELTENDEN GESETZE ZULÄSSIG, ÜBERNEHMEN DER ANBIETER, SEINE ANGESTELLTEN UND SEINE LIZENZGEBER KEINERLEI HAFTUNG FÜR ENTGANGENE GEWINNE, ERTRÄGE ODER VERKÄUFE. VON DER HAFTUNG AUSGESCHLOSSEN SIND AUSSERDEM DATENVERLUSTE, BESCHAFFUNGSKOSTEN FÜR ERSATZTEILE ODER DIENSTE, SACH- UND PERSONENSCHÄDEN, GESCHÄFTSUNTERBRECHUNGEN, DER VERLUST VON GESCHÄFTSINFORMATIONEN SOWIE JEGLICHE ANDERE NEBEN-, VERMÖGENS- ODER FOLGESCHÄDEN, DIE INFOLGE DER NUTZUNG ODER UNMÖGLICHKEIT DER NUTZUNG DER SOFTWARE ENTSTEHEN. DA IN BESTIMMTEN LÄNDERN UND UNTER BESTIMMTEN GESETZEN EIN HAFTUNGSAUSSCHLUSS NICHT ZULÄSSIG IST, EINE HAFTUNGSBESCHRÄNKUNG JEDOCH MÖGLICH, BESCHRÄNKT SICH DIE HAFTUNG DES ANBIETERS, SEINER ANGESTELLTEN UND LIZENZGEBER AUF DEN FÜR DIE LIZENZ ENTRICHTETEN PREIS.

14. Gesetzlich verankerte Verbraucherrechte haben im Konfliktfall Vorrang vor den Bestimmungen dieser Vereinbarung.

15. **Technischer Support**. ESET bzw. die von ESET beauftragten Dritten erbringen jeglichen technischen Support ausschließlich nach eigenem Ermessen und ohne diesbezügliche Zusicherungen oder Gewährleistungen. Endbenutzer sind verpflichtet, vor der Inanspruchnahme von Supportleistungen eine Sicherungskopie aller vorhandenen Daten, Softwareanwendungen und sonstigen Programme zu erstellen. ESET bzw. die von ESET beauftragten Dritten übernehmen keinerlei Haftung für Datenverluste, Sach- und Vermögensschäden (insb. Schäden an Software und Hardware) oder entgangene Gewinne infolge der Erbringung von Supportleistungen. ESET bzw. die von ESET beauftragten Dritten sichern nicht zu, dass ein bestimmtes Problem auf dem Wege des technischen Support gelöst werden kann, und behalten sich das Recht vor, die Arbeit an einem Problem ggf. einzustellen. ESET behält sich das Recht vor, die Erbringung von Supportleistungen nach eigenem Ermessen vorübergehend auszusetzen, ganz einzustellen oder im konkreten Einzelfall abzulehnen. Für die Bereitstellung des technischen Supports sind unter Umständen Lizenzinformationen, Informationen und andere Daten gemäß der Datenschutzrichtlinie erforderlich.

16. **Übertragung der Lizenz**. Die Software darf von einem Computersystem auf ein anderes übertragen werden,

sofern dabei nicht gegen Bestimmungen dieser Vereinbarung verstoßen wird. Sofern in dieser Vereinbarung nicht anderweitig geregelt, ist es dem Endbenutzer gestattet, die Lizenz und alle Rechte aus dieser Vereinbarung an einen anderen Endbenutzer zu übertragen, sofern der Anbieter dem zustimmt und die folgenden Voraussetzungen beachtet werden: (i) Der ursprüngliche Endbenutzer darf keine Kopien der Software zurückbehalten. (ii) Die Übertragung der Rechte muss direkt erfolgen, d. h. vom ursprünglichen Endbenutzer an den neuen Endbenutzer. (iii) Der neue Endbenutzer muss sämtliche Rechte und Pflichten des ursprünglichen Endbenutzers aus dieser Vereinbarung übernehmen. (iv) Der ursprüngliche Endbenutzer muss dem neuen Endbenutzer einen der in Abschnitt 17 genannten Nachweise für die Gültigkeit des Softwarelizenz übereignen.

17.**Gültigkeitsnachweis für die Softwarelizenz**. Der Endbenutzer kann seine Nutzungsrechte an der Software auf eine der folgenden Arten nachweisen: (i) über ein Lizenzzertifikat, das vom Anbieter oder einem von diesem beauftragten Dritten ausgestellt wurde; (ii) über eine schriftliche Lizenzvereinbarung, falls abgeschlossen; (iii) durch Vorlage einer E-Mail des Anbieters mit den Lizenzdaten (Benutzername und Passwort). Zur Überprüfung der Echtheit der Software sind unter Umständen Lizenzinformationen und Identifikationsdaten des Endbenutzers gemäß der Datenschutzrichtlinie erforderlich.

18. **Lizenzvergabe an Behörden und die US-Regierung**. Für die Lizenzvergabe an Behörden, insbesondere an Stellen der US-Regierung, gelten ausschließlich die in dieser Vereinbarung beschriebenen Lizenzrechte und Einschränkungen.

19. **Einhaltung von Handelskontrollen**.

(a) Sie werden die Software nicht direkt oder indirekt an andere Personen exportieren, reexportieren, übertragen oder auf andere Arten verfügbar machen, auf eine Art verwenden oder sich an Handlungen beteiligen, die zu einer Verletzung der Handelskontrollgesetze durch oder zu sonstigen negativen Folgen für ESET oder eines der übergeordneten Unternehmen, die Tochtergesellschaften von ESET oder die Tochtergesellschaften der übergeordneten Unternehmen sowie die Entitäten unter der Kontrolle der übergeordneten Unternehmen (im Folgenden „angeschlossene Unternehmen“) führen könnten. Zu diesen Handelskontrollgesetzen zählen:

i. alle Gesetze, die Lizenzierungsanforderungen zum Export, Reexport oder zur Übertragung von Waren, Software, Technologie oder Dienstleistungen kontrollieren, einschränken oder auferlegen und die von Regierungen, Bundesstaaten/Bundesländern oder Regulierungsbehörden in den USA, in Singapur, in Großbritannien, der Europäischen Union oder ihren Mitgliedsstaaten oder in anderen Ländern eingeführt oder übernommen wurden, in denen die Verpflichtungen der Vereinbarung gelten, oder in denen ESET oder eines der angeschlossenen Unternehmen sesshaft oder tätig ist (im Folgenden „Exportkontrollgesetze“)

ii. alle sonstigen wirtschaftlichen, finanziellen oder handelsbezogenen Sanktionen, Einschränkungen, Embargos, Import- oder Exportbeschränkungen, Verbote von Vermögens- oder Assetübertragungen oder von Dienstleistungen sowie alle gleichwertigen Maßnahmen, die von Regierungen, Bundesstaaten/Bundesländern oder Regulierungsbehörden in den USA, in Singapur, in Großbritannien, der Europäischen Union oder ihren Mitgliedsstaaten oder in anderen Ländern eingeführt oder übernommen wurden, in denen die Verpflichtungen der Vereinbarung gelten, oder in denen ESET oder eines der angeschlossenen Unternehmen sesshaft oder tätig ist (im Folgenden „Sanktionsgesetze“).

(b) ESET behält sich das Recht vor, die eigenen Verpflichtungen im Rahmen dieser Bestimmungen fristlos aufzuheben oder die Bestimmungen fristlos aufzukündigen, falls Folgendes eintritt:

i. ESET hat nach eigenem Ermessen festgestellt, dass ein Benutzer die Bestimmungen in Artikel 19.a dieser Vereinbarung verletzt hat oder vermutlich verletzen wird; oder

ii. ein Endbenutzer und/oder die Software fällt unter die Handelskontrollgesetze, und ESET ist nach eigenem Ermessen der Ansicht, dass die weitere Erfüllung der Verpflichtungen aus der Vereinbarung dazu führen könnte, dass ESET oder ein angeschlossenes Unternehmen die Handelskontrollgesetze verletzt oder dass sonstige

negative Folgen zu erwarten sind.

(c) Die Vereinbarung ist nicht darauf ausgelegt und darf nicht so interpretiert oder ausgelegt werden, dass eine der Parteien dazu aufgefordert oder verpflichtet wird, auf irgendeine Weise zu handeln oder Handlungen zu unterlassen (oder Handlungen bzw. deren Unterlassung zuzustimmen), die geltende Handelskontrollgesetze verletzt oder gemäß dieser Gesetze unter Strafe steht oder verboten ist.

20. **Kündigungen**. Alle Kündigungen sowie zurückgegebene Software und Dokumentation sind an folgende Adresse zu senden: ESET, spol. s r. o., Einsteinova 24, 851 01 Bratislava, Slovak Republic.

21. **Geltendes Recht, Gerichtsstand**. Diese Vereinbarung unterliegt slowakischem Recht. Endbenutzer und Anbieter vereinbaren, dass gesetzliche Bestimmungen zur Konfliktlösung und UN-Kaufrecht nicht zur Anwendung kommen. Sie erklären sich ausdrücklich damit einverstanden, dass als Gerichtsstand für alle Streitfälle mit dem Anbieter oder bezüglich Ihrer Verwendung der Software das Amtsgericht Bratislava I, Slowakische Republik vereinbart wird.

22. **Allgemeine Bestimmungen**. Wenn eine der Bestimmungen dieser Vereinbarung ungültig oder uneinklagbar ist, beeinträchtigt dies nicht die Gültigkeit der übrigen Bestimmungen der Vereinbarung. Diese bleiben unter den hier festgelegten Bedingungen gültig und einklagbar. Bei Widersprüchen zwischen übersetzten Versionen dieser Vereinbarung hat die englische Version Vorrang. Änderungen an dieser Vereinbarung bedürfen der Schriftform und müssen von einem bevollmächtigten Vertreter des Anbieters unterzeichnet werden.

Dies ist die vollständige Vereinbarung zwischen dem Anbieter und Ihnen in Bezug auf die Software. Sie ersetzt alle vorigen Darstellungen, Diskussionen, Unternehmungen, Kommunikationen und Werbungen in Bezug auf die Software.

EULA ID: BUS-STANDARD-20-01

Datenschutzrichtlinie

ESET, spol. s r. o., mit eingetragenem Firmensitz in Einsteinova 24, 851 01 Bratislava, Slowakei, eingetragen im Handelsregister Bratislava I, Abschnitt Sro, Eintragsnummer 3586/B, Firmenregisternummer 31333532 als Datenverarbeiter („ESET“ oder „Wir“) hat das Ziel, die persönlichen Daten und die Privatsphäre seiner Kunden transparent zu behandeln. Daher veröffentlichen wir diese Datenschutzerklärung mit dem ausschließlichen Ziel, unsere Kunden („Endkunde“ oder „Sie“) über die folgenden Themen zu informieren:

- Verarbeitung persönlicher Daten,
- Vertraulichkeit der Daten,
- Rechte betroffener Personen.

Verarbeitung persönlicher Daten

Die von ESET angebotenen und in unserem Produkt implementierten Dienste werden unter den Bestimmungen der Endbenutzer-Lizenzvereinbarung („EULA“) bereitgestellt. Einige dieser Dienste erfordern jedoch möglicherweise zusätzliche Aufmerksamkeit. Wir möchten Ihnen weitere Details zur Datensammlung im Zusammenhang mit der Bereitstellung unserer Dienste liefern. Wir bieten verschiedene in der EULA und der Produktdokumentation beschriebene Dienste an, darunter die Upgrade- und Updatedienste, ESET LiveGrid®, den Schutz vor dem Missbrauch von Daten, Support usw. Für die Erbringung dieser Dienste erfassen wir die folgenden Informationen:

• Update- und sonstige Statistiken und Informationen zum Installationsprozess und Ihrem Computer, z. B. die Plattform, auf der unser Produkt installiert wird, oder Informationen zum Betrieb und Funktionsumfang unserer Produkte wie Betriebssystem, Hardwareinformationen, Installations- und Lizenz-IDs, IP-Adresse, MAC-Adresse und Konfigurationseinstellungen des Produkts.

• Einweg-Hashes für Schadsoftware als Teil unseres LiveGrid®-Reputationssystems, das die Wirksamkeit der Sicherheitslösungen verbessert, indem es gescannte Dateien mit Positiv- und Negativlisten in einer Datenbank in der Cloud vergleicht.

• Verdächtige Samples und Metadaten „aus freier Wildbahn“ als Teil unseres ESET LiveGrid®-Reputationssystems, mit denen ESET unmittelbar auf die Anforderungen unserer Kunden reagieren und sie vor den neuesten Bedrohungen schützen kann. Wir benötigen die folgenden Daten von Ihnen:

  oEingedrungene Schadsoftware, z. B. potenzielle Sample von Viren und anderen Schadprogrammen, sowie verdächtige, problematische, potenziell unerwünschte oder potenziell unsichere Objekte wie ausführbare Dateien oder E-Mail-Nachrichten, die von Ihnen als Spam markiert oder von unserem Produkt markiert wurden;

  oInformationen zu Geräten im lokalen Netzwerk wie Art, Hersteller, Modell und/oder Name des Geräts;

  oInformationen zur Internetnutzung wie IP-Adresse und geografische Informationen, IP-Pakete, URLs und Ethernet-Frames;

  oAbsturzabbilder und darin enthaltenen Informationen.

Wir haben kein Interesse daran, Daten außerhalb des genannten Umfangs zu erfassen, allerdings lässt sich dies manchmal nicht vermeiden. Versehentlich erfasste Daten können in der Schadsoftware (ohne Ihr Wissen oder Ihre Zustimmung erfasst) oder als Teil von Dateinamen oder URLs enthalten sein. Es ist nicht unsere Absicht, diese Daten in unseren Systemen oder für die in dieser Datenschutzerklärung genannten Zwecke zu verarbeiten.

• Lizenzinformationen wie die Lizenz-ID und persönliche Daten wie Vor- und Nachname, Adresse und E-Mail-Adresse werden zu Abrechnungszwecken, zur Überprüfung der Echtheit der Lizenz und zur Erbringung unserer Dienste benötigt.

• Kontaktinformationen und andere Daten in Ihren Supportanfragen werden für möglicherweise für die Erbringung von Supportdiensten benötigt. Je nachdem, über welchen Kanal Sie uns kontaktieren, speichern wir möglicherweise Ihre E-Mail-Adresse, Telefonnummer, Lizenzinformationen, Produktdetails und eine Beschreibung Ihres Supportfalls. Möglicherweise werden Sie aufgefordert, uns weitere Informationen bereitzustellen, um die Bearbeitung der Supportanfrage zu erleichtern.

Vertraulichkeit der Daten

ESET ist ein weltweit operierendes Unternehmen über angeschlossene Unternehmen oder Partner im Rahmen unseres Distributions-, Dienst- und Supportnetzwerks. Die von ESET verarbeiteten Informationen können zur Erbringung der EULA von und zu angeschlossenen Unternehmen übertragen werden, beispielsweise für die Bereitstellung von Diensten, Supportleistungen oder Abrechnungen. Je nach Ihrem Standort und den von Ihnen ausgewählten Diensten müssen wir Ihre Daten unter Umständen in Länder ohne Gleichstellungsbeschluss der Europäischen Kommission übertragen. Selbst in diesem Fall unterliegen alle Datenübertragungen den Datenschutzbestimmungen und finden nur bei Bedarf statt. Übliche Vertragsklauseln, bindende Unternehmensregeln oder andere geeignete Mechanismen müssen ausnahmslos umgesetzt werden.

Wir unternehmen größte Anstrengungen, um zu verhindern, dass Ihre Daten bei der Bereitstellung von Diensten im Rahmen der EULA länger als notwendig gespeichert werden. Unser Aufbewahrungszeitraum ist unter Umständen länger als die Gültigkeitsdauer Ihrer Lizenz, um Ihnen eine problemlose und komfortable Erneuerung zu ermöglichen. Minimierte und pseudonymisierte Statistiken und sonstige Daten aus ESET LiveGrid® können zu

statistischen Zwecken weiterverarbeitet werden.

ESET implementiert angemessene technische und organisatorische Maßnahmen, um einen angemessenen Schutz vor potenziellen Risiken zu bieten. Wir bemühen uns nach Kräften, die fortlaufende Vertraulichkeit, Integrität, Verfügbarkeit und Ausfallsicherheit der Verarbeitungssysteme und Dienste zu gewährleisten. Falls jedoch Ihre Rechte und Freiheiten durch einen Datenangriff gefährdet sind, müssen wir die Aufsichtsbehörden sowie die betroffenen Personen informieren. Betroffene Personen haben das Recht, Beschwerde bei einer Aufsichtsbehörde einzulegen.

Rechte betroffener Personen

ESET unterliegt slowakischem Recht und ist als Teil der Europäischen Union an die Datenschutzgesetze gebunden. Im Rahmen der geltenden Datenschutzgesetze haben Sie als betroffene Person die folgenden Rechte:

- das Recht, Ihre persönlichen Daten von ESET anzufordern,
- das Recht, Ihre persönlichen Daten bei Bedarf zu berichtigen (Sie haben auch das Recht, unvollständige persönliche Daten zu vervollständigen),
- das Recht, die Löschung Ihrer persönlichen Daten anzufordern,
- das Recht, eine Einschränkung der Verarbeitung Ihrer persönlichen Daten anzufordern,
- Einlegen von Einspruch gegen die Verarbeitung
- Einlegen von Beschwerden sowie
- das Recht auf Übertragbarkeit der Daten.

Wir sind davon überzeugt, dass alle von uns verarbeiteten Informationen wertvoll und notwendig für die Erfüllung unserer legitimen Interessen sind, also der Bereitstellung von Diensten und Produkten für unsere Kunden.

Falls Sie Ihre Rechte als betroffene Person in Anspruch nehmen möchten oder Fragen oder Bedenken haben, schicken Sie uns eine Nachricht an:

ESET, spol. s r.o.
Data Protection Officer
Einsteinova 24
85101 Bratislava
Slovak Republic
dpo@eset.sk