ESET NOD32 Antivirus

Benutzerhandbuch

Klicken Sie hier um die Hilfe-Version dieses Dokuments anzuzeigen

Digital Security
Progress. Protected.

ESET NOD32 Antivirus wurde entwickelt von ESET, spol. s r.o.

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

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

REV. 12.04.2024

1 ESET NOD32 Antivirus 1
1.1 Neuerungen 2
1.2 Welches Produkt verwende ich? 2
1.3 Systemanforderungen 3
1.3 Ihre Version von Windows 7 ist veraltet 4
1.3 Windows 7 wird von Microsoft nicht mehr unterstützt 4
1.3 Windows Vista wird nicht mehr unterstützt 5
1.4 Prävention 5
1.5 Hilfeseiten 6
2 Installation 8
2.1 Live-Installer 8
2.2 Offline-Installation 9
2.3 Produktaktivierung 11
2.3 Eingabe Ihres Lizenzschlüssels bei der Aktivierung 12
2.3 ESET HOME-Konto verwenden 12
2.3 Testlizenz aktivieren 13
2.3 Kostenloser ESET-Lizenzschlüssel 14
2.3 Fehler bei der Aktivierung - häufige Szenarien 15
2.3 Fehler bei der Aktivierung aufgrund von überbeanspruchter Lizenz 15
2.3 Lizenz-Upgrade 16
2.3 Produkt-Upgrade 17
2.3 Lizenz-Downgrade 17
2.3 Produkt-Downgrade 18
2.4 Fehlerbehebung bei der Installation 19
2.5 Erstprüfung nach Installation 19
2.6 Upgrade auf eine aktuellere Version 20
2.6 Automatisches Upgrade für veraltete Produkte 21
2.7 ESET-Produkte an Freunde weiterempfehlen 21
2.7 ESET NOD32 Antivirus wird installiert 22
2.7 Zu einer anderen Produktreihe ändern 22
2.7 Registrierung 22
2.7 Aktivierungsfortschritt 22
2.7 Aktivierung erfolgreich 22
3 Erste Schritte 23
3.1 Verbinden Sie sich mit ESET HOME 23
3.1 Bei ESET HOME anmelden 24
3.1 Anmeldung fehlgeschlagen – häufige Fehler 25
3.1 Gerät in ESET HOME hinzufügen 26
3.2 Das Haupt-Programmfenster 26
3.3 Updates 29
4 Arbeiten mit ESET NOD32 Antivirus 30
4.1 Computerschutz 32
4.1 Malware Scan Engine 33
4.1 Erweiterte Einstellungen für die Erkennungsroutine 38
4.1 Eingedrungene Schadsoftware wurde erkannt 38
4.1 Echtzeit-Dateischutz 40
4.1 Säuberungsstufen 42
4.1 Wann sollten die Einstellungen für den Echtzeit-Dateischutz geändert werden? 43
4.1 Echtzeit-Dateischutz prüfen 43
4.1 Vorgehensweise bei fehlerhaftem Echtzeit-Dateischutz 43

4.1 Ausgeschlossene Prozesse 44
4.1 Ausgeschlossene Prozesse hinzufügen oder bearbeiten 45
4.1 Cloudbasierter Schutz 45
4.1 Ausschlussfilter für den cloudbasierten Schutz 48
4.1 Computer-Scan 48
4.1 Benutzerdefinierte Prüfung 51
4.1 Stand der Prüfung 52
4.1 Computerprüfungs-Log 54
4.1 Malware-Scans 56
4.1 Scan im Leerlaufbetrieb 56
4.1 Prüfprofile 57
4.1 Zu prüfende Objekte 57
4.1 Medienkontrolle 58
4.1 Regel-Editor für die Medienkontrolle 59
4.1 Erkannte Geräte 60
4.1 Gerätegruppen 60
4.1 Hinzufügen von Regeln für die Medienkontrolle 61
4.1 HIPS 64
4.1 HIPS-Interaktionsfenster 66
4.1 Mögliches Ransomware-Verhalten erkannt 68
4.1 HIPS-Regelverwaltung 69
4.1 HIPS-Regeleinstellungen 70
4.1 Anwendung/Registrierungspfad für HIPS hinzufügen 73
4.1 Erweiterte HIPS-Einstellungen 74
4.1 Treiber dürfen immer geladen werden 74
4.1 Gamer-Modus 74
4.1 Scan der Systemstartdateien 75
4.1 Prüfung Systemstartdateien 75
4.1 Dokumentenschutz 76
4.1 Ausschlussfilter 76
4.1 Leistungsausschlüsse 77
4.1 Leistungsausschluss hinzufügen oder bearbeiten 78
4.1 Format für ausgeschlossene Pfade 79
4.1 Ereignisausschlüsse 80
4.1 Ereignisausschluss hinzufügen oder bearbeiten 82
4.1 Assistent zum Erstellen von Ereignisausschlüssen 83
4.1 HIPS-Ausschlüsse 84
4.1 ThreatSense-Parameter 84
4.1 Von der Prüfung ausgeschlossene Dateiendungen 88
4.1 Zusätzliche ThreatSense-Parameter 88
4.2 Internet-Schutz 89
4.2 Prüfen von Anwendungsprotokollen 90
4.2 Ausgeschlossene Anwendungen 91
4.2 Ausgeschlossene IP-Adressen 92
4.2 IPv4-Adresse hinzufügen 93
4.2 IPv6-Adresse hinzufügen 93
4.2 SSL/TLS 93
4.2 Zertifikate 95
4.2 Verschlüsselte Netzwerkverbindung 95
4.2 Liste bekannter Zertifikate 96
4.2 Liste der vom SSL/TLS-Filter betroffenen Anwendungen 97

4.2 E-Mail-Client-Schutz ... 97
4.2 Integration in E-Mail-Programme ... 98
4.2 Microsoft Outlook-Symbolleiste ... 99
4.2 Symbolleisten für Outlook Express und Windows Mail ... 99
4.2 Bestätigungsfenster ... 99
4.2 E-Mails erneut prüfen ... 100
4.2 E-Mail-Protokolle ... 100
4.2 POP3, POP3S-Prüfung ... 101
4.2 E-Mail-Tags ... 102
4.2 Web-Schutz ... 102
4.2 Erweiterte Einstellungen für den Web-Schutz ... 105
4.2 Webprotokolle ... 105
4.2 URL-Adressverwaltung ... 106
4.2 URL-Adressliste ... 107
4.2 Erstellen einer neuen URL-Adressliste ... 108
4.2 Hinzufügen einer URL-Maske ... 109
4.2 Phishing-Schutz ... 110
4.3 Aktualisieren des Programms ... 112
4.3 Einstellungen für Updates ... 114
4.3 Update-Rollback ... 116
4.3 Rollback-Zeitintervall ... 118
4.3 Produktupdates ... 119
4.3 Verbindungsoptionen ... 119
4.3 So erstellen Sie Update-Tasks ... 120
4.3 Dialogfenster – Neustart erforderlich ... 120
4.4 Tools ... 120
4.4 Tools in ESET NOD32 Antivirus ... 121
4.4 Log-Dateien ... 122
4.4 Log-Filter ... 124
4.4 Log-Dateien ... 126
4.4 Ausgeführte Prozesse ... 127
4.4 Sicherheitsbericht ... 129
4.4 ESET SysInspector ... 130
4.4 Taskplaner ... 131
4.4 Optionen für geplante Scans ... 134
4.4 Übersicht über geplante Tasks ... 135
4.4 Taskdetails ... 135
4.4 Task-Zeitplanung ... 135
4.4 Task-Zeitplanung – Einmalig ... 135
4.4 Task-Zeitplanung – Täglich ... 136
4.4 Task-Zeitplanung – Wöchentlich ... 136
4.4 Task-Zeitplanung – Bei Ereignis ... 136
4.4 Übersprungener Task ... 136
4.4 Taskdetails – Update ... 137
4.4 Taskdetails – Anwendung ausführen ... 137
4.4 System Cleaner ... 138
4.4 ESET SysRescue Live ... 139
4.4 Quarantäne ... 139
4.4 Proxyserver ... 142
4.4 Probe für die Analyse auswählen ... 143
4.4 Probe für die Analyse auswählen - Verdächtige Datei ... 144

4.4 Probe für die Analyse auswählen - Verdächtige Webseite ... 145
4.4 Probe für die Analyse auswählen - Fehlalarm Datei ... 145
4.4 Probe für die Analyse auswählen - Fehlalarm Webseite ... 145
4.4 Probe für die Analyse auswählen - Sonstiges ... 146
4.4 Microsoft Windows® update ... 146
4.4 Dialogfenster – System-Updates ... 146
4.4 Update-Informationen ... 147
4.5 Benutzeroberfläche ... 147
4.5 Elemente der Benutzeroberfläche ... 147
4.5 Einstellungen für den Zugriff ... 148
4.5 Passwort für erweiterte Einstellungen ... 149
4.5 Symbol im Infobereich der Taskleiste ... 150
4.5 Unterstützung für Sprachausgabeprogramme ... 151
4.5 Hilfe und Support ... 151
4.5 Info zu ESET NOD32 Antivirus ... 152
4.5 ESET-Ankündigungen ... 152
4.5 Systemkonfigurationsdaten senden ... 153
4.5 Technischer Support ... 154
4.6 Benachrichtigungen ... 154
4.6 Dialogfenster – Anwendungsstatus ... 155
4.6 Desktophinweise ... 155
4.6 Liste der Desktophinweise ... 157
4.6 Interaktive Warnungen ... 158
4.6 Bestätigungsnachrichten ... 160
4.6 Wechselmedien ... 161
4.6 Weiterleitung ... 162
4.7 Datenschutzeinstellungen ... 164
4.8 Profile ... 165
4.9 Tastaturbefehle ... 166
4.10 Diagnose ... 167
4.10 Technischer Support ... 168
4.10 Import-/Export-Einstellungen ... 169
4.10 Alle Einstellungen in aktuellem Bereich zurücksetzen ... 169
4.10 Auf Standardeinstellungen zurücksetzen ... 170
4.10 Fehler beim Speichern der Konfiguration ... 170
4.11 Befehlszeilenscanner ... 170
4.12 ESET CMD ... 173
4.13 Leerlauferkennung ... 174
5 Häufig gestellte Fragen ... 175
5.1 So aktualisieren Sie ESET NOD32 Antivirus ... 176
5.2 So entfernen Sie einen Virus von Ihrem PC ... 176
5.3 So erstellen Sie eine neue Aufgabe im Taskplaner ... 176
5.4 So planen Sie eine wöchentliche Computerprüfung ... 177
5.5 So entsperren Sie die erweiterten Einstellungen ... 178
5.6 Beheben der Produktdeaktivierung in ESET HOME ... 178
5.6 Produkt deaktiviert, Geräteverbindung getrennt ... 179
5.6 Produkt nicht aktiviert ... 179
6 Programm für ein besseres Kundenerlebnis ... 179
7 Endbenutzer-Lizenzvereinbarung ... 180
8 Datenschutzerklärung ... 192

ESET NOD32 Antivirus

ESET NOD32 Antivirus ist ein neuer Ansatz für vollständig integrierte Computersicherheit. Die neueste Version des ESET LiveGrid®-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 können.

ESET NOD32 Antivirus ist eine umfassende Sicherheitslösung, die maximalen Schutz mit minimalen Anforderungen an die Systemressourcen verbindet. Die modernen Technologien setzen künstliche Intelligenz ein, um ein Eindringen von Viren, Spyware, Trojanern, Würmern, Adware, Rootkits und anderen Bedrohungen zu vermeiden, ohne dabei die Systemleistung zu beeinträchtigen oder die Computerprozesse zu unterbrechen.

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 NOD32 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 NOD32 Antivirus überprüfen.
Medienkontrolle	Prüft automatisch alle USB-Speicher, Speicherkarten und CDs/DVDs. Sperrt den Zugriff auf Wechselmedien anhand von Kriterien wie Medientyp, Hersteller, Größe und weiteren Attributen.
HIPS-Funktion	Sie können das Verhalten des Systems detailliert anpassen, Regeln für die Systemregistrierung und für aktive Prozesse und Programme festlegen und Ihre Sicherheitsposition genau konfigurieren.
Gamer-Modus	Unterdrückt Popup-Fenster, Updates und andere systemintensive Aktivitäten, um Systemressourcen für Spiele oder andere Anwendungen im Vollbildmodus zu bewahren.

Die Funktionen von ESET NOD32 Antivirus arbeiten nur mit einer ordnungsgemäß aktivierten Lizenz. Wir empfehlen, die Lizenz für ESET NOD32 Antivirus einige Wochen vor dem Ablauf zu verlängern.

Neuerungen

Neuigkeiten in ESET NOD32 Antivirus 15

ESET HOME (ehemals myESET)

Bietet verbesserte Sichtbarkeit und Kontrolle über Ihre Sicherheit. Schützen Sie neue Geräte, fügen Sie Lizenzen hinzu und teilen sie, und erhalten Sie wichtige Benachrichtigungen in der mobilen App und im Web-Portal. Weitere Informationen finden Sie in der ESET HOME-Online-Hilfe.

Verbessert: Host-based Intrusion Prevention System (HIPS)

Scannt Speicherbereiche, die durch ausgeklügelte Malware-Injektionstechniken modifiziert werden können. Mit den neuen Verbesserungen kann die Software auch modernste Malware-Einbruchsversuche erkennen.

Bilder und zusätzliche Informationen zu den neuen Funktionen in ESET NOD32 Antivirus finden Sie unter Neuerungen in der aktuellen Version der ESET Home-Produkte.

> Um die Anzeige von **Benachrichtigungen für Neuerungen** zu deaktivieren, klicken Sie auf **Erweiterte Einstellungen** > **Benachrichtigungen** > **Desktophinweise**. Klicken Sie auf **Bearbeiten** neben **Desktophinweise** und deaktivieren Sie das Kontrollkästchen neben **Benachrichtigungen für Neuerungen anzeigen**. Weitere Informationen zu Benachrichtigungen finden Sie im Abschnitt Benachrichtigungen.

Welches Produkt verwende ich?

ESET bietet verschiedene Schutzebenen mit neuen Produkten von einer umfassenden und leistungsstarken Virenschutzlösung bis hin zur All-in-One-Sicherheitslösung mit minimaler Systembelastung:

- **ESET NOD32 Antivirus**
- **ESET Internet Security**
- **ESET Smart Security Premium**

Um herauszufinden, welches Produkt Sie installiert haben, öffnen Sie das Programmfenster. Dort wird der Name des Produkts am oberen Rand angezeigt (siehe Knowledgebase-Artikel).

Die folgende Tabelle enthält die verfügbaren Funktionen der einzelnen Produkte.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
Malware Scan Engine	✔	✔	✔
Erweitertes Machine Learning	✔	✔	✔
Exploit-Blocker	✔	✔	✔
Skriptbasierter Angriffsschutz	✔	✔	✔
Phishing-Schutz	✔	✔	✔

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
Web-Schutz	✔	✔	✔
HIPS (inklusive Ransomware Shield)	✔	✔	✔
Spam-Schutz		✔	✔
Firewall		✔	✔
Sicheres Heimnetzwerk		✔	✔
Webcam-Schutz		✔	✔
Netzwerkangriffsschutz		✔	✔
Botnet-Erkennung		✔	✔
Sicheres Online-Banking und Bezahlen		✔	✔
Kindersicherung		✔	✔
Anti-Theft		✔	✔
Password Manager			✔
ESET Secure Data			✔
ESET LiveGuard			✔

Möglicherweise sind nicht alle aufgeführten Produkte für Ihre Sprache oder Region verfügbar.

Systemanforderungen

Ihr System muss die folgenden Hardware- und Softwareanforderungen erfüllen, um ESET NOD32 Antivirus mit optimaler Leistung ausführen zu können:

Unterstützte Prozessoren

Intel- oder AMD- Prozessor, 32-Bit (x86) mit SSE2-Anweisungssatz oder 64 Bit (x64), 1 GHz oder höher
ARM64-basierter Prozessor, 1 GHz oder höher

Unterstützte Betriebssysteme*

Microsoft® Windows® 11
Microsoft® Windows® 10
Microsoft® Windows® 8.1
Microsoft® Windows® 8
Microsoft® Windows® 7 SP1 mit den neuesten Windows-Updates
Microsoft® Windows® Home Server 2011 64-bit

Halten Sie Ihr Betriebssystem immer auf dem neuesten Stand.

Sonstige

Eine Internetverbindung ist erforderlich, um ESET NOD32 Antivirus zu aktivieren und aktualisieren zu können.

Parallel ausgeführte Virenschutzprogramme auf einem einzigen Gerät führen unweigerlich zu

Systemressourcenkonflikten und können das System verlangsamen oder unbrauchbar machen.

* ESET kann nach Februar 2021 keinen Schutz mehr für nicht unterstützte Betriebssysteme bieten.

Ihre Version von Windows 7 ist veraltet

Problem

Sie verwenden eine veraltete Version Ihres Betriebssystems. Halten Sie Ihr Betriebssystem immer auf dem neuesten Stand, um sich auch weiterhin zu schützen.

Lösung

Sie haben ESET NOD32 Antivirus auf {GET_OSNAME} {GET_BITNESS} installiert.

Vergewissern Sie sich, dass Sie Windows 7 Service Pack 1 (SP1) mit den neuesten Windows-Updates installiert haben (zumindest KB4474419 und KB4490628).

Falls Ihr Windows 7 nicht für automatische Updates konfiguriert ist, klicken Sie auf **Startmenü** > **Systemsteuerung** > **System und Sicherheit** > **Windows Update** > **Nach Updates suchen** und klicken Sie dann auf **Updates installieren**.

Siehe auch Windows 7 wird von Microsoft nicht mehr unterstützt.

Windows 7 wird von Microsoft nicht mehr unterstützt

Problem

Der Support von Microsoft für Windows 7 wurde am 14. Januar 2020 eingestellt. Was bedeutet das?

Wenn Sie Windows 7 nach dem Ende des Supports weiterhin verwenden, funktioniert Ihr PC weiterhin, kann jedoch anfälliger für Sicherheitsrisiken und Viren werden. Ihr PC empfängt keine Windows-Updates mehr (dies betrifft auch Sicherheitsupdates).

Lösung

Upgrade von Windows 7 auf Windows 10? Aktualisieren Sie Ihr ESET-Produkt

Der Upgradevorgang ist relativ einfach, und in vielen Fällen können Sie den Vorgang ohne Verlust Ihrer Dateien ausführen. Vor dem Upgrade auf Windows 10:

1. Ihr ESET-Produkt prüfen/aktualisieren
2. Sichern wichtiger Daten
3. Lesen Sie den Microsoft-Artikel Upgrade auf Windows 10: Häufig gestellte Fragen und aktualisieren Sie Ihr Windows-Betriebssystem

Sie erhalten einen neuen Computer oder ein neues Gerät? ESET-Produkt übertragen

Wenn Sie einen neuen Computer oder ein neues Gerät gekauft haben oder dies planen: Hier erfahren Sie, wie Sie Ihr vorhandenes ESET-Produkt auf ein neues Gerät übertragen.

Siehe auch Support für Windows 7 ist abgelaufen.

Windows Vista wird nicht mehr unterstützt

Problem

Aufgrund von technischen Einschränkungen in Windows Vista kann ESET NOD32 Antivirus nach **Februar 2021** keinen Schutz mehr anbieten. Das ESET-Produkt wird **seine Funktion einstellen**. Ihr System ist ab diesem Zeitpunkt möglicherweise anfällig für Angriffe.

Der Support von Microsoft für Windows Vista wurde am 11. April 2017 eingestellt. Was bedeutet das?

Wenn Sie Windows Vista nach dem Ende des Supports weiterhin verwenden, funktioniert Ihr PC weiterhin, kann jedoch anfälliger für Sicherheitsrisiken und Viren werden. Ihr PC empfängt keine Windows-Updates mehr (dies betrifft auch Sicherheitsupdates).

Lösung

Upgrade von Windows Vista auf Windows 10? Besorgen Sie einen neuen Computer oder ein neues Gerät, und übertragen Sie das ESET-Produkt.

Vor dem Upgrade auf Windows 10:

1. Sichern wichtiger Daten
2. Lesen Sie den Microsoft-Artikel Upgrade auf Windows 10: Häufig gestellte Fragen und aktualisieren Sie Ihr Windows-Betriebssystem
3. Installieren oder übertragen Sie Ihr vorhandenes ESET-Produkt auf ein neues Gerät.

Siehe auch Support für Windows Vista ist abgelaufen.

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 im ESET-Virenlabor 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

Willkommen zum ESET NOD32 Antivirus-Benutzerhandbuch. Die hier bereitgestellten Informationen machen Sie mit dem Produkt vertraut und Ihren Computer sicherer.

Erste Schritte

Bevor Sie ESET NOD32 Antivirus einsetzen, sollten Sie sich mit den verschiedenen Ereignistypen und Remoteangriffen vertraut machen, die beim Arbeiten mit dem Computer auftreten können.

Außerdem haben wir eine Liste der neuen Funktionen in ESET NOD32 Antivirus sowie einen Leitfaden für die Konfiguration der Grundeinstellungen zusammengestellt.

So finden Sie sich auf den Hilfeseiten von ESET NOD32 Antivirus zurecht

Die Hilfethemen sind in Kapitel und Unterkapitel unterteilt. Drücken Sie **F1**, um Informationen zum aktuellen Fenster anzuzeigen.

Im Programm können Sie entweder Stichwörter oder Wörter und Formulierungen eingeben, um nach Hilfethemen zu suchen. 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 im Text enthalten.

Aus Konsistenzgründen und um Verwechslungen zu vermeiden, basiert die Terminologie in dieser Anleitung auf den ESET NOD32 Antivirus-Parameternamen. Außerdem verwenden wir einheitliche Symbole, um besonders wichtige Themen hervorzuheben.

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.

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

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.

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.

Installation

Zur Installation von ESET NOD32 Antivirus auf Ihrem Computer stehen verschiedene Methoden zur Verfügung. Die verfügbaren Installationsmethoden unterscheiden sich je nach Land und Vertriebsart:

- Live-Installationsprogramm – Von der ESET-Website oder einer CD/DVD heruntergeladen. Das Installationspaket gilt für alle Sprachen (wählen Sie die geeignete Sprache aus). Das Live-Installationsprogramm ist eine kleine Datei. Zusätzliche für die Installation von ESET NOD32 Antivirus erforderliche Dateien werden automatisch heruntergeladen.

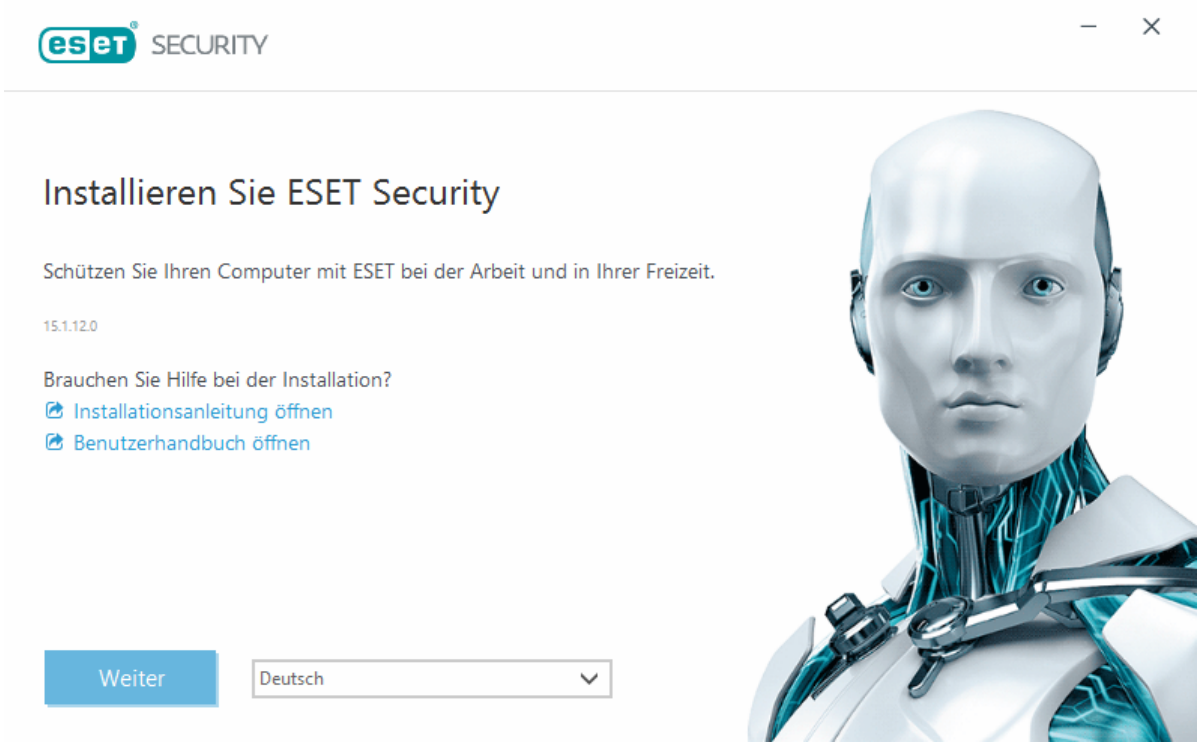
- Offline-Installation – Verwendet eine .exe-Datei, die größer ist als die Datei des Live-Installationsprogramms. Es ist keine Internetverbindung erforderlich, und es werden auch keine zusätzlichen Dateien benötigt, um die Installation abzuschließen.

Stellen Sie sicher, dass keine anderen Virenschutzprogramme auf Ihrem Computer installiert sind, bevor Sie mit der Installation von ESET NOD32 Antivirus beginnen. 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 ESET-Knowledgebase-Artikel (in englischer und in bestimmten weiteren Sprachen verfügbar).

Live-Installer

Nachdem Sie das Live-Installationsprogramm-Installationspaketheruntergeladen haben, doppelklicken Sie auf die Installationsdatei und befolgen Sie die schrittweisen Anweisungen im Installationsassistenten.

Für diese Art der Installation ist eine Internetverbindung erforderlich.



1. Wählen Sie im Dropdownmenü die geeignete Sprache aus, und klicken Sie auf **Weiter**.

Falls Sie eine neuere Version über die vorherige Version mit passwortgeschützten Einstellungen installieren, geben Sie Ihr Passwort ein. Sie können das Einstellungspasswort unter Passwort für Einstellungen konfigurieren.

2. Wählen Sie die gewünschten Einstellungen für die folgenden Funktionen aus, lesen Sie die Endbenutzer-Lizenzvereinbarung und die Datenschutzerklärung und klicken Sie auf **Weiter**, oder klicken Sie auf **Alle zulassen und fortfahren**, um alle Funktionen zu aktivieren:

- ESET LiveGrid®-Feedbacksystem
- Potenziell unerwünschte Anwendungen
- Programm für ein besseres Kundenerlebnis

Wenn Sie auf **Weiter** oder auf **Alle zulassen und fortfahren** klicken, stimmen Sie der Endbenutzer-Lizenzvereinbarung zu und akzeptieren die Bedingungen der Datenschutzerklärung.

3. Um die Gerätesicherheit mit dem ESET HOME aktivieren, verwalten und anzeigen zu können, verbinden Sie Ihr Gerät mit dem ESET HOME-Benutzerkonto. Klicken Sie auf **Anmeldung überspringen**, um den Vorgang fortzusetzen, ohne sich mit ESET HOME zu verbinden. Sie können Ihr Gerät später mit Ihrem ESET HOME Konto verbinden.

4. Wählen Sie eine Aktivierungsoption aus, falls Sie fortfahren möchten, ohne sich mit ESET HOME zu verbinden. Falls Sie eine neuere Version über eine ältere Version installieren, wird Ihr Lizenzschlüssel automatisch ausgefüllt.

5. Der Installationsassistent legt anhand Ihrer Lizenz fest, welches ESET-Produkt installiert wird. Die Version mit den größten Anzahl an Sicherheitsfunktionen ist immer vorausgewählt. Klicken Sie auf **Produkt ändern**, wenn Sie eine andere Version des ESET-Produkts installieren möchten. Klicken Sie auf **Weiter**, um die Installation zu starten. Dieser Vorgang kann einige Minuten dauern.

Falls Überreste (Dateien oder Ordner) von älteren installierten ESET Produkten vorhanden sind, werden Sie aufgefordert, deren Löschung zuzulassen. Klicken Sie auf **Installieren**, um fortzufahren.

6. Klicken Sie auf **Fertig stellen**, um den Installationsassistenten zu beenden.

Fehlerbehebung bei der Installation.

Der Download der Module beginnt, nachdem das Produkt installiert und aktiviert wurde. Der Schutz wird gestartet, und ein Teil der Funktionen ist bis zum Abschluss des Downloads unter Umständen nicht vollständig einsatzbereit.

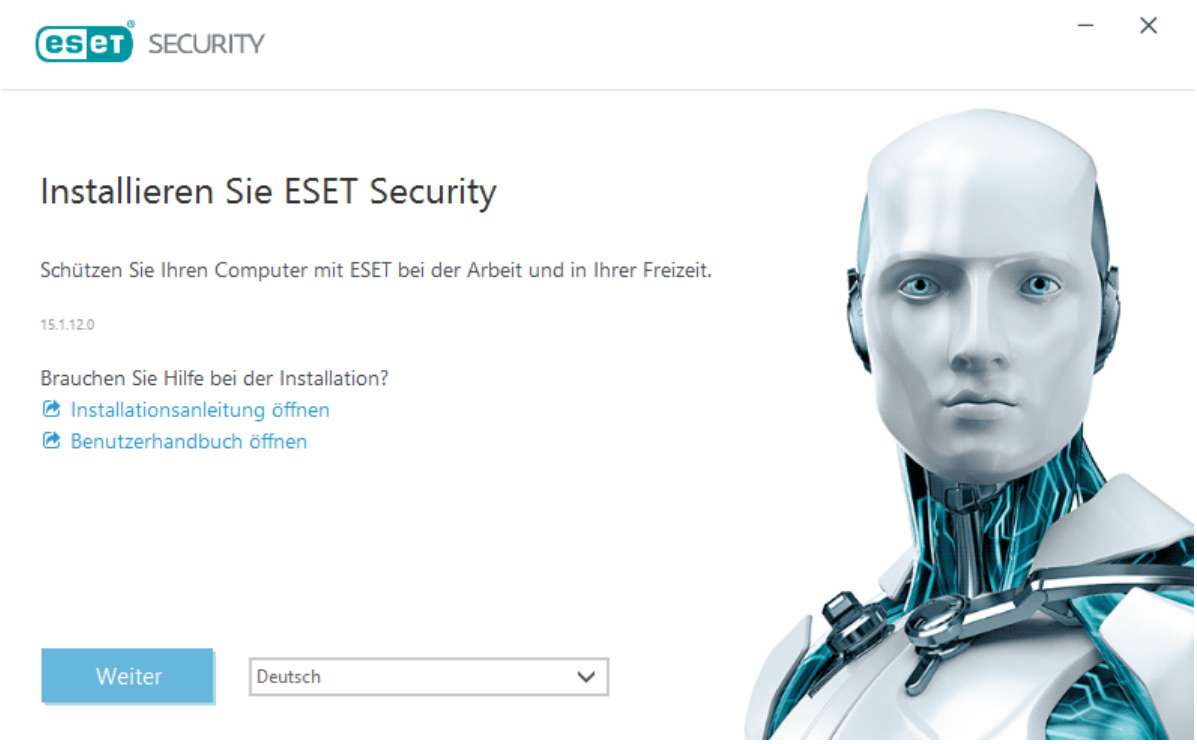
Offline-Installation

Laden Sie Ihr ESET Windows Home-Produkt mit dem unten genannten Offline-Installationsprogramm (.exe) herunter und installieren es. Wählen Sie aus, welche Version des ESET HOME-Produkts heruntergeladen werden soll (32-Bit, 64-Bit oder ARM).

ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
64-Bit-Download 32-Bit-Download ARM-Download	64-Bit-Download 32-Bit-Download ARM-Download	64-Bit-Download 32-Bit-Download ARM-Download

Falls Sie mit dem Internet verbunden sind, installieren Sie Ihr ESET-Produkt mit einem Live-Installationsprogramm.

Nachdem Sie die Offline-Installation (.exe) gestartet haben, führt Sie der Installationsassistent durch die Einrichtung.



1. Wählen Sie im Dropdownmenü die geeignete Sprache aus, und klicken Sie auf **Weiter**.

Falls Sie eine neuere Version über die vorherige Version mit passwortgeschützten Einstellungen installieren, geben Sie Ihr Passwort ein. Sie können das Einstellungspasswort unter Passwort für Einstellungen konfigurieren.

2. Wählen Sie die gewünschten Einstellungen für die folgenden Funktionen aus, lesen Sie die Endbenutzer-Lizenzvereinbarung und die Datenschutzerklärung und klicken Sie auf **Weiter**, oder klicken Sie auf **Alle zulassen und fortfahren**, um alle Funktionen zu aktivieren:

- ESET LiveGrid®-Feedbacksystem
- Potenziell unerwünschte Anwendungen
- Programm für ein besseres Kundenerlebnis

Wenn Sie auf **Weiter** oder auf **Alle zulassen und fortfahren** klicken, stimmen Sie der Endbenutzer-Lizenzvereinbarung zu und akzeptieren die Bedingungen der Datenschutzerklärung.

3. Klicken Sie auf **Anmeldung überspringen**. Wenn Sie mit dem Internet verbunden sind, können Sie Ihr Gerät mit Ihrem ESET HOME-Konto verbinden.

4. Klicken Sie auf **Aktivierung überspringen**. ESET NOD32 Antivirus muss nach der Installation aktiviert werden, um vollständig funktionsfähig zu sein. Für die Produktaktivierung ist eine aktive Internetverbindung erforderlich.

5. Der Installationsassistent zeigt auf Basis des heruntergeladenen Offline-Installationsprogramms an, welches ESET-Produkt installiert wird. Klicken Sie auf **Weiter**, um die Installation zu starten. Dieser Vorgang kann einige Minuten dauern.

Falls Überreste (Dateien oder Ordner) von älteren installierten ESET Produkten vorhanden sind, werden Sie aufgefordert, deren Löschung zuzulassen. Klicken Sie auf **Installieren**, um fortzufahren.

6. Klicken Sie auf **Fertig stellen**, um den Installationsassistenten zu beenden.

Fehlerbehebung bei der Installation.

Produktaktivierung

Für die Aktivierung Ihres Produkts stehen verschiedene Methoden zur Verfügung. Die Verfügbarkeit einzelner Aktivierungsmöglichkeiten im Aktivierungsfenster hängt vom Land und von der Vertriebsart (CD/DVD, ESET-Webseite usw.) ab:

- Wenn Sie das Produkt in einer Einzelhandelsverpackung erworben oder eine E-Mail mit Lizenzdetails erhalten haben, klicken Sie auf **Gekauften Lizenzschlüssel verwenden**, um Ihr Produkt zu aktivieren. Den Lizenzschlüssel finden Sie normalerweise in der Produktverpackung oder auf deren Rückseite. Der Lizenzschlüssel muss unverändert eingegeben werden, damit die Aktivierung erfolgreich ausgeführt werden kann. Lizenzschlüssel – Eine eindeutige Zeichenfolge im Format XXXX-XXXX-XXXX-XXXX-XXXX oder XXXX-XXXXXXXX zur Identifizierung des Lizenzinhabers und der Aktivierung der Lizenz.

- Nachdem Sie die Option ESET HOME-Konto verwenden ausgewählte haben, werden Sie dazu aufgefordert, sich bei Ihrem ESET HOME-Konto anzumelden.

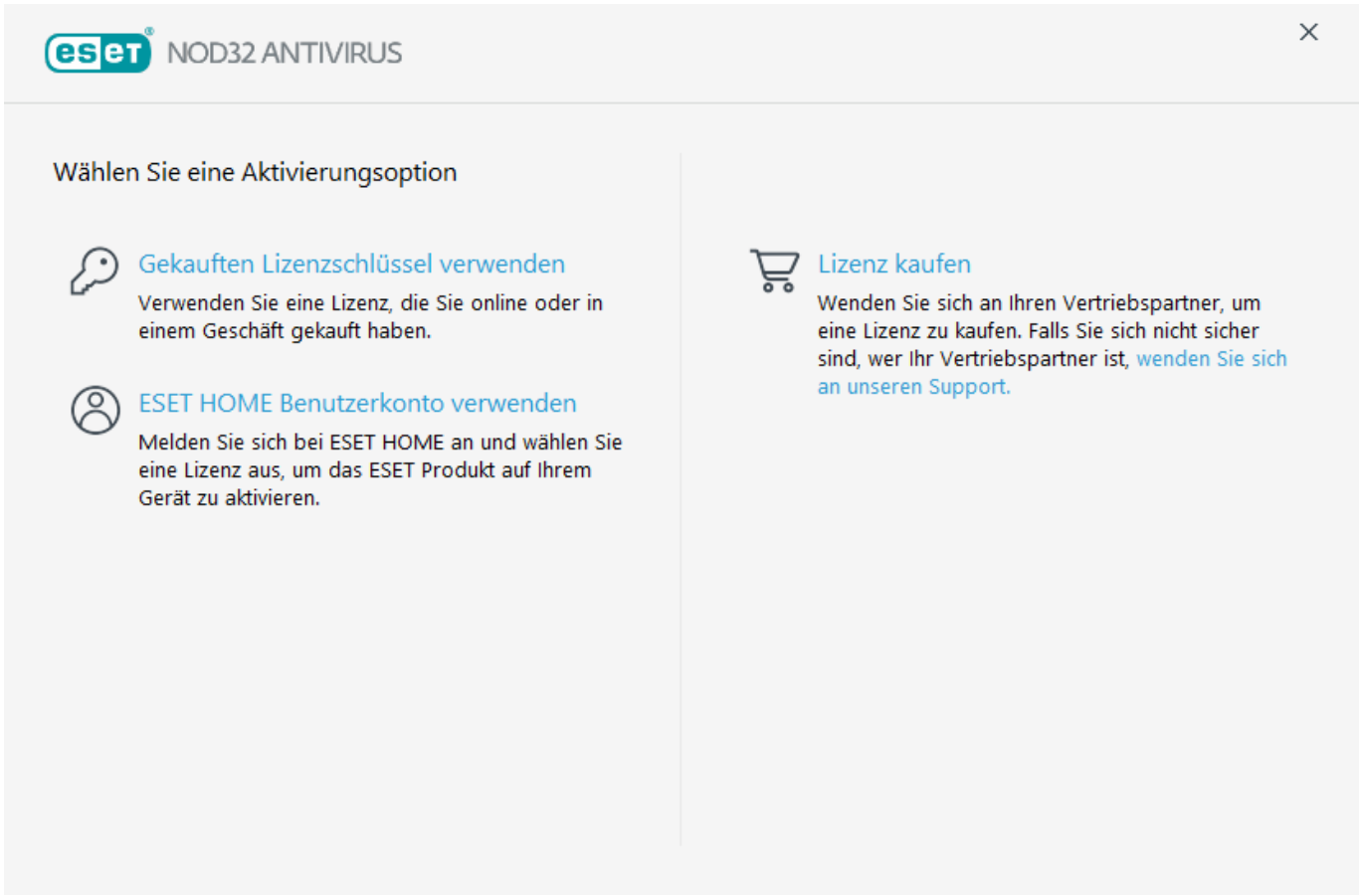
- Wenn Sie ESET NOD32 Antivirus vor dem Kauf testen möchten, wählen Sie Kostenloser Test aus. Geben Sie Ihre E-Mail-Adresse und Ihr Land ein, um ESET NOD32 Antivirus für begrenzte Zeit zu aktivieren. Sie erhalten die Testlizenz per E-Mail. Eine Testlizenz kann pro Kunde nur ein einziges Mal aktiviert werden.

- Wenn Sie noch keine Lizenz haben und eine erwerben möchten, klicken Sie auf **Lizenz kaufen**. Hiermit gelangen Sie zur Website Ihres lokalen ESET-Distributors. Die vollständigen Lizenzen für ESET Windows Home-Produkte sind nicht kostenlos.

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.

Wenn Sie einen Benutzernamen und ein Passwort für ein älteres ESET-Produkt haben und nicht wissen, wie Sie ESET NOD32 Antivirus aktivieren können, klicken Sie auf Legacy-Anmeldeinformationen zu einem Lizenzschlüssel konvertieren.

Fehler bei Produktaktivierung?



Eingabe Ihres Lizenzschlüssels bei der Aktivierung

Automatische Updates sind wichtig für Ihre Sicherheit. ESET NOD32 Antivirus erhält erst Updates, nachdem Sie das Produkt aktiviert haben.

Geben Sie Ihren **Lizenzschlüssel** unbedingt exakt nach Vorgabe ein:

- Ihr Lizenzschlüssel ist eine eindeutige Zeichenfolge im Format XXXX-XXXX-XXXX-XXXX-XXXX und dient zur Identifizierung des Lizenzinhabers und zur Aktivierung der Lizenz.

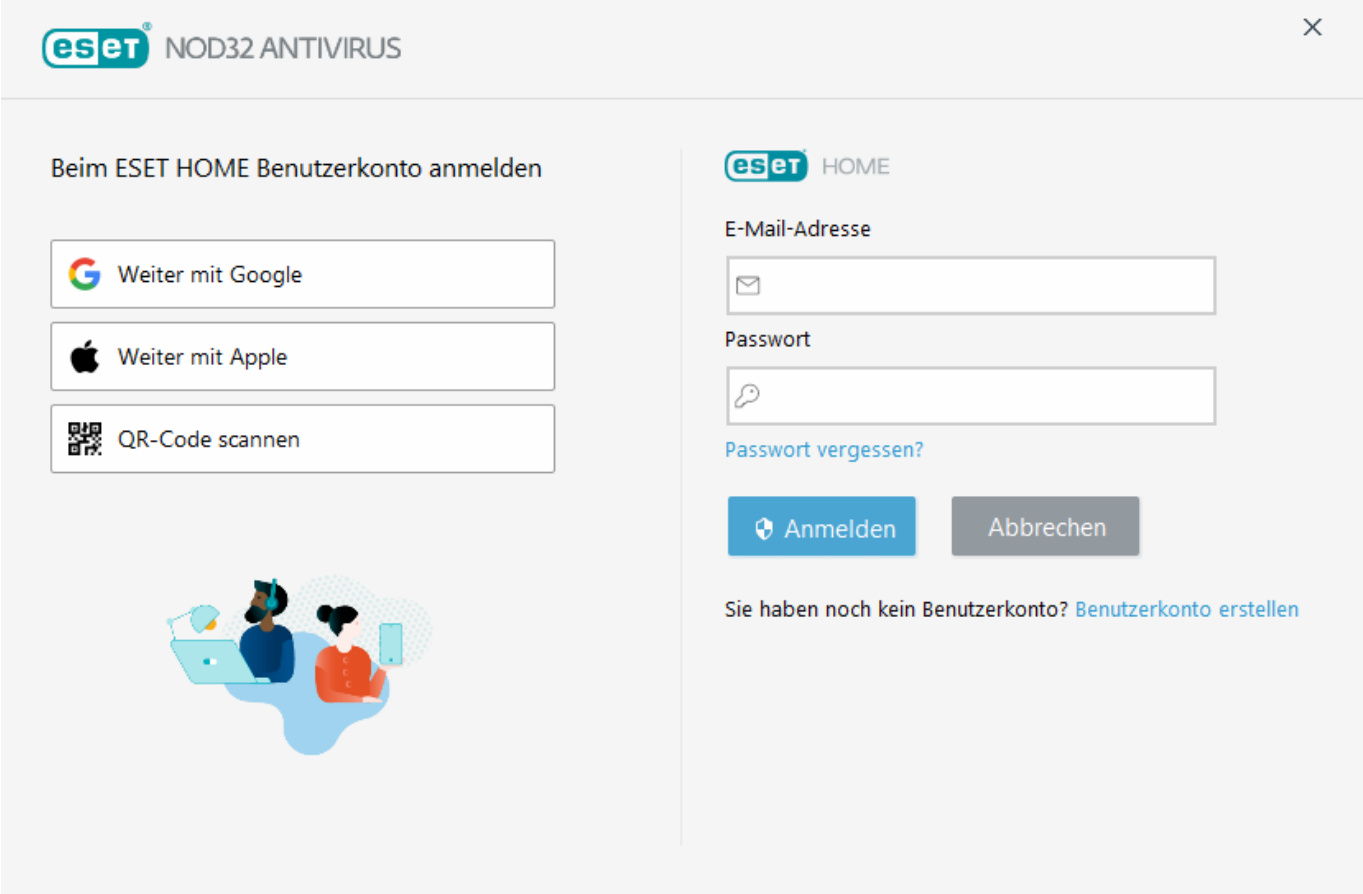
Kopieren Sie den Lizenzschlüssel aus der Registrierungs-E-Mail und fügen Sie ihn in das Feld ein, um Tippfehler zu vermeiden.

Wenn Sie Ihren Lizenzschlüssel nach der Installation nicht eingegeben haben, wird Ihr Produkt nicht aktiviert. Sie können ESET NOD32 Antivirus im Hauptprogrammfenster unter **Hilfe und Support** > **Lizenz aktivieren** aktivieren.

Die vollständigen Lizenzen für ESET Windows Home-Produkte sind nicht kostenlos.

ESET HOME-Konto verwenden

Verbinden Sie Ihr Gerät mit dem ESET HOME, um all Ihre aktivierten ESET-Lizenzen und -Geräte anzuzeigen und zu verwalten. Sie können Ihre Lizenz verlängern, aktualisieren oder erweitern und wichtige Lizenzdetails anzeigen. Im ESET HOME-Verwaltungsportal oder in der mobilen App können Sie und weitere Lizenzen hinzufügen, Produkte auf Ihre Geräte herunterladen, den Produktsicherheitsstatus überprüfen oder Lizenzen per E-Mail teilen. Weitere Informationen finden Sie auf den ESET HOME-Onlinehilfeseiten.



Führen Sie die folgenden Schritte aus, nachdem Sie **ESET HOME-Konto verwenden** als Aktivierungsmethode ausgewählt haben oder während Sie im Rahmen der Installation eine Verbindung zum ESET HOME-Konto herstellen:

1. Melden Sie sich bei Ihrem ESET HOME-Konto an.

> Wenn Sie kein ESET HOME-Konto haben, klicken Sie zum Registrieren auf **Konto erstellen**, oder lesen Sie die Anweisungen in der ESET HOME-Online-Hilfe.
> Sollten Sie Ihr P vergessen haben, klicken Sie auf **Ich habe mein Passwort vergessen** und folgen den Anweisungen auf dem Bildschirm, oder lesen Sie die Anweisungen in der ESET HOME-Online-Hilfe.

2. Legen Sie einen **Gerätenamen** für das Gerät fest, das für alle ESET HOME-Dienste verwendet werden soll, und klicken Sie auf **Weiter**.

3. Wählen Sie eine Lizenz für die Aktivierung aus, oder fügen Sie eine neue Lizenz hinzu. Klicken Sie auf **Weiter**, um ESET NOD32 Antivirus zu aktivieren.

Testlizenz aktivieren

Um Ihre ESET NOD32 Antivirus-Testversion zu aktivieren, geben Sie eine gültige E-Mail-Adresse in die Felder **E-Mail-Adresse** und **E-Mail-Adresse bestätigen** ein. Nach der Aktivierung wird Ihre ESET-Lizenz und an Ihre E-Mail-Adresse gesendet. Diese E-Mail-Adresse wird auch für Benachrichtigungen über das Ablaufen des Produkts und anderweitige Kommunikation mit ESET verwendet. Die Testversion kann nur einmal aktiviert werden.

Wählen Sie Ihr **Land** aus der Liste aus, um ESET NOD32 Antivirus bei Ihrem zuständigen Vertriebspartner zu registrieren. Dorthin können Sie auch Ihre Supportanfragen richten.

Kostenloser ESET-Lizenzschlüssel

Die vollständige Lizenz ESET NOD32 Antivirus ist nicht kostenlos.

Der ESET-Lizenzschlüssel ist eine eindeutige Abfolge von Buchstaben und Ziffern (getrennt durch einen Gedankenstrich) und wird von ESET bereitgestellt, um die rechtmäßige Nutzung von ESET NOD32 Antivirus gemäß der Endbenutzer-Lizenzvereinbarung zu erlauben. Die Endbenutzer dürfen den Lizenzschlüssel für ESET NOD32 Antivirus nur in dem Umfang eingeben, für die entsprechende Anzahl von Lizenzen von ESET erteilt wurde. Der Lizenzschlüssel ist vertraulich und darf nicht weitergegeben werden. Sie können die Lizenzplätze jedoch mit dem ESET HOME weitergeben.

Im Internet gibt es Websites, die „kostenlose“ ESET-Lizenzschlüssel anbieten. Beachten Sie dabei jedoch Folgendes:

- Wenn Sie auf eine Werbung für eine „Kostenlose ESET-Lizenz“ klicken, kann es passieren, dass Ihr Computer oder Ihr Gerät mit Malware infiziert wird. Malware verbirgt sich in inoffiziellen Webinhalten (z. B. Videos), auf Webseiten, die sich über Werbung und Besuche finanzieren usw. Diese Angebote sind normalerweise eine Falle.

- ESET deaktiviert unrechtmäßige Lizenzen.

- Die Nutzung von unrechtmäßigen Lizenzschlüsseln verstößt gegen die Endbenutzer-Lizenzvereinbarung, die Sie bei der Installation von ESET NOD32 Antivirus akzeptieren müssen.

- Kaufen Sie ESET-Lizenzen nur über offizielle Kanäle wie etwa www.eset.com, Distributoren oder Wiederverkäufer von ESET (kaufen Sie keine Lizenzen von inoffiziellen externen Webseiten wie eBay oder gemeinsam genutzte Lizenzen von externen Anbietern).

- Der Download von ESET NOD32 Antivirus ist kostenlos, aber für die Aktivierung bei der Installation ist ein gültiger ESET-Lizenzschlüssel erforderlich. Sie können die Software also herunterladen und installieren, aber ohne Aktivierung nicht verwenden.

- Teilen Sie Ihre Lizenz nicht im Internet oder in sozialen Netzwerken, da sie sich ansonsten unkontrolliert weiterverbreiten kann.

Falls Sie eine unrechtmäßige ESET-Lizenz melden möchten, finden Sie weitere Hinweise in unserem Knowledgebase-Artikel.

Falls Sie mit dem Gedanken spielen, ein ESET-Sicherheitsprodukt zu kaufen, können Sie eine Testversion verwenden, um die Entscheidung zu erleichtern:

1. ESET NOD32 Antivirus mit einer kostenlosen Probelizenz aktivieren

2. Teilnahme am ESET Beta-Programm

3. Installieren Sie ESET Mobile Security, falls Sie ein Android-Mobilgerät verwenden. Die Software ist Freemium.

Rabatte / Lizenzverlängerungen:

- Empfehlen Sie ESET NOD32 Antivirus Ihren Freunden

- Verlängern Sie Ihre ESET-Lizenz (falls Sie bereits eine aktive Lizenz hatten), oder aktivieren Sie die Software für einen längeren Zeitraum.

Fehler bei der Aktivierung - häufige Szenarien

Falls bei der Aktivierung von ESET NOD32 Antivirus Probleme auftreten, sind dies die häufigsten Ursachen:

- Lizenzschlüssel wird bereits verwendet
- Ungültiger Lizenzschlüssel. Fehler im Produktaktivierungsformular
- Für die Aktivierung erforderliche Zusatzinformationen 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

Überprüfen Sie, ob Sie den richtigen Lizenzschlüssel eingegeben haben, und versuchen Sie es erneut. Falls Sie ein ESET HOME-Benutzerkonto für die Aktivierung verwenden, finden Sie weitere Informationen unter ESET HOME-Lizenzverwaltung – Onlinehilfe.

Wenn Sie ihr Produkt immer noch nicht aktivieren können, finden Sie unter ESET Activation Troubleshooter Informationen zu häufig gestellten Fragen, Fehlern und Problemen in den Bereichen Aktivierung und Lizenzierung (auf Englisch und in verschiedenen anderen Sprachen).

Fehler bei der Aktivierung aufgrund von überbeanspruchter Lizenz

Problem

- Ihre Lizenz wurde möglicherweise überbeansprucht oder missbraucht
- Fehler bei der Aktivierung aufgrund von überbeanspruchter Lizenz

Lösung

Diese Lizenz wird von mehr Geräten verwendet als erlaubt. Möglicherweise sind Sie Opfer von Software-Piraterie oder Fälschungen geworden. Diese Lizenz kann nicht zur Aktivierung weiterer ESET Produkte verwendet werden. Sie können dieses Problem direkt beheben, falls Sie zur Verwaltung der Lizenz in Ihrem ESET HOME-Konto berechtigt sind oder die Lizenz aus einer legalen Quelle erworben haben. Falls Sie noch kein Konto haben, können Sie jederzeit eines erstellen.

Falls Sie Eigentümer der Lizenz sind und nicht zur Eingabe Ihrer E-Mail-Adresse aufgefordert wurden:

1. Um Ihre ESET-Lizenz zu verwalten, öffnen Sie einen Webbrowser und navigieren zu. https://home.eset.com. Öffnen Sie ESET License Manager, und entfernen bzw. deaktivieren Sie Lizenzplätze. Weitere Informationen

finden Sie unter Vorgehensweise bei einer Lizenzüberbeanspruchung.

2. Falls Sie eine unrechtmäßige ESET-Lizenz melden möchten, finden Sie weitere Hinweise in unserem Artikel zum Identifizieren und Melden von unrechtmäßigen ESET-Lizenzen.

3. Falls Sie sich nicht sicher sind, klicken Sie auf „**Zurück**“ und schicken Sie eine E-Mail an den ESET-Support.

Wenn Sie kein Lizenzinhaber sind, wenden Sie sich an den Besitzer der Lizenz mit dem Hinweis, dass die Lizenz überbeansprucht ist und Sie Ihr ESET Produkt nicht aktivieren können. Der Besitzer kann dieses Problem im ESET HOME-Portal beheben.

Falls Sie aufgefordert werden, Ihre E-Mail-Adresse zu bestätigen (in verschiedenen Fällen möglich), geben Sie die E-Mail-Adresse ein, die Sie beim Kauf oder bei der Aktivierung von ESET NOD32 Antivirus verwendet haben.

Lizenz-Upgrade

Dieses Benachrichtigungsfenster wird angezeigt, wenn die Lizenz, mit der Sie Ihr ESET-Produkt aktiviert haben, geändert wurde. Mit der neuen Lizenz können Sie ein Produkt mit größerem Funktionsumfang aktivieren. Wenn keine Änderung vorgenommen wurde, zeigt ESET NOD32 Antivirus einmalig das Hinweisfenster **Zu einem Produkt mit mehr Features wechseln** an.

Ja (empfohlen) - Das Produkt mit größerem Funktionsumfang wird automatisch installiert.

Nein danke - Es werden keine Änderungen vorgenommen, und die Benachrichtigung wird nicht mehr angezeigt.

Falls Sie das Produkt später ändern möchten, finden Sie weitere Informationen in unserem ESET Knowledgebase-Artikel. Weitere Informationen zu ESET-Lizenzen finden Sie in den Häufig gestellten Fragen zur Lizenzierung.

Die folgende Tabelle enthält die verfügbaren Funktionen der einzelnen Produkte.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
Malware Scan Engine	✔	✔	✔
Erweitertes Machine Learning	✔	✔	✔
Exploit-Blocker	✔	✔	✔
Skriptbasierter Angriffsschutz	✔	✔	✔
Phishing-Schutz	✔	✔	✔
Web-Schutz	✔	✔	✔
HIPS (inklusive Ransomware Shield)	✔	✔	✔
Spam-Schutz		✔	✔
Firewall		✔	✔
Sicheres Heimnetzwerk		✔	✔
Webcam-Schutz		✔	✔
Netzwerkangriffsschutz		✔	✔
Botnet-Erkennung		✔	✔
Sicheres Online-Banking und Bezahlen		✔	✔
Kindersicherung		✔	✔

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
Anti-Theft		✔	✔
Password Manager			✔
ESET Secure Data			✔
ESET LiveGuard			✔

Produkt-Upgrade

Sie haben ein Installationsprogramm heruntergeladen und das zu aktivierende Produkt geändert, oder Sie möchten ein Produkt mit größerem Funktionsumfang als Ihre aktuell installierte Version verwenden.

Produkt während der Installation ändern.

Die folgende Tabelle enthält die verfügbaren Funktionen der einzelnen Produkte.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
Malware Scan Engine	✔	✔	✔
Erweitertes Machine Learning	✔	✔	✔
Exploit-Blocker	✔	✔	✔
Skriptbasierter Angriffsschutz	✔	✔	✔
Phishing-Schutz	✔	✔	✔
Web-Schutz	✔	✔	✔
HIPS (inklusive Ransomware Shield)	✔	✔	✔
Spam-Schutz		✔	✔
Firewall		✔	✔
Sicheres Heimnetzwerk		✔	✔
Webcam-Schutz		✔	✔
Netzwerkangriffsschutz		✔	✔
Botnet-Erkennung		✔	✔
Sicheres Online-Banking und Bezahlen		✔	✔
Kindersicherung		✔	✔
Anti-Theft		✔	✔
Password Manager			✔
ESET Secure Data			✔
ESET LiveGuard			✔

Lizenz-Downgrade

Dieses Dialogfenster wird angezeigt, wenn die Lizenz, mit der Sie Ihr ESET-Produkt aktiviert haben, geändert wurde. Ihre geänderte Lizenz kann nur mit einem anderen ESET-Produkt mit geringerem Funktionsumfang verwendet werden. Das Produkt wurde automatisch geändert, um Sie auch weiterhin zu schützen.

Weitere Informationen zu ESET-Lizenzen finden Sie in den Häufig gestellten Fragen zur Lizenzierung.

Die folgende Tabelle enthält die verfügbaren Funktionen der einzelnen Produkte.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
Malware Scan Engine	✔	✔	✔
Erweitertes Machine Learning	✔	✔	✔
Exploit-Blocker	✔	✔	✔
Skriptbasierter Angriffsschutz	✔	✔	✔
Phishing-Schutz	✔	✔	✔
Web-Schutz	✔	✔	✔
HIPS (inklusive Ransomware Shield)	✔	✔	✔
Spam-Schutz		✔	✔
Firewall		✔	✔
Sicheres Heimnetzwerk		✔	✔
Webcam-Schutz		✔	✔
Netzwerkangriffsschutz		✔	✔
Botnet-Erkennung		✔	✔
Sicheres Online-Banking und Bezahlen		✔	✔
Kindersicherung		✔	✔
Anti-Theft		✔	✔
Password Manager			✔
ESET Secure Data			✔
ESET LiveGuard			✔

Produkt-Downgrade

Das aktuell installierte Produkt hat mehr Sicherheitsfunktionen als das Produkt, das Sie aktivieren möchten.

Die folgende Tabelle enthält die verfügbaren Funktionen der einzelnen Produkte.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
Malware Scan Engine	✔	✔	✔
Erweitertes Machine Learning	✔	✔	✔
Exploit-Blocker	✔	✔	✔
Skriptbasierter Angriffsschutz	✔	✔	✔
Phishing-Schutz	✔	✔	✔
Web-Schutz	✔	✔	✔
HIPS (inklusive Ransomware Shield)	✔	✔	✔
Spam-Schutz		✔	✔
Firewall		✔	✔

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
Sicheres Heimnetzwerk		✔	✔
Webcam-Schutz		✔	✔
Netzwerkangriffsschutz		✔	✔
Botnet-Erkennung		✔	✔
Sicheres Online-Banking und Bezahlen		✔	✔
Kindersicherung		✔	✔
Anti-Theft		✔	✔
Password Manager			✔
ESET Secure Data			✔
ESET LiveGuard			✔

Fehlerbehebung bei der Installation

Wenn bei der Installation Probleme auftreten, finden Sie im Installationsassistenten eine Fehlerbehebungsfunktion, mit der Sie das Problem nach Möglichkeit beheben können.

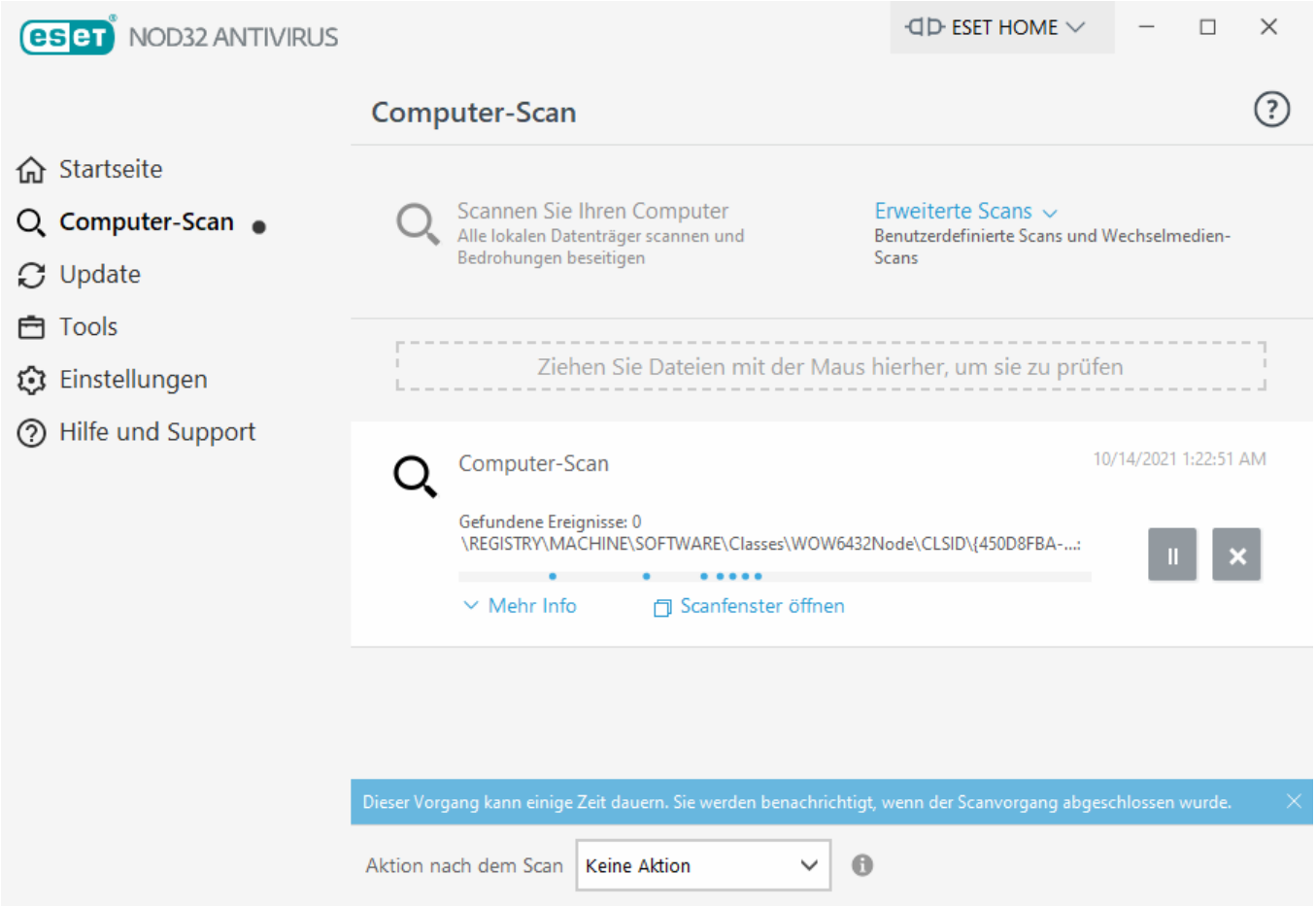
Klicken Sie zum Starten der Fehlerbehebung auf **Fehlerbehebung ausführen**. Folgen Sie nach Abschluss der Fehlerbehebung der empfohlenen Lösung.

Falls das Problem weiterhin auftritt, finden Sie eine Liste der häufigsten Fehler bei der Installation sowie Lösungen.

Erstprüfung nach Installation

Nach der Installation von ESET NOD32 Antivirus und dem ersten erfolgreichen Update wird der Computer auf Schadsoftware geprüft.

Sie können die Prüfung des Computers auch manuell aus dem Haupt-Programmfenster auslösen, indem Sie auf **Computer-Scan** > **Computer-Scan** klicken. Weitere Informationen zur Prüfung des Computers finden Sie im Abschnitt Computer-Scan.



Upgrade auf eine aktuellere Version

Neuere Versionen von ESET NOD32 Antivirus werden veröffentlicht, um Verbesserungen oder Patches zu implementieren, die mit automatischen Updates der Programmmodule behoben werden können. Es gibt verschiedene Möglichkeiten, ein Upgrade auf eine aktuellere Version durchzuführen:

1. Automatische Aktualisierung durch ein Programm-Update
Da das Programm-Update an alle Benutzer des Programms ausgegeben wird und Auswirkungen auf bestimmte Systemkonfigurationen haben kann, wird es erst nach einer langen Testphase veröffentlicht, wenn sicher ist, dass es in allen möglichen Konfigurationen funktioniert. Wenn Sie sofort nach der Veröffentlichung eines Upgrades auf die neue Version aufrüsten möchten, befolgen Sie eine der nachstehenden Methoden.
Stellen Sie sicher, dass Sie die Option **Updates für Anwendungsfeatures** unter **Erweiterte Einstellungen** (F5) > **Update** > **Profile** > **Updates** aktiviert haben.

2. Manuell im Hauptfenster unter **Nach Updates suchen** im Bereich **Update**.

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

Weitere Informationen und illustrierte Anweisungen finden Sie unter:

- ESET Produkte aktualisieren - Nach aktuellen Produktmodulen suchen
- Welche Produktupdates und Versionstypen sind von ESET erhältlich?

Automatisches Upgrade für veraltete Produkte

Ihre ESET-Produktversion wird nicht mehr unterstützt, und Ihr Produkt wurde auf die neueste Version aktualisiert.

Bekannte Probleme bei der Installation

Jede neue Version der ESET-Produkte enthält zahlreiche Bugfixes und Verbesserungen. Vorhandene Kunden mit einer gültigen Lizenz für ein ESET-Produkt können ihr Produkt kostenlos auf die neueste Version desselben Produkts aktualisieren.

Zum Abschluss der Installation:

1. Klicken Sie auf **Akzeptieren und fortfahren**, um die Endbenutzer-Lizenzvereinbarung und die Datenschutzerklärung zu akzeptieren. Falls Sie mit der Endbenutzer-Lizenzvereinbarung nicht einverstanden sind, klicken Sie auf **deinstallieren**. Die vorherige Version kann nicht wiederhergestellt werden.

2. Klicken Sie auf **Alle zulassen und fortfahren**, um das ESET LiveGrid®-Feedbacksystem und das Programm für ein besseres Kundenerlebnis zuzulassen, oder klicken Sie auf **Weiter**, falls Sie nicht teilnehmen möchten.

3. Nachdem Sie das neue ESET Produkt mit Ihrem Lizenzschlüssel aktiviert haben, wird die Startseite angezeigt. Falls Ihre Lizenzinformationen nicht gefunden wurden, fahren Sie mit einer neuen Testlizenz fort. Falls Ihre Lizenz aus dem vorherigen Produkt nicht gültig ist, aktivieren Sie Ihr ESET-Produkt.

4. Zum Abschluss der Installation muss das Gerät neu gestartet werden.

ESET-Produkte an Freunde weiterempfehlen

Mit der aktuellen Version von ESET NOD32 Antivirus wurden Empfehlungsboni eingeführt, damit Sie Ihr ESET-Produkterlebnis mit Freunden oder Familienmitgliedern teilen können. Sie können sogar Empfehlungen von einem Produkt teilen, das mit einer Probelizenz aktiviert wurde. Falls Sie eine Probelizenz verwenden, erhalten Sie und die andere Person für jede erfolgreich verschickte Empfehlung, die zu einer Produktaktivierung führt, eine Verlängerung Ihrer Probelizenz.

Sie können die Empfehlungen in Ihrem installierten ESET NOD32 Antivirus verschicken. Die Produkte, die Sie empfehlen können, hängen von dem Produkt ab, das Sie verwenden.

Ihr installiertes Produkt	Produkte, die Sie empfehlen können
ESET NOD32 Antivirus	ESET Internet Security
ESET Internet Security	ESET Internet Security
ESET Smart Security Premium	ESET Smart Security Premium

Empfehlen von Produkten

Um einen Empfehlungslink zu verschicken, klicken Sie auf **Einem Freund empfehlen** im Hauptmenü von ESET NOD32 Antivirus. Klicken Sie auf **Mit Empfehlungslink empfehlen**. Der von Ihrem Produkt generierte Empfehlungslink wird in einem neuen Fenster angezeigt. Kopieren Sie den Link und senden Sie ihn an Freunde und Familienmitglieder. Kopieren Sie den Link und senden Sie ihn an Freunde und Familienmitglieder, oder teilen Sie ihn direkt in Ihrem ESET-Produkt mit den Optionen **Auf Facebook teilen**, **Ihren Gmail-Kontakten empfehlen**

und **Auf Twitter teilen**.

Wenn einer Ihrer Freunde auf Ihren Empfehlungslink klickt, wird die Person auf eine Webseite weitergeleitet, auf der sie das Produkt herunterladen und ihren KOSTENLOSEN Schutz um einen Monat verlängern können. Falls Sie eine Probelizenz verwenden, erhalten Sie eine Benachrichtigung für jede erfolgreich verschickte Empfehlung, die zu einer Produktaktivierung führt, und Ihre Lizenz wird automatisch KOSTENLOS um einen Monat verlängert. Auf diese Weise können Sie Ihren KOSTENLOSEN Schutz um bis zu fünf Monate verlängern. Sie finden die Anzahl der erfolgreich aktivierten Empfehlungslinks im Fenster **Einem Freund empfehlen** in Ihrem ESET-Produkt.

Die Empfehlungsfunktion ist möglicherweise nicht für Ihre Sprache oder Region verfügbar.

ESET NOD32 Antivirus wird installiert

Das folgende Dialogfenster wird angezeigt:

- Während der Installation – Klicken Sie auf **Weiter**, um ESET NOD32 Antivirus zu installieren.
- Wenn Sie eine Lizenz in ESET NOD32 Antivirus ändern – Klicken Sie auf **Aktivieren**, um die Lizenz zu ändern und ESET NOD32 Antivirus zu aktivieren.

Mit der Option **Produkt wechseln** können Sie zwischen ESET Windows Home-Produkten in Ihrer ESET-Lizenz wechseln. Weitere Informationen finden Sie unter Welches Produkt verwende ich?.

Zu einer anderen Produktreihe ändern

Je nach Ihrer ESET Lizenz können Sie zwischen verschiedenen ESET Windows Home-Produkten wechseln. Weitere Informationen finden Sie unter Welches Produkt verwende ich?.

Registrierung

Registrieren Sie Ihre Lizenz, indem Sie die Felder im Registrierungsformular ausfüllen und auf Aktivieren klicken. Bei den Feldern, neben denen in Klammern „erforderlich“ steht, handelt es sich um Pflichtfelder. Diese Informationen wird nur in Bezug auf Ihre ESET Lizenz verwendet.

Aktivierungsfortschritt

Warten Sie einige Sekunden, bis die Aktivierung abgeschlossen wurde (Die Dauer hängt von der Geschwindigkeit Ihrer Internetverbindung und Ihrem Computer ab).

Aktivierung erfolgreich

Der Aktivierungsvorgang ist abgeschlossen.

Ein Modul-Update wird in wenigen Sekunden gestartet. Reguläre Updates von ESET NOD32 Antivirus werden sofort gestartet.

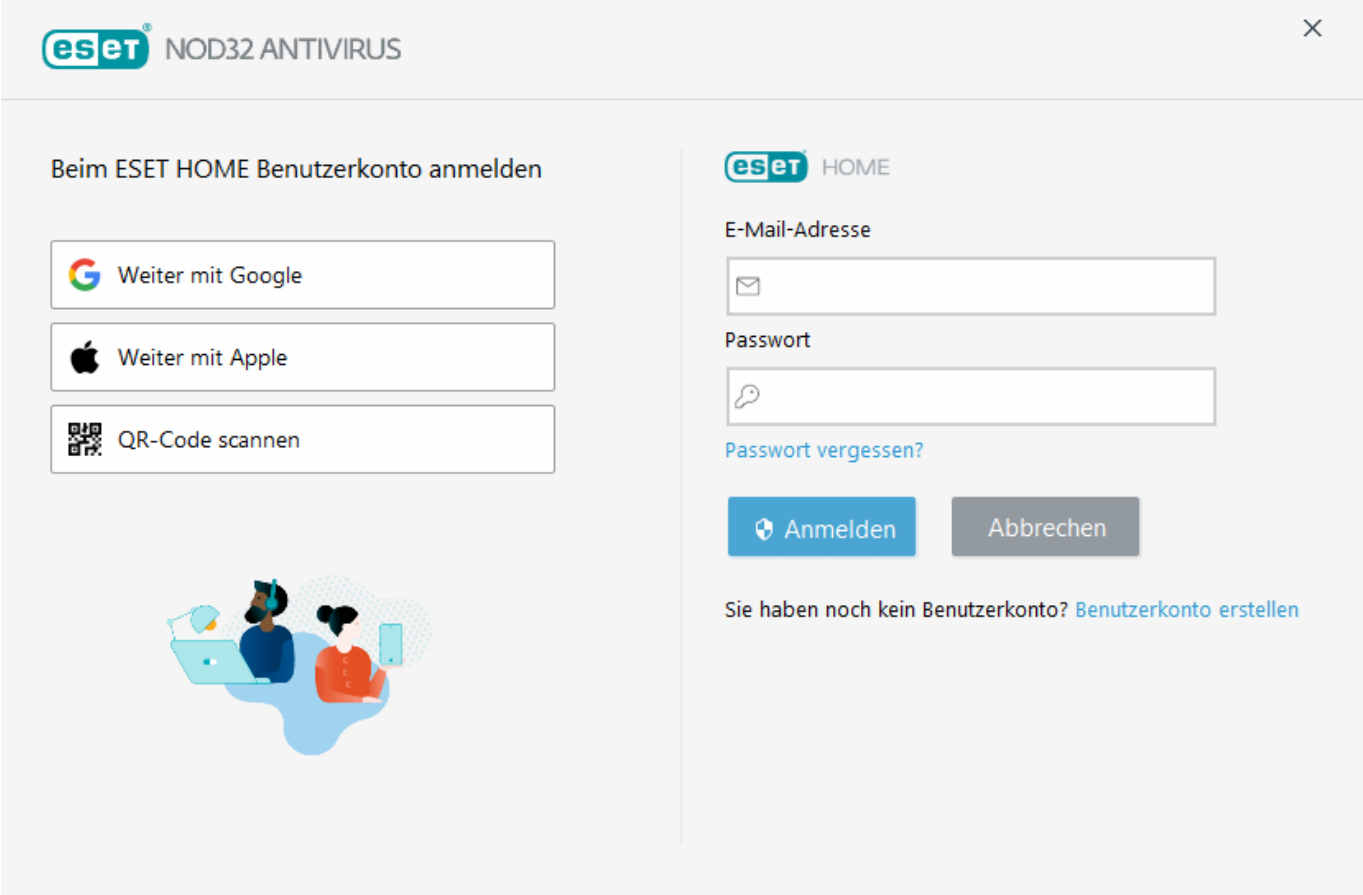
Innerhalb von 20 Minuten nach dem Modul-Update wird automatisch ein Erstscan gestartet.

Erste Schritte

Dieses Kapitel enthält eine einführende Übersicht über ESET NOD32 Antivirus und die Grundeinstellungen des Programms.

Verbinden Sie sich mit ESET HOME

Verbinden Sie Ihr Gerät mit dem ESET HOME, um all Ihre aktivierten ESET-Lizenzen und -Geräte anzuzeigen und zu verwalten. Sie können Ihre Lizenz verlängern, aktualisieren oder erweitern und wichtige Lizenzdetails anzeigen. Im ESET HOME-Verwaltungsportal oder in der mobilen App können Sie und weitere Lizenzen hinzufügen, Produkte auf Ihre Geräte herunterladen, den Produktsicherheitsstatus überprüfen oder Lizenzen per E-Mail teilen. Weitere Informationen finden Sie auf den ESET HOME-Onlinehilfeseiten.



Verbinden Sie Ihr Gerät mit dem ESET HOME:

Falls Sie sich während der Installation mit ESET HOME verbinden oder wenn Sie **ESET HOME Konto verwenden** als Aktivierungsmethode verwenden, folgen Sie den Anweisungen im Thema ESET HOME Konto verwenden.

Falls Sie ESET NOD32 Antivirus bereits installiert und mit einer Lizenz aktiviert haben, die Sie zu Ihrem ESET HOME-Konto hinzugefügt haben, können Sie Ihr Gerät über das ESET HOME-Portal mit ESET HOME verbinden. Weitere Anweisungen finden Sie in der ESET HOME-Online-Hilfe und unter Verbindung mit ESET NOD32 Antivirus zulassen.

1. Klicken Sie im Hauptprogrammfenster in der Benachrichtigung **Dieses Gerät mit einem ESET HOME-Konto**

verbinden auf **ESET HOME** > **Mit ESET HOME** verbinden oder auf **Mit ESET HOME verbinden**.

2. Melden Sie sich bei Ihrem ESET HOME-Konto an.

> Wenn Sie kein ESET HOME-Konto haben, klicken Sie zum Registrieren auf **Konto erstellen**, oder lesen Sie die Anweisungen in der ESET HOME-Online-Hilfe.
> Sollten Sie Ihr P vergessen haben, klicken Sie auf **Ich habe mein Passwort vergessen** und folgen den Anweisungen auf dem Bildschirm, oder lesen Sie die Anweisungen in der ESET HOME-Online-Hilfe.

3. Legen Sie einen **Gerätenamen** fest, und klicken Sie auf **Weiter**.

4. Nach der erfolgreichen Verbindung wird ein Detailfenster angezeigt. Klicken Sie auf **Fertig**.

Bei ESET HOME anmelden

Es gibt diverse Methoden, sich bei Ihrem ESET HOME-Konto anzumelden:

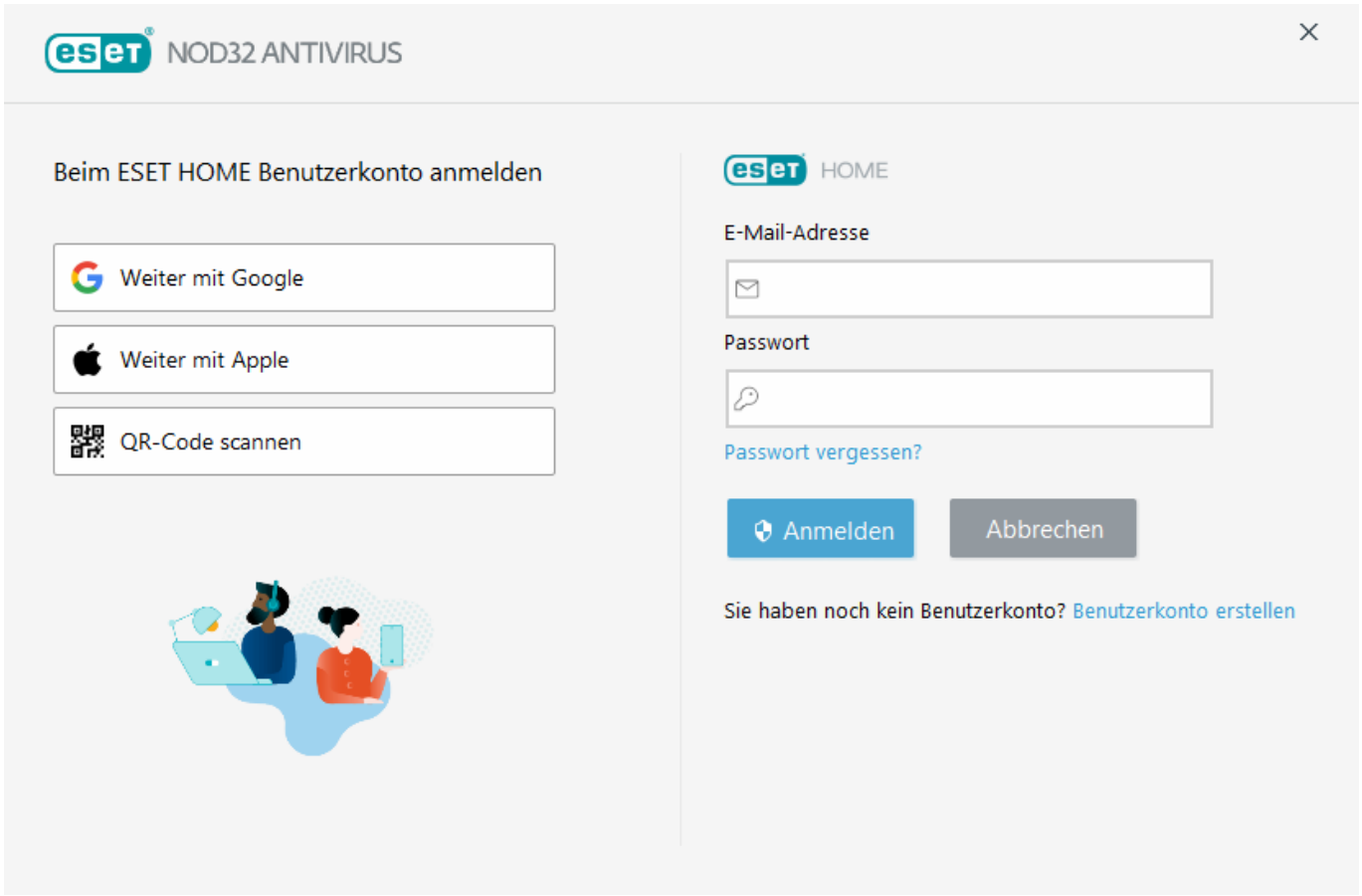
- **ESET HOME-E-Mail-Adresse und Passwort verwenden** – Geben Sie die **E-Mail-Adresse** und das **Passwort** ein, die Sie bei der Erstellung Ihres ESET HOME-Kontos verwendet haben, und klicken Sie auf **Anmelden**.

- **Google-Konto/AppleID** verwenden – Klicken Sie auf **Weiter mit Google** oder **Weiter mit Apple**, und melden Sie sich an dem jeweiligen Konto an. Nach der erfolgreichen Anmeldung werden Sie auf die ESET HOME-Bestätigungs-Webseite weitergeleitet. Wechseln Sie zum Fortsetzen des Vorgangs zurück zum ESET-Produktfenster. Weitere Informationen zur Anmeldung über das Google-Konto oder über die AppleID finden Sie in den Anweisungen in der ESET HOME-Online-Hilfe.

- **QR-Code scannen** – Klicken Sie auf **QR-Code scannen**, um den QR-Code anzuzeigen. Öffnen Sie Ihre ESET HOME Mobile App, und scannen Sie den QR-Code, oder halten Sie Ihre Gerätekamera über den QR-Code. Weitere Informationen finden Sie in den Anweisungen in der ESET HOME-Online-Hilfe.

> Wenn Sie kein ESET HOME-Konto haben, klicken Sie zum Registrieren auf **Konto erstellen**, oder lesen Sie die Anweisungen in der ESET HOME-Online-Hilfe.
> Sollten Sie Ihr P vergessen haben, klicken Sie auf **Ich habe mein Passwort vergessen** und folgen den Anweisungen auf dem Bildschirm, oder lesen Sie die Anweisungen in der ESET HOME-Online-Hilfe.

Anmeldung fehlgeschlagen – häufige Fehler.



Anmeldung fehlgeschlagen – häufige Fehler

Wir haben kein Konto mit der eingegebenen E-Mail-Adresse gefunden.

Die eingegebene E-Mail-Adresse stimmt mit keinem ESET HOME-Konto überein. Klicken Sie auf **Zurück** und geben Sie die richtige E-Mail-Adresse und das richtige Passwort ein.

Zum Anmelden müssen Sie ein ESET HOME-Konto erstellen. Wenn Sie noch kein ESET HOME-Konto eingerichtet haben, klicken Sie auf **Zurück** > **Konto erstellen**, oder lesen Sie die Informationen unter Ein neues ESET HOME-Konto erstellen.

Benutzername und Passwort stimmen nicht überein

Das eingegebene Passwort darf nicht mit der eingegebenen E-Mail-Adresse übereinstimmen. Klicken Sie auf **Zurück**, geben Sie das richtige Passwort ein und überprüfen Sie die eingegebene E-Mail-Adresse. Wenn Sie sich weiterhin nicht anmelden können, klicken Sie auf **Zurück** > **Ich habe mein Passwort vergessen**, um das Passwort zurückzusetzen, und folgen Sie dann den Anweisungen auf dem Bildschirm, oder lesen Sie die Informationen unter Ich habe mein ESET HOME-Passwort vergessen.

Die ausgewählte Anmeldeoption stimmt nicht mir Ihrem Benutzerkonto überein.

Ihr Konto ist mit Ihrem Social-Media-Konto verknüpft. Klicken Sie für die Anmeldung bei ESET HOME auf **Weiter mit Google** oder **Weiter mit Apple**, und melden Sie sich bei dem jeweiligen Konto an. Nach der erfolgreichen

Anmeldung werden Sie zur Bestätigungs-Webseite von ESET HOME weitergeleitet. Sie können Ihr Social-Media-Konto über das ESET HOME-Portal von Ihrem ESET HOME-Konto trennen.

Falsches Passwort

Dieser Fehler kann auftreten, wenn ESET NOD32 Antivirus bereit mit ESET HOME verbunden ist und Sie Änderungen vornehmen, die eine Anmeldung erfordern (wenn Sie z. B. Anti-Theft deaktivieren) und das von Ihnen eingegebene Passwort nicht mit Ihrem Konto übereinstimmt. Klicken Sie auf **Zurück** und geben Sie das richtige Passwort ein. Wenn Sie sich weiterhin nicht anmelden können, klicken Sie auf **Zurück** > **Ich habe mein Passwort vergessen**, um das Passwort zurückzusetzen, und folgen Sie dann den Anweisungen auf dem Bildschirm, oder lesen Sie die Informationen unter Ich habe mein ESET HOME-Passwort vergessen.

Gerät in ESET HOME hinzufügen

Falls Sie ESET NOD32 Antivirus bereits installiert und mit einer Lizenz aktiviert haben, die Sie zu Ihrem ESET HOME-Konto hinzugefügt haben, können Sie Ihr Gerät über das ESET HOME-Portal mit ESET HOME verbinden:

1. Senden Sie eine Verbindungsanfrage an Ihr Gerät.

2. ESET NOD32 Antivirus zeigt das Dialogfenster **Dieses Gerät mit einem ESET HOME-Konto verbinden** mit einem ESET HOME-Kontonamen an. Klicken Sie auf **Zulassen**, um das Gerät mit dem entsprechenden ESET HOME-Konto zu verbinden.

> **i** Wenn keine Interaktion erfolgt, wird die Verbindungsanfrage nach ca. 30 Minuten automatisch abgebrochen.

Das Haupt-Programmfenster

Das Hauptprogrammfenster von ESET NOD32 Antivirus ist in zwei Abschnitte unterteilt. Das primäre Fenster (rechts) zeigt Informationen zu den im Hauptmenü (links) ausgewählten Optionen an.

> **i** Illustrierte Anweisungen
> Weitere Informationen mit illustrierten Anweisungen in Englisch und in weiteren Sprachen finden Sie unter Hauptprogrammfenster von ESET Windows-Produkten öffnen.

ESET HOME – Verbinden Sie Ihr Gerät mit ESET HOME. Verwenden Sie ESET HOME zum Anzeigen und Verwalten Ihrer aktivierte ESET-Lizenzen und -Geräte anzeigen und verwalten.

Im Folgenden werden die Optionen des Hauptmenüs beschrieben:

Startseite - Informationen zum Schutzstatus von ESET NOD32 Antivirus.

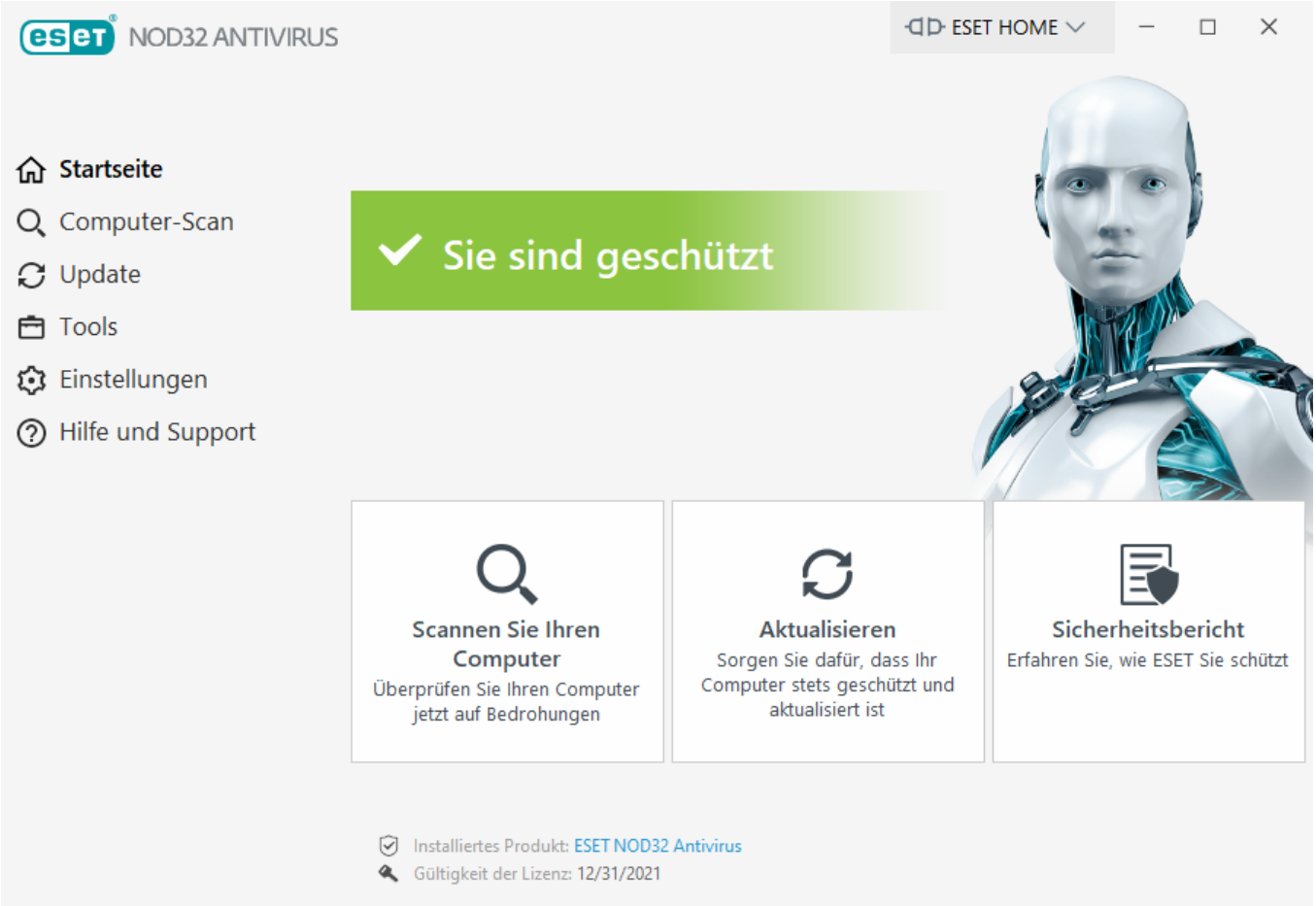
Computerprüfung – Konfigurieren und starten Sie eine Prüfung Ihres Computers oder erstellen Sie eine benutzerdefinierte Prüfung.

Update – Dieser Bereich zeigt Informationen zu Updates der Erkennungsroutine an.

Tools – Enthält die Optionen Module zur einfacheren Verwaltung des Programms sowie zusätzliche Optionen für fortgeschrittene Benutzer. Weitere Informationen finden Sie unter Tools in ESET NOD32 Antivirus.

Einstellungen - Mit dieser Option können Sie die Sicherheitsebene für Ihren Computer, Ihre Internetverbindung.

Hilfe und Support - Dieser Bereich bietet Zugriff auf die Hilfedateien, die ESET-Knowledgebase und die ESET-Website und enthält Links zum Übermitteln von Supportanfragen.

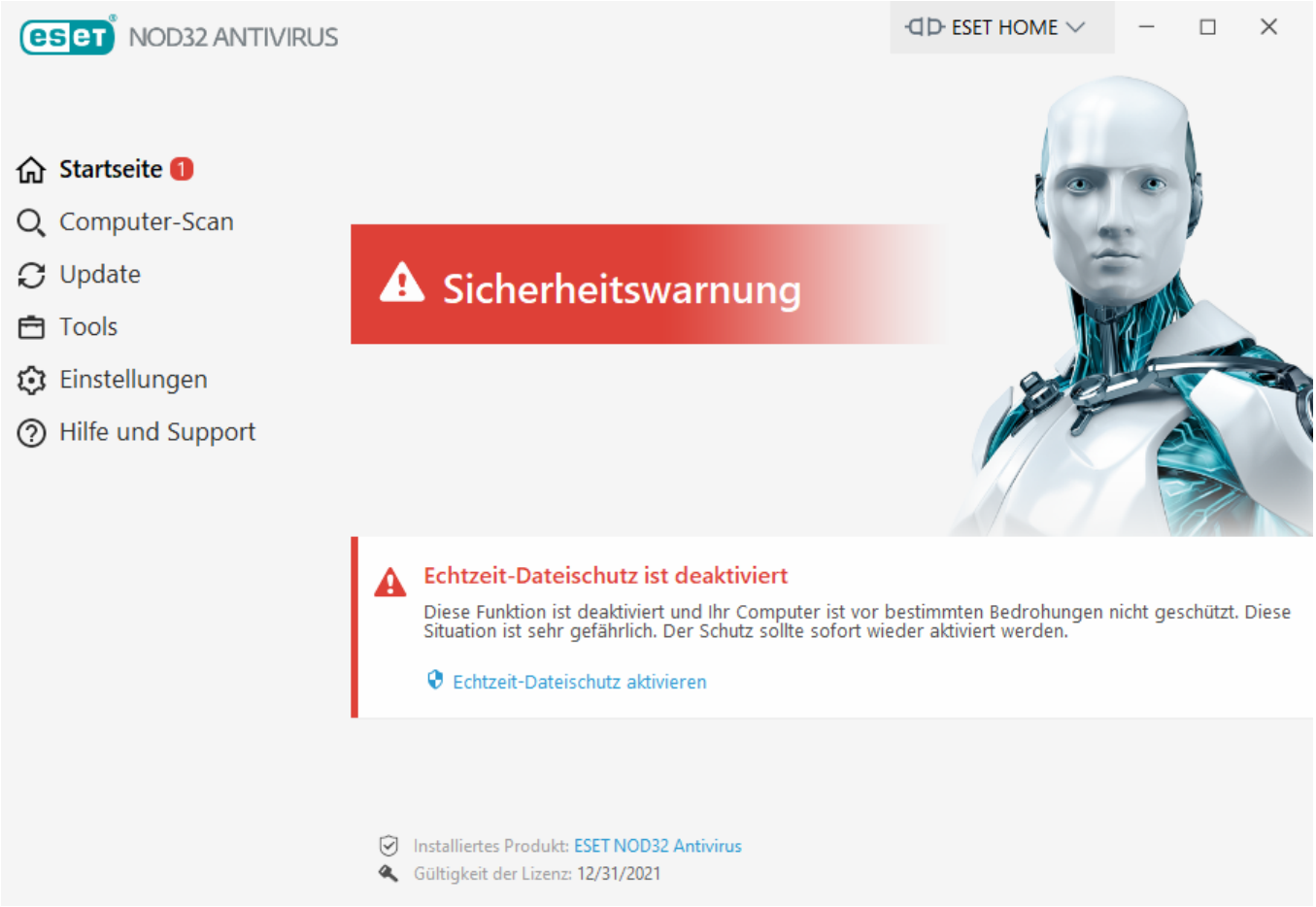


Der **Startbildschirm** enthält wichtige Informationen zur aktuellen Schutzstufe Ihres Computers. Im Statusfenster werden die am häufigsten verwendeten Funktionen von ESET NOD32 Antivirus angezeigt. Hier finden Sie außerdem Informationen zum installierten Produkt und zum Ablaufdatum der Lizenz. Klicken Sie auf **ESET NOD32 Antivirus**, wenn Sie eine andere Version des ESET-Produkts installieren möchten. Weitere Informationen zu den Funktionen der einzelnen Produkte.

Das grüne Icon und der grüne Status **Sie sind geschützt** deuten auf maximalen Schutz hin.

Vorgehensweise bei fehlerhafter Ausführung des Programms

Wenn ein aktiviertes Schutzmodul ordnungsgemäß arbeitet, wird ein grünes Schutzstatussymbol angezeigt. Ein rotes Ausrufezeichen oder ein orangefarbener Hinweis weisen auf ein nicht optimales Schutzniveau hin. Unter **Startseite** werden zusätzliche Informationen zum Schutzstatus der einzelnen Module und empfohlene Lösungen zum Wiederherstellen des vollständigen Schutzes angezeigt. Um den Status einzelner Module zu ändern, klicken Sie auf **Einstellungen** und wählen Sie das gewünschte Modul aus.



Das rote Icon und der Status **Sicherheitswarnung** weisen auf kritische Probleme hin. Dieser Status kann verschiedene Ursachen haben, zum Beispiel:

- **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.
- **Erkennungsroutine ist veraltet** – Dieser Fehler wird angezeigt, wenn die Erkennungsroutine trotz wiederholter Versuche nicht aktualisiert werden konnte. Sie sollten in diesem Fall die Update-Einstellungen überprüfen. Die häufigste Fehlerursache sind falsch eingegebene Lizenzdaten oder fehlerhaft konfigurierte Verbindungseinstellungen.
- **Echtzeit-Dateischutz ist deaktiviert**- Der Echtzeit-Schutz wurde vom Benutzer deaktiviert. Ihr Computer ist nicht vor Bedrohungen geschützt. Klicken Sie auf **Echtzeit-Dateischutz aktivieren**, um diese Funktion erneut zu aktivieren.
- **Viren- und Spyware-Schutz deaktiviert** – Sie können den Virenschutz und den Spyware-Schutz wieder aktivieren, indem Sie auf **Viren- und Spyware-Schutz aktivieren** klicken.

Das orangefarbene Symbol deutet auf eingeschränkten Schutz hin. Möglicherweise bestehen Probleme bei der Aktualisierung des Programms, oder Ihre Lizenz läuft demnächst ab.
Dieser Status kann verschiedene Ursachen haben, zum Beispiel:

- **Gamer-Modus aktiviert** – Im Gamer-Modus besteht ein erhöhtes Risiko. Aktivieren Sie dieses Feature, um alle Popupfenster zu unterdrücken und alle geplanten Tasks zu beenden.
- **Lizenz läuft bald ab** – Dieser Status wird durch ein Schutzstatussymbol mit einem Ausrufezeichen neben der Systemuhr angezeigt. Nach dem Ablaufen der Lizenz ist kein Programm-Update mehr

möglich und das Schutzstatussymbol ist rot.

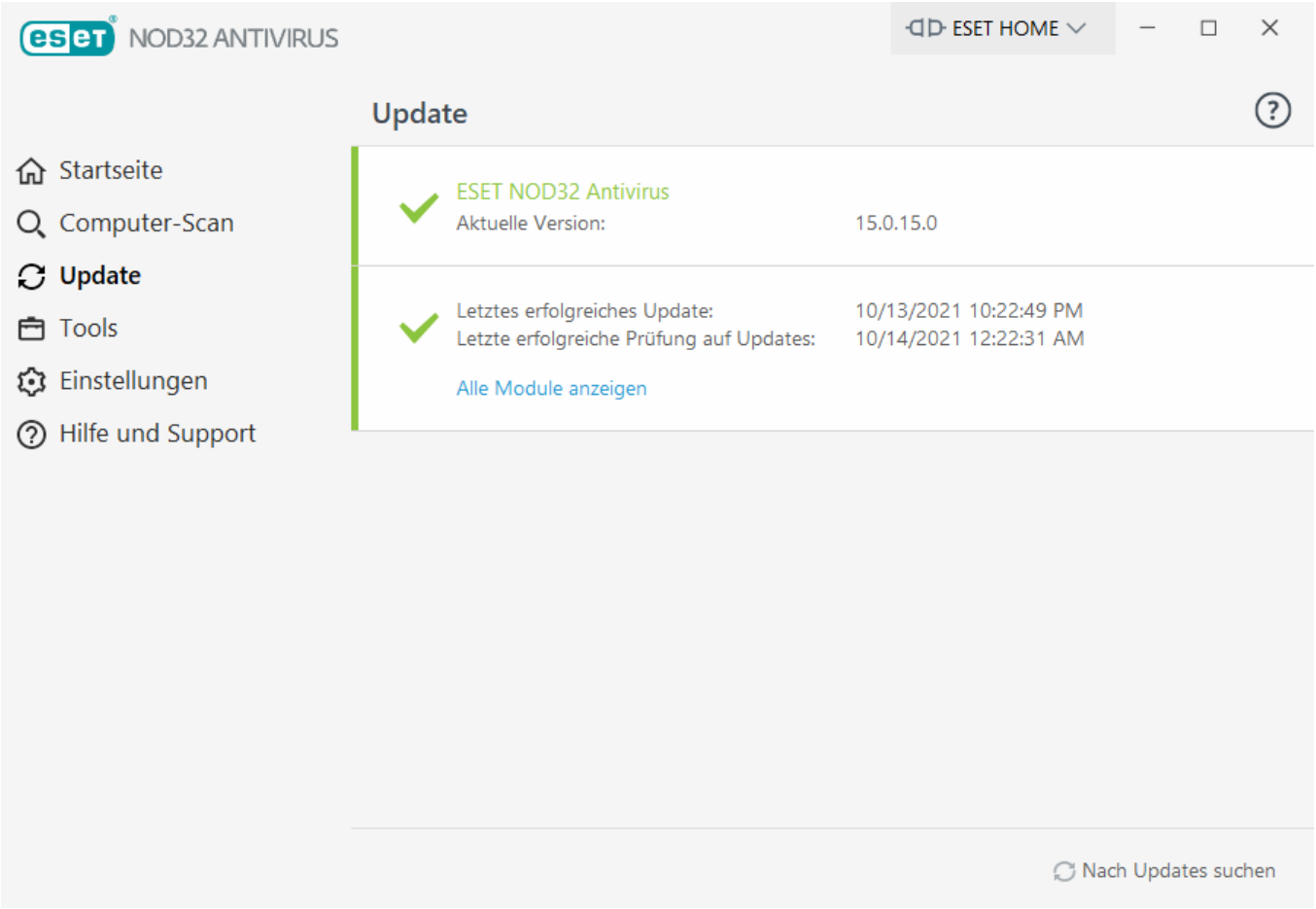
Wenn Sie ein Problem mit den vorgeschlagenen Lösungen nicht beheben können, klicken Sie auf **Hilfe und Support**, um die Hilfedateien oder die ESET-Knowledgebase zu öffnen. Wenn Sie weiterhin Unterstützung benötigen, können Sie eine Support-Anfrage senden. Der ESET-Support wird sich umgehend mit bei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

Updates

Den optimalen Schutz Ihres Computers gewährleisten Sie, indem Sie ESET NOD32 Antivirus regelmäßig aktualisieren. Das Updatemodul hält Programmmodule und Systemkomponenten fortlaufend auf dem neuesten Stand.

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.

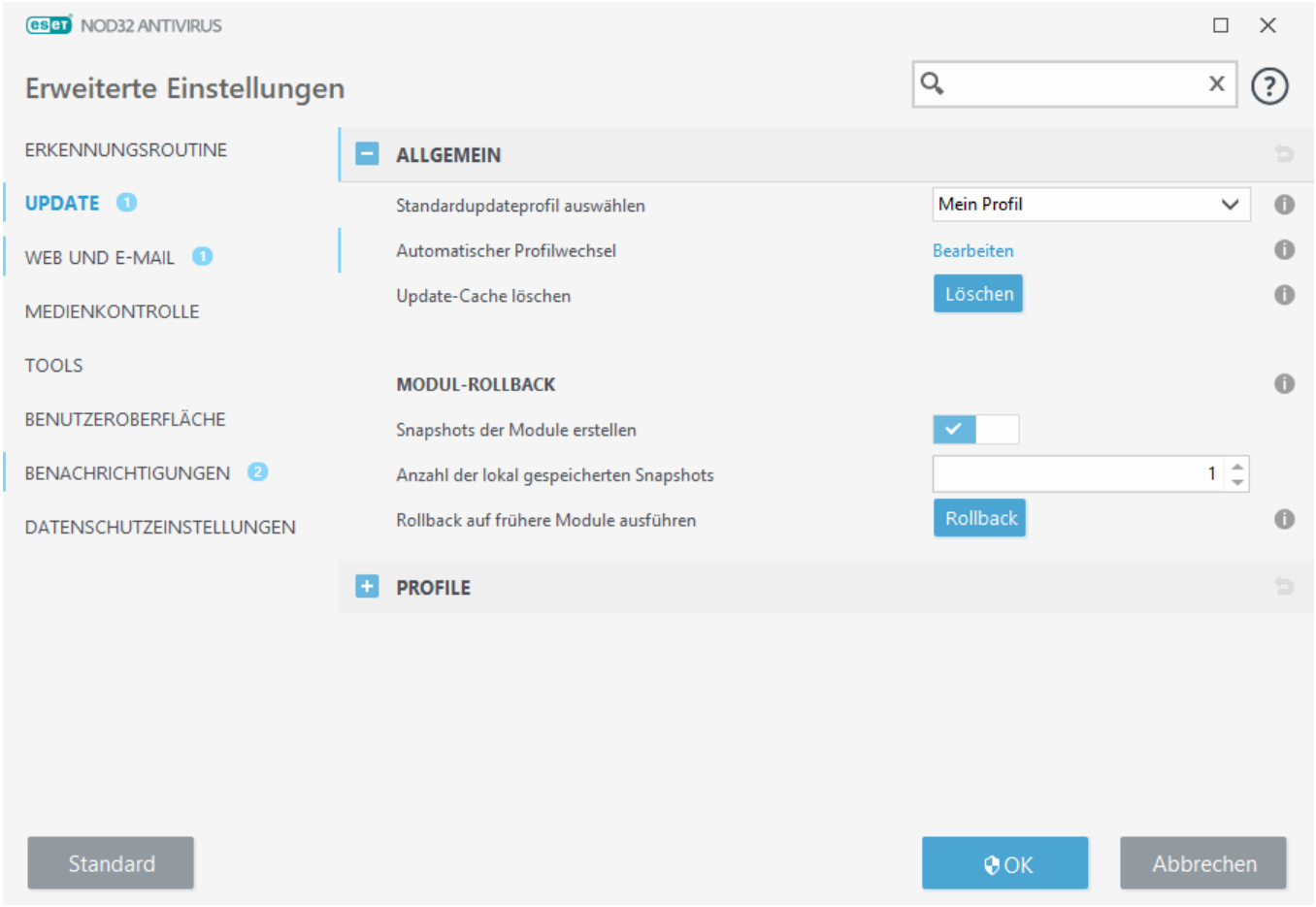
Neben automatischen Updates können Sie auch auf **Nach Updates suchen** klicken, um ein manuelles Update zu starten.



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

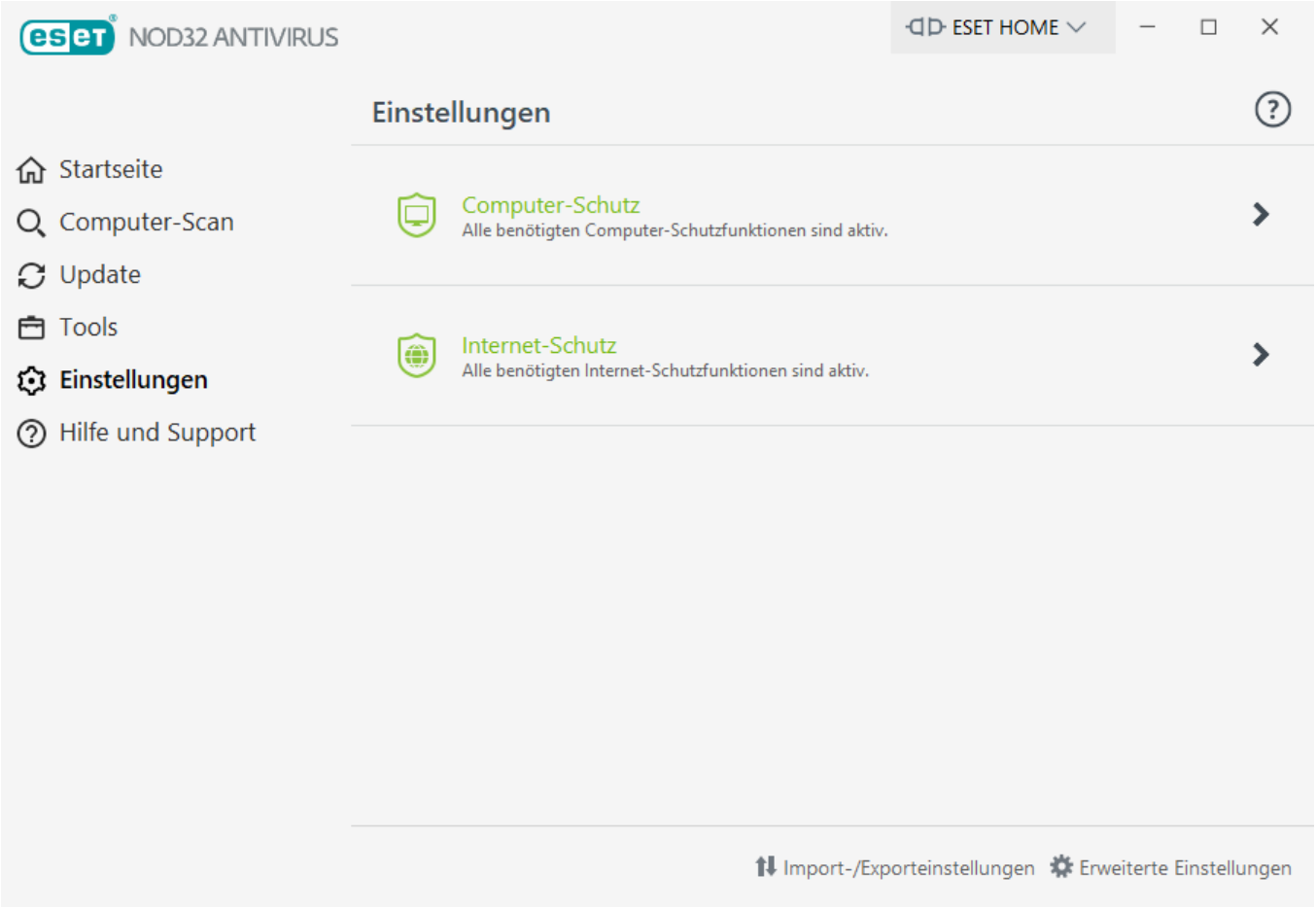
Wenn bei einem Update Fehler auftreten, klicken Sie auf **Löschen**, um den Update-Cache zu löschen. Falls Sie die Programm-Module weiterhin nicht aktualisieren können, finden Sie weitere Hinweise unter So beheben Sie das

Problem „Modulupdate fehlgeschlagen“.



Arbeiten mit ESET NOD32 Antivirus

ESET NOD32 Antivirus Mit den Konfigurationsoptionen können Sie Feinabstimmungen rund um den Schutz Ihres Computers vornehmen.



Das Menü **Einstellungen** enthält die folgenden Bereiche:

Computerschutz

Internet-Schutz

Klicken Sie auf eine Komponente, um die erweiterten Einstellungen des entsprechenden Schutzmoduls anzupassen.

In den Einstellungen für den **Computer**-Schutz können Sie folgende Komponenten aktivieren oder deaktivieren:

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

- **Medienkontrolle** – Mit diesem Modul können Sie Medien bzw. Geräte prüfen oder sperren oder über erweiterte Filter- und Berechtigungseinstellungen festlegen, wie der Benutzer diese Geräte öffnen und verwenden kann (CD/DVD/USB...).

- **HIPS** – Das HIPS-System überwacht Ereignisse auf Betriebssystemebene und führt Aktionen gemäß individueller Regeln aus.

- **Gamer-Modus** – Aktiviert / deaktiviert den Gamer-Modus. Nach der Aktivierung des Gamer-Modus wird eine Warnung angezeigt (erhöhtes Sicherheitsrisiko) und das Hauptfenster wird orange.

In den Einstellungen für den Internet-Schutz können Sie folgende Komponenten aktivieren oder deaktivieren:

- **Web-Schutz** – Wenn diese Option aktiviert ist, werden alle über HTTP oder HTTPS übertragenen Daten auf Malware gescannt.

- **E-Mail-Client-Schutz** – Überwacht eingehende E-Mails, die mit den Protokollen POP3(S) oder IMAP(S) übertragen werden.

- **Phishing-Schutz** – Filtert Websites, für die der Verdacht besteht, dass sie Inhalte enthalten, die den Benutzer zum Einreichen vertraulicher Informationen verleiten.

Um eine deaktivierte Sicherheitskomponente erneut zu aktivieren, klicken Sie auf den Schieberegler  , um sie mit einem grünen Häkchen  zu markieren.

Wenn Sie den Schutz auf diese Weise deaktivieren, werden alle deaktivierten Schutzmodule nach einem Computerneustart wieder aktiviert.

Am unteren Rand des Fensters „Einstellungen“ finden Sie weitere Optionen. Über den Link **Erweiterte Einstellungen** können Sie weitere Parameter für die einzelnen Module konfigurieren. Unter **Einstellungen importieren/exportieren** können Sie Einstellungen aus einer .xml-Konfigurationsdatei laden oder die aktuellen Einstellungen in einer Konfigurationsdatei speichern.

Computerschutz

Klicken Sie auf **Computer-Schutz** in den **Einstellungen**, um eine Übersicht über alle Schutzmodule anzuzeigen.

- Echtzeit-Dateischutz
- Medienkontrolle
- HIPS
- Gamer-Modus

Um einzelne Schutzmodule anzuhalten oder zu deaktivieren, klicken Sie das Schieberegler-Symbol  .

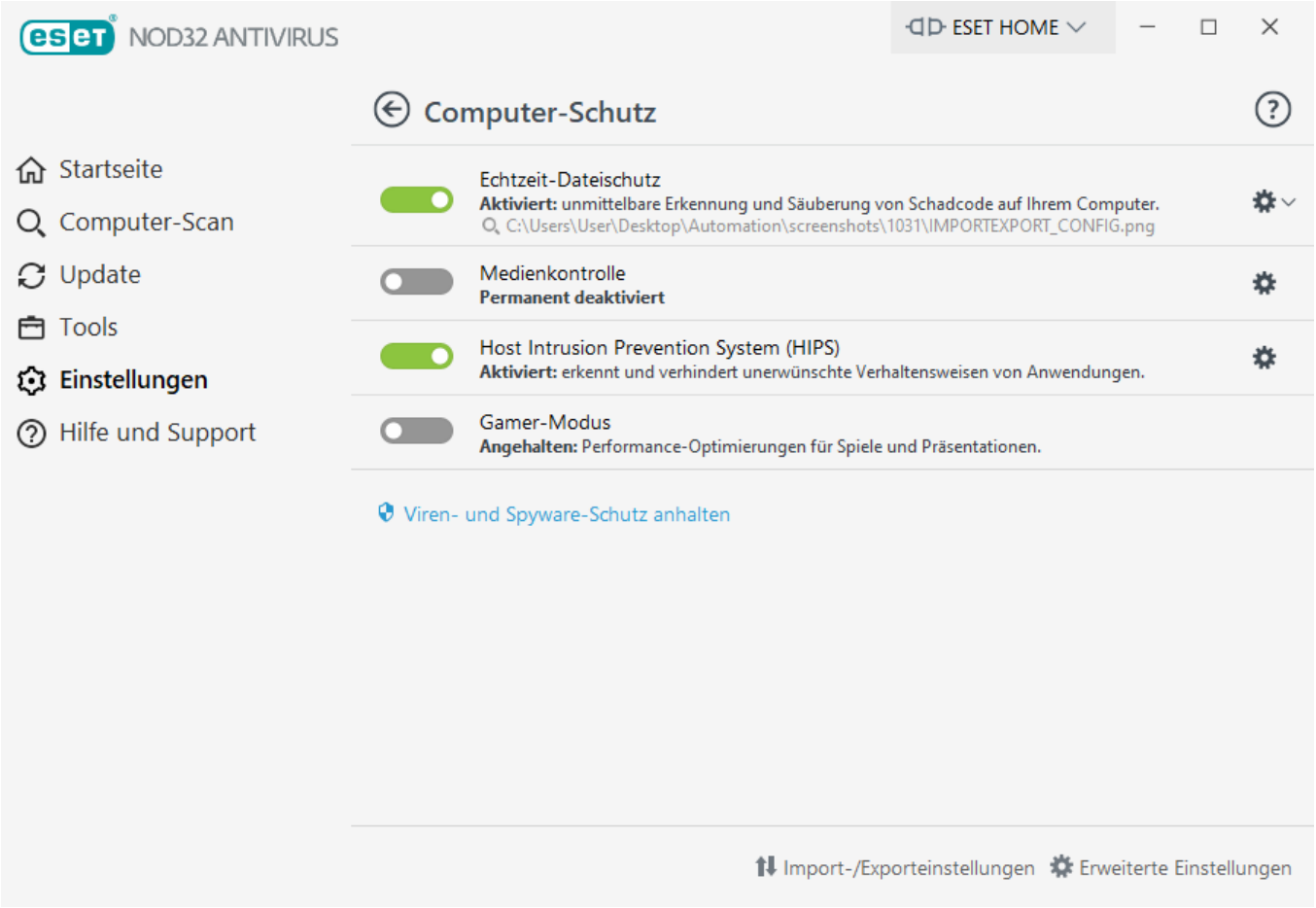
Wenn Sie die Schutzmodule deaktivieren, kann der Schutz Ihres Computers beeinträchtigt werden.

Klicken Sie auf das Zahnradsymbol neben einem Schutzmodul, um erweiterte Einstellungen für dieses Modul zu öffnen.

Klicken Sie für **Echtzeit-Dateischutz** auf das Zahnradsymbol und wählen aus den folgenden Optionen:

- **Konfigurieren** – Öffnet die erweiterten Einstellungen für den Echtzeit-Dateischutz.

- **Ausschlüsse bearbeiten** – Öffnet das Fenster für die Ausschlusseinstellungen, in dem Sie Dateien und Ordner von den Scans ausschließen können.



Viren- und Spyware-Schutz vorübergehend deaktivieren – Deaktiviert alle Viren- und Spyware-Schutzmodule. Wenn Sie den Schutz deaktivieren, wird ein Fenster geöffnet, in dem Sie im Dropdownmenü **Zeitraum** festlegen können, wie lange der Schutz deaktiviert werden soll. Verwenden Sie diese Anwendung nur, wenn Sie ein erfahrener Benutzer sind oder vom technischen Support bei ESET angewiesen wurden.

Malware Scan Engine

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 den Einstellungen der Erkennungsroutine sollten nur von erfahrenen Benutzern vorgenommen werden. Falsch konfigurierte Einstellungen können die Schutzebene reduzieren.

In diesem Abschnitt:

- Kategorien Echtzeit- & Machine-Learning-Schutz
- Malware-Scans
- Einrichten der Berichterstellung

- Einrichten des Schutzes

Kategorien Echtzeit- & Machine-Learning-Schutz

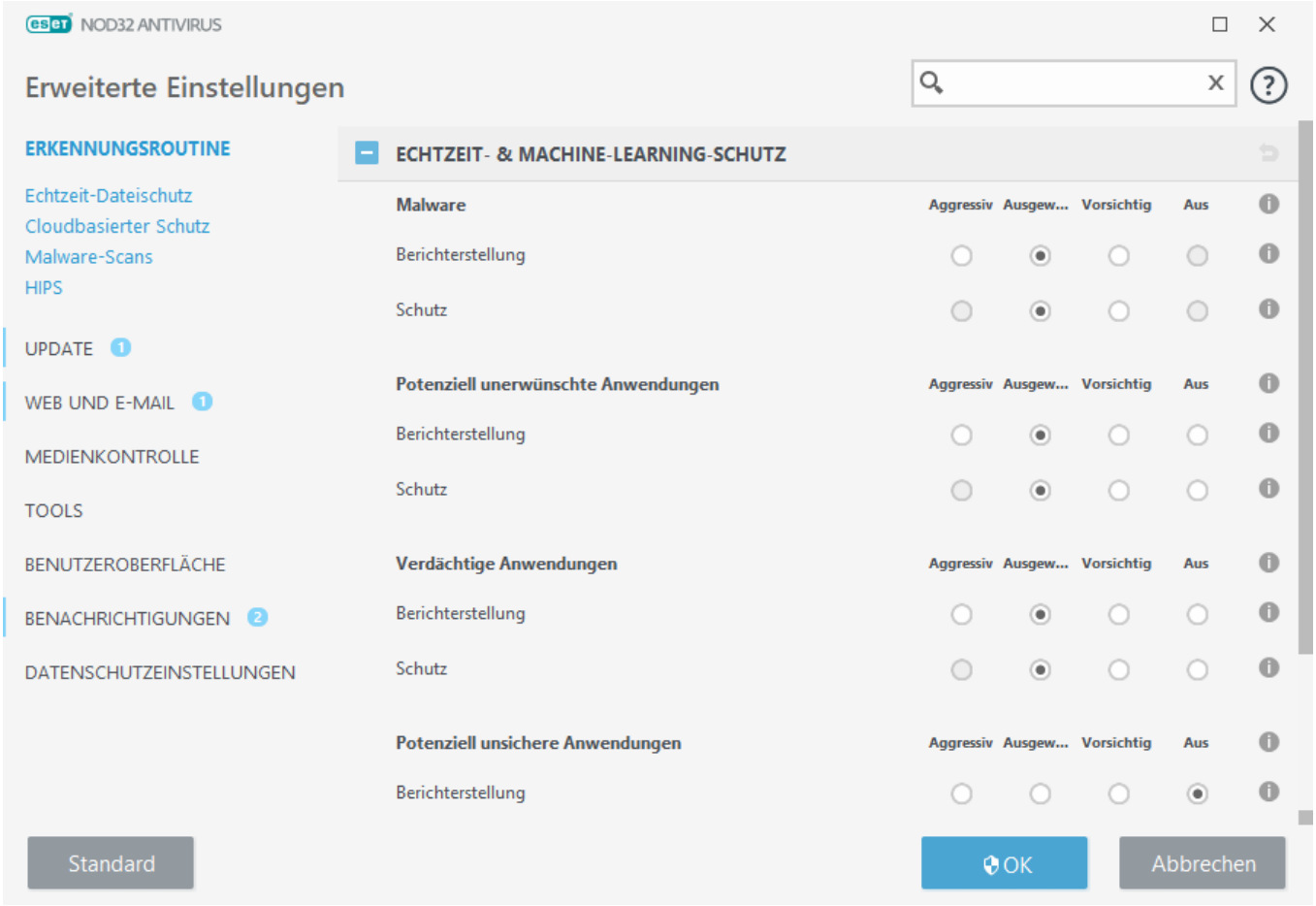
Mit dem **Echtzeit- & Machine-Learning-Schutz** für alle Schutzmodule (z. B. Echtzeit-Dateischutz, Web-Schutz usw.) können Sie Berichte und Schutzebenen für die folgenden Kategorien konfigurieren:

- **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.

- **Verdächtige Anwendungen** umfassen Programme, die mit Packprogrammen oder Schutzprogrammen komprimiert wurden. Diese Art von Programmen wird häufig von Malware-Autoren eingesetzt, um einer Erkennung zu entgehen.

- **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.



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. Weitere Informationen finden Sie unter Malware-Scans.

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 NOD32 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 NOD32 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 NOD32 Antivirus Version 13.1 und höher.
** Nicht empfohlen

Ermitteln von Produktversion, Versionen der Programmmodule und Builddaten

1. Klicken Sie auf **Hilfe und Support** > **Über ESET NOD32 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 NOD32 Antivirus (13.0 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 NOD32 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 ESET NOD32 Antivirus 13.0 und niedriger

Beim Upgrade von Version 13.0 und niedriger auf Version 13.1 und höher gilt der folgende neue Schwellenwertstatus:

Kategorieschalter vor dem Upgrade	✓	✗

Neuer KATEGORIE-Schwellenwert nach dem Upgrade	Ausgewogen	Aus

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).

Eingedrungene Schadsoftware wurde erkannt

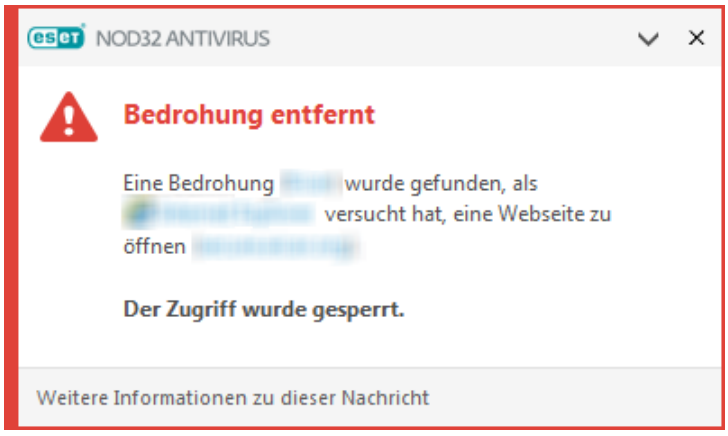
Schadsoftware kann auf vielen Wegen in das System gelangen. Mögliche Eintrittsstellen sind Websites, freigegebene Ordner, E-Mails oder Wechselmedien (USB-Sticks, externe Festplatten, CDs, DVDs, usw.).

Standardmäßiges Verhalten

ESET NOD32 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 erkannten und gesäuberten Objekten finden Sie unter Log-Dateien. Weitere Informationen zu den Säuberungsstufen und zum Verhalten des Produkts finden Sie unter Säuberungsstufe.



Computer auf infizierte Dateien scannen

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

1. Öffnen Sie ESET NOD32 Antivirus und klicken Sie auf „**Computer-Scan**“.

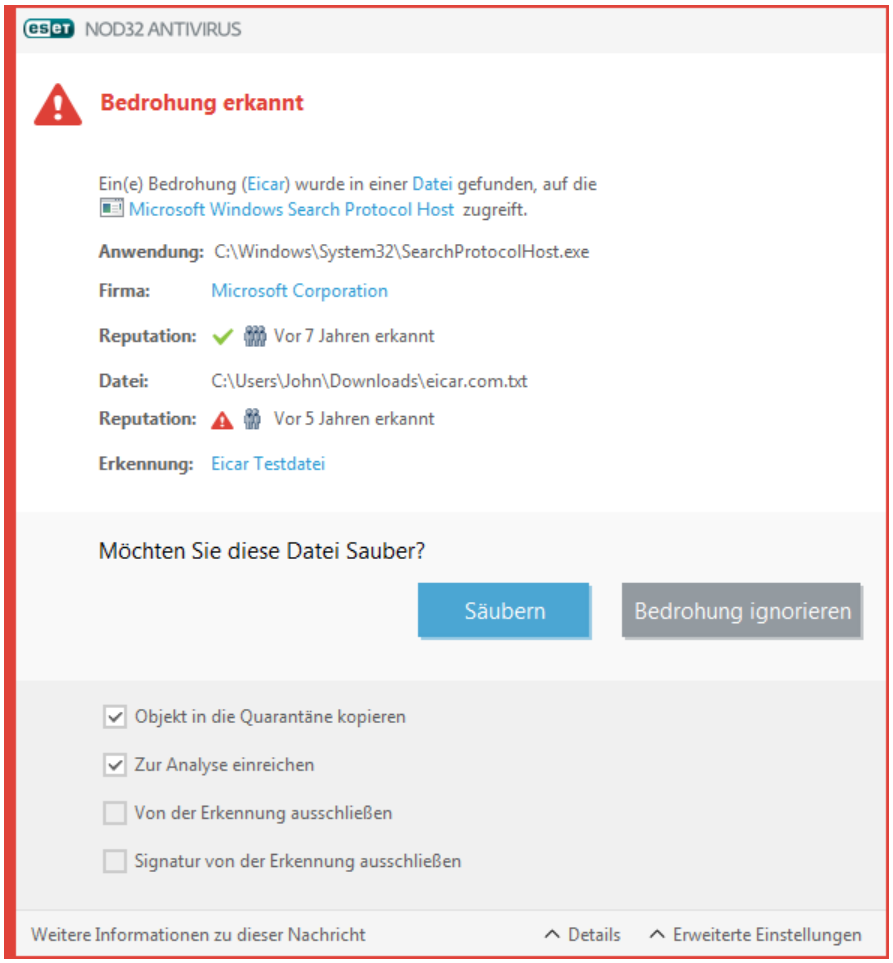
2. Klicken Sie auf **Computerprüfung** (weitere Informationen siehe Computerprüfung).

3. Nachdem der Scan abgeschlossen ist, überprüfen Sie im Log die Anzahl der gescannten, infizierten und gesäuberten Dateien.

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

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.

Wiederherstellen aus der Quarantäne

Sie finden die Quarantäne im Hauptprogrammfenster von ESET NOD32 Antivirus unter **Tools** > **Quarantäne**.

Die Dateien in der Quarantäne können an Ihrem ursprünglichen Speicherort wiederhergestellt werden:

- Verwenden Sie dazu die Funktion **Wiederherstellen** im Kontextmenü, indem Sie mit der rechten Maustaste auf eine Datei in der Quarantäne klicken.
- Wenn eine Datei als potenziell unerwünschte Anwendung markiert ist, wird die Option **Wiederherstellen und von Scans ausschließen** aktiviert. Siehe auch Ausschlüsse.
- Mit der Option **Wiederherstellen nach** im Kontextmenü können Sie eine Datei an einem anderen Ort als an ihrem ursprünglichen Speicherort wiederherstellen.
- Die Funktion zum Wiederherstellen ist nicht immer verfügbar, z. B. für Dateien in schreibgeschützten Netzwerkfreigaben.

Mehrere Bedrohungen

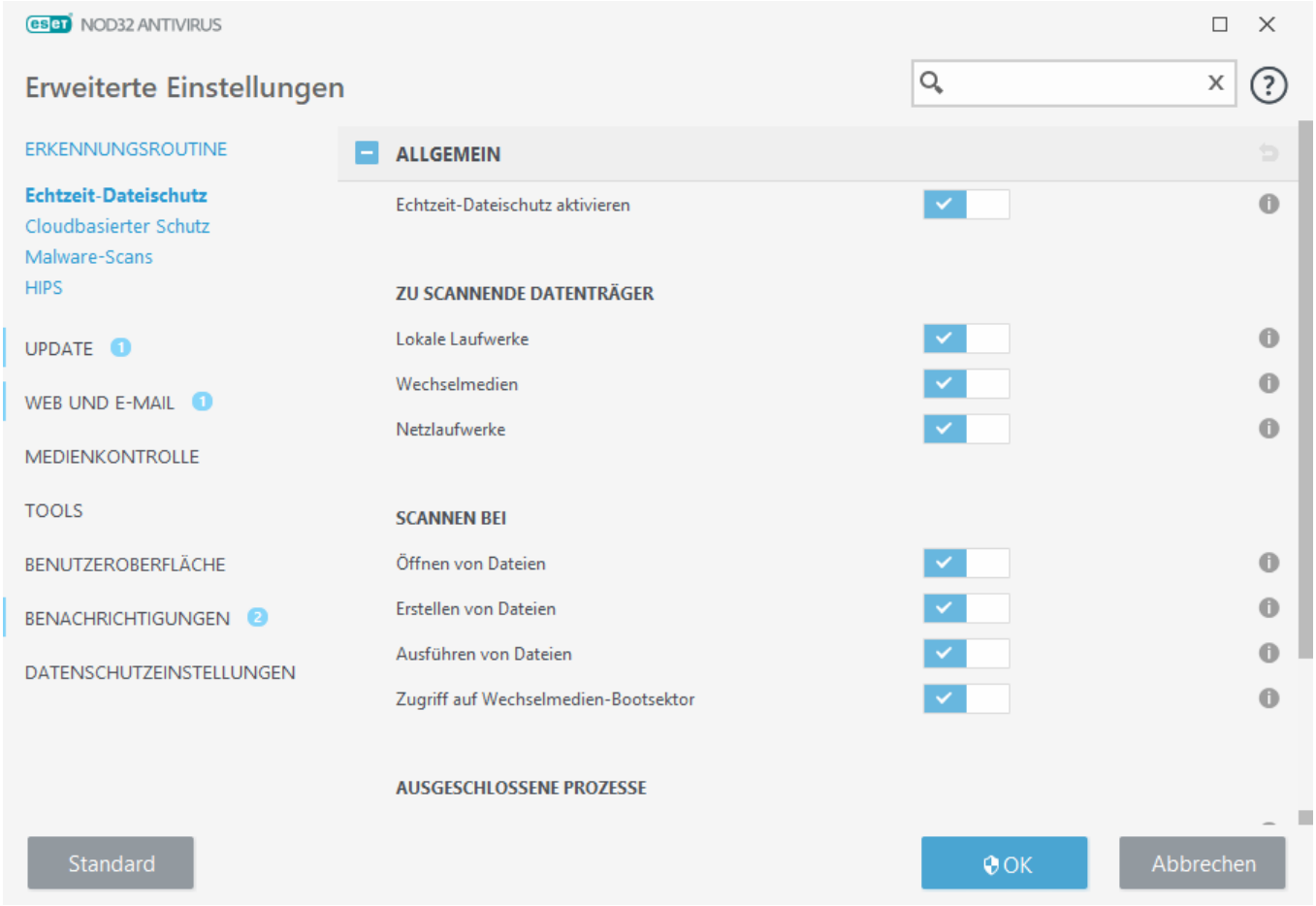
Falls infizierte Dateien während der Prüfung des Computers nicht gesäubert wurden (oder die Säuberungsstufe auf **Nicht säubern** festgelegt wurde), so wird ein Warnfenster angezeigt. In diesem wird danach gefragt, wie mit den Dateien verfahren werden soll. Wählen Sie Aktionen für die Dateien aus (diese werden für jede Datei in der Liste separat festgelegt). Klicken Sie dann auf **Fertig stellen**.

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.

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.

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 einem Update der Erkennungsroutine werden die Dateien sofort wieder 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 die **erweiterten Einstellungen** durch Drücken der Taste **F5** und erweitern Sie anschließend den Eintrag **Erkennungsroutine** > **Echtzeit-Dateischutz**. Klicken Sie auf **Einstellungen für ThreatSense** > **Sonstige** und aktivieren bzw. deaktivieren Sie die Option **Smart-Optimierung aktivieren**.

Säuberungsstufen

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

In den ThreatSense-Parametern sind die folgenden Korrekturstufen (Säuberungsstufen) verfügbar.

Behebung in ESET NOD32 Antivirus

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.
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 für die meisten Fälle 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.

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

Der Echtzeit-Dateischutz 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 NOD32 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 .

Echtzeit-Dateischutz prüfen

Um sicherzustellen, dass der Echtzeit-Dateischutz aktiv ist und Viren erkennt, verwenden Sie eine Testdatei von *www.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.

Vorgehensweise bei fehlerhaftem Echtzeit-Dateischutz

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

Echtzeit-Dateischutz ist deaktiviert

Wenn ein Benutzer den Echtzeit-Schutz versehentlich deaktiviert hat, sollten Sie die Funktion erneut aktivieren. Um den Echtzeit-Dateischutz erneut zu aktivieren, öffnen Sie die **Einstellungen** im Hauptprogrammfenster und klicken Sie auf **Computerschutz** > **Echtzeit-Dateischutz**.

Wenn der Echtzeit-Dateischutz beim Systemstart nicht initialisiert wird, ist die Option **Echtzeit-Dateischutz aktivieren** vermutlich deaktiviert. Um diese Option zu aktivieren, klicken Sie unter **Erweiterte Einstellungen** (**F5**) auf **Virenschutz** > **Echtzeit-Dateischutz**.

Echtzeit-Dateischutz erkennt und entfernt keinen Schadcode

Stellen Sie sicher, dass keine anderen Virenschutzprogramme auf Ihrem Computer installiert sind. Zwei parallel installierte Antivirenprogramme können Konflikte verursachen. 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. Um dieses Problem zu beheben, erstellen Sie ein SysInspector-Log und übermitteln Sie es zur Analyse an den technischen ESET-Support.

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. 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.

Verwechseln Sie diese Funktion nicht mit Ausgeschlossenen Dateierweiterungen, HIPS-Ausschlüssen, Ereignisausschlüssen oder Leistungsausschlüssen.

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.

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 NOD32 Antivirus überwacht, und die ausgeführten Dateioperationen werden nicht gescannt.

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**.

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*).

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 NOD32 Antivirus überwacht, und die ausgeführten Dateioperationen werden nicht gescannt.

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**.

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. Das System nutzt die übermittelten Daten von ESET-Benutzern sendet diese an das ESET-Virenlabor. ESET LiveGrid® stellt verdächtige Proben 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.

Folgende Optionen stehen zur Verfügung:

ESET LiveGrid®-Reputationssystem aktivieren

Das ESET LiveGrid®-Reputationssystem bietet Cloud-basierte 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.

ESET LiveGrid®-Feedbacksystem aktivieren

Zusätzlich zum ESET LiveGrid®-Reputationssystem sammelt das ESET LiveGrid®-Feedbacksystem Informationen zu neuen Bedrohungen, die auf Ihrem Computer erkannt wurden. Diese Informationen können Folgendes umfassen:

- Sample oder Kopie der Datei, in der die Bedrohung aufgetreten ist
- Pfad zur Datei
- Dateiname
- Datum und Zeit

- Der Prozess, über den die Bedrohung auf Ihrem Computer aufgetreten ist
- Informationen zum Betriebssystem Ihres Computers

ESET NOD32 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.

Weitere Informationen zur Übertragung der relevanten Daten finden Sie in der Datenschutzerklärung.

Sie können sich dazu entscheiden, ESET LiveGrid® nicht zu aktivieren

Sie werden keine Funktionalität in der Software verlieren, jedoch wird ESET NOD32 Antivirus deutlich schneller auf neue Bedrohungen reagieren, wenn ESET LiveGrid® aktiviert ist. Wenn Sie ESET LiveGrid® bereits zuvor verwendet und es deaktiviert haben, kann es sein, dass 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.

Weitere Informationen zu ESET LiveGrid® finden Sie im Glossar.
Weitere Informationen zum Aktivieren und Deaktivieren von ESET LiveGrid® in ESET NOD32 Antivirus finden Sie in unseren illustrieren Abbildungen, die in Englisch und weiteren Sprachen verfügbar sind.

Cloudbasierten Schutz in den erweiterten Einstellungen konfigurieren

Um die Einstellungen für ESET LiveGrid®zu öffnen, öffnen Sie **Erweiterte Einstellungen** (F5) > **Erkennungsroutine** > **Cloud-basierter 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.
- **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

Sample manuell einreichen – Über diese Option können Sie Samples manuell über das Kontextmenü, über die Quarantäne oder über Tools an ESET übermitteln.

Erkannte Samples automatisch einreichen

Wählen Sie aus, welche Arten von Samples zur Analyse an ESET übermittelt werden sollen. So können Sie auch die künftige Erkennung verbessern (die standardmäßige Maximalgröße einer Sample-Datei beträgt 64 MB). Folgende Optionen stehen zur Verfügung:

- **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 Schutzmodule in ESET NOD32 Antivirus als verdächtig oder unbekannt eingestuft wurden (die standardmäßige Maximalgröße einer Sample-Datei beträgt 64 MB).

- **Ausführbare Dateien** - Ausführbare Dateien, wie etwa .exe, .dll, .sys.
- **Archive** - Archivdateitypen mit den Endungen .zip, .rar, .7z, .arch, .arj, .bzip, .gzip, .ace, .arc, .cab.
- **Skripts** - Skriptdateitypen 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 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 der Ausschlussliste weitere Dateien hinzufügen.

Um Dateien auszuschließen, die von `download.domain.com` heruntergeladen wurden, klicken Sie auf **Erweiterte Einstellungen** > **Erkennungsroutine** > **Cloudbasierter Schutz** > **Samples einreichen** und auf **Bearbeiten** neben **Ausschlüsse**. Fügen Sie den Ausschluss für `.download.domain.com` hinzu.

Maximalgröße für Samples (MB) - Definiert die maximale Größe für Samples (1-64 MB).

Ausschlussfilter für den cloudbasierten Schutz

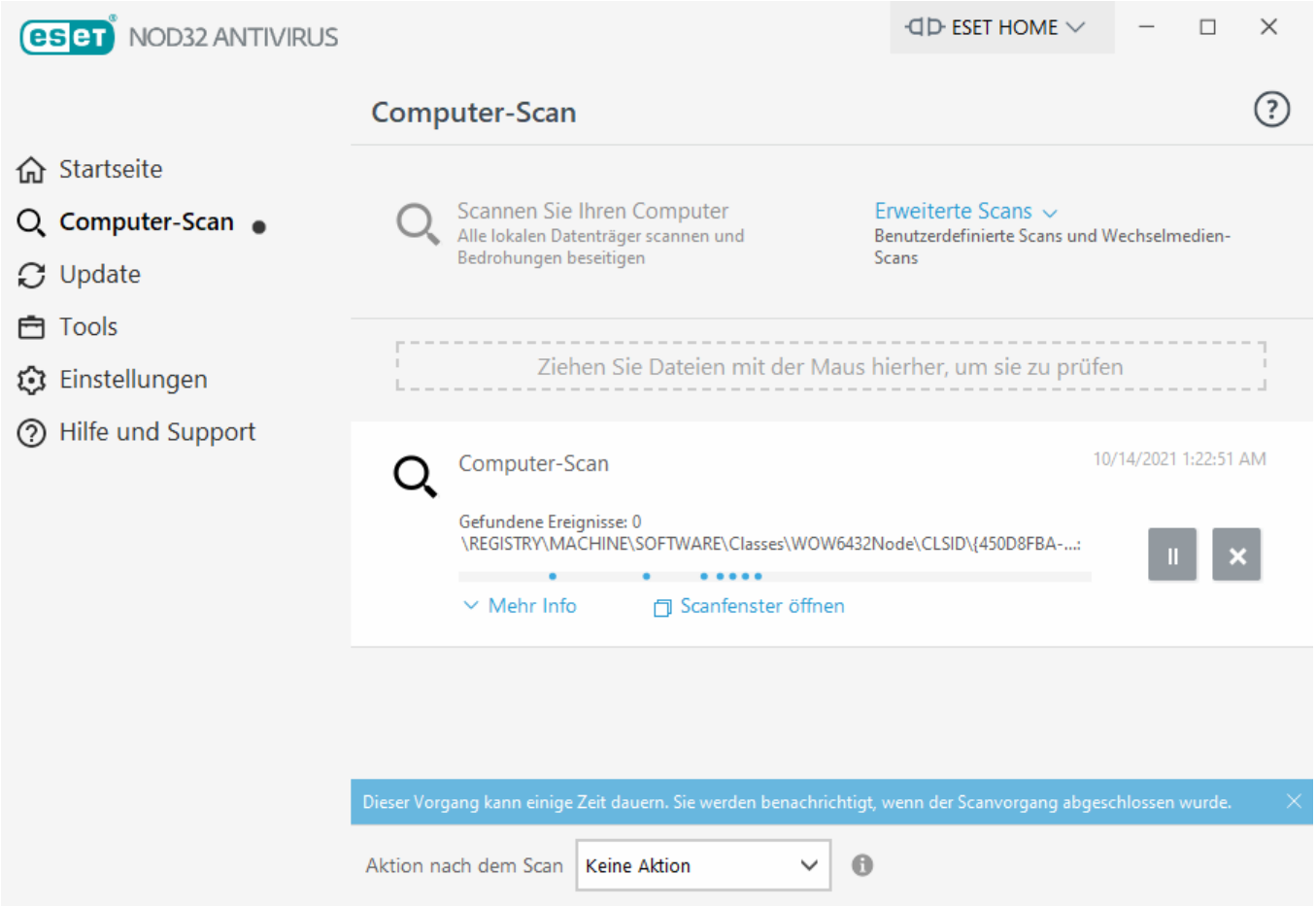
Mit dem Ausschlussfilter können Sie bestimmte Dateien/Ordner von der Sample-Übermittlung ausschließen. Hier eingetragene Dateien werden nicht an ESET übermittelt, auch wenn sie verdächtigen Code enthalten. Gängige Dateitypen (.doc usw.) sind bereits in der Standardeinstellung in die Liste eingetragen.

Diese Funktion eignet sich dazu, Dateien einzutragen, die eventuell vertrauliche Informationen enthalten, wie zum Beispiel Textdokumente oder Tabellen.

Um Dateien auszuschließen, die von download.domain.com heruntergeladen wurden, klicken Sie auf **Erweiterte Einstellungen** > **Erkennungsroutine** > **Cloudbasierter Schutz** > **Samples einreichen** > **Ausschlüsse** und fügen Sie den Ausschluss für *download.domain.com* hinzu.

Computer-Scan

Die manuelle Prüfung ist ein wichtiger Teil Ihrer Virenschutzlösung. Sie dient zur Prüfung von Dateien und Ordnern auf dem Computer. Aus Sicherheitsgründen sollten Sie Ihren Computer regelmäßig im Rahmen Ihrer Sicherheitsvorkehrungen prüfen, und nicht nur bei Infektionsverdacht. Es wird empfohlen, regelmäßig eine umfassende Prüfung des Computers vorzunehmen, um Viren zu entdecken, die nicht vom Echtzeit-Dateischutz erfasst wurden, als sie auf die Festplatte gelangten. Dies kommt z. B. vor, wenn der Echtzeit-Dateischutz zu diesem Zeitpunkt deaktiviert oder die Erkennungsroutine nicht auf dem neuesten Stand ist oder die Datei beim Speichern auf dem Datenträger nicht als Virus erkannt wird.



Sie haben zwei Arten von **Computer-Scans** zur Auswahl. **Scannen Sie Ihren Computer** führt einen schnellen System-Scan ohne spezielle Scan-Parameter durch. Beim **Benutzerdefinierten Scan** (unter „Erweiterte Scans“) können Sie eines der vordefinierten Scanprofile für bestimmte Speicherorte auswählen oder bestimmte Scan-Ziele festlegen.

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

Standardmäßig versucht ESET NOD32 Antivirus, während des Computer-Scans gefundene Ereignisse automatisch zu säubern oder zu löschen. In einigen Fällen, wenn keine Aktion durchgeführt werden kann, erhalten sie eine interaktive Warnmeldung und müssen eine Säuberungsaktion auswählen (beispielsweise Löschen oder Ignorieren). Um die Säuberungsebene zu ändern und weitere detaillierte Informationen zu erhalten, informieren Sie sich unter Säuberung. Um vorherige Scans zu prüfen, informieren Sie sich unter Log-Dateien.

Scannen Sie Ihren Computer

Mit der Option **Scannen Sie Ihren Computer** können Sie eine schnelle Systemprüfung durchführen und infizierte Dateien entfernen, ohne eingreifen zu müssen. Ihr Vorteil der Option **Scannen Sie Ihren Computer** ist die einfache Bedienung, bei der Sie keine detaillierten Prüfeinstellungen festlegen müssen. Bei diesem Scan werden alle Dateien auf den lokalen Datenträgern geprüft, und erkannte Infiltrationen werden automatisch gesäubert oder gelöscht. Als Säuberungsstufe wird automatisch der Standardwert festgelegt. Weitere Informationen zu den Säuberungstypen finden Sie unter Säubern.

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.

Die folgenden Prüfoptionen sind unter **Erweiterte Prüfungen** verfügbar:

Benutzerdefinierter Scan

Beim **benutzerdefinierten Scan** können Sie verschiedene Scan-Parameter festlegen, z. B. die zu scannenden Objekte und die Methoden. **Benutzerdefiniertes Scans** bieten den Vorteil, dass Sie die Parameter ausführlich konfigurieren können. Verschiedene Konfigurationen können in benutzerdefinierten Scan-Profilen gespeichert werden, um Scans wiederholt mit denselben Parametern ausführen zu können.

Wechselmedien-Scan

Diese Prüfung ähnelt der Option „**Computerscan**“ 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 **Benutzerdefinierte Prüfung** starten, indem Sie im Dropdown-Menü **Zu prüfende Objekte** den Eintrag **Wechselmedien** auswählen und auf **Prüfen** 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 eine Aktion festlegen, die nach Abschluss eines Scans automatisch ausgeführt wird:

- **Keine Aktion** - Nach dem Scan wird keine Aktion ausgeführt.
- **Herunterfahren**- Der Computer wird nach dem Scan heruntergefahren.
- **Neustart**- Nach dem Scan werden alle offenen Programme geschlossen und der Computer wird neu gestartet.
- **Bei Bedarf neu starten** – Der Computer wird bei Bedarf neu gestartet, um erkannte Bedrohungen zu säubern.
- **Neustart erzwingen** – Nach Abschluss des Scans werden alle geöffneten Programme ohne Eingreifen des Benutzers geschlossen, und der Computer wird neu gestartet.
- **Neustart bei Bedarf erzwingen** – Der Computer wird bei Bedarf neu gestartet, um erkannte Bedrohungen zu säubern.
- **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.

Die Verfügbarkeit der Aktionen **Energiesparmodus** und **Ruhezustand** hängt von Ihren Energieeinstellungen im Betriebssystem und vom Funktionsumfang Ihres Computers oder Laptops ab. Beachten Sie, dass der Computer im Energiesparmodus weiter arbeitet. Es führt weiterhin grundlegende Funktionen aus und verbraucht Strom, wenn Ihr Computer mit Batteriestrom betrieben wird. Um die Akkubetriebsdauer beispielsweise unterwegs zu verlängern, empfiehlt es sich, den Ruhezustand zu verwenden.

Die ausgewählte Aktion wird gestartet, nachdem alle laufenden Scans abgeschlossen wurden. Wenn Sie **Herunterfahren** oder **Neu starten** auswählen, wird ein 30-sekündiger Countdown in einem Bestätigungsdialog angezeigt und Sie können auf **Abbrechen** klicken, um die Aktion abzubrechen.

Sie sollten Ihren Computer mindestens einmal im Monat scannen. Sie können die Scans als Task unter **Tools** > **Taskplaner** konfigurieren. So planen Sie eine wöchentliche Computerprüfung

Benutzerdefinierte Prüfung

Mit dem benutzerdefinierten Scan können Sie den Arbeitsspeicher, das Netzwerk oder bestimmte Teile eines Datenträgers anstelle des gesamten Datenträgers überprüfen. Klicken Sie dazu auf **Erweiterte Scans** > **Benutzerdefinierter Scan** oder wählen Sie die Scan-Ziele in der Ordner- bzw. Baumstruktur aus.

Im Dropdownmenü **Profil** können Sie ein Scan-Profil für bestimmte Ziele auswählen. Das Standardprofil ist **Smart-Scan**. Außerdem haben Sie drei weitere vordefinierte Scan-Profile zur Auswahl: **Tiefen-Scan**, **Scan via Kontextmenüs** und **Computer-Scan**. Diese Scan-Profile verwenden unterschiedliche ThreatSense-Einstellungen. Sie finden eine Beschreibung der verfügbaren Optionen unter **Erweiterte Einstellungen** (F5) > **Erkennungsroutine** > **Malware-Scans** > **On-demand-Scan** > ThreatSense-Parameter.

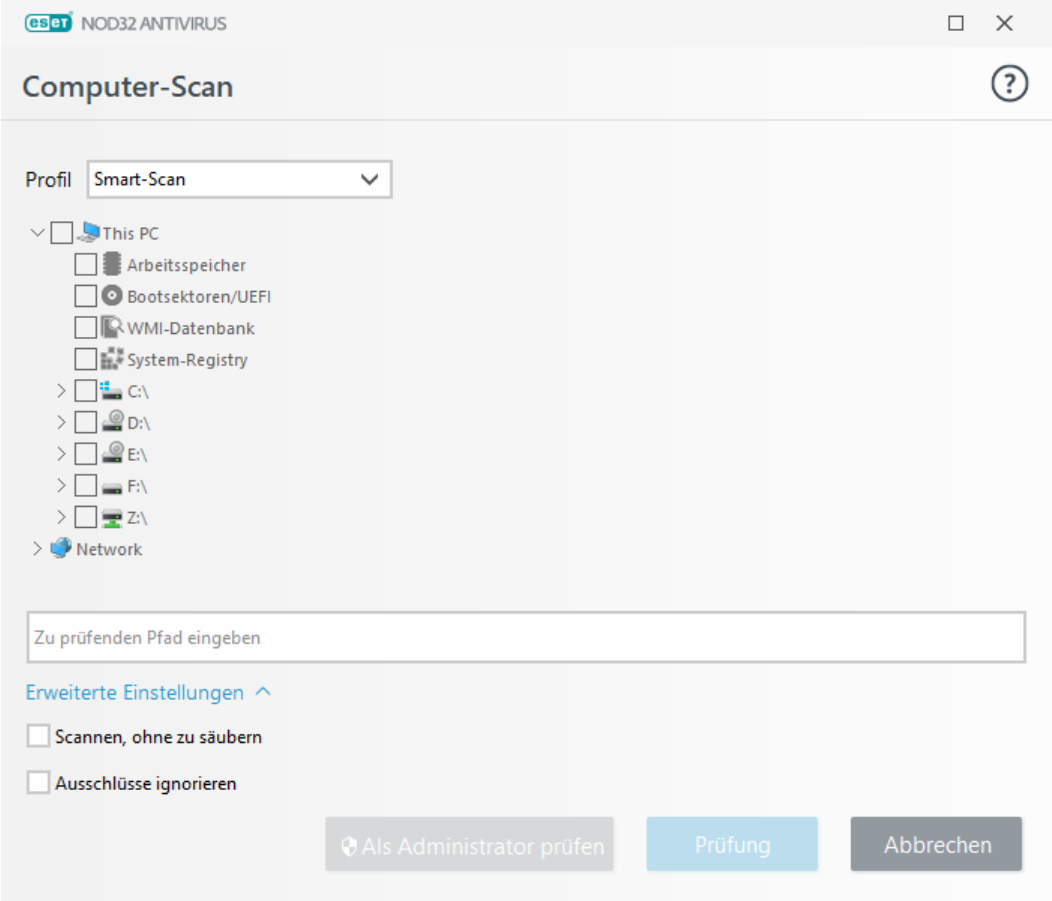
Die Ordnerstruktur (Baumstruktur) enthält außerdem bestimmte Scan-Ziele.

- **Arbeitsspeicher** – Alle aktuell vom Arbeitsspeicher verwendeten Prozesse und Daten werden gescannt.
- **Bootsektoren/UEFI** – Bootsektoren und UEFI werden auf Malware gescannt. Weitere Informationen zum UEFI-Scanner finden Sie im Glossar.
- **WMI-Datenbank** - Scannt die gesamte Windows Management Instrumentation (WMI)-Datenbank, alle Namespaces, alle Klasseninstanzen und alle Eigenschaften. Sucht nach Verweisen auf infizierte Dateien oder Malware, die als Daten eingebettet sind.
- **Systemregistrierung** – Scannt die gesamte Systemregistrierung inklusive aller Schlüssel und Unterschlüssel. Sucht nach Verweisen auf infizierte Dateien oder Malware, die als Daten eingebettet sind. Beim Säubern der Ereignisse werden die Verweise nicht aus der Registrierung gelöscht, um sicherzustellen, dass keine wichtigen Daten verloren gehen.

Um schnell zu einem Scan-Ziel (Datei oder Ordner) zu navigieren, geben Sie den Pfad in das Textfeld unter der Baumstruktur ein. Der Pfad unterscheidet zwischen Groß- und Kleinschreibung. Markieren Sie das entsprechende Kontrollkästchen in der Baumstruktur, um ein Objekt als Scan-Ziel hinzuzufügen.

So planen Sie eine wöchentliche Computerprüfung

Um einen regelmäßigen Task zu planen, lesen Sie das Kapitel So planen Sie einen wöchentlichen Computer-Scan.



Sie können die Säuberungsparameter für die Prüfung unter **Erweiterte Einstellungen** (F5) > **Erkennungsroutine** > **On-Demand-Prüfung** > **ThreatSense-Parameter** > **Säuberung** festlegen. Wählen Sie **Nur prüfen, keine Aktion** aus, um eine **Prüfung ohne Säuberungsaktion** durchzuführen. Der Prüfungsverlauf wird im Prüfung-Log gespeichert.

Wenn Sie die Option **Ausschlüsse ignorieren** auswählen, werden Dateien mit zuvor ausgeschlossenen Erweiterungen ohne Ausnahme gescannt.

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. Verwenden Sie diese Option, wenn der aktuelle Benutzer keine Zugriffsrechte für die zu prüfenden Dateien hat. Diese Schaltfläche ist nur verfügbar, wenn der aktuell angemeldete Benutzer keine UAC-Vorgänge als Administrator aufrufen darf.

Klicken Sie auf Logs anzeigen.

Stand der Prüfung

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

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. Weitere Informationen finden Sie in unserem Knowledgebase-Artikel.

So planen Sie eine wöchentliche Computerprüfung

Um einen regelmäßigen Task zu planen, lesen Sie das Kapitel So planen Sie einen wöchentlichen Computer-Scan.

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 – Zeigt die Gesamtzahl der während der Prüfung geprüften Dateien, gefundenen Bedrohungen und gesäuberten Bedrohungen an.

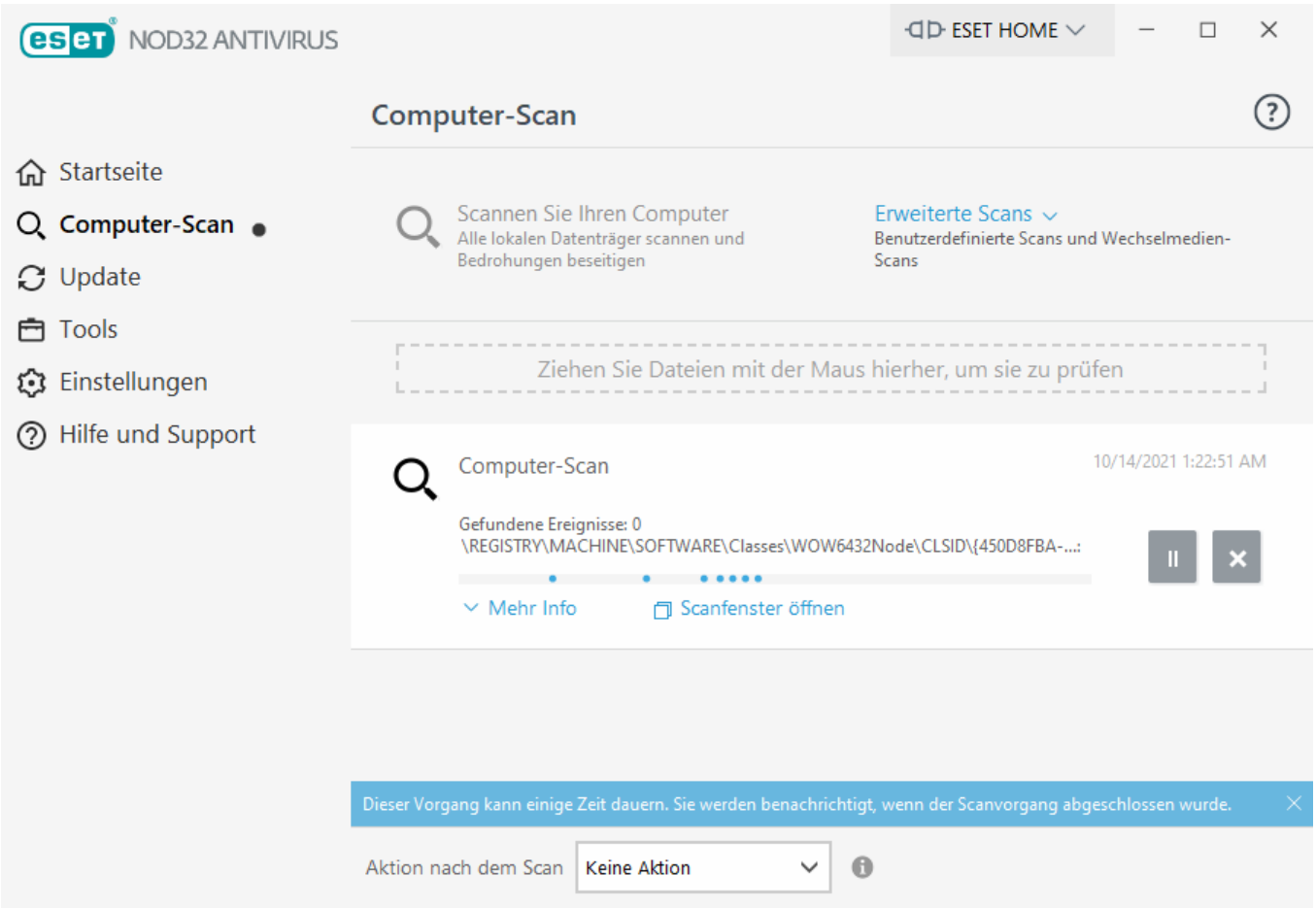
Anhalten - Unterbrechen der Prüfung.

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.

Klicken Sie auf die Lupe oder den Pfeil, um Details zum aktuell ausgeführten Scan anzuzeigen. Sie können gleichzeitig einen weiteren Scan ausführen, indem Sie auf **Scannen Sie Ihren Computer** oder auf **Erweiterte Scans** > **Benutzerdefinierter Scan** klicken.



Im Dropdownmenü **Aktion nach dem Scan** können Sie eine Aktion festlegen, die nach Abschluss eines Scans automatisch ausgeführt wird:

- **Keine Aktion** - Nach dem Scan wird keine Aktion ausgeführt.
- **Herunterfahren**- Der Computer wird nach dem Scan heruntergefahren.
- **Neustart**- Nach dem Scan werden alle offenen Programme geschlossen und der Computer wird neu gestartet.
- **Bei Bedarf neu starten** – Der Computer wird bei Bedarf neu gestartet, um erkannte Bedrohungen zu säubern.
- **Neustart erzwingen** – Nach Abschluss des Scans werden alle geöffneten Programme ohne Eingreifen des Benutzers geschlossen, und der Computer wird neu gestartet.
- **Neustart bei Bedarf erzwingen** – Der Computer wird bei Bedarf neu gestartet, um erkannte Bedrohungen zu säubern.
- **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.

> Die Verfügbarkeit der Aktionen **Energiesparmodus** und **Ruhezustand** hängt von Ihren Energieeinstellungen im Betriebssystem und vom Funktionsumfang Ihres Computers oder Laptops ab. Beachten Sie, dass der Computer im Energiesparmodus weiter arbeitet. Es führt weiterhin grundlegende Funktionen aus und verbraucht Strom, wenn Ihr Computer mit Batteriestrom betrieben wird. Um die Akkubetriebsdauer beispielsweise unterwegs zu verlängern, empfiehlt es sich, den Ruhezustand zu verwenden.

Die ausgewählte Aktion wird gestartet, nachdem alle laufenden Scans abgeschlossen wurden. Wenn Sie **Herunterfahren** oder **Neu starten** auswählen, wird ein 30-sekündiger Countdown in einem Bestätigungsdialog angezeigt und Sie können auf **Abbrechen** klicken, um die Aktion abzubrechen.

Computer-Scan-Log

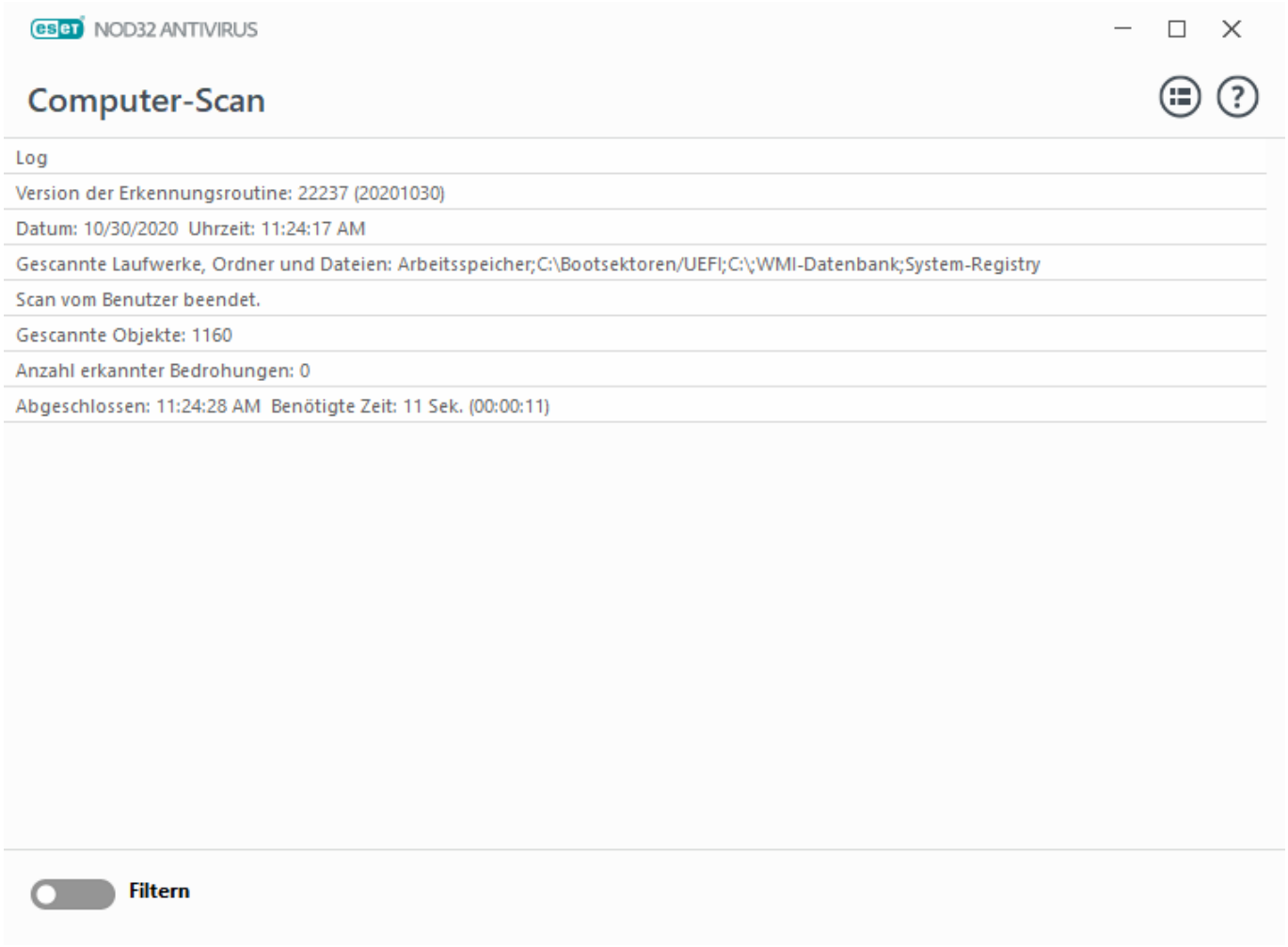
Nach Abschluss des Scans wird das Computer-Scan-Log mit allen relevanten Informationen zum jeweiligen Scan geöffnet. Im Scan-Log finden Sie beispielsweise die folgenden Informationen:

- Version der Erkennungsroutine
- Datum und Uhrzeit des Scans
- Gescannte Laufwerke, Ordner und Dateien
- Name des geplanten Scans (nur geplante Scans)
- Scanstatus
- Anzahl geprüfter Objekte

- Anzahl der gefundenen Ereignisse
- Abschlusszeit
- Prüfdauer

> Geplante Computer-Scan-Tasks werden nicht erneut ausgeführt, wenn die letzte Ausführung des geplanten Tasks immer noch ausgeführt wird. Der übersprungene geplante Scan-Task erstellt ein Computer-Scan-Log mit 0 gescannten Objekten und dem Status **Scan wurde nicht gestartet, weil der vorherige Scan noch ausgeführt wurde**.

Um ältere Scan-Logs zu finden, wählen Sie im Haupt-Programmfenster **Tools** > **Log-Dateien** aus. Wählen Sie im Dropdownmenü die Option **Computer-Scan** aus und doppelklicken Sie auf den gewünschten Eintrag.



> Weitere Informationen zu Datensätzen mit den Attributen „Öffnen nicht möglich“, „Fehler beim Öffnen“ und/oder „Archiv beschädigt“ finden Sie in unserem ESET-Knowledgebase-Artikel.

Klicken Sie auf das Schieberegler-Symbol **Filtern** , um das Fenster Log-Filter zu öffnen, in dem Sie Ihre Suche mit benutzerdefinierten Kriterien eingrenzen können. Klicken Sie zum Öffnen des Kontextmenüs mit der rechten Maustaste auf einen bestimmten Log-Eintrag:

Aktion	Nutzung
Gleiche Datensätze filtern	Aktiviert den Log-Filter. Daraufhin werden im Log nur Einträge mit dem ausgewählten Typ angezeigt.

Aktion	Nutzung
Filter	Diese Option öffnet das Fenster „Log-Filter“, in dem Sie Kriterien für bestimmte Log-Einträge definieren können. Tastenkombination: `Ctrl+Shift+F`
Filter aktivieren	Aktiviert die Filtereinstellungen. Wenn Sie den Filter zum ersten Mal aktivieren, müssen Sie die Einstellungen definieren, und das Fenster „Log-Filter“ wird geöffnet.
Filter deaktivieren	Deaktiviert den Filter (gleicher Effekt wie der Schalter am unteren Rand).
Kopieren	Kopiert die markierten Einträge in die Zwischenablage. Tastenkombination: `Ctrl+C`
Alle kopieren	Kopiert alle Einträge im Fenster.
Exportieren	Exportiert die markierten Einträge in der Zwischenablage in eine XML-Datei.
Alle exportieren	Diese Option exportiert alle Einträge im Fenster in eine XML-Datei.
Ereignisbeschreibung	Öffnet die ESET-Virenenzyklopädie mit detaillierten Informationen zu den Gefahren und Symptomen der hervorgehobenen Infiltration.

Malware-Scans

Der Bereich **Schadsoftware-Scans** befindet sich unter **Erweiterte Einstellungen** (F5) > **Erkennungsroutine** > **Schadsoftware-Scans** und enthält die folgenden Optionen für die Scan-Parameter: Dieser Bereich enthält die folgenden Elemente:

Ausgewähltes Profil - Ein bestimmter Satz von Parametern für den On-Demand-Scan. Klicken Sie neben der **Profilliste** auf **Bearbeiten**, um einen neuen Parameter zu erstellen. Weitere Details finden Sie unter Scan-Profile.

Scan-Ziele - Um nur ein bestimmtes Objekt zu scannen, können Sie neben **Scan-Ziele** auf **Bearbeiten** klicken und eine Option im Dropdown-Menü oder bestimmte Objekte in der Ordnerstruktur auswählen. 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

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

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

Aktivieren Sie den Schieberegler neben der Option **Logging aktivieren** in den erweiterten Einstellungen, um die Ausgabe eines Computer-Scans in den Log-Dateien abzulegen (klicken Sie im Hauptprogrammfenster auf **Tools**). > **Log-Dateien** und wählen Sie **Computer-Scan** im Dropdownmenü **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

In ESET NOD32 Antivirus sind vier vordefinierte Scan-Profile verfügbar:

- **Smart-Scan** – Dies ist das standardmäßig verwendete erweiterte Scan-Profil. Das Smart-Scan-Profil verwendet die Smart-Optimierungstechnologie, um Dateien auszuschließen, die bei einem vorherigen Scan als sauber eingestuft und seit dem Scan nicht mehr geändert wurden. Auf diese Weise können Sie schnellere Scans mit minimalen Auswirkungen auf die Systemsicherheit ausführen.

- **Scan via Kontextmenüs** – Im Kontextmenü können Sie bei Bedarf beliebige Dateien scannen. Mit dem Profil „Scan via Kontextmenüs“ können Sie definieren, welche Scan-Konfiguration für die auf diese Weise gestarteten Scans verwendet werden soll.

- **Tiefen-Scan** – Das Tiefen-Scan-Profil verwendet standardmäßig keine Smart-Optimierung, daher werden mit diesem Profil keine Dateien von der Prüfung ausgeschlossen.

- **Computer-Scan** – Dies ist das Standardprofil, das bei standardmäßigen Computer-Scans verwendet wird.

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.

> Nehmen wir an, Sie möchten Ihr eigenes Prüfprofil erstellen. Die Option **Computerprüfung** eignet sich in gewissem Maße, aber Sie möchten keine laufzeitkomprimierten Dateien oder potenziell unsichere Anwendungen prüfen. Außerdem möchten Sie die Option **Ereignis immer beheben** 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 Dropdown-Menü **Zu prüfende Objekte** können Sie vordefinierte Optionen für die zu prüfenden Objekte auswählen.

- **Nach Profileinstellungen** - Im Prüfprofil festgelegte Prüfziele.

- **Wechselmedien** - Wählt Disketten, USB-Speichergeräte, CDs/DVDs aus.
- **Lokale Laufwerke** - Alle lokalen Systemlaufwerke
- **Netzlaufwerke** - Alle zugeordneten Netzlaufwerke
- **Benutzerdefinierte Auswahl** – Hebt die bisherige Auswahl auf.

Die Ordnerstruktur (Baumstruktur) enthält außerdem bestimmte Scan-Ziele.

- **Arbeitsspeicher** – Alle aktuell vom Arbeitsspeicher verwendeten Prozesse und Daten werden gescannt.
- **Bootsektoren/UEFI** – Bootsektoren und UEFI werden auf Malware gescannt. Weitere Informationen zum UEFI-Scanner finden Sie im Glossar.
- **WMI-Datenbank** - Scannt die gesamte Windows Management Instrumentation (WMI)-Datenbank, alle Namespaces, alle Klasseninstanzen und alle Eigenschaften. Sucht nach Verweisen auf infizierte Dateien oder Malware, die als Daten eingebettet sind.
- **Systemregistrierung** – Scannt die gesamte Systemregistrierung inklusive aller Schlüssel und Unterschlüssel. Sucht nach Verweisen auf infizierte Dateien oder Malware, die als Daten eingebettet sind. Beim Säubern der Ereignisse werden die Verweise nicht aus der Registrierung gelöscht, um sicherzustellen, dass keine wichtigen Daten verloren gehen.

Um schnell zu einem Scan-Ziel (Datei oder Ordner) zu navigieren, geben Sie den Pfad in das Textfeld unter der Baumstruktur ein. Der Pfad unterscheidet zwischen Groß- und Kleinschreibung. Markieren Sie das entsprechende Kontrollkästchen in der Baumstruktur, um ein Objekt als Scan-Ziel hinzuzufügen.

Medienkontrolle

ESET NOD32 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:

- Datenträger (Festplatten, USB-Wechseldatenträger)
- CD/DVD
- USB Drucker
- FireWire Speicher
- Bluetooth Gerät
- Smartcard-Leser
- Bildverarbeitungsgerät
- Modem

- LPT/COM port
- Mobiles Gerät
- Alle Gerätetypen

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

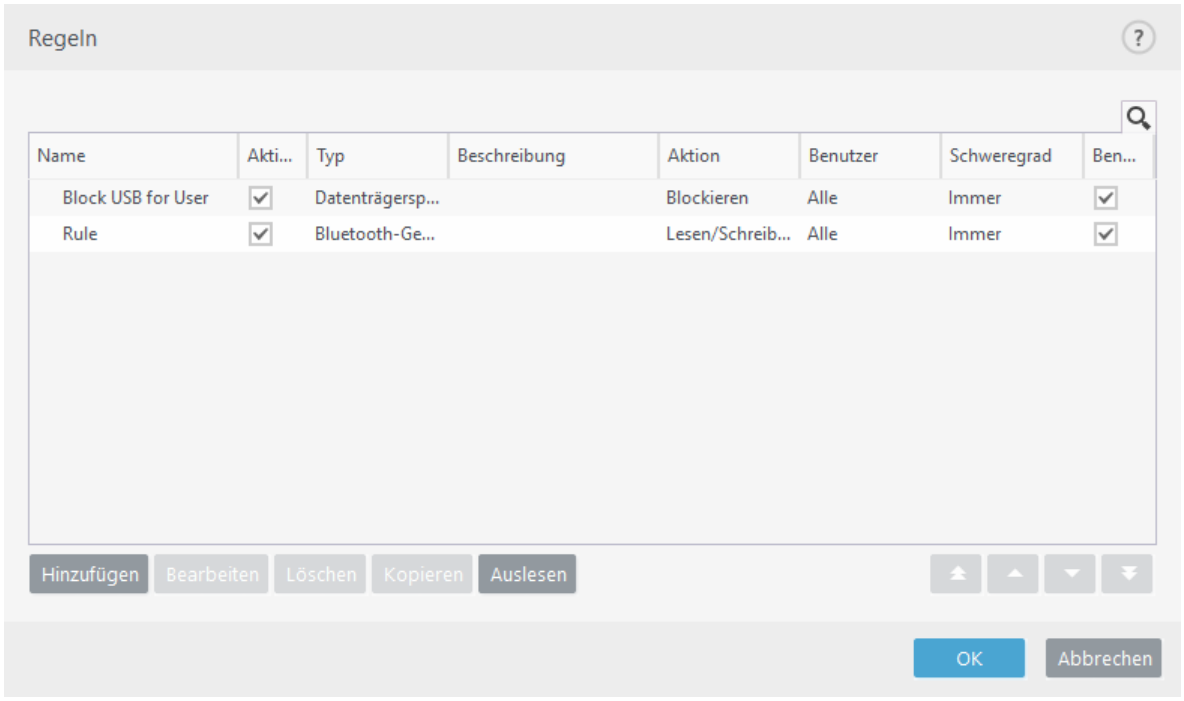
Aktivieren Sie den Schieberegler neben **Medienkontrolle aktivieren**, um die Funktion „Medienkontrolle“ in ESET NOD32 Antivirus zu aktivieren. Sie müssen Ihren Computer neu starten, um die Änderungen zu übernehmen. Wenn die Medienkontrolle aktiviert ist, wird die Option **Regeln** verfügbar, über die Sie das Fenster Regel-Editor öffnen können.

> 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.

Wenn ein von einer bestehenden Regel blockiertes Gerät eingefügt wird, wird ein Benachrichtigungsfenster 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 für 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. Siehe auch Hinzufügen von Regeln für die Medienkontrolle.

Klicken Sie zum Bearbeiten von Regeln auf **Hinzufügen** oder **Bearbeiten**. Klicken Sie auf **Kopieren**, um eine neue Regel mit vordefinierten Optionen auf Grundlage der ausgewählten Regel zu erstellen. Die XML-Zeichenketten, die beim Klicken auf eine Regel angezeigt werden, können in den Zwischenspeicher kopiert werden, um den Systemadministrator beim Exportieren/Importieren der Daten zu unterstützen.

Halten Sie die Steuerungstaste (**STRG**) gedrückt, um mehrere Regeln auszuwählen und Aktionen (Löschen, Verschieben in der Liste) auf alle ausgewählten Regeln anzuwenden. Mit dem Kontrollkästchen **Aktiviert** können Sie eine Regel deaktivieren und aktivieren. Dies ist hilfreich, wenn Sie eine Regel nicht dauerhaft löschen möchten, um sie später wieder verwenden zu können.

Die Regeln sind in nach absteigender Priorität geordnet (Regeln mit höchster Priorität werden am Anfang der Liste angezeigt).

Um Log-Einträge anzuzeigen, klicken Sie im Hauptfenster von ESET NOD32 Antivirus auf **Tools** > **Log-Dateien**.

Im Log der Medienkontrolle werden alle ausgelösten Vorkommnisse der Medienkontrolle aufgezeichnet.

Erkannte Geräte

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

Wählen Sie ein Gerät aus der Liste der erkannten Geräte aus und klicken Sie auf **OK**, um eine Regel für die Gerätesteuerung mit vordefinierten Informationen hinzuzufügen (alle Einstellungen können angepasst werden).

Geräte im Energiesparmodus werden mit einem Warnsymbol markiert. Gehen Sie wie folgt vor, um die **OK**-Schaltfläche zu aktivieren und eine Regel für ein solches Gerät hinzuzufügen:

- Schließen Sie das Gerät erneut an.
- Verwenden Sie das Gerät (starten Sie z. B. die Kamera-App unter Windows, um eine Webcam zu aktivieren).

Gerätegruppen

⚠ 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 Textdatei. Die Textdatei muss korrekt formatiert sein, um Geräte importieren zu können:

- Jedes Gerät wird in einer separaten Zeile definiert.
- **Hersteller**, **Modell** und **Seriennummer** müssen für jedes Gerät angegeben und durch ein Komma getrennt sein.

Hier sehen Sie ein Beispiel für den Inhalt der Textdatei:

```
Kingston,DT 101 G2,001CCE0DGRFC0371
04081-0009432,USB2.0 HD WebCam,20090101
```

Exportieren – Exportiert eine Geräteliste in eine Datei.

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

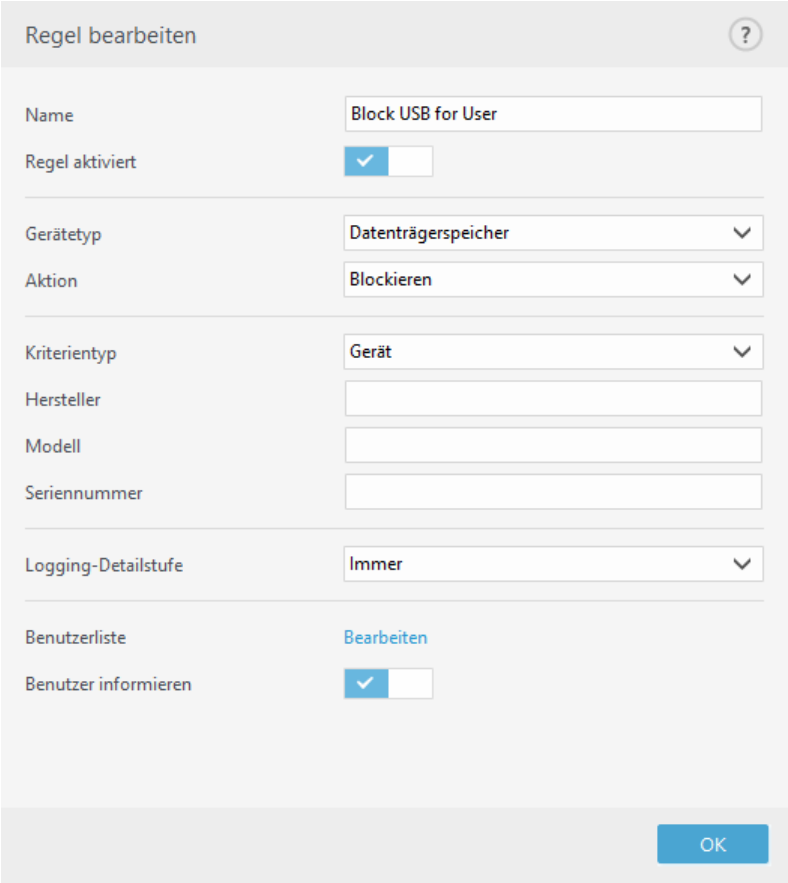
Klicken Sie auf **OK**, wenn Sie die Bearbeitung abgeschlossen haben. Klicken Sie auf **Abbrechen**, wenn Sie das Fenster **Gerätegruppen** schließen möchten, ohne die Änderungen zu speichern.

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. Für nicht-Speichergeräte sind nur drei Aktionen verfügbar. (**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. Klicken Sie auf den Schieberegler neben **Regel aktiviert**, um diese Regel zu deaktivieren bzw. zu aktivieren. Dies ist beispielsweise nützlich, wenn Sie eine Regel deaktivieren, jedoch nicht dauerhaft löschen möchten.

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.

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. Für nicht-Speichergeräte sind nur drei Aktionen verfügbar. (**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 CD Laufwerk.

> 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.

> 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

ESET NOD32 Antivirus speichert alle wichtigen Vorgänge in einer Log-Datei, die direkt vom Hauptmenü aus aufgerufen werden kann. Klicken Sie auf **Tools** > **Log-Dateien** und wählen Sie **Medienkontrolle** aus dem Dropdown-Menü **Log** aus.

- **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.
- **Warnung**– Kritische Fehler und Warnungen werden protokolliert.
- **Keine** – Es werden keine Logs aufgezeichnet.

Benutzerliste

Sie können die Regeln auf bestimmte Benutzer oder Benutzergruppen beschränken, indem Sie neben der **Benutzerliste** auf **Bearbeiten** klicken und sie 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.

Einschränkungen für die Benutzerliste

Die Benutzerliste kann nicht für Regeln mit bestimmten Gerätetypendefiniert werden:

- USB-Drucker
- Bluetooth-Gerät
- Smartcard-Leser
- Bildverarbeitungsgerät
- Modem
- LPT/COM-Port

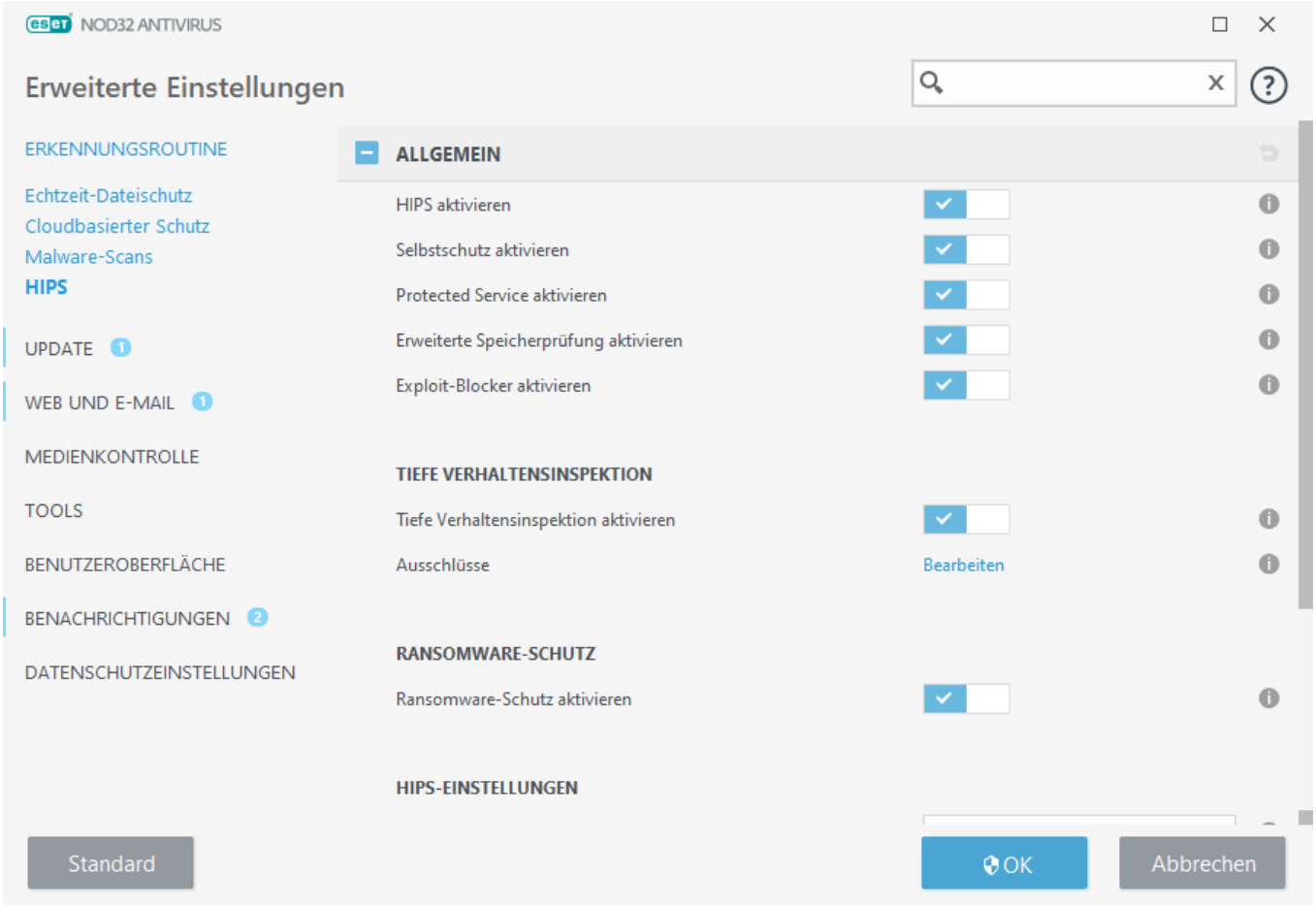
Benutzer informieren - Wenn ein von einer bestehenden Regel blockiertes Gerät angeschlossen wird, wird ein Hinweisfenster angezeigt.

HIPS

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

Das**Host 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.

Sie finden die HIPS-Einstellungen unter **Erweiterte Einstellungen** (F5) > **Erkennungsroutine** > **HIPS** > **Einfach**. Der HIPS-Status (aktiviert/deaktiviert) wird im Hauptprogrammfenster von ESET NOD32 Antivirus unter **Einstellungen** > **Computer-Schutz** angezeigt.



Einfach

HIPS aktivieren - HIPS ist in ESET NOD32 Antivirus standardmäßig aktiviert. Wenn Sie HIPS deaktivieren, werden auch die anderen HIPS-Funktionen wie etwa der Exploit-Blocker deaktiviert.

Selbstschutz aktivieren - ESET NOD32 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.

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 höher 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. 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.

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.

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 aber eine niedrigere Priorität als manuell oder im automatischen Modus erstellte Regeln. Wenn Sie die Option **Trainingsmodus** im Dropdownmenü **Filtermodus** auswählen, wird die Einstellung **Ende des Trainingsmodus** verfügbar, und Sie können eine Dauer für den Trainingsmodus auswählen. Die maximale Dauer beträgt 14 Tage. Nach Ablauf der Dauer 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).

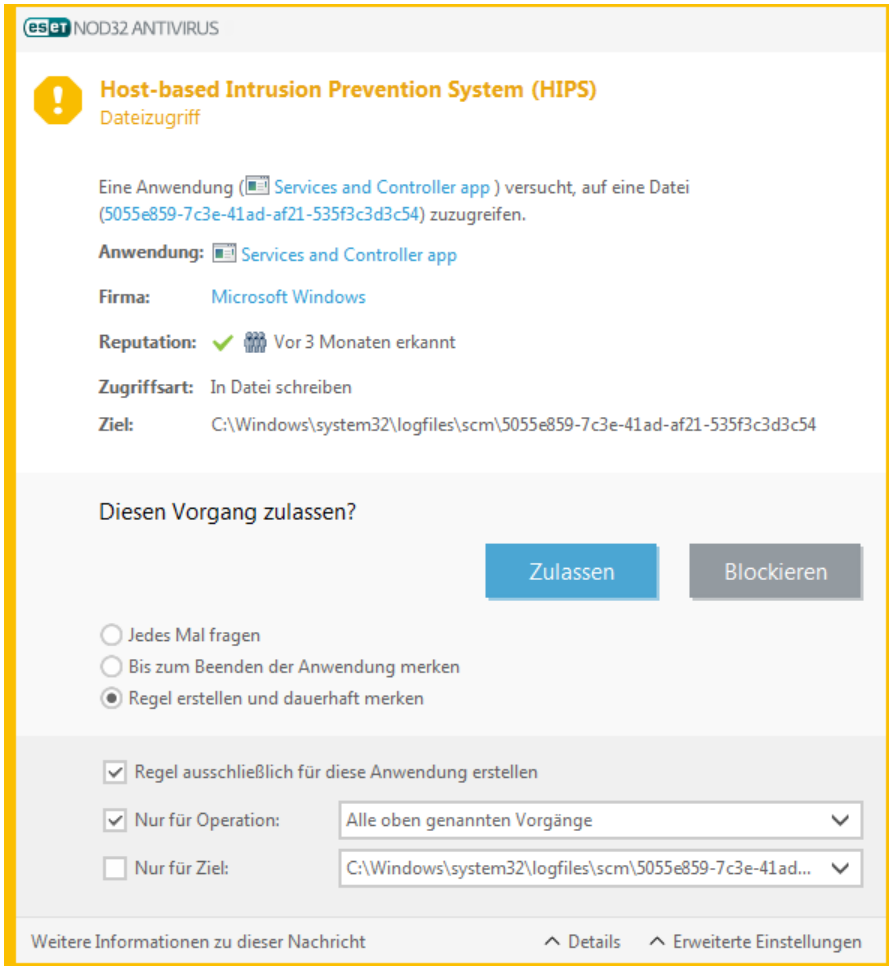
Klicken Sie auf unten auf **Details**, um herauszufinden, welche Anwendung den Vorgang ausgelöst hat, welche Reputation die Datei hat oder welche Art von Vorgang Sie zulassen oder blockieren können.

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 Operation** - Wählen Sie Datei-, Anwendungs- oder Registrierungsziele für diese Regel aus.

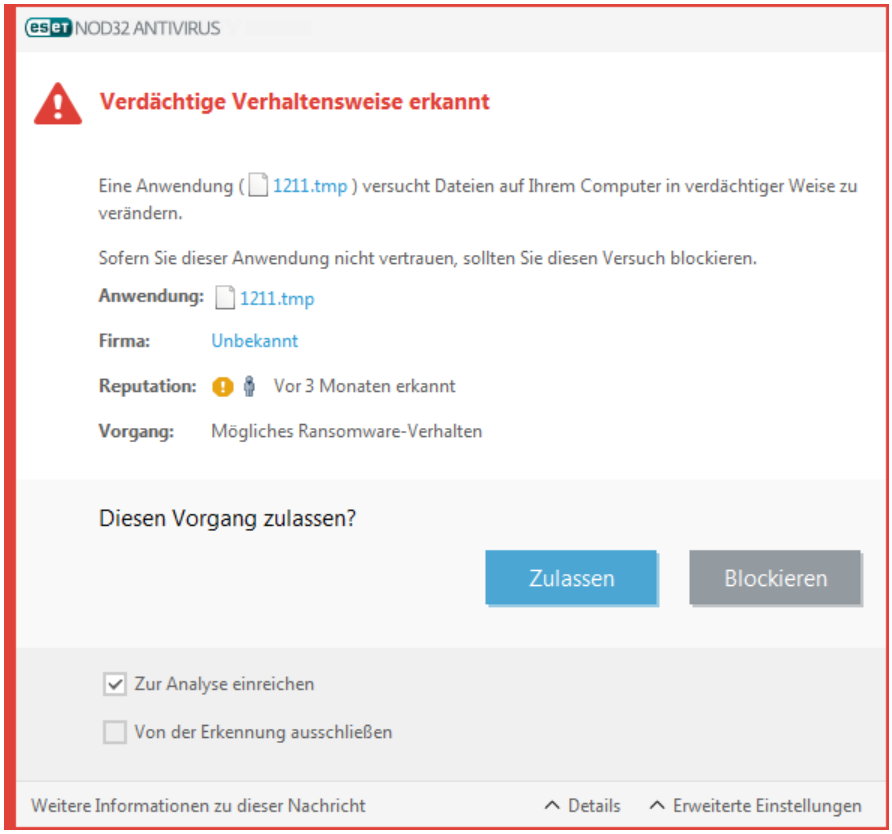
Erhalten Sie zu viele HIPS-Meldungen?

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 **Blockieren** 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.

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

HIPS-Regelverwaltung

Eine Liste benutzerdefinierter und automatisch hinzugefügter Regeln vom HIPS-System. Weitere Informationen zum Erstellen von Regeln und zu HIPS-Vorgängen finden Sie im Kapitel HIPS-Regeleinstellungen. Siehe auch Funktionsprinzip von HIPS.

Spalten

Regel - Benutzerdefinierter oder automatisch ausgewählter Regelname.

Aktiviert – Deaktivieren Sie den Schieberegler, wenn Sie die Regel in der Liste erhalten, sie aber nicht verwenden möchten.

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

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

Benachrichtigen - In der rechten unteren Ecke wird ein kleines Fenster 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 werden.

- 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-Regel bearbeiten

Lesen Sie zunächst den Abschnitt 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 den Schieberegler, wenn Sie die Regel in der Liste erhalten, sie jedoch nicht anwenden möchten.

Logging-Schweregrad – 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.

Zieldateien - Die Regel wird nur angewendet, wenn sich der Vorgang auf dieses Ziel bezieht. Wählen Sie **Bestimmte Dateien** im Dropdownmenü aus und klicken Sie auf **Hinzufügen**, um neue Dateien oder Ordner hinzuzufügen. Mit dem Eintrag **Alle Dateien** im Dropdownmenü können Sie alle Dateien hinzufügen.

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, oder auf **Alle Anwendungen**, 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, oder auf **Registrierungseditor öffnen**, um einen Registrierungsschlüssel auszuwählen. Alternativ können Sie **Alle Einträge** auswählen, um alle Anwendungen hinzuzufügen.

> 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.

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.

Sie können eingeschränkt Platzhalter bei der Eingabe des Ziels verwenden. Anstatt eines bestimmten Schlüssels können Sie das Sonderzeichen * (Sternchen) im Registrierungspfad eingeben. *HKEY_USERS*\software* kann zum Beispiel *HKEY_USER\.default\software* bedeuten, jedoch nicht *HKEY_USERS\S-1-2-21-2928335913-73762274-491795397-7895\.default\software*. *HKEY_LOCAL_MACHINE\system\ControlSet** ist kein gültiger Pfad für einen Registrierungsschlüssel. Enthält ein Registrierungspfad „*“, bedeutet dies „dieser Pfad oder jeder untergeordnete Pfad nach diesem Symbol“. Nur auf diese Weise können Platzhalter für Zieldateien verwendet werden. Erst wird der angegebene Teil des Pfades überprüft, dann der Pfad nach dem Platzhalter (*).

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. Wählen Sie den Schieberegler **Benutzer informieren**, damit bei jedem Anwenden 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**.

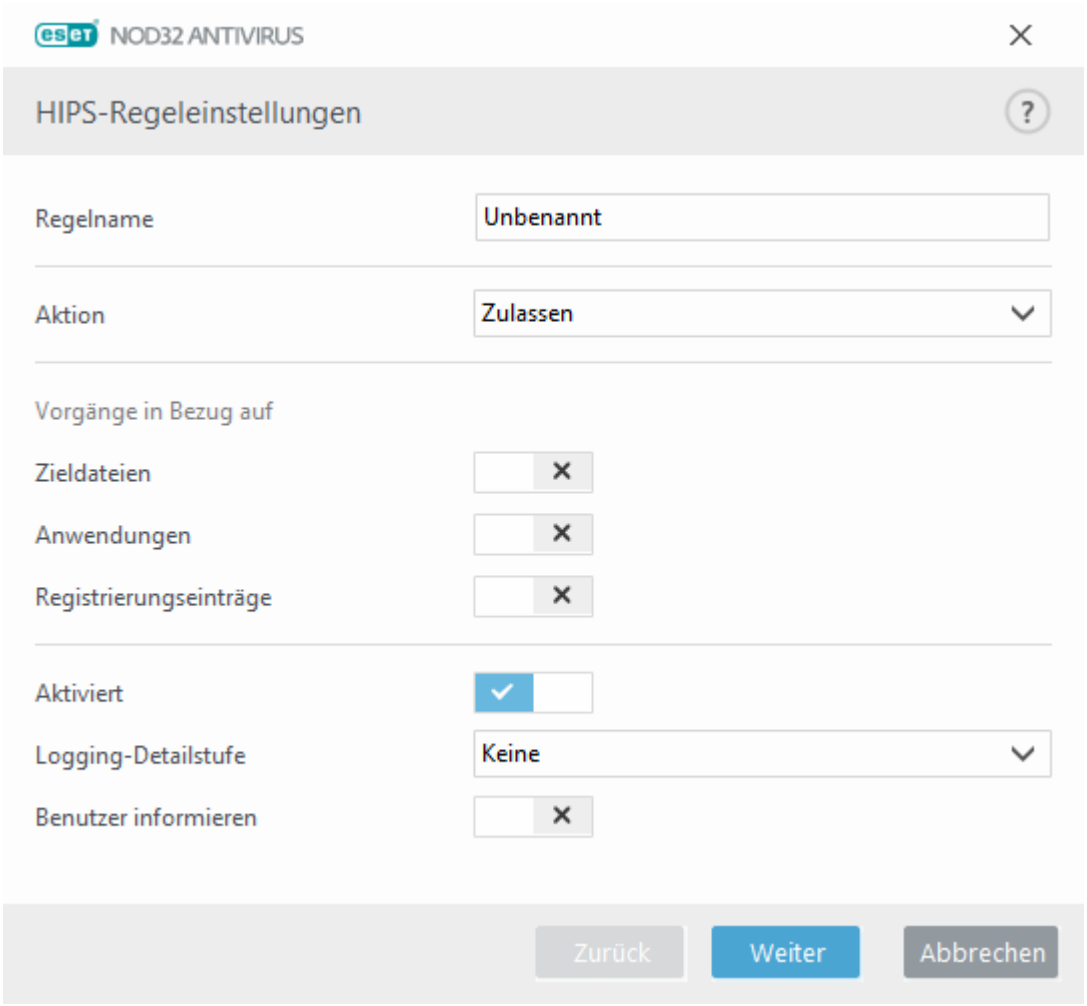
5. Wählen Sie im Fenster **Quellanwendungen** die Option **Bestimmte Anwendungen** im Dropdownmenü aus, um Ihre neue Regel für alle Anwendungen anzuwenden, die versuchen, eine der ausgewählten Anwendungsoperationen für die angegebenen Anwendungen auszuführen.

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.



Anwendung/Registrierungspfad für HIPS hinzufügen

Wählen Sie einen Datei-Anwendungspfad, indem Sie auf die Option **...** klicken. Bei Auswahl eines Ordners werden alle darin enthaltenen Anwendungen ausgewählt.

Die Option **Registrierungseditor öffnen** startet den Windows-Registrierungseditor (RegEdit). Achten Sie beim Hinzufügen eines Registrierungspfades darauf, dass Sie den richtigen Speicherort in das Feld **Wert** eingeben.

Beispiele für einen Datei- oder Registrierungspfad:

- *C:\Programme\Internet Explorer\iexplore.exe*
- *HKEY_LOCAL_MACHINE\system\ControlSet*

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 das HIPS-Log geschrieben. Verwenden Sie diese Funktion nur zur Fehlerbehebung oder wenn Sie vom technischen ESET Support dazu aufgefordert werden, da in diesem Fall sehr große Log-Dateien erstellt werden und die Leistung Ihres Computers beeinträchtigt werden kann.

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.

> 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.

Gamer-Modus

Der Gamer-Modus ist eine Funktion für Benutzer, die ihre Software ununterbrochen nutzen, nicht durch Popup-Fenster gestört werden und die CPU-Auslastung reduzieren möchten. Der Gamer-Modus kann auch während Präsentationen verwendet werden, die nicht durch eine Aktion des Virenschutzes unterbrochen werden dürfen. In diesem Modus werden alle Popup-Fenster deaktiviert, und die Aktivität des Taskplaners wird komplett gestoppt. Der Systemschutz läuft weiter im Hintergrund, doch es sind keine Eingaben durch Benutzer erforderlich.

Sie können den Gamer-Modus im Hauptfenster unter **Einstellungen** > **Computer-Schutz** aktivieren, indem Sie neben  auf oder  klicken. Im Gamer-Modus besteht ein erhöhtes Risiko. Daher wird das Schutzstatus-Symbol in der Taskleiste orange und mit einer Warnung angezeigt. Diese Warnung wird auch im Hauptprogrammfenster zusammen mit dem orangefarbenen Hinweis **Gamer-Modus aktiv** angezeigt.

Mit der Option **Gamer-Modus automatisch aktivieren, wenn Anwendungen im Vollbildmodus ausgeführt werden** unter **Erweiterte Einstellungen** (F5) > **Tools** > **Gamer-Modus** wird der Gamer-Modus gestartet, sobald Sie eine Anwendung im Vollbildmodus ausführen und automatisch beendet, sobald Sie die Anwendung beenden.

Mit der Option **Gamer-Modus automatisch deaktivieren nach** können Sie außerdem festlegen, nach wie vielen Minuten der Gamer-Modus automatisch deaktiviert werden soll.

Scan der Systemstartdateien

Die automatische Prüfung der Systemstartdateien wird standardmäßig beim Systemstart und beim Update der Erkennungsroutine ausgeführt. Die Ausführung der Prüfung ist abhängig davon, wie der Taskplaner konfiguriert ist und welche Tasks eingerichtet wurden.

Die Option der Systemstartprüfung ist Bestandteil der Task **Prüfung der Systemstartdateien** im Taskplaner. Navigieren Sie zu **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. Wenn Sie eine niedrigere Scan-Tiefe für Dateien auswählen, die beim Systemstart ausgeführt werden, werden nicht gescannte

Dateien beim Öffnen oder Ausführen gescannt.

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, öffnen Sie **Erweiterte Einstellungen** (F5) > **Erkennungsroutine** > **Malware-Scans** > **Dokumentenschutz**, und klicken Sie auf den Schieberegler neben **Dokumentenschutz aktivieren**.

> 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.

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

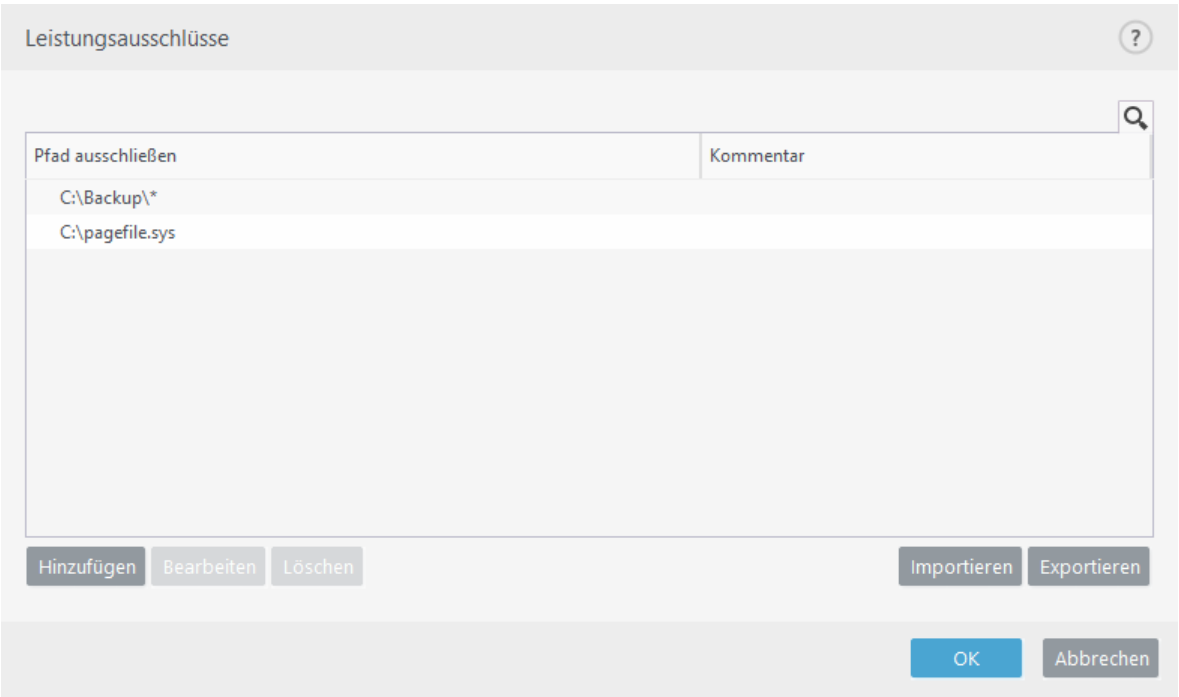
Mit Leistungsausschlüssen können Sie Dateien und Ordner vom Scannen ausschließen.

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.

Verwechseln Sie diese Funktion nicht mit Ereignisausschlüssen, Ausschlüssen für Dateierweiterungen, HIPS-Ausschlüssen oder ausgeschlossenen Prozessen.

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.



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

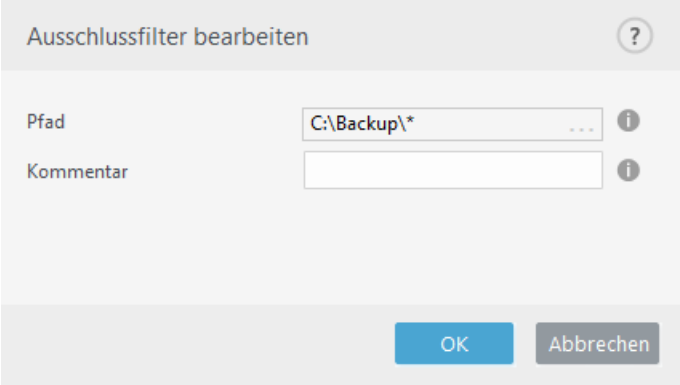
- **Hinzufügen** - Objekte von der Prüfung ausnehmen
- **Bearbeiten** - Ausgewählten Eintrag bearbeiten
- **Löschen** – Ausgewählte Einträge entfernen (CTRL + Klicken, um mehrere Einträge auszuwählen.

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 und Unterordner 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.)

Beispiele:

- *C:\Tools** – Der Pfad muss mit umgekehrtem Schrägstrich (\) und Sternchen (*) enden, um anzugeben, dass es sich um einen Ordner handelt und alle Ordnerinhalte (Dateien und Unterordner) ausgeschlossen werden.
- *C:\Tools*.** – Gleiche Verhaltensweise wie *C:\Tools**
- *C:\Tools* - Der Ordner *Tools* wird nicht ausgeschlossen. Aus der Perspektive des Scanners könnte *Tools* auch ein Dateiname sein.
- *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.

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.

Platzhalter in der Mitte von Pfaden werden nicht unterstützt

Die Verwendung von Platzhaltern in der Mitte von Pfaden (beispielsweise *C:\Tools*\Data\file.dat*) kann funktionieren, wird für Leistungsausschlüsse jedoch nicht offiziell unterstützt. Weitere Informationen finden Sie im folgenden 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 und Unterordner 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.)

Beispiele:
• *C:\Tools** – Der Pfad muss mit umgekehrtem Schrägstrich (\) und Sternchen (*) enden, um anzugeben, dass es sich um einen Ordner handelt und alle Ordnerinhalte (Dateien und Unterordner) ausgeschlossen werden.
• *C:\Tools*.** – Gleiche Verhaltensweise wie *C:\Tools**
• *C:\Tools* - Der Ordner *Tools* wird nicht ausgeschlossen. Aus der Perspektive des Scanners könnte *Tools* auch ein Dateiname sein.
• *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.

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%*

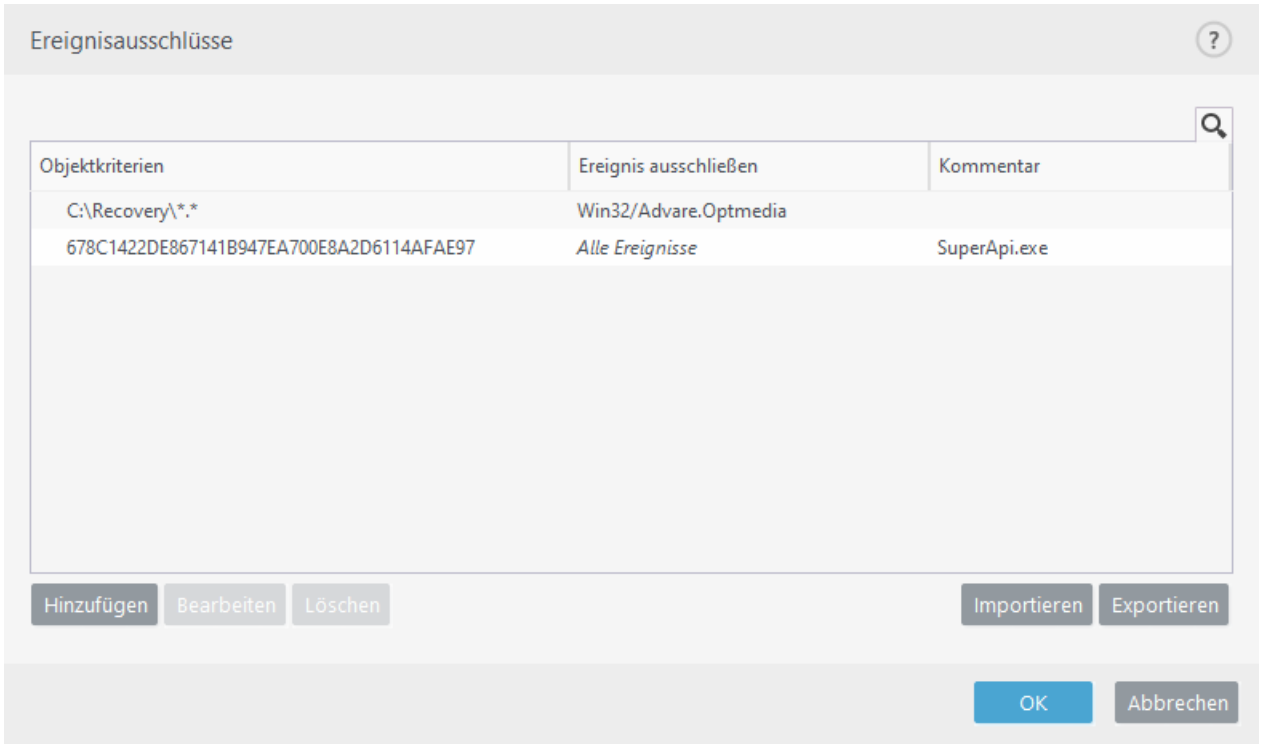
Benutzerspezifische Systemvariablen (z. B. *%TEMP%* oder *%USERPROFILE%*) oder Umgebungsvariablen (z. B. *%PATH%*) werden nicht unterstützt.

Ereignisausschlüsse

Mit Ereignisausschlüssen können Sie Objekte von der Ereignis 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.

> Verwechseln Sie diese Funktion nicht mit Leistungsausschlüssen, Ausschlüssen für Dateierweiterungen, HIPS-Ausschlüssen oder ausgeschlossenen Prozessen.

Um ein Objekt (nach Ereignisname oder Hash) aus der Erkennungsroutine auszuschließen, klicken Sie auf **Hinzufügen**.

Für potenziell unerwünschte Anwendungen und potenziell unsichere Anwendungen können Sie Ausschlüsse anhand des Ereignisnamens erstellen:

- Im Hinweisfenster für das Ereignis (klicken Sie auf **Erweiterte Einstellungen anzeigen** und wählen Sie **Von der Erkennung ausschließen** aus).
- Im Kontextmenü der Log-Dateien mit dem Assistenten zum Erstellen von Ereignisausschlüssen.
- Mit einem Klick auf **Tools** > **Quarantäne** und dann mit einem Klick mit der rechten Maustaste auf die Datei in der Quarantäne und das Auswählen des Befehls **Wiederherstellen und vom Scannen ausschließen** aus dem Kontextmenü.

Objektkriterien für Ereignisausschlüsse

- **Pfad** - Beschränkt einen Ereignisausschluss auf einen bestimmten Pfad (oder alle Pfade).
- **Ereignisname** – Falls neben einer ausgeschlossenen Datei der Name eines Ereignisses steht, gilt die Ausnahme dieser Datei nur für das entsprechende Ereignis und nicht allgemein. Wenn diese Datei später mit einer anderen Malware infiziert wird, erkennt der Virenschutz dies.

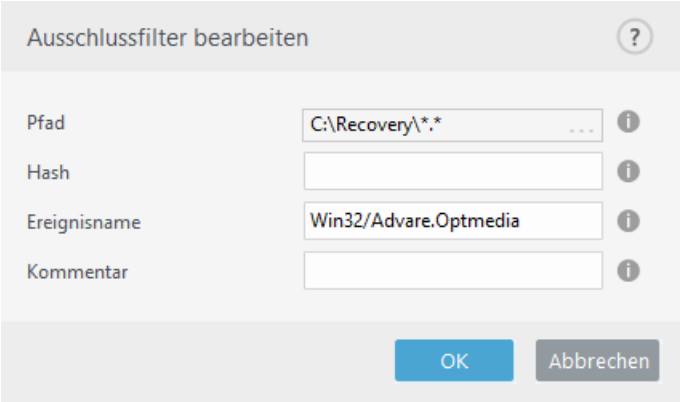
- **Hash** – Schließt eine Datei auf Basis eines angegebenen Hashs SHA-1 aus, unabhängig von Dateityp, Speicherort, Name oder Erweiterung.

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 NOD32 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.

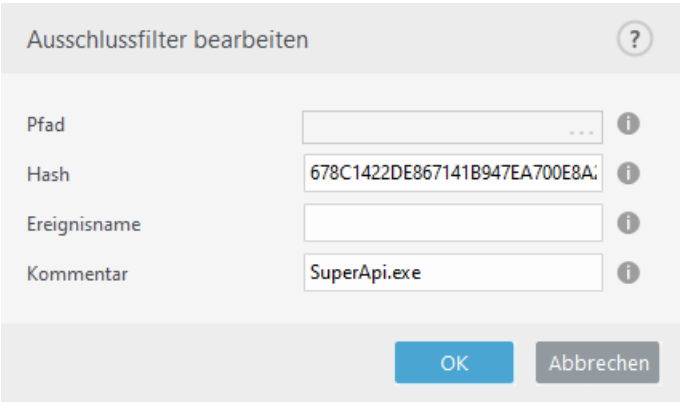
Siehe auch Format für ausgeschlossene Pfade.



Beachten Sie das unten gezeigte Beispiel für Ereignisausschlüsse.

Hash ausschließen

Schließt eine Datei auf Basis eines angegebenen Hashs SHA-1 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 NOD32 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):

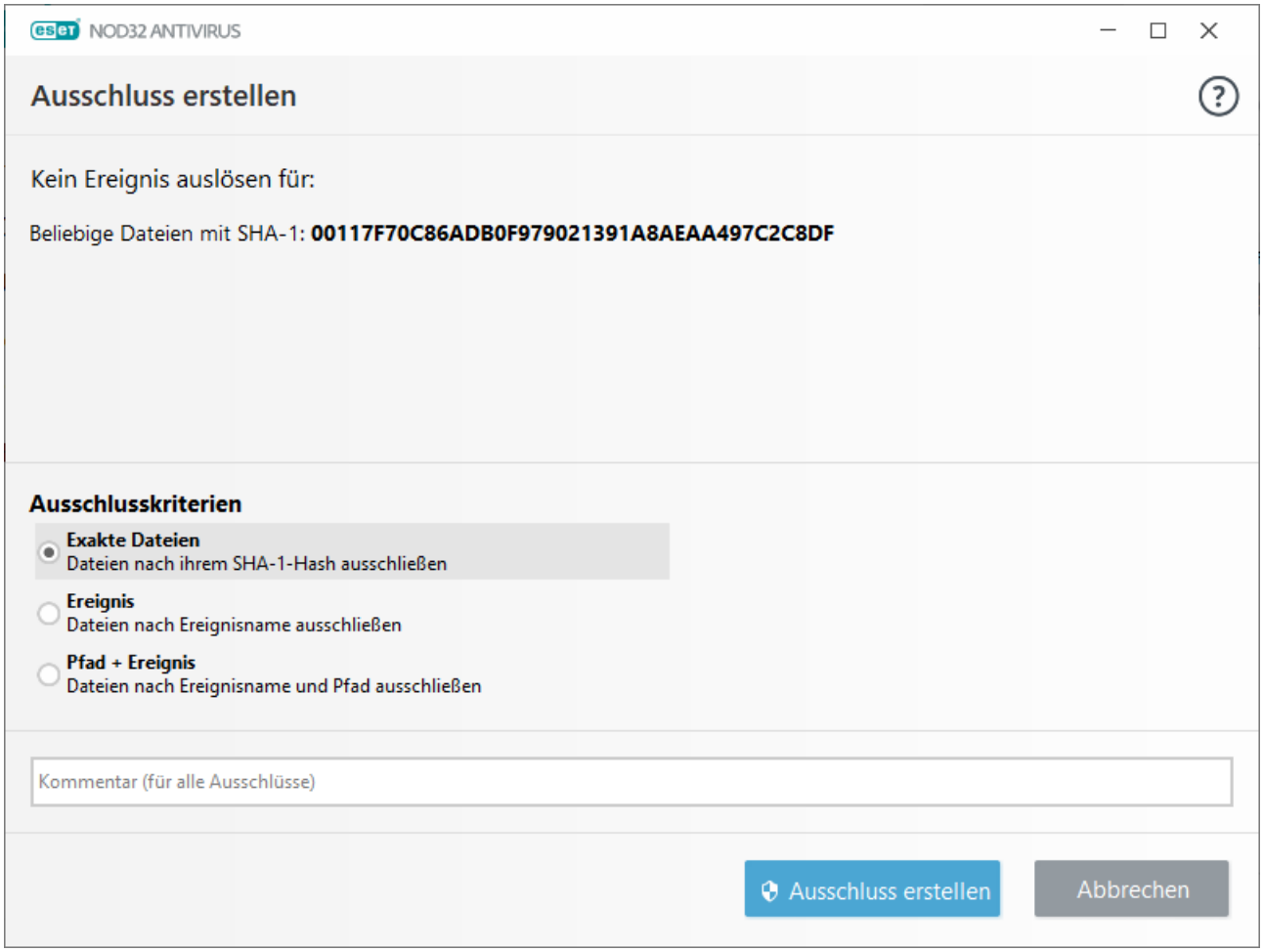
1. Klicken Sie im Hauptprogrammfenster auf **Tools** > **Log-Dateien**.
2. Klicken Sie mit der rechten Maustaste auf eine Erkennung im **Erkennungs-Log**.
3. Klicken Sie auf **Ausschluss erstellen**.

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.



HIPS-Ausschlüsse

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

Um HIPS-Ausschlüsse zu bearbeiten, navigieren Sie zu **Erweiterte Einstellungen** (F5) > **Erkennungsroutine** > **HIPS** > **Einfach** > **Ausschlüsse** > **Bearbeiten**.

> Verwechseln Sie diese Funktion nicht mit Ausgeschlossenen Dateierweiterungen, Ereignisausschlüssen, Leistungsausschlüssen oder ausgeschlossenen Prozessen.

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. ThreatSense -Technologie ist auch in der Lage, Rootkits zu vermeiden.

in den Einstellungen für ThreatSense können Sie verschiedene Prüfparameter festlegen:

- Dateitypen und -erweiterungen, die gescannt 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
- Scan der Systemstartdateien
- Dokumentenschutz
- E-Mail-Schutz
- Web-Schutz
- Computer-Scan

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.

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 - Folgende Erweiterungen werden vom Programm unterstützt: 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 Gegensatz zu herkömmlichen Archiven 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 NOD32 Antivirus beim Säubern von Objekten vorgeht. Sie haben vier Säuberungsstufen zur Auswahl:

In den ThreatSense-Parametern sind die folgenden Korrekturstufen (Säuberungsstufen) verfügbar.

Behebung in ESET NOD32 Antivirus

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.
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 für die meisten Fälle 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.

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 beim Scannen nur die benutzerdefinierten Einstellungen im ThreatSense-Kern der einzelnen Module angewendet.

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 den Scan von Dateien in Containerobjekten (z. B. RAR/ZIP-Archive oder E-Mails mit mehreren Anlagen). Diese Einstellung gilt nicht für eigenständige Dateien. Wenn ein benutzerdefinierter Wert eingegeben wurde und die Frist verstrichen ist, wird der Scan schnellstmöglich beendet, und zwar unabhängig davon, ob alle Dateien in einem Containerobjekt gescannt wurden.
Im Fall von Archiven mit großen Dateien wird der Scan erst beendet, wenn eine Datei aus dem Archiv extrahiert wird (z. B. wenn der benutzerdefinierte Wert 3 Sekunden festgelegt wurde und die Extraktion einer Datei 5 Sekunden dauert). Die restlichen Dateien im Archiv werden nach Ablauf dieser Zeit nicht gescannt.
Um die Scandauer auch für größere Archive zu begrenzen, können Sie die Einstellungen **Maximale Objektgröße** und **Maximalgröße von Dateien im Archiv** verwenden (nicht empfohlen aufgrund möglicher Sicherheitsrisiken).

Standardwert: unbegrenzt.

Einstellungen für Archivprüfung

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

Maximalgröße von Dateien im Archiv – Hier können Sie die maximale Dateigröße für Dateien in (extrahierten) Archiven festlegen, die gescannt werden sollen. Der Maximalwert ist **3 GB**.

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

Von der Prüfung ausgeschlossene Dateiendungen

Ausgeschlossene Dateierweiterungen sind ein Teil der ThreatSense-Parameter. Um ausgeschlossene Dateierweiterungen zu konfigurieren, klicken Sie auf **ThreatSense-Parameter** in den erweiterten Einstellungen für beliebige Module, die die ThreatSense-Technologie verwenden.

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.

> Verwechseln Sie diese Funktion nicht mit den ausgeschlossenen Prozessen, den HIPS-Ausschlüssen oder den Datei-/Ordnerausschlüssen.

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.

> 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 Folgendes ein: `edb;eml;tmp`).
> Das Sonderzeichen ? (Fragezeichen) steht für ein beliebiges Zeichen (z. B. `?db`).

> 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

Um diese Einstellungen zu bearbeiten, navigieren Sie zu **Erweiterte Einstellungen** (F5) > **Erkennungsroutine** > **Echtzeit-Dateischutz** > **Zusätzliche ThreatSense-Parameter**.

Zusätzliche ThreatSense-Parameter für neu erstellte und geänderte Dateien

Das Infektionsrisiko für neu erstellte oder geänderte Dateien ist höher als für vorhandene Dateien. Daher scannt das Programm solche Dateien mit zusätzlichen Parametern. ESET NOD32 Antivirus verwendet Advanced Heuristik zusammen mit signaturbasierten Scan-Methoden, um neue Bedrohungen zu erkennen, bevor ein Update der Erkennungsroutine veröffentlicht wird.

Neben neu erstellten Dateien werden auch **selbstentpackende Archive** (.sfx) und **laufzeitkomprimierte Dateien** (intern komprimierte, ausführbare Dateien) gescannt. Standardmäßig werden Archive unabhängig von ihrer tatsächlichen Größe bis zur zehnten Verschachtelungsebene gescannt. Deaktivieren Sie die Option **Standardeinstellungen Archivscan**, um die Scan-Einstellungen für Archive zu ändern.

Zusätzliche ThreatSense-Parameter für ausführbare Dateien

Advanced Heuristik bei der Dateiausführung - 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.

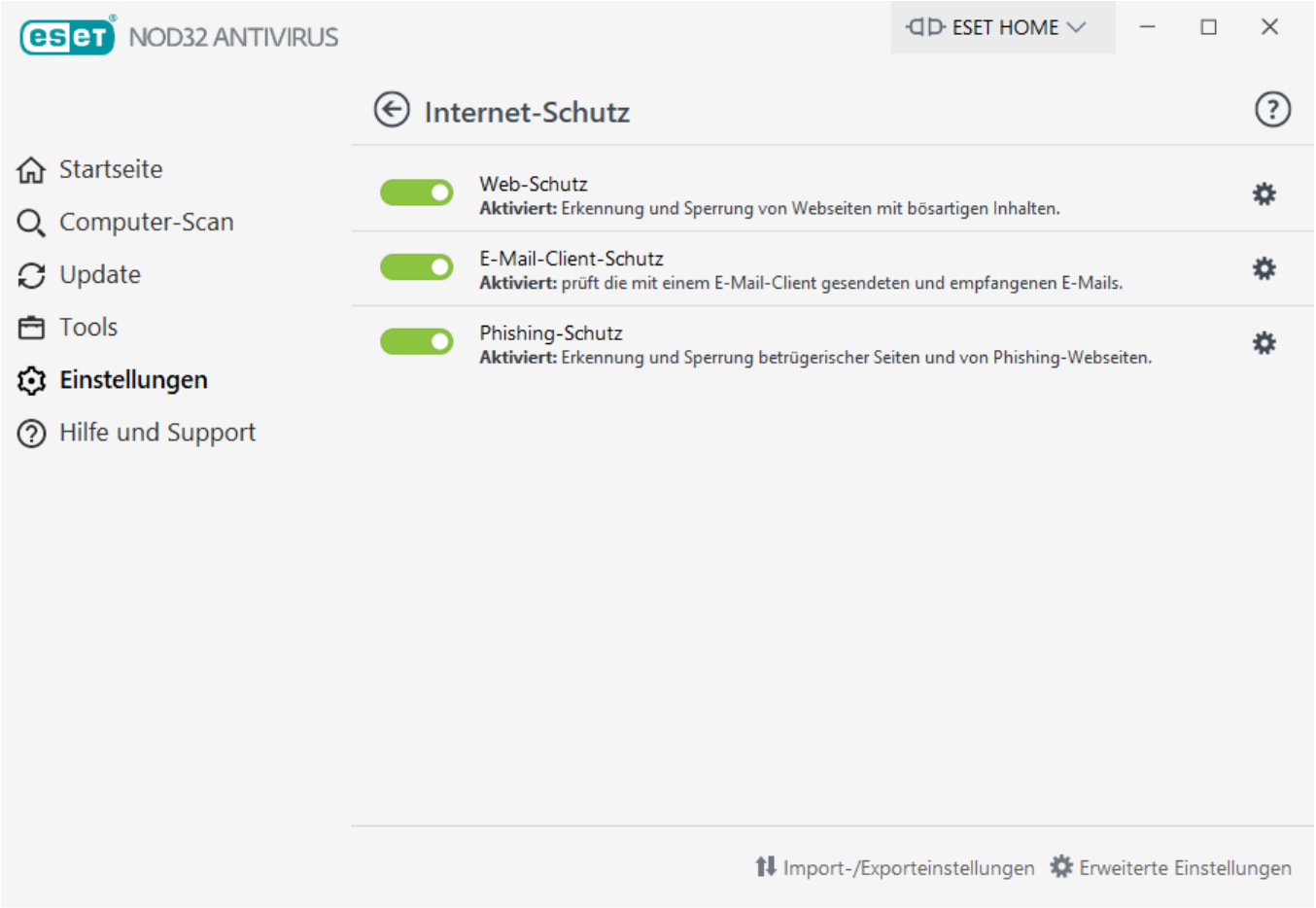
Advanced Heuristik bei der Ausführung von Dateien auf Wechselmedien – Advanced Heuristik emuliert Code in einer virtuellen Umgebung und prüft dessen Verhalten, bevor der Code von einem Wechseldatenträger ausgeführt wird.

Internet-Schutz

Klicken Sie im Fenster **Einstellungen** auf **Internet-Schutz**, um den Web- und E-Mail-Schutz zu konfigurieren. Von hier aus können Sie auf erweiterte Einstellungen des Programms zugreifen.

Um einzelne Schutzmodule anzuhalten oder zu deaktivieren, klicken Sie das Schieberegler-Symbol  .

⚠ Wenn Sie die Schutzmodule deaktivieren, kann der Schutz Ihres Computers beeinträchtigt werden.



Klicken Sie auf das Zahnradsymbol, um den Web-/E-Mail-/Phishing-Schutz zu öffnen. Schutzeinstellungen in den erweiterten Einstellungen zu öffnen.

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 NOD32 Antivirus Kontrollfunktionen für die gesamte E-Mail-Kommunikation bereit.

Der Phishing-Schutz blockiert Webseiten, die bekanntermaßen Phishing-Inhalte verbreiten. Es wird dringend empfohlen, den Phishing-Schutz aktiviert zu lassen.

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/TLS) 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 NOD32 Antivirus wie Web-Schutz, E-Mail-Schutz, Phishing-Schutz und Kindersicherung 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.

Hinzufügen (zum Beispiel *2001:718:1c01:16:214:22ff:fec9:ca5*).

Subnetz – Hier können Sie durch eine IP-Adresse und eine Maske ein Subnetz definieren. (Beispiel: *2002:c0a8:6301:1::1/64*)

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.

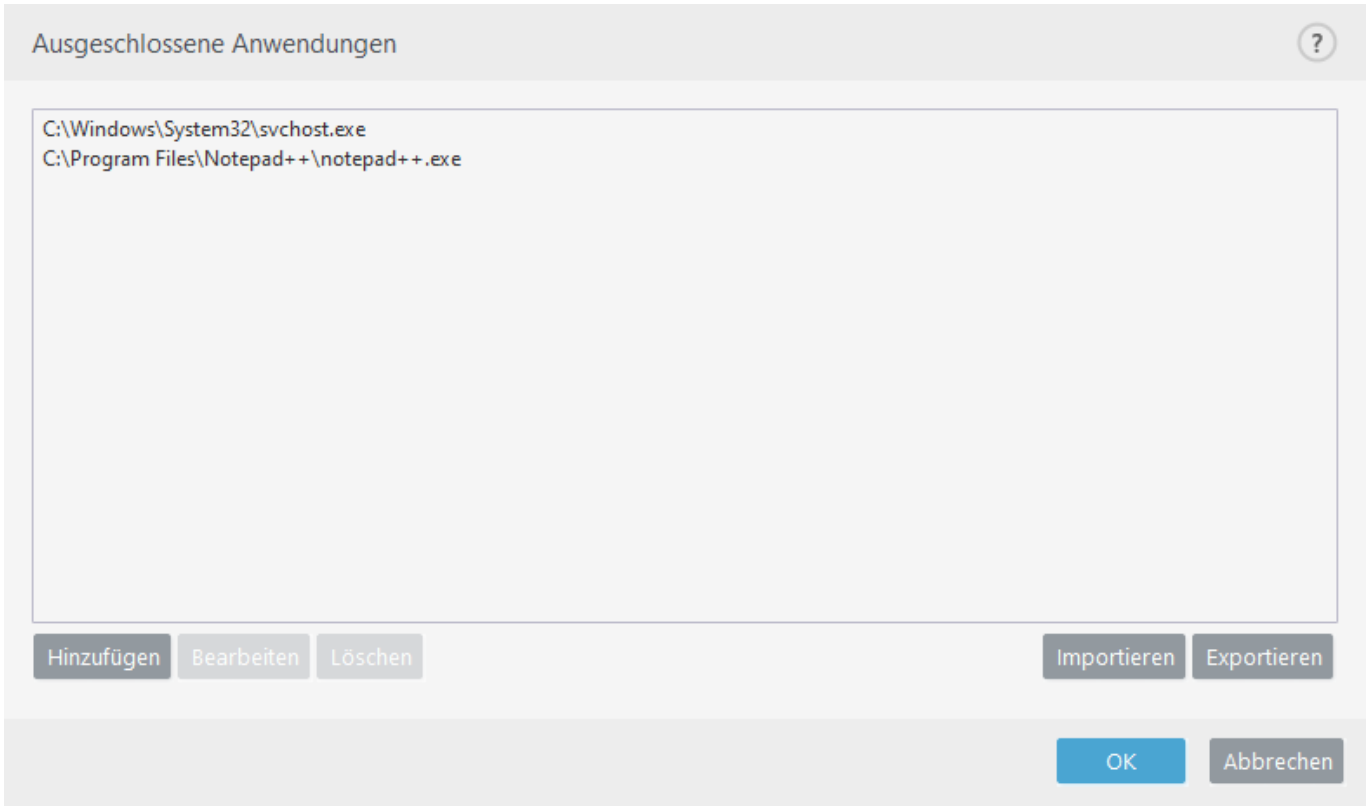
IPv6-Adresse und Maske:

- *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

Wählen Sie aus der Liste die Netzwerk-Anwendungen, für deren Datenkommunikation keine Inhaltsprüfung erfolgen soll. Dies schließt die HTTP/POP3/IMAP-Datenkommunikation ausgewählter Anwendungen von der Prüfung auf Bedrohungen aus. Wir empfehlen, diese Option nur für Anwendungen zu aktivieren, deren Datenkommunikation mit aktivierter Prüfung nicht ordnungsgemäß funktioniert.

Aktuell ausgeführte Anwendungen und Dienste stehen hier automatisch zur Verfügung. Klicken Sie auf **Hinzufügen**, um manuell eine Anwendung auszuwählen, die nicht in der Protokollprüfliste angezeigt wird.

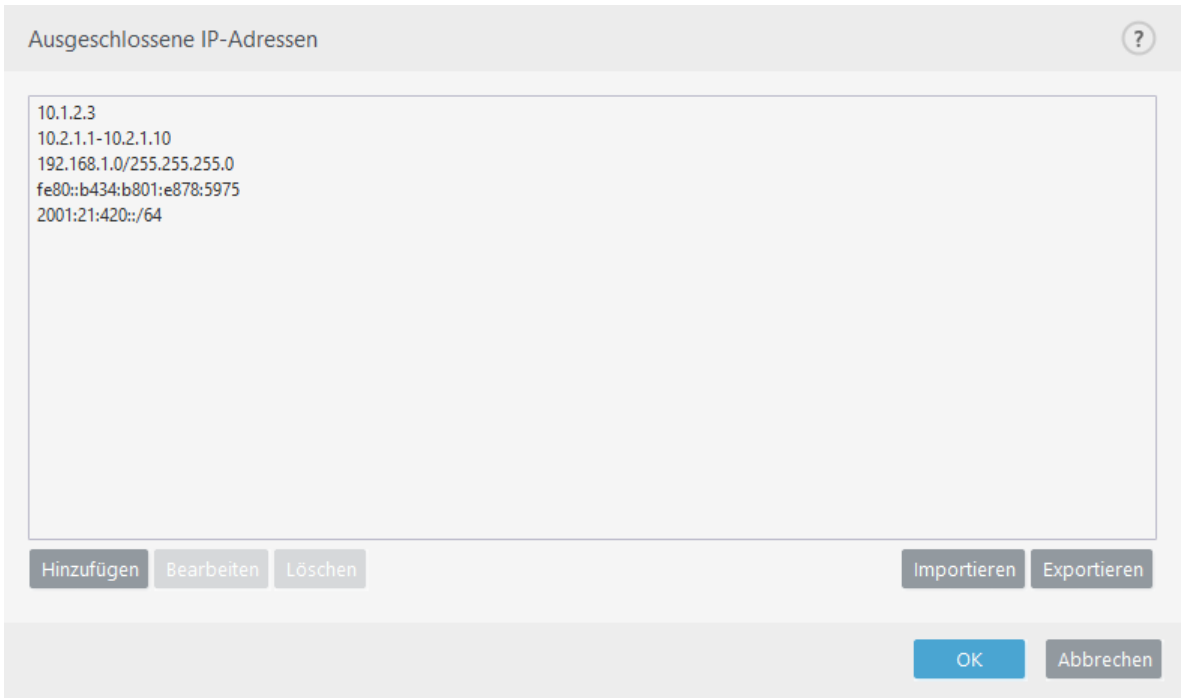


Ausgeschlossene IP-Adressen

Die in der Liste eingetragenen Adressen werden von der Protokollinhaltsprüfung ausgeschlossen. 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.

Klicken Sie auf **Hinzufügen**, um eine IP-Adresse, einen Bereich von Adressen oder ein Subnetz für die Gegenstelle zur Liste für die Protokollprüfung hinzuzufügen.

Klicken Sie auf **Löschen**, um ausgewählte Einträge aus der Liste zu entfernen.



IPv4-Adresse hinzufügen

Hier können Sie eine IP-Adresse, einen Bereich von Adressen oder ein Subnetz für die Gegenstelle festlegen, die von der Regel erfasst wird. Version 4 ist eine ältere Version des Internetprotokolls.

Einzelne Adresse – Hinzufügen der IP-Adresse eines einzelnen Computers, auf den die Regel angewendet werden soll (zum Beispiel *192.168.0.10*).

Adressbereich – Geben Sie die Start- und Endadresse eines Bereichs von IP-Adressen ein (von mehreren Computern), auf die die Regel angewendet werden soll (z. B. *192.168.0.1* bis *192.168.0.99*).

Subnetz – Hier können Sie durch eine IP-Adresse und eine Maske ein Subnetz (eine Gruppe von Computern) definieren.

255.255.255.0 ist z. B. die Netzwerkmaske für das Präfix *192.168.1.0/24*, also der Adressbereich *192.168.1.1* bis 192.168.1.254.

IPv6-Adresse hinzufügen

Hier können Sie eine IPv6-Adresse/ein IPv6-Subnetz für die Gegenstelle festlegen, auf die die Regel angewendet werden soll. IPv6 ist die neueste Version des Internetprotokolls, und wird die bisherige Version 4 ersetzen.

Einzelne Adresse – Hier können Sie die IP-Adresse eines einzelnen Computers eingeben, auf den die Regel angewendet werden soll (z. B. *2001:718:1c01:16:214:22ff:fec9:ca5*).

Subnetz – Hier können Sie durch eine IP-Adresse und eine Maske ein Subnetz definieren. (Beispiel: *2002:c0a8:6301:1::1/64*)

SSL/TLS

ESET NOD32 Antivirus kann Verbindungen, die das SSL-Protokoll verwenden, auf Bedrohungen untersuchen. Für die Untersuchung von durch SSL geschützten Verbindungen gibt es verschiedene Filtermodi mit vertrauenswürdigen und unbekannten Zertifikaten sowie Zertifikaten, die von der Prüfung SSL-geschützter Verbindungen ausgeschlossen sind.

SSL/TLS-Protokollfilterung aktivieren – Wenn der Protokollfilter deaktiviert ist, werden SSL-Verbindungen nicht geprüft.

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.

Filtermodus	Beschreibung
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 NOD32 Antivirus für bestimmte Anwendungen anpassen.

Liste der bekannten Zertifikate – Mit dieser Liste können Sie das Verhalten von ESET NOD32 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.

Stammzertifikat

Stammzertifikat zu bekannten Browsern hinzufügen – Damit die SSL-Kommunikation in Ihren Browsern/E-Mail-Programmen ordnungsgemäß funktioniert, muss das Stammzertifikat für ESET zur Liste der bekannten Stammzertifikate (Herausgeber) hinzugefügt werden. Mit dieser Option fügt ESET NOD32 Antivirus das ESET SSL Filter CA-Zertifikat automatisch zu den bekannten Browsern (z. B. Opera) hinzu. Wenn ein Browser den Systemzertifizierungsspeicher verwendet, wird das Zertifikat automatisch hinzugefügt. Firefox vertraut beispielsweise automatisch den Stammzertifizierungsstellen im Systemzertifizierungsspeicher.

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 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 auswählen, die für verschlüsselte Verbindungen ausgeführt wird. Mit der Option **Kommunikation blockieren, die das Zertifikat verwendet** können Sie verschlüsselte Verbindungen zu Sites, die nicht verifizierte Zertifikate verwenden, immer beenden.

Wenn das Zertifikat beschädigt ist – In diesem Fall ist das Zertifikat entweder fehlerhaft signiert oder beschädigt. In diesem Fall empfiehlt ESET, die Option **Kommunikation blockieren, die das Zertifikat verwendet** ausgewählt zu lassen. Wenn Sie **Gültigkeit des Zertifikats erfragen** auswählen, muss der Benutzer eine Aktion auswählen, die für verschlüsselte Verbindungen ausgeführt wird.

Beispiele mit Abbildungen

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

- Zertifikatbenachrichtigungen in ESET Windows Home-Produkten
- „Verschlüsselte Netzwerkverbindung: Nicht vertrauenswürdiges Zertifikat" wird beim Besuch von Webseiten 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.

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 erhalten ist, ist das Fenster rot hinterlegt. Wenn das Zertifikat in der Liste vertrauenswürdiger Stammzertifizierungsstellen erhalten ist, ist das Fenster grün hinterlegt.

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 NOD32 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

NOD32 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 Windows Home-Produkten
> - „Verschlüsselte Netzwerkverbindung: Nicht vertrauenswürdiges Zertifikat" wird beim Besuch von Webseiten 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 NOD32 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 – Fügen Sie ein neues Zertifikat hinzu und passen Sie die Einstellungen für Zugriffs- und Prüfoptionen an.

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 NOD32 Antivirus für bestimmte Anwendungen anpassen und ausgewählte Aktionen speichern, wenn **Interaktiver 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 - Wählen Sie eine ausführbare Datei aus dem Verzeichnis, klicken Sie auf die Option **...** oder geben Sie den Pfad per Hand ein.

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 die Anwendung aus und klicken Sie auf **Bearbeiten**.

Löschen – Wählen Sie die Anwendung aus und klicken Sie auf **Löschen**.

Importieren/Exportieren – Importieren Sie Anwendungen aus einer Datei oder speichern Sie Ihre aktuelle Liste mit Anwendungen in einer Datei.

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

E-Mail-Client-Schutz

Weitere Konfigurationshinweise für die Integration finden Sie unter Integration von ESET NOD32 Antivirus Ihrem E-Mail-Client.

Sie finden die E-Mail-Programm-einstellungen unter **Erweiterte Einstellungen** (F5) > **Web und E-Mail** > **E-Mail-Schutz** > **E-Mail-Programme**.

E-Mail-Programme

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

Zu scannende E-Mails

Wählen Sie zu scannende E-Mails aus:

- **Eingehende E-Mails**
- **Ausgehende E-Mails**
- **E-Mails lesen**
- **Geänderte E-Mail**

> 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.

Integration in E-Mail-Programme

Die Integration von ESET NOD32 Antivirus mit Ihrem E-Mail-Programm verbessert den aktiven Schutz vor Schadcode in E-Mail-Nachrichten. Wenn Ihr E-Mail-Programm dies unterstützt, kann die Integration in ESET NOD32 Antivirus aktiviert werden. Mit der Integration in Ihren E-Mail-Client wird die ESET NOD32 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** > **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.

Deaktivieren Sie die Optionen **Optimierte Verarbeitung von Anhängen** und **Erweiterte E-Mail-Clientverarbeitung**, falls beim Abrufen von E-Mails die Systemleistung beeinträchtigt wird.

Microsoft Outlook-Symbolleiste

Die Sicherheitslösung für Microsoft Outlook ist ein Plug-In. Nach der Installation von ESET NOD32 Antivirus wird in Microsoft Outlook diese Symbolleiste für den Viren- und mit folgenden Schutzoptionen angezeigt:

ESET NOD32 Antivirus – Doppelklicken Sie auf das Symbol, um das Hauptfenster von ESET NOD32 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 NOD32 Antivirus wird in Outlook Express bzw. Windows Mail diese Symbolleiste für den Viren- und mit folgenden Schutzoptionen angezeigt:

ESET NOD32 Antivirus – Doppelklicken Sie auf das Symbol, um das Hauptfenster von ESET NOD32 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 NOD32 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.

E-Mail-Protokolle

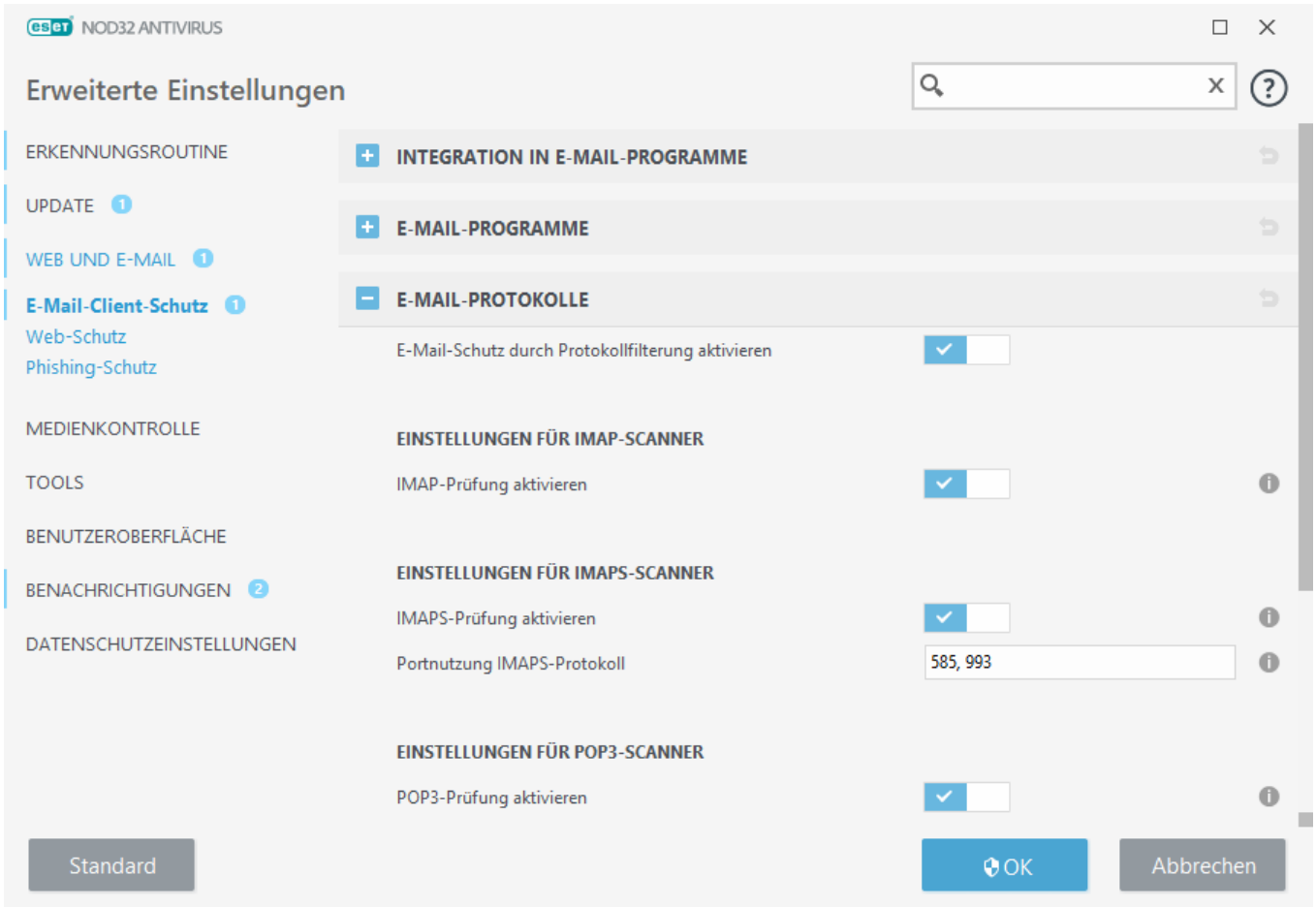
IMAP und POP3 sind die gängigsten Protokolle für den Empfang von E-Mails in E-Mail-Clientanwendungen. Das Internet Message Access Protocol (IMAP) ist ein weiteres Internetprotokoll für den E-Mail-Abruf. IMAP bietet einige Vorteile gegenüber POP3, z. B. können sich mehrere Clients gleichzeitig mit demselben 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 NOD32 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 IMAP-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 NOD32 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 NOD32 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. Bei Bedarf können weitere Kommunikationsports hinzugefügt werden. Mehrere Portnummern müssen durch Kommas getrennt angegeben werden.

Verschlüsselter Datenverkehr wird standardmäßig gescannt. Um die Scaneinstellungen anzuzeigen, öffnen Sie die erweiterten Einstellungen und navigieren Sie zu **Web und E-Mail** > **SSL/TLS**.



POP3, POP3S-Prüfung

Das POP3-Protokoll ist das am weitesten verbreitete Protokoll für den Empfang von E-Mails mit einer E-Mail-Client-Anwendung. ESET NOD32 Antivirus bietet Schutz für dieses Protokoll unabhängig vom verwendeten E-Mail-Client.

Das Schutzmodul, das diese Kontrolle bereitstellt, wird beim Systemstart automatisch initialisiert und ist anschließend im Arbeitsspeicher aktiv. Um das Modul einsetzen zu können, muss es aktiviert sein. Die POP3-Prüfung wird automatisch ausgeführt, ohne dass das E-Mail-Programm neu konfiguriert werden muss. Standardmäßig wird der gesamte Datenverkehr über Port 110 geprüft; weitere Kommunikationsports können bei Bedarf hinzugefügt werden. Mehrere Portnummern müssen durch Kommas getrennt angegeben werden.

Verschlüsselter Datenverkehr wird standardmäßig gescannt. Um die Scaneinstellungen anzuzeigen, öffnen Sie die erweiterten Einstellungen und navigieren Sie zu **Web und E-Mail** > **SSL/TLS**.

In diesem Abschnitt können Sie die Prüfung der Protokolle POP3 und POP3S konfigurieren.

POP3-Prüfung aktivieren – Wenn diese Option aktiviert ist, werden alle Daten geprüft, die über POP3 übertragen werden.

Portnutzung POP3-Protokoll – Eine Liste von Ports, die vom POP3-Protokoll verwendet werden (standardmäßig 110).

ESET NOD32 Antivirus unterstützt auch die Überwachung von POP3S-Protokollen. Bei dieser Kommunikationsart wird zur Datenübertragung zwischen Server und Client ein verschlüsselter Kanal verwendet. ESET NOD32 Antivirus überwacht die mit Hilfe der Verschlüsselungsverfahren SSL (Secure Socket Layer) und TLS (Transport

Layer Security) abgewickelte Kommunikation.

Keine POP3S-Prüfung verwenden – Verschlüsselte Kommunikation wird nicht geprüft.

POP3S-Protokollprüfung für ausgewählte Ports durchführen – Die POP3S-Prüfung wird nur für die unter **Portnutzung POP3-Protokoll** festgelegten Ports durchgeführt.

Portnutzung POP3S-Protokoll – Eine Liste zu prüfender POP3S-Ports (standardmäßig 995).

E-Mail-Tags

Die Optionen für diese Funktion finden Sie unter **Erweiterte Einstellungen** > **Web und E-Mail** > **E-Mail-Client-Schutz** > **Warnungen und Hinweise**.

Nachdem eine E-Mail gescannt wurde, kann ein Hinweis mit dem Scan-Ergebnis an die Nachricht angehängt 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 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.

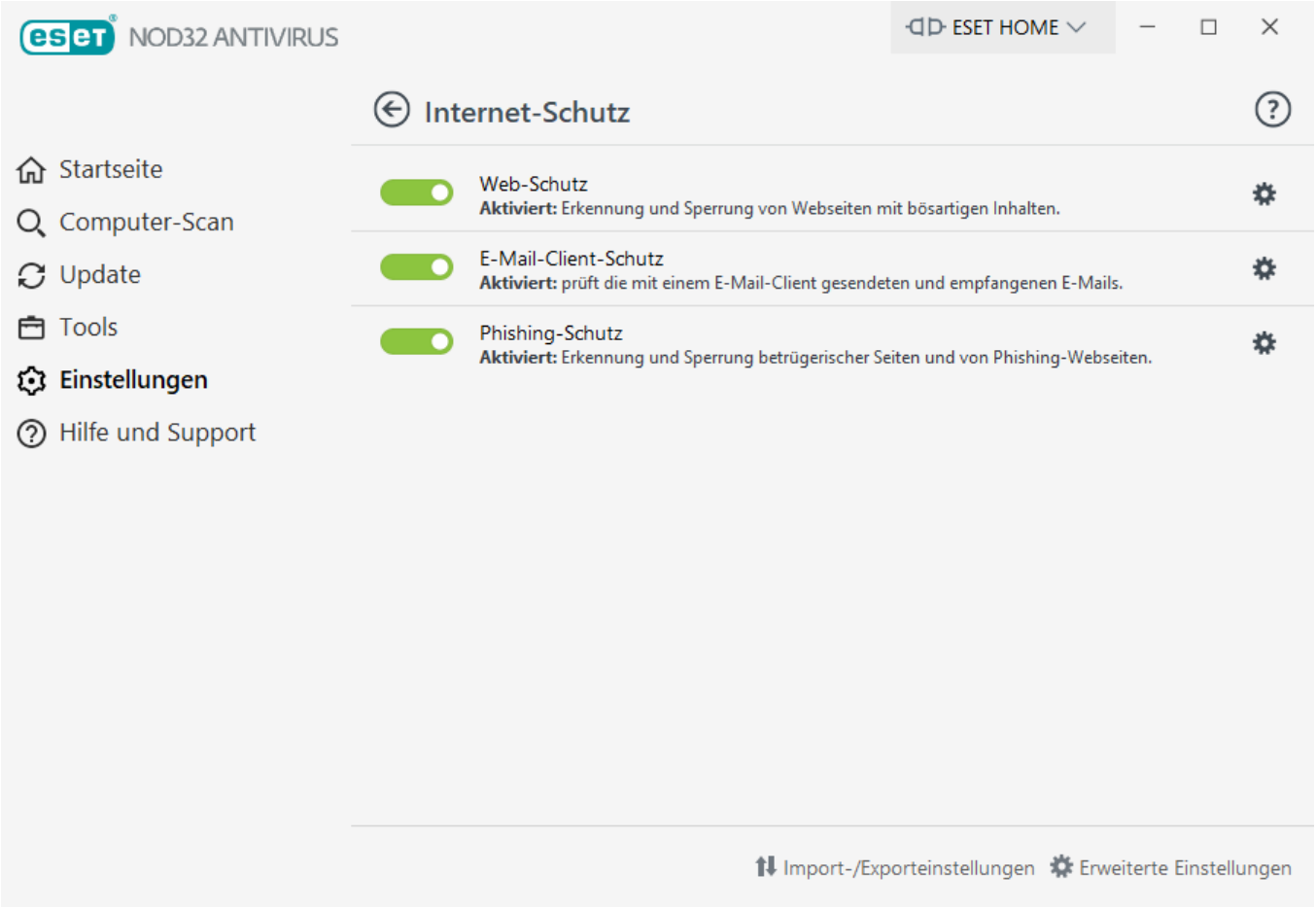
Text, der zum Betreff der erkannten E-Mail hinzugefügt wird - Geben Sie hier den Text ein, der das Präfix in der Betreffzeile von infizierten E-Mails ersetzen soll. Mit dieser Funktion wird der Nachrichtenbetreff „Hallo“ folgendermaßen formatiert: „[Ereignis %DETECTIONNAME%] Hallo“. Die Variable %DETECTIONNAME% steht dabei für das erkannte Ereignis.

Web-Schutz

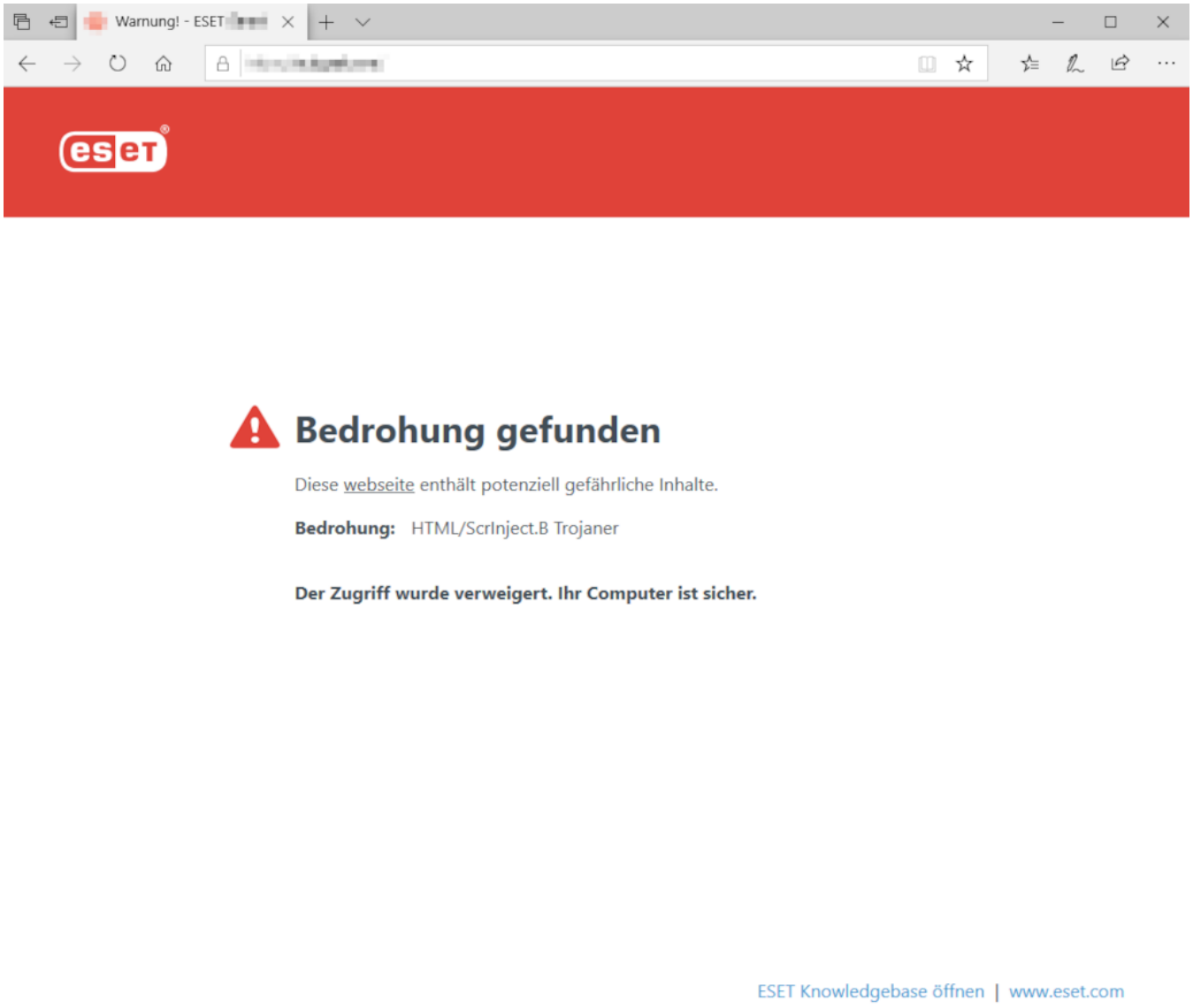
Der Internetzugang ist eine Standardfunktion von Computern. Leider ist diese technische Möglichkeit mittlerweile auch der wichtigste Weg zur Verbreitung von Schadsoftware. Der Web-Schutz besteht in der Überwachung der Kommunikation zwischen Webbrowsern und Remoteservern und entspricht den Regeln für HTTP (Hypertext Transfer Protocol) und HTTPS (verschlüsselte Kommunikation).

Der Zugriff auf Webseiten, die bekanntermaßen 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 > **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:

- Sichere Website von der Web-Schutz-Sperrung ausschließen
- Blockieren einer Website mit ESET NOD32 Antivirus

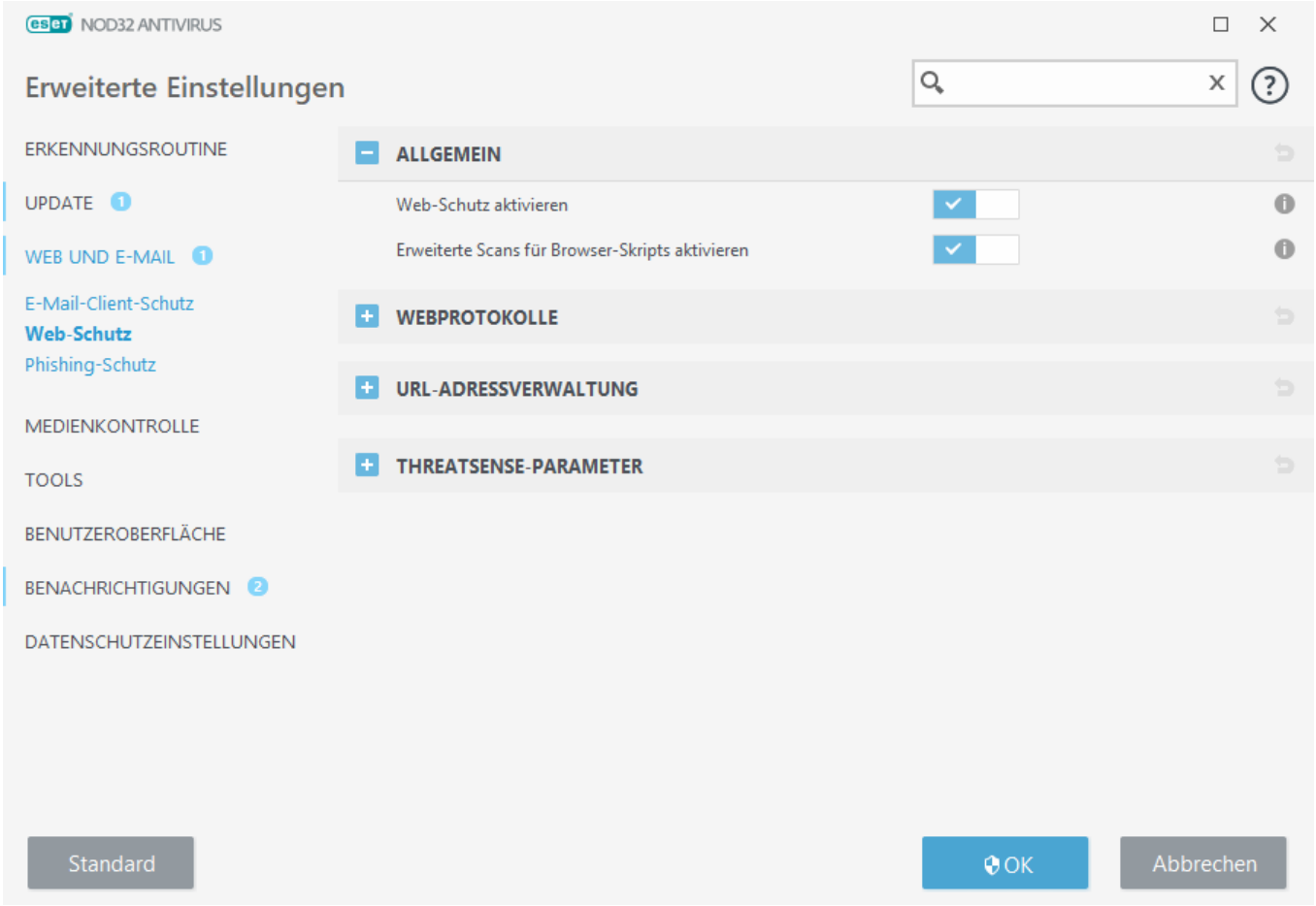
In **Erweiterte Einstellungen** (F5) > **Web und E-Mail** > **Web-Schutz** stehen die folgenden Optionen zur Verfügung

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. Diese Option ist nur verfügbar, wenn die SSL/TLS-Protokollprüfung aktiviert ist.

Erweiterte Scans für Browser-Skripts aktivieren - Wenn diese Option aktiviert ist, werden alle in Webbrowsern ausgeführten JavaScript-Programme von der Erkennungsroutine gescannt.

Der Web-Schutz sollte unbedingt immer aktiviert sein.

Webprotokolle

ESET NOD32 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 NOD32 Antivirus unterstützt auch die HTTPS-Protokollprüfung. Bei der HTTPS-Kommunikation wird zur Datenübertragung zwischen Server und Client ein verschlüsselter Kanal verwendet. ESET NOD32 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, öffnen Sie die erweiterten Einstellungen und navigieren Sie zu **Web und E-Mail** > **SSL/TLS**.

URL-Adressverwaltung

In der URL-Adressverwaltung können Sie festlegen, welche HTTP-Adressen blockiert, zugelassen oder von den Inhalts-Scans ausgeschlossen werden sollen.

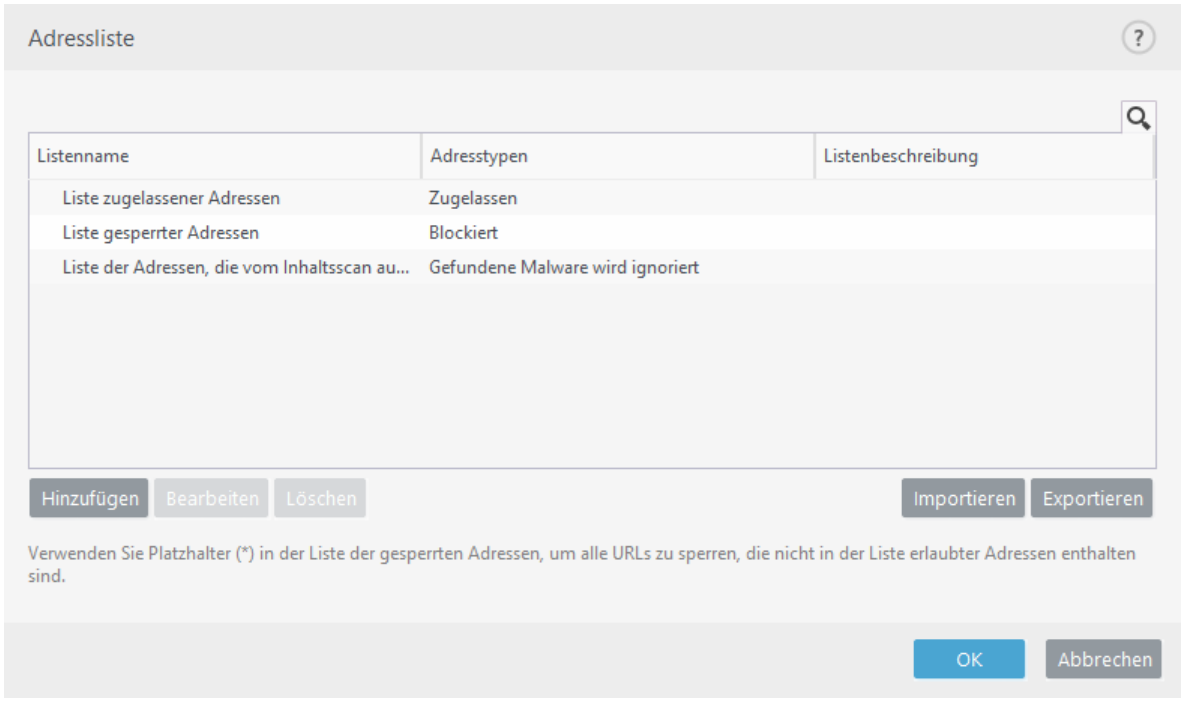
Wenn neben HTTP-Webseiten auch HTTPS-Adressen gefiltert werden sollen, muss die Option SSL/TLS-Protokollfilterung aktivieren aktiviert sein. Andernfalls werden nur die Domains besuchter HTTPS-Sites hinzugefügt, nicht aber die URL.

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.

> **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.

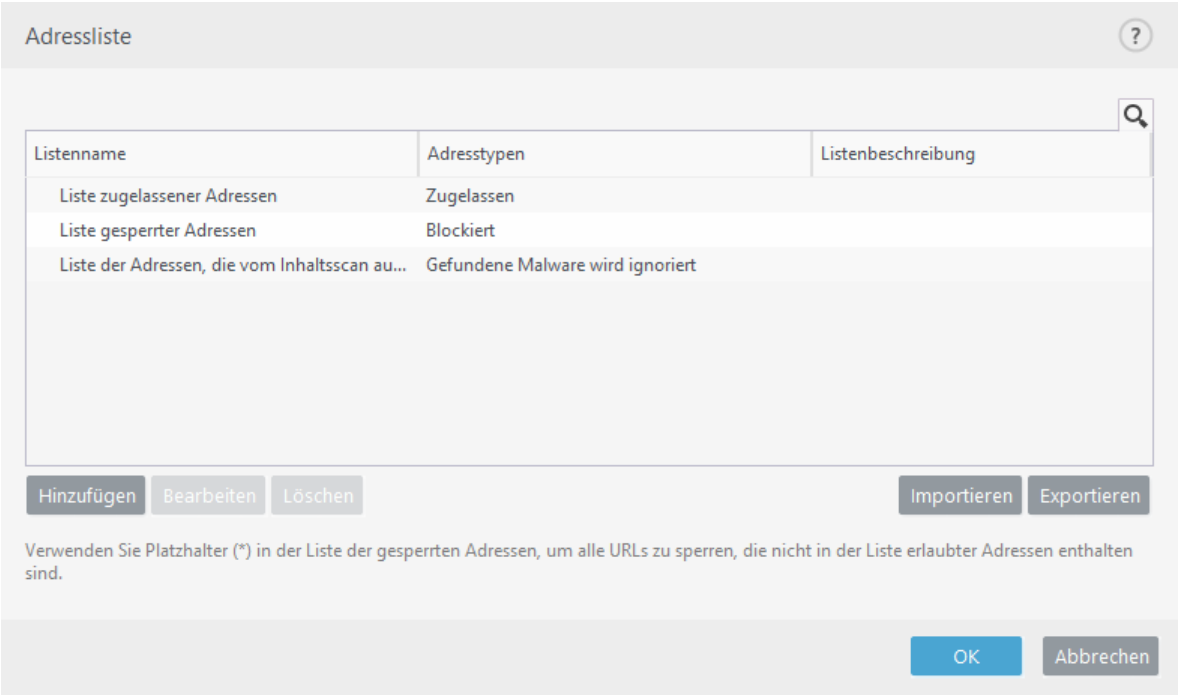
Standardmäßig stehen die drei folgenden Listen zur Verfügung:

- **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:

- Sichere Website von der Web-Schutz-Sperrung ausschließen
- Blockieren einer Website mit ESET Windows Home-Produkten

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 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.
- **Erlaubt** – 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.

Listenname - Geben Sie den Namen der Liste ein. Bei der Bearbeitung einer der drei vordefinierten Listen wird dieses Feld grau dargestellt.

Listenbeschreibung – Geben Sie eine kurze Beschreibung für die Liste ein (optional). Wird bei der Bearbeitung

einer der drei vordefinierten Listen grau dargestellt.

Um eine Liste zu aktivieren, wählen Sie **Liste aktiv** neben der gewünschten Liste. Wenn Sie benachrichtigt werden wollen, wenn eine bestimmte Liste bei der Prüfung einer von Ihnen besuchten HTTP-Site verwendet wird, aktivieren Sie die Option **Bei Anwendung benachrichtigen**. 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 Namen der Liste mit der angegebenen Website.

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 NOD32 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 bezieht sich beispielsweise auf 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 **.domain.com* erfasst z. B. nicht die URL *http://anydomain.com/anypath#.domain.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

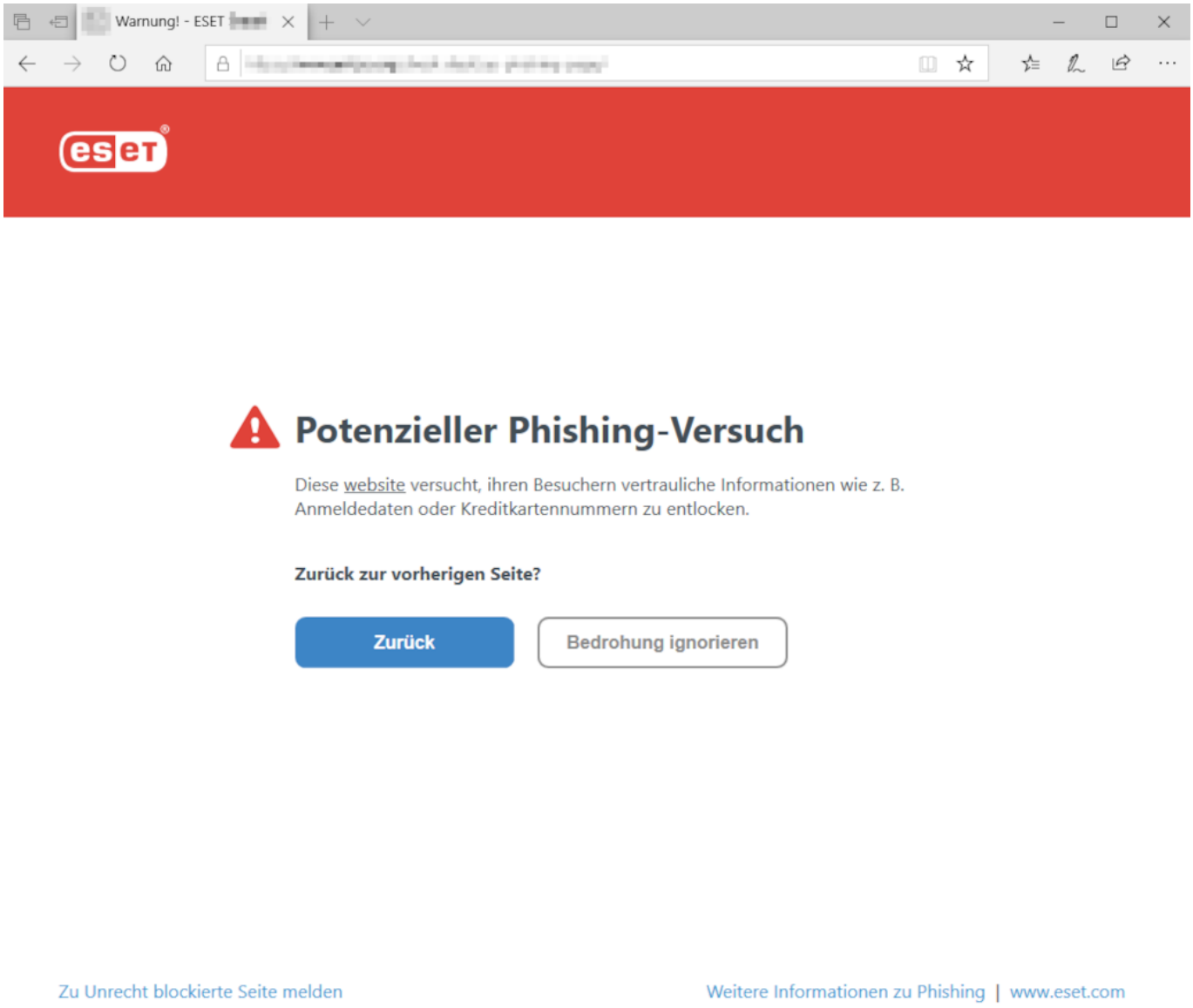
Der Begriff Phishing bezeichnet eine kriminelle Vorgehensweise, die sich Social Engineering-Techniken (Manipulation von Benutzern zur Erlangung vertraulicher Informationen) zunutze macht. Phishing wird oft eingesetzt, um Zugriff auf vertrauliche Daten zu erlangen, wie Kontonummern oder PIN-Codes. Weitere Informationen zu dieser Aktivität finden Sie im Glossar. ESET NOD32 Antivirus enthält einen Phishing-Schutz: Webseiten, die dafür bekannt sind, Phishing-Inhalte zu enthalten, können gesperrt werden.

Wir empfehlen, den Phishing-Schutz in ESET NOD32 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 NOD32 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 **Bedrohung ignorieren** (nicht empfohlen).



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) > **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.

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 eine Zu Unrecht blockierte Seite 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.).

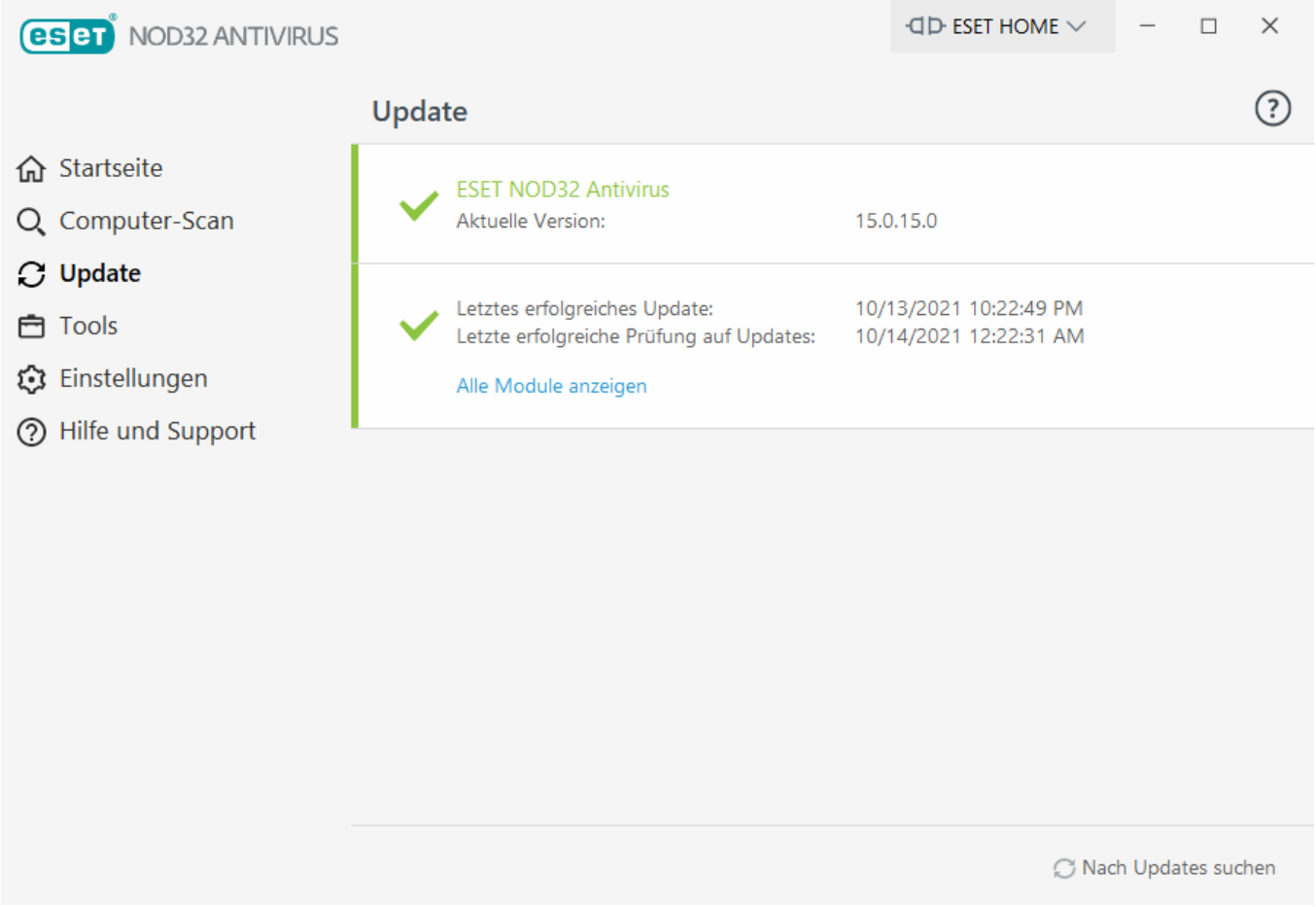
Aktualisieren des Programms

Den optimalen Schutz Ihres Computers gewährleisten Sie, indem Sie ESET NOD32 Antivirus regelmäßig aktualisieren. Das Updatemodul hält Programmmodule und Systemkomponenten fortlaufend auf dem neuesten Stand.

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.

Neben automatischen Updates können Sie auch auf **Nach Updates suchen** klicken, um ein manuelles Update zu starten. Regelmäßige Updates von Programmmodulen und Komponenten sind ein wichtiger Aspekt für einen möglichst umfassenden Schutz vor Schadcode. Seien Sie deshalb bei Konfiguration und Ausführung der Produktmodule besonders sorgfältig. Aktivieren Sie Ihr Produkt mit Ihrem Lizenzschlüssel, um Updates zu erhalten. Falls Sie dies bei der Installation nicht erledigt haben, müssen Sie Ihren Lizenzschlüssel eingeben, um Ihr Produkt zu aktivieren und auf die ESET-Updateserver zuzugreifen.

Sie haben den Lizenzschlüssel nach dem Kauf von ESET NOD32 Antivirus per E-Mail von ESET erhalten.



Aktuelle Version – Zeigt die Nummer der aktuell installierten Version an.

Letztes erfolgreiches Update – Zeigt das Datum des letzten erfolgreichen Updates an. Wenn das angezeigte Datum bereits einige Zeit zurückliegt, ist Ihr Produkt möglicherweise nicht auf dem neuesten Stand.

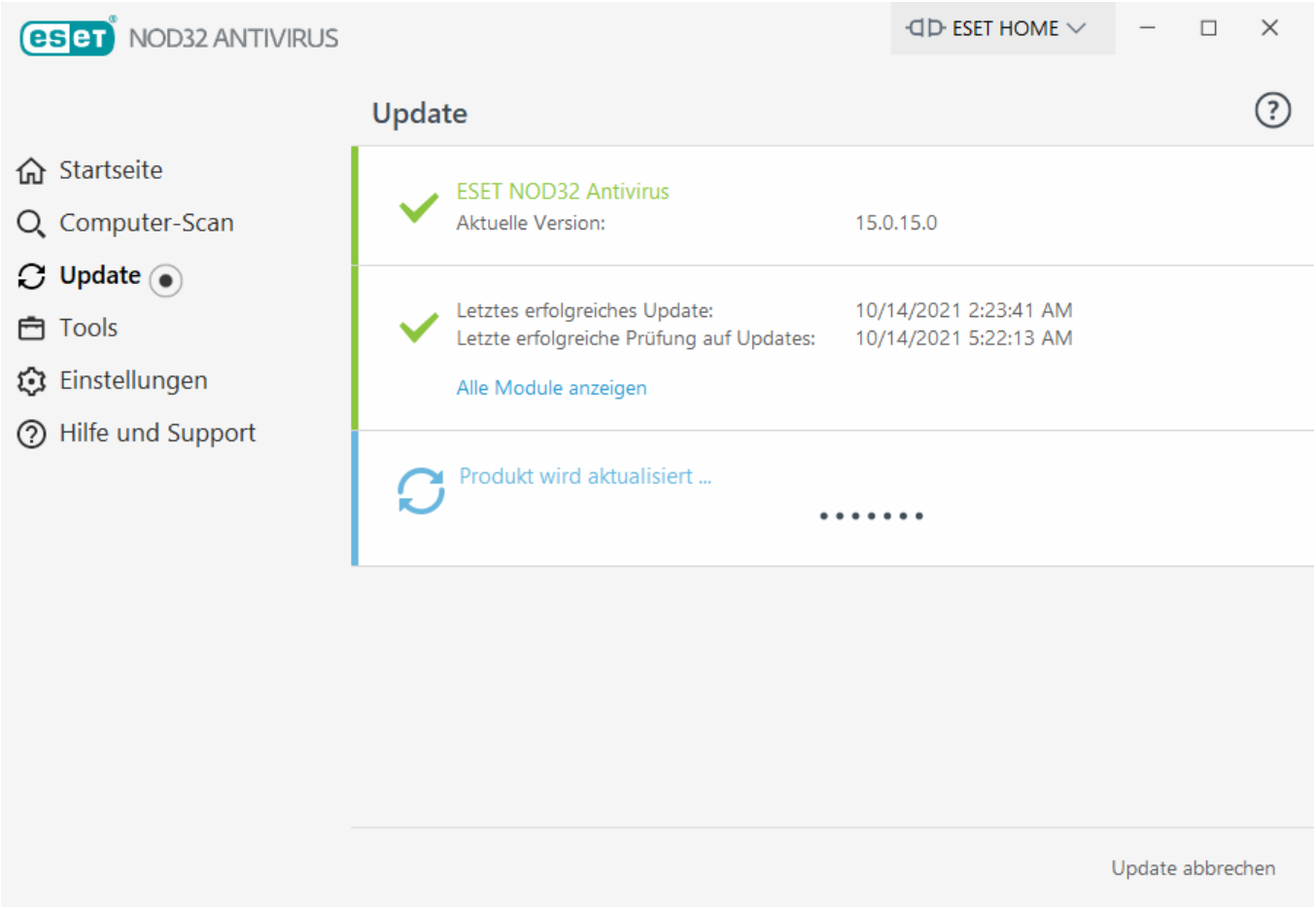
Letzte erfolgreiche Prüfung auf Updates – Zeigt das Datum der letzten erfolgreichen Prüfung auf Updates an.

Alle Module anzeigen – Zeigt Informationen zur Liste der installierten Programmmodule an.

Klicken Sie auf **Nach Updates suchen**, um die neueste verfügbare Version ESET NOD32 Antivirus zu ermitteln.

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**.



Unter normalen Umständen weist ein grünes Häkchen im Fenster **Update** darauf hin, dass das Programm auf dem neuesten Stand ist. Wenn kein grünes Häkchen angezeigt wird, ist das Programm nicht auf dem neuesten Stand und anfälliger für Infektionen. Aktualisieren Sie die Programmmodule in diesem Fall so schnell wie möglich.

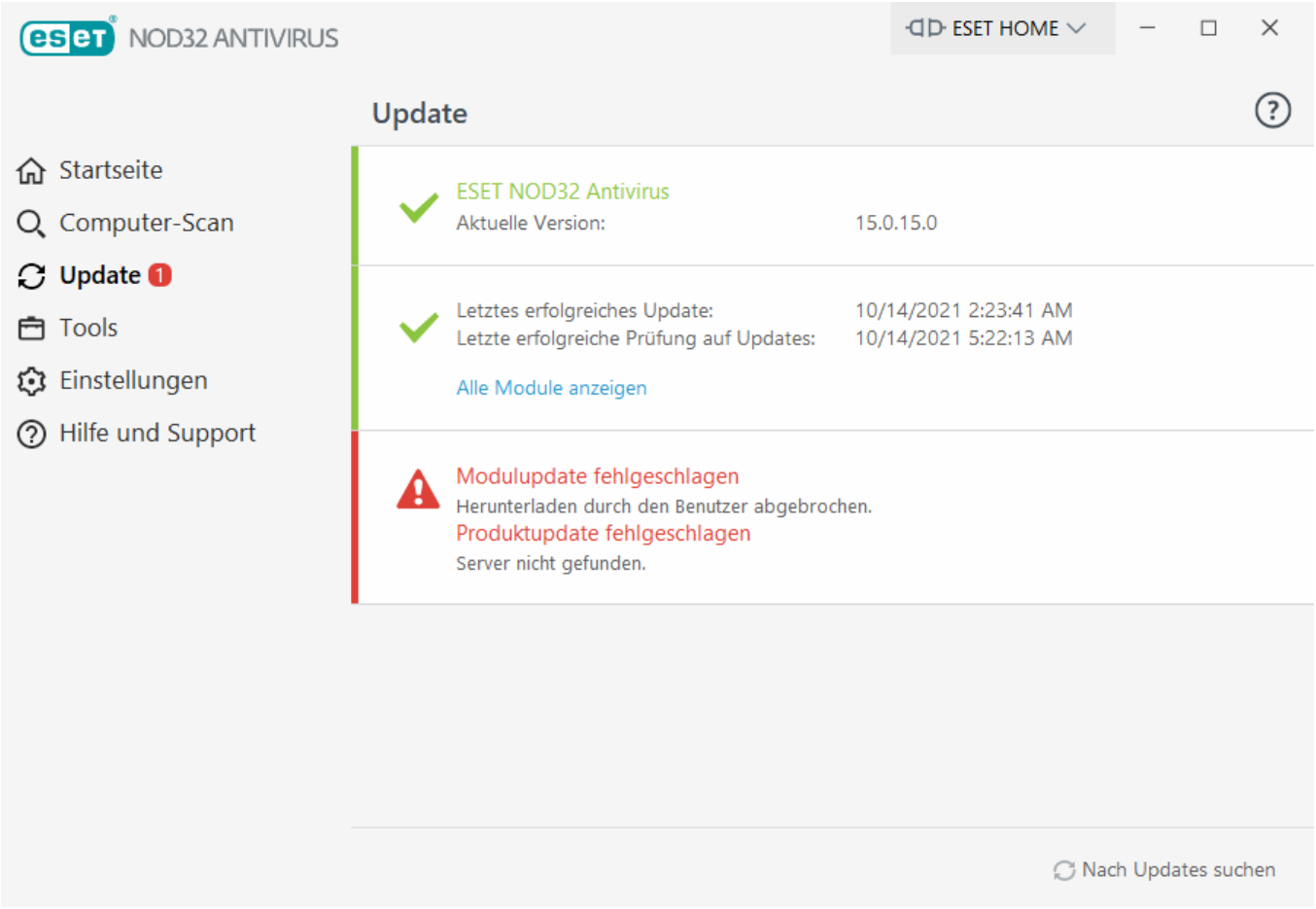
Fehler bei Update

Falls bei den Modulupdates ein Fehler auftritt, liegt möglicherweise eines der folgenden Probleme vor:

1. **Ungültige Lizenz** – Die Lizenz für die Aktivierung ist ungültig oder abgelaufen. Klicken Sie im Hauptprogrammfenster auf **Hilfe und Support** > **Lizenz ändern** und geben Sie einen neuen Lizenzschlüssel ein.

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.



Starten Sie Ihren Computer nach einem erfolgreichen Update von ESET NOD32 Antivirus auf eine neuere Produktversion nach Möglichkeit neu, um sicherzustellen, dass alle Programmmodule korrekt aktualisiert wurden. Nach gewöhnlichen Modulupdates ist kein Neustart des Computers erforderlich.

Weitere Informationen finden Sie unter So beheben Sie das Problem „Modulupdate fehlgeschlagen“.

Einstellungen für Updates

Die Optionen für die Update-Einstellungen finden Sie im Fenster **Erweiterte Einstellungen** (F5) unter **Update** > **Einfach**. In diesem Bereich finden Sie Informationen zum Abruf von Updates, z. B. die Liste der Update-Server und die Anmeldedaten für diese Server.

Einfach

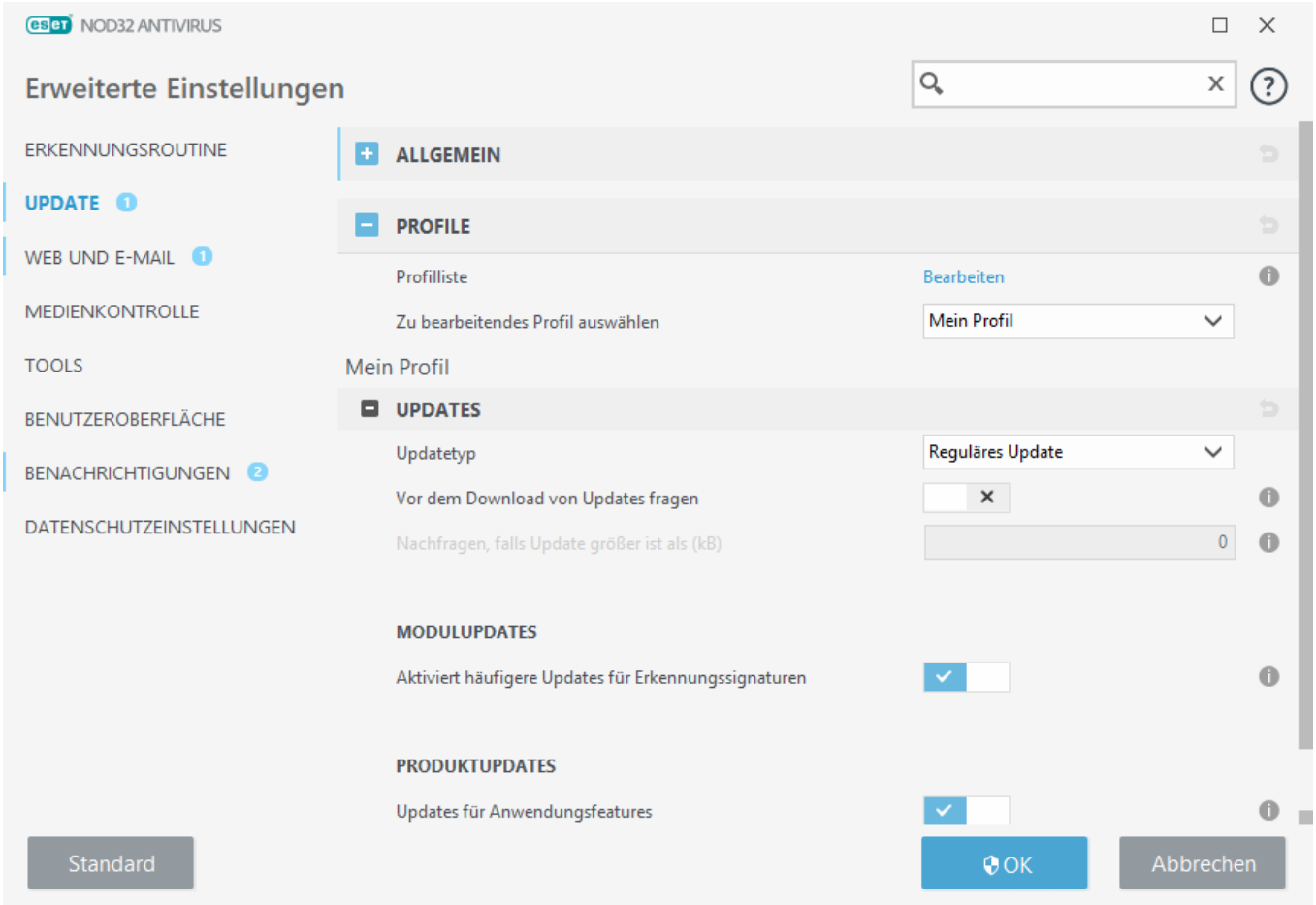
Das aktuell verwendete Updateprofil (sofern nicht unter **Erweiterte Einstellungen** > **Firewall** > **Bekannte Netzwerke** ein spezielles Profil festgelegt wurde) wird im Dropdownmenü **Standardprofil für Updates auswählen** angezeigt.

Im Abschnitt Update-Profile können Sie ein neues Profil erstellen.

Wenn beim Download der Updates für Erkennungsroutine oder Module Fehler auftreten, klicken Sie auf **Löschen**, um temporäre Update-Dateien und den Cache zu löschen.

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.



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 HTTP-Verbindungen).

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 **Testmodus**) 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 im Produktivbetrieb vorgesehen, die durchgängig stabil und verfügbar laufen müssen.

Vor dem Download von Updates fragen - Das Programm zeigt eine Benachrichtigung an, und Sie können die Dateidownloads bestätigen oder ablehnen.

Nachfragen, falls Update größer ist als (kB) - Das Programm zeigt ein Bestätigungsfenster an, wenn die Größe der Updatedatei den angegebenen Wert überschreitet. Wenn Sie die Updategröße auf 0 kB festlegen, zeigt das Programm immer eine Benachrichtigung an.

Benachrichtigungen über erfolgreiche Updates deaktivieren - Deaktiviert die Benachrichtigungen im Infobereich der Taskleiste rechts unten auf dem Bildschirm. Diese Option ist sinnvoll, wenn eine Anwendung im Vollbildmodus oder ein Spiel ausgeführt wird. Beachten Sie, dass die Anzeige von Meldungen im Gamer-Modus deaktiviert ist.

Modul-Updates

Aktiviert häufigere Updates für Erkennungssignaturen – Die Erkennungssignaturen werden in kürzeren Abständen aktualisiert. Das Deaktivieren dieser Einstellung kann die Erkennungsrate beeinträchtigen.

Produktupdates

Updates für Anwendungsfeatures – Neue Versionen von ESET NOD32 Antivirus werden automatisch installiert.

Verbindungsoptionen

Falls Sie einen Proxyserver verwenden möchte, um Updates herunterzuladen, finden Sie weitere Informationen im Abschnitt Verbindungsoptionen.

Update-Rollback

Wenn Sie befürchten, dass ein neues Update der Erkennungsroutine oder eines Programm-Moduls beschädigt oder nicht stabil ist, können Sie einen Rollback zur vorigen Version ausführen und die Updates vorübergehend deaktivieren. Hier können Sie die Updates auch wieder aktivieren, wenn Sie sie zuvor auf unbegrenzte Zeit deaktiviert haben.

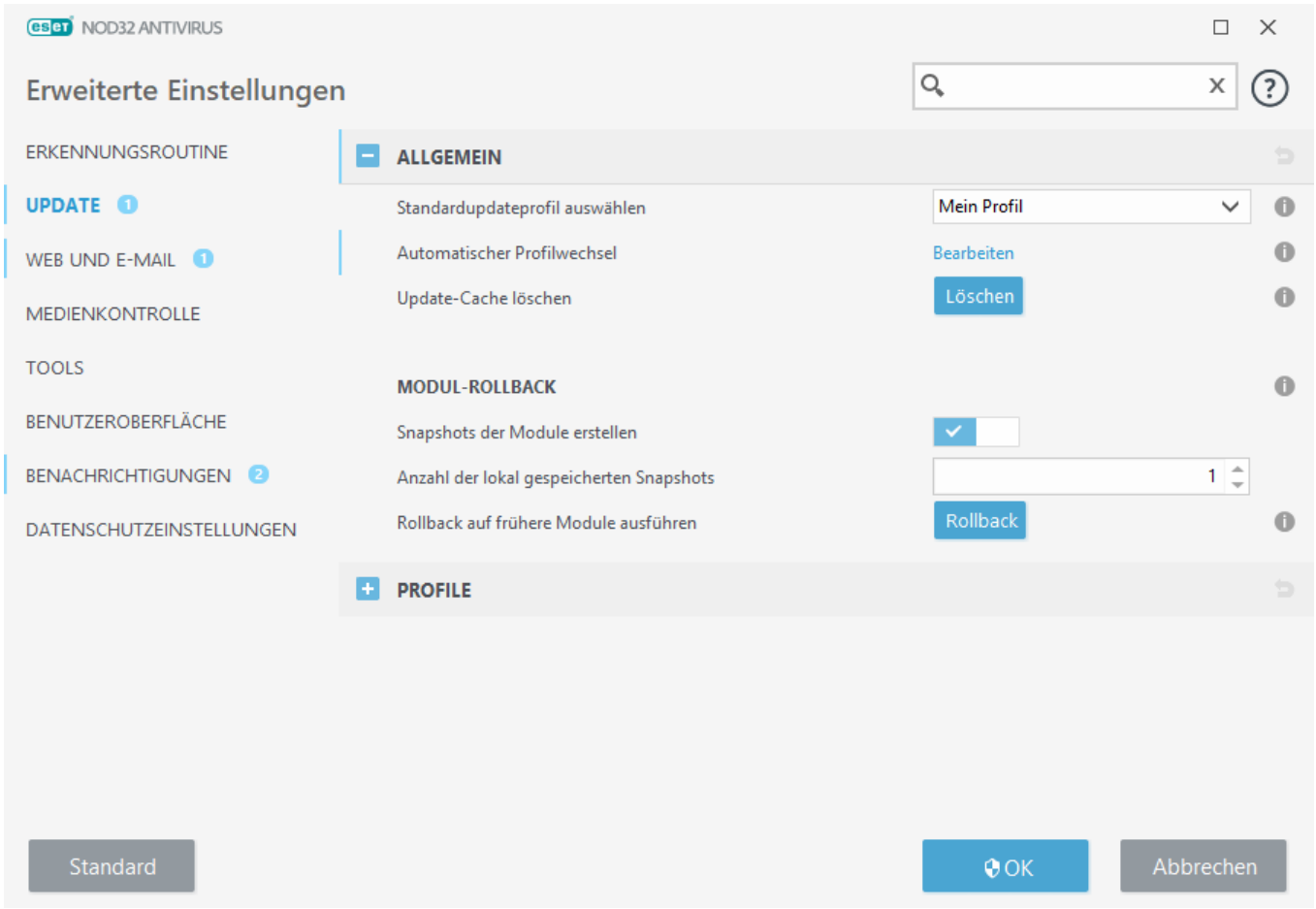
ESET NOD32 Antivirus erfasst Snapshots der Erkennungsroutine und der Programm-Module zur späteren Verwendung mit der Rollback-Funktion. Um Snapshots der Virendatenbank zu erstellen, lassen Sie die Option **Snapshots der Module erstellen** aktiviert. Wenn die Option **Snapshots der Module erstellen** aktiviert ist, wird der erste Snapshot beim ersten Update erstellt. Ein weiterer Snapshot nach 48 Stunden. Das Feld **Zahl der lokal gespeicherten Snapshots** legt fest, wie viele Snapshots der Erkennungsroutine gespeichert werden.

Wenn die maximale Anzahl an Snapshots erreicht ist (z. B. drei), wird der älteste Snapshot alle 48 Stunden durch einen neuen Snapshot ersetzt. ESET NOD32 Antivirus führt ein Rollback der Updateversionen für Erkennungsroutine und Programm-Module auf den ältesten Snapshot durch.

Wenn Sie auf **Rollback ausführen** (**Erweiterte Einstellungen** (F5) > **Update** > **Einfach**) klicken, müssen Sie im Dropdownmenü **Dauer** festlegen, wie lange die Updates der Erkennungsroutine und der Programmkomponenten ausgesetzt werden.

Wählen Sie **Bis zur Aufhebung** aus, um regelmäßige Updates auszusetzen, bis Sie die Updatefunktion manuell erneut aktivieren. ESET rät davon ab, diese Option zu verwenden, weil sie mit potenziellen Sicherheitsrisiken verbunden ist.

Wenn ein Rollback durchgeführt wird, wechselt die Schaltfläche **Rollback** zu **Updates erlauben**. Wenn ein Rollback durchgeführt wird, wechselt die Schaltfläche Rollback zu Updates erlauben, und Updates werden für die im Dropdownmenü **Updates anhalten** angegebene Dauer ausgesetzt. Die Erkennungsroutine wird auf die älteste verfügbare Version herabgestuft und als Snapshot im lokalen Dateisystem des Computers gespeichert.



Angenommen, die aktuellste Version der Erkennungsroutine ist 22700, und die Versionen 22698 und 22696 sind als Snapshots gespeichert. Version 22697 ist nicht verfügbar. In diesem Beispiel war der Computer während des Updates auf 22697 heruntergefahren, und ein aktuelleres Update war verfügbar, bevor Version 22697 heruntergeladen wurde. Wenn Sie unter **Zahl der lokal gespeicherten Snapshots** den Wert „zwei“ eingegeben haben und auf **Rollback ausführen** klicken, wird die Version 22696 der Erkennungsroutine (inklusive Programm-Module) wiederhergestellt. Dieser Vorgang kann einige Zeit dauern. Überprüfen Sie im Bildschirm Update, ob die Version der Erkennungsroutine herabgestuft wurde.

Rollback-Zeitintervall

Wenn Sie auf **Rollback ausführen** (**Erweiterte Einstellungen** (F5) > **Update** > **Einfach**) klicken, müssen Sie im Dropdownmenü **Dauer** festlegen, wie lange die Updates der Erkennungsroutine und der Programmkomponenten ausgesetzt werden.

Wählen Sie **Bis zur Aufhebung** aus, um regelmäßige Updates auszusetzen, bis Sie die Updatefunktion manuell erneut aktivieren. ESET rät davon ab, diese Option zu verwenden, weil sie mit potenziellen Sicherheitsrisiken verbunden ist.

Produktupdates

Im Bereich **Produktupdates** können Sie neue Funktionsupdates automatisch installieren, sobald diese verfügbar sind.

Updates für Anwendungsfeatures können neue Funktionen hinzufügen oder bereits vorhandene Funktionen ändern. Die Updates können automatisch oder nach Bestätigung durch den Benutzer gestartet werden. Nach der Installation von Update für Anwendungsfeatures muss der Computer möglicherweise neu gestartet werden.

Updates für Anwendungsfeatures – Wenn diese Option aktiviert ist, werden Updates für Anwendungsfeatures automatisch installiert.

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**. 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 NOD32 Antivirus genutzt wird.

Wählen Sie die Option Verbindung über Proxyserver in den folgenden Fällen aus:

- Für Updates von ESET NOD32 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 NOD32 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.

> Die Felder **Benutzername** und **Passwort** in diesem Bereich gelten nur für den Proxyserver. Füllen Sie diese Felder nur aus, wenn Sie über einen Proxyserver auf das Internet zugreifen. Und für den Zugriff auf den Proxyserver ein Benutzername und ein Passwort benötigt werden.

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 NOD32 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 im Abschnitt Taskplaner.

Dialogfenster – Neustart erforderlich

Nach einem Update von ESET NOD32 Antivirus auf eine neue Version müssen Sie den Computer neu starten. Neuere Versionen von ESET NOD32 Antivirus dienen dazu, Verbesserungen zu implementieren oder Probleme zu beheben, die mit automatischen Updates der Programm-Module nicht behoben werden können.

Die neue Version von ESET NOD32 Antivirus wird je nach Ihren Einstellungen für Programm-Updates entweder automatisch installiert oder manuell, indem Sie eine neue Version herunterladen und über die vorherige Version installieren.

Klicken Sie auf **Jetzt neu starten**, um Ihren Computer neu zu starten. Falls Sie Ihren Computer später neu starten möchten, klicken Sie auf **Später erinnern**. Später können Sie Ihren Computer manuell im **Startbereich** des Programmfensters neu starten.

Tools

Das Menü **Tools** enthält Module, die die Verwaltung des Programms vereinfachen und zusätzliche Optionen für erfahrene Benutzer bereitstellen.

Weitere Informationen finden Sie unter Tools in ESET NOD32 Antivirus.

Tools in ESET NOD32 Antivirus

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 NOD32 Antivirus aktiviert ist)

 ESET SysInspector

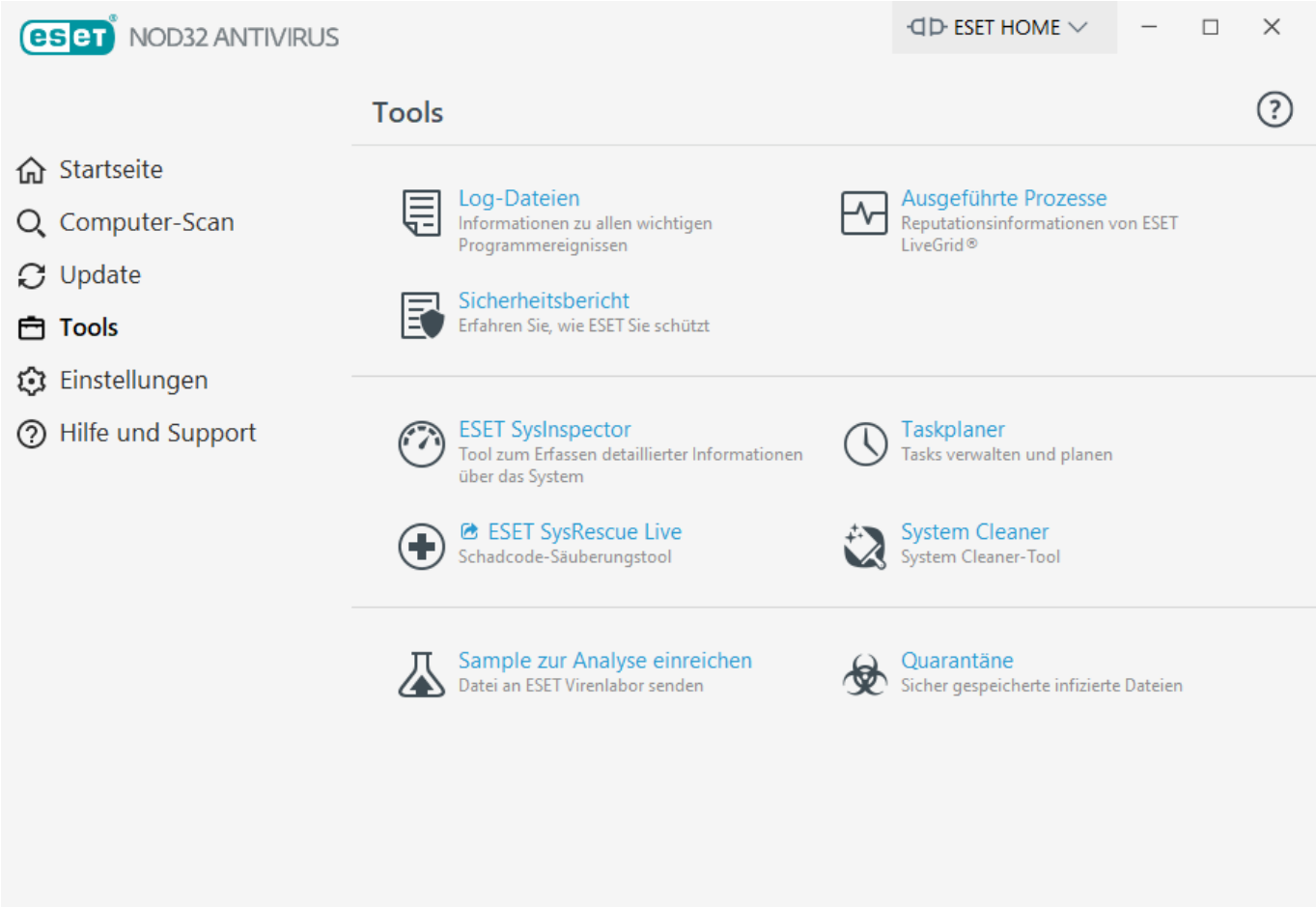
 ESET SysRescue Live – Leitet Sie zur ESET SysRescue Live-Seite weiter, auf der Sie das ESET SysRescue Live .iso CD/DVD-Abbild herunterladen können.

 Taskplaner

 System Cleaner – Ein Tool, mit dem Sie den Computer nach der Säuberung der Bedrohung auf einen nutzbaren Zustand wiederherstellen können.

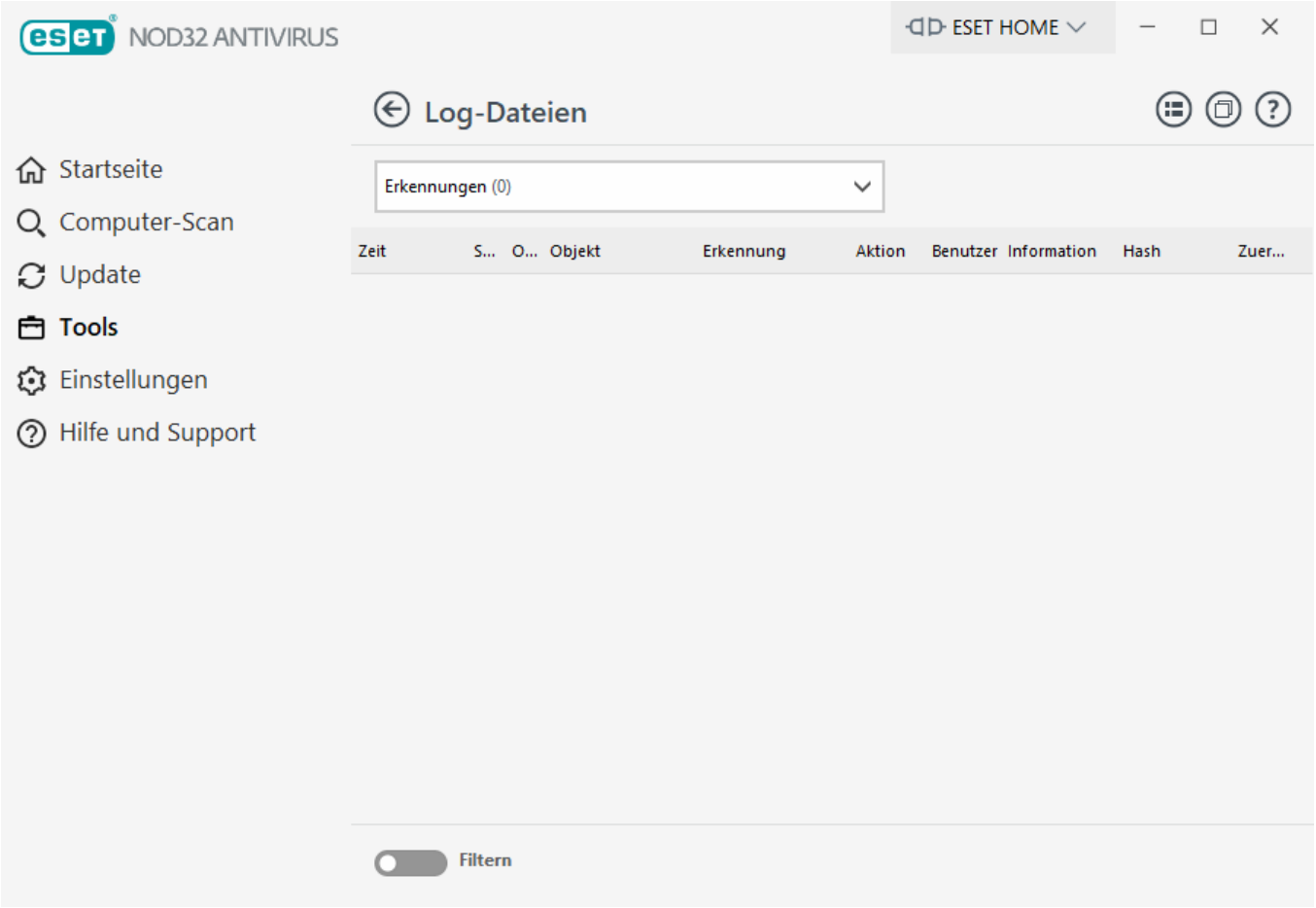
 Sample zur Analyse einreichen – Mit dieser Option können Sie verdächtige Dateien zur Analyse an das ESET-Virenlabor einreichen (je nach Konfiguration von ESET LiveGrid® unter Umständen nicht verfügbar).

 Quarantäne



Log-Dateien

Log-Dateien enthalten Informationen zu wichtigen aufgetretenen Programmereignissen und geben einen Überblick über erkannte Bedrohungen. Das Erstellen von Logs ist unabdingbar für die Systemanalyse, die Erkennung von Bedrohungen 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 NOD32 Antivirus heraus angezeigt werden. Das Archivieren von Logs erfolgt ebenfalls direkt über das Programm.



Sie können die Log-Dateien abrufen, indem Sie im Hauptprogrammfenster auf **Tools** > **Log-Dateien**. Wählen Sie im Dropdown-Menü **Log** den gewünschten Log-Typ aus. Folgende Logs sind verfügbar:

- **Ereignisen** – Dieses Log enthält detaillierte Informationen über die von ESET NOD32 Antivirus entdeckten Ereignisse und Infiltrationen. Darunter Erkennungszeitpunkt, Scanner-Typ, Typ und Ort des Objekts, Name des Ereignisses, ausgeführte Aktion und Name des Benutzers, der zum jeweiligen Zeitpunkt angemeldet war, und Zeitpunkt des ersten Auftretens. Nicht gesäuberte Bedrohungen werden immer mit rotem Text auf hellrotem Hintergrund angezeigt. Gesäuberte Bedrohungen werden mit gelbem Text auf weißem Hintergrund angezeigt. Nicht gesäuberte potenziell unsichere oder unerwünschte Anwendungen werden ebenfalls mit gelbem Text auf weißem Hintergrund angezeigt.

- **Ereignisse** – Alle von ESET NOD32 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.

- **Computerprüfung** – In diesem Fenster werden die Ergebnisse aller durchgeführten Prüfungen angezeigt. Jede Zeile entspricht der Überprüfung eines einzelnen Computers. Doppelklicken Sie auf einen Eintrag, um Details zum ausgewählten Scan anzuzeigen.

- **HIPS** – Enthält Einträge spezifischer HIPS-Regeln, die zum Aufzeichnen markiert wurden. Das Protokoll zeigt die Anwendung an, die den Vorgang ausgelöst hat, das Ergebnis (ob der Vorgang zugelassen oder blockiert wurde) sowie den Regelnamen.

- **Gefilterte Websites** – Diese Liste enthält die durch den Web-Schutz gesperrten Websites. Jedes Log enthält die Uhrzeit, die URL-Adresse, den Benutzer und die Anwendung, die sich mit einer bestimmten Website verbunden hat.

- **Medienkontrolle** – Enthält Datensätze zu Wechselmedien oder externen Geräten, die an den Computer angeschlossen wurden. Nur Geräte mit einer entsprechenden 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. Außerdem können Sie 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** oder **SHIFT** gedrückt, um mehrere Einträge auszuwählen.

Klicken Sie auf **Filter**, um das Fenster Log-Filter zu öffnen, in dem Sie 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** – 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/Alle exportieren** – Exportiert Informationen zu den ausgewählten Einträgen oder zu allen Einträgen im XML-Format.
- **Suchen/Weitersuchen/Rückwärts suchen** – Wenn Sie diese Option anklicken, können Sie im Fenster „Log-Filter“ Filterkriterien festlegen, um einen bestimmten Eintrag hervorzuheben.
- **Ereignisbeschreibung** – Öffnet die ESET-Virenenzyklopädie mit detaillierten Informationen zu den Gefahren und Symptomen der aufgezeichneten Infiltration.
- **Ausschluss erstellen** - Erstellen Sie einen neuen Ereignisausschluss mit einem Assistenten (Nicht verfügbar für Malware-Erkennungen).

Log-Filter

Klicken Sie auf **Filtern** in **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. Nur Einträge, die diese Zeichenfolge enthalten, werden angezeigt. 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 NOD32 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.

> 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 - Ist diese Option aktiviert, werden die Log-Dateien automatisch defragmentiert, wenn die Prozentzahl höher ist als der unter **Wenn ungenutzte Einträge größer als (%)** angegebene Wert.

Klicken Sie zum Defragmentieren der Log-Dateien auf **Optimieren**. Um die Systemleistung und -geschwindigkeit beim Verarbeiten der Log-Dateien zu erhöhen, werden alle leeren Log-Einträge entfernt. 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). Jeder Log-Bereich verfügt über eine eigene Datei mit einem vordefinierten Dateinamen (z. B. virlog.txt für den Bereich

Erkennungen von Log-Dateien, wenn Logs im Nur-Text-Format gespeichert werden).

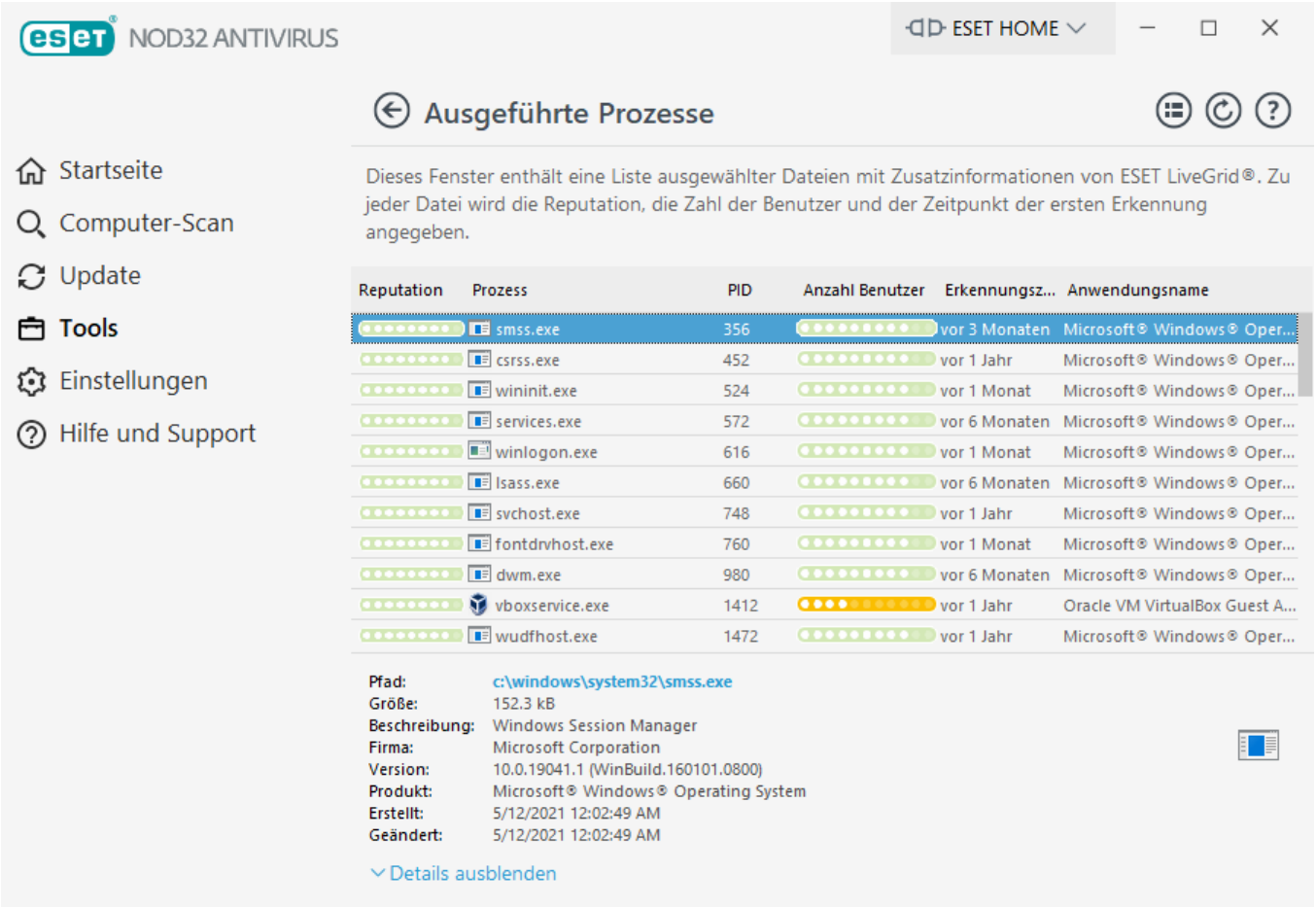
• **Typ** - Mit dem Dateiformat **Text** werden Logs in einer Textdatei gespeichert, wobei die Daten durch Tabulatorzeichen getrennt werden. Gleiches gilt für das kommagetrennte Dateiformat **CSV**. Mit der Option **Ereignis** werden die Logs im Windows-Ereignis-Log anstatt in einer Datei gespeichert (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.

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.

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 NOD32 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 NOD32 Antivirus und die ESET LiveGrid®-Technologie normalerweise einen Satz heuristischer Regeln, mit denen die Merkmale des Objekts untersucht werden, um anschließend nach entsprechender Gewichtung das Potenzial für schädliche Aktivitäten abzuschätzen. Auf der Grundlage dieser Heuristik wird den

Objekten so eine Risikostufe von 1 – In Ordnung (grün) bis 9 – Risikoreich (rot) zugeordnet.

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 in der Taskleiste und dann auf **Taskmanager** klicken, oder indem Sie **Strg**+**Umschalt**+**Esc** auf Ihrer Tastatur drücken.

Bekannte Anwendungen, die als In Ordnung (grün) markiert sind und bekanntermaßen keinen Schadcode enthalten (Positivliste), werden von der Prüfung ausgeschlossen, um die Prüfung zu beschleunigen.

PID – Die Prozesskennung kann als Parameter in verschiedenen Funktionsaufrufen verwendet werden, z. B. um die Priorität des Prozesses anzupassen.

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.

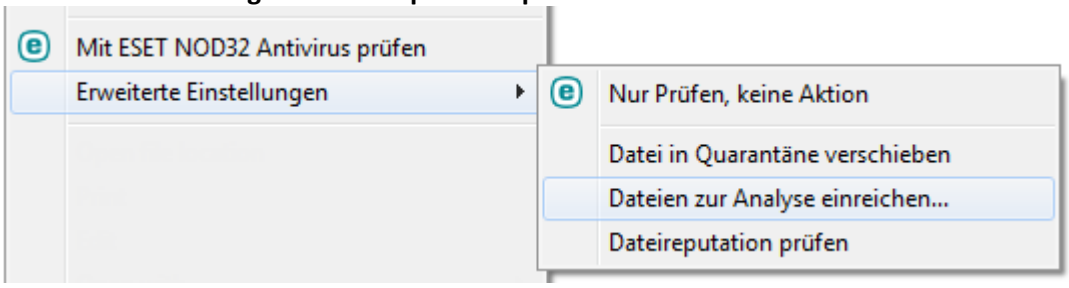
Eine als Unbekannt (gelb) eingestufte Anwendung enthält nicht unbedingt Schadcode. In der Regel ist es einfach eine neuere Anwendung. Wenn Sie sich bei einer Datei unsicher sind, können Sie diese über die Funktion Dateien zur Analyse einreichen an das ESET-Virenlabor schicken. Falls die Datei tatsächlich Schadcode enthält, wird die Erkennung der entsprechenden Signatur in einem zukünftigen Update hinzugefügt.

Anwendungsname - Der Name eines Programms oder Prozesses.

Klicken Sie auf eine Anwendung, um die folgenden Details zu dieser Anwendung anzuzeigen:

- **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/Geändert** – Datum und Uhrzeit der Erstellung bzw. der letzten Änderung.

Sie können auch die Reputation von Dateien überprüfen, die nicht als Programme oder Prozesse ausgeführt werden. Klicken Sie dazu eine Datei im Datei-Explorer mit der rechten Maustaste an, und wählen Sie **Erweiterte Einstellungen** > **Dateireputation prüfen** aus.



Sicherheitsbericht

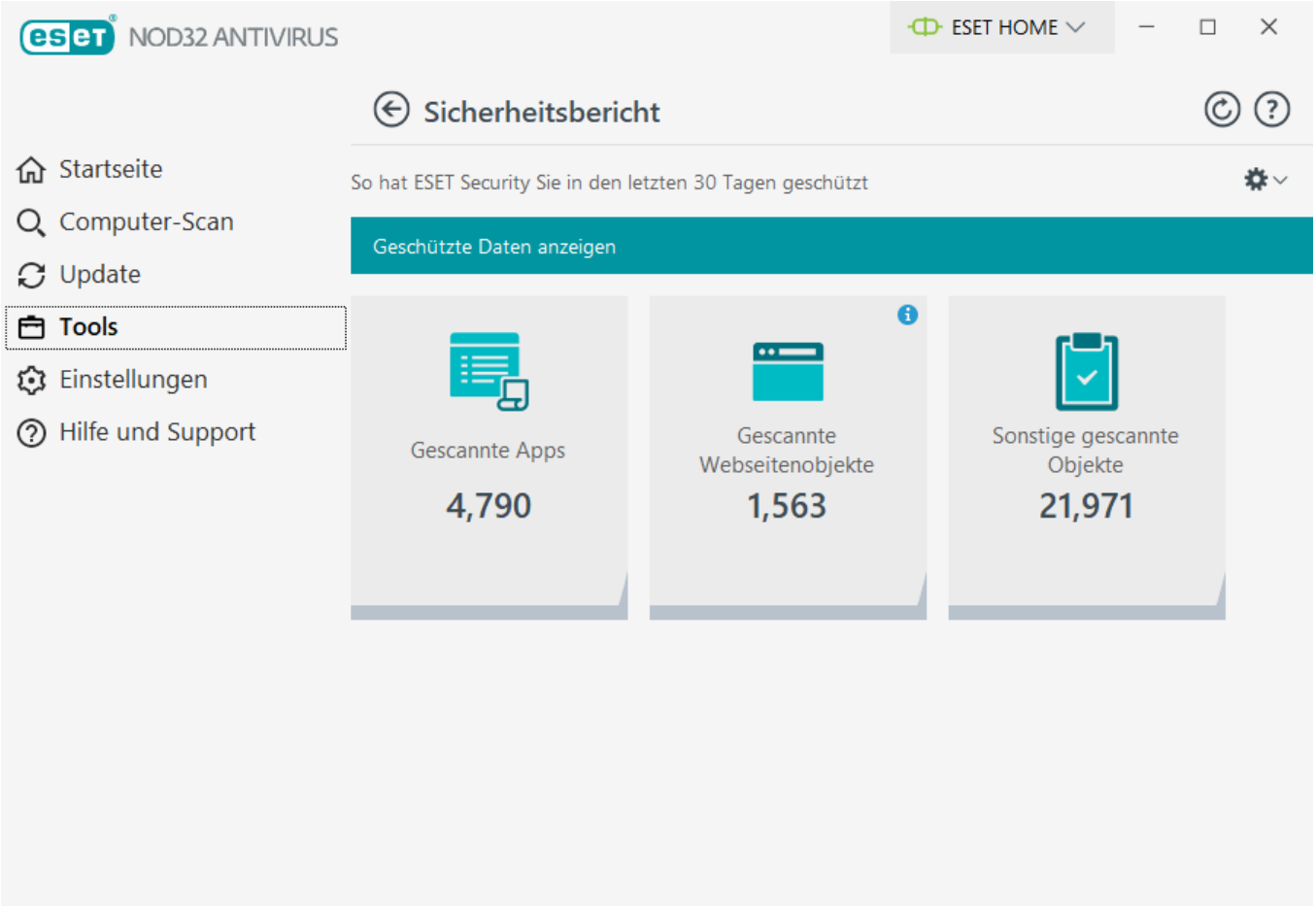
Diese Funktion enthält eine Übersicht über die Statistiken für die folgenden Kategorien:

- **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.
- **Überprüfte sonstige 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.

Aktivierte Funktionen werden im Sicherheitsbericht nicht mehr als „nicht funktionsfähig“ angezeigt.

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 NOD32 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** > **Benachrichtigungen** > **Interaktive Warnungen** > **Bestätigungsnachrichten** > **Bearbeiten** deaktiviert.

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 zur Verwendung von ESET SysInspector finden Sie in der ESET SysInspector Onlinehilfe.

Im ESET SysInspector Fenster werden die folgenden Informationen zu den Logs angezeigt:

- **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 ausgewählte Log in ESET SysInspector. 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 erstellt wurde (Status **Erstellt**), bevor Sie versuchen, auf das Log 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 erstellt wurde (Status **Erstellt**), bevor Sie versuchen, auf das Log zuzugreifen.

• **Löschen** - Löschen der ausgewählten Logs aus der Liste.

• **Alle löschen** - Löschen aller Logs.

• **Exportieren** - Exportieren des Logs in eine .xml-Datei oder eine komprimierte .xml-Datei. Das Log wird nach C:\ProgramData\ESET\ESET Security\SysInspector exportiert.

Taskplaner

Der Taskplaner verwaltet und startet Tasks mit vordefinierter Konfiguration und voreingestellten Eigenschaften.

Sie erreichen den Taskplaner im Hauptprogrammfenster von ESET NOD32 Antivirus unter **Tools** > **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: Module aktualisieren, 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**). Sie können die Liste der geplanten Tasks auf den Standard zurücksetzen und alle Änderungen löschen, indem Sie auf **Standard** klicken. 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:

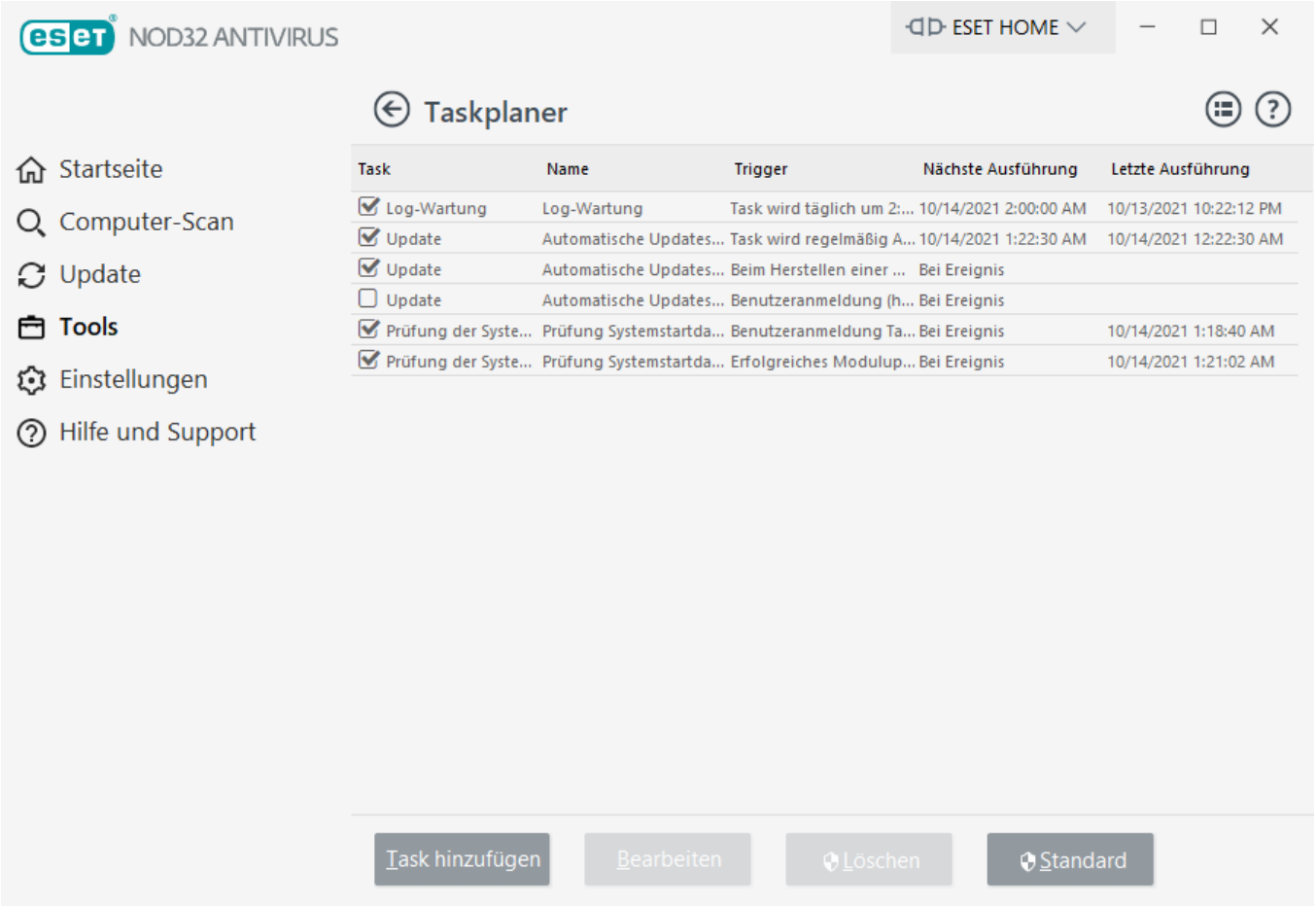
• **Log-Wartung**

• **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 Update der Erkennungsroutine)

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 dann den gewünschten Task aus der Liste.
   - **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.

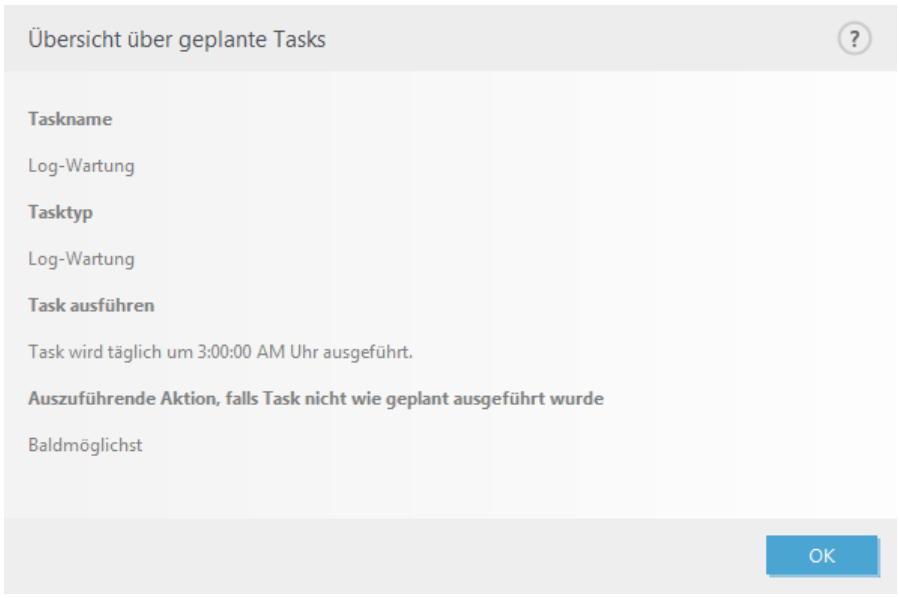
4. Klicken Sie auf den Schieberegler neben **Aktivieren**, um die Aufgabe zu aktivieren (Sie können diesen Schritt auch später durchführen, wenn Sie das Kontrollkästchen in der Liste der geplanten Aufgaben aktivieren/deaktivieren), und klicken Sie dann auf **Weiter**, um eine der folgenden Zeitangaben auszuwählen:

- **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** 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. 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, wenn die Zeit seit der letzten Ausführung größer ist als (Stunden)** – Die verstrichene Zeit seit der ersten übersprungenen Ausführung des Tasks. Wenn diese Zeit überschritten ist, wird der Task sofort ausgeführt. Legen Sie das Intervall mit dem folgenden Drehelement fest.

Sie können den geplanten Task durch Klicken mit der rechten Maustaste und Auswählen der Option **Task-Eigenschaften** überprüfen.



Optionen für geplante Scans

In diesem Fenster können Sie erweiterte Einstellungen für geplante Computer-Scan-Tasks festlegen.

Um einen Scan ohne Säuberung zu starten, klicken Sie auf **Erweiterte Einstellungen** und wählen Sie **Scannen, ohne zu säubern** aus. Der Scan-Verlauf wird im Scan-Log gespeichert.

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

Im Dropdownmenü können Sie eine Aktion festlegen, die nach Abschluss des Scans automatisch ausgeführt wird:

- **Keine Aktion** - Nach dem Scan wird keine Aktion ausgeführt.
- **Herunterfahren**- Der Computer wird nach dem Scan heruntergefahren.
- **Neustart**- Nach dem Scan werden alle offenen Programme geschlossen und der Computer wird neu gestartet.
- **Bei Bedarf neu starten** – Der Computer wird bei Bedarf neu gestartet, um erkannte Bedrohungen zu säubern.
- **Neustart erzwingen** – Nach Abschluss des Scans werden alle geöffneten Programme ohne Eingreifen des Benutzers geschlossen, und der Computer wird neu gestartet.
- **Neustart bei Bedarf erzwingen** – Der Computer wird bei Bedarf neu gestartet, um erkannte Bedrohungen zu säubern.
- **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.

> Die Verfügbarkeit der Aktionen **Energiesparmodus** und **Ruhezustand** hängt von Ihren Energieeinstellungen im Betriebssystem und vom Funktionsumfang Ihres Computers oder Laptops ab. Beachten Sie, dass der Computer im Energiesparmodus weiter arbeitet. Es führt weiterhin grundlegende Funktionen aus und verbraucht Strom, wenn Ihr Computer mit Batteriestrom betrieben wird. Um die Akkubetriebsdauer beispielsweise unterwegs zu verlängern, empfiehlt es sich, den Ruhezustand zu verwenden.

Wählen Sie **Scan-Vorgang kann nicht abgebrochen werden** aus, um zu verhindern, dass nicht berechtigte Benutzer die Ausführung der Aktionen nach dem Scannen unterbrechen 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.

Siehe auch Scan-Fortschritt.

Übersicht über geplante Tasks

In diesem Fenster werden detaillierte Informationen zum ausgewählten geplanten Task angezeigt, wenn Sie auf einen benutzerdefinierten Task doppelklicken oder mit der rechten Maustaste auf einen benutzerdefinierten Taskplaner klicken und anschließend **Task-Eigenschaften** auswählen.

Taskdetails

Geben Sie den **Tasknamen** ein, wählen Sie eine der Optionen unter **Tasktyp** aus und klicken Sie auf **Weiter**:

- **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.

Task-Zeitplanung

Der Task wird in dem angegebenen Zeitabstand wiederholt ausgeführt. Wählen Sie eine Zeitangabe aus:

- **Einmalig** - Der Task wird nur einmalig zu einem festgelegten Zeitpunkt ausgeführt.
- **Wiederholt** - Der Task wird in den (in Stunden) angegebenen Zeitabständen ausgeführt.
- **Täglich** - Der Task wird täglich zur festgelegten Uhrzeit ausgeführt.
- **Wöchentlich** - Der Task wird an einem oder mehreren Wochentagen zur festgelegten Uhrzeit ausgeführt.
- **Bei Ereignis** - Der Task wird ausgeführt, wenn ein bestimmtes Ereignis eintritt.

Task im Akkubetrieb überspringen- Wenn sich der Computer zum geplanten Startzeitpunkt des Task im Akkubetrieb befindet, wird der Task nicht gestartet. Dies gilt auch für Computer, die ihren Strom über eine USV (unterbrechungsfreie Stromversorgung) beziehen.

Task-Zeitplanung – Einmalig

Taskausführung- Der angegebene Task wird zum angegeben Zeitpunkt einmalig ausgeführt.

Task-Zeitplanung – Täglich

Der Task wird täglich zur festgelegten Uhrzeit ausgeführt.

Task-Zeitplanung – Wöchentlich

Der Task wird jede Woche an den ausgewählten Wochentagen zur ausgewählten Uhrzeit ausgeführt.

Task-Zeitplanung – Bei Ereignis

Die Task wird durch eines der folgenden Ereignisse ausgelöst:

- **Bei jedem Computerstart**
- **Jeden Tag beim ersten Start des Computers**
- **DFÜ-Verbindung zum Internet/VPN**
- **Erfolgreiches Modulupdate**
- **Erfolgreiches Produktupdate**
- **Benutzeranmeldung**
- **Erkennung von Bedrohungen**

Beim Planen eines Vorgangs, der durch ein Ereignis ausgelöst wird, können Sie einen Mindestzeitraum zwischen Ausführungen des Task angeben. Wenn Sie sich z. B. mehrmals täglich auf Ihrem Computer anmelden, können Sie „24 Stunden“ auswählen, damit der Task nur bei der ersten Anmeldung des Tages und dann erst wieder am nächsten Tag ausgeführt wird.

Übersprungener Task

Tasks können übersprungen werden, wenn der Computer ausgeschaltet ist oder im Akkubetrieb läuft. Wählen Sie mit einer der Optionen aus, wann der übersprungene Task ausgeführt werden soll, und klicken Sie auf **Weiter**:

- **Zur nächsten geplanten Ausführungszeit** – Der Task wird ausgeführt, wenn der Computer zur nächsten geplanten Ausführungszeit eingeschaltet ist.
- **Schnellstmöglich** – Der Task wird ausgeführt, wenn der Computer eingeschaltet wird.
- **Sofort, wenn die Zeit seit der letzten geplanten Ausführung um diese Dauer überschritten wurde (in Stunden)** – Die verstrichene Zeit seit der ersten übersprungenen Ausführung des Tasks. Wenn diese Zeit überschritten ist, wird der Task sofort ausgeführt.

Sofort, wenn die Zeit seit der letzten geplanten Ausführung um diese Dauer überschritten wurde (in Stunden) – beispiele

Ein Beispiel-Task wird stündlich ausgeführt. Die Option **Sofort, wenn die Zeit seit der letzten geplanten Ausführung um diese Dauer überschritten wurde (in Stunden)** ist ausgewählt, und die verstrichene Zeit ist auf zwei Stunden festgelegt. Der Task wird um 13:00 Uhr ausgeführt, und der Computer wird anschließend in den Energiesparmodus versetzt:

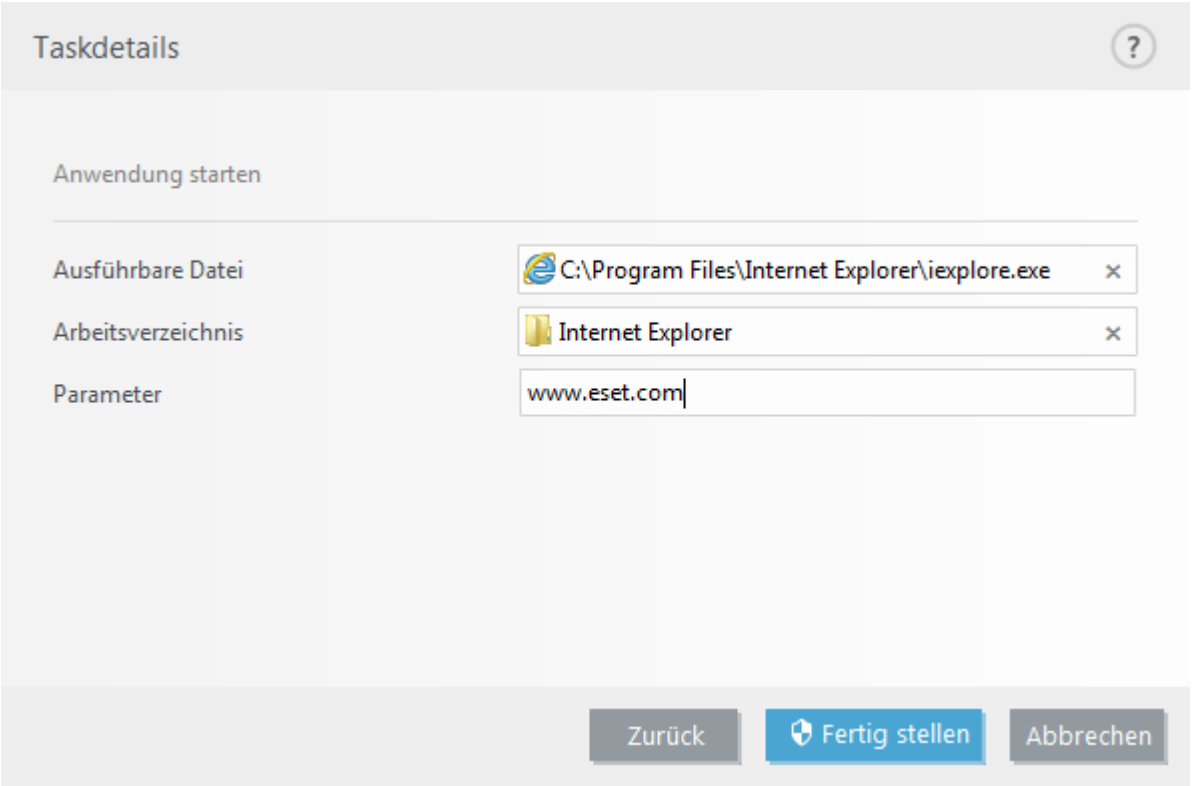
- Der Computer wird um 15:30 Uhr aktiviert. Die erste übersprungene Ausführung des Task war um 14:00 Uhr. Seit 14:00 Uhr sind nur 1,5 Stunden vergangen, darum wird der Task um 16:00 Uhr ausgeführt.
- Der Computer wird um 16:30 Uhr erneut aktiviert. Die erste übersprungene Ausführung des Task war um 14:00 Uhr. Seit 14:00 Uhr sind 2,5 Stunden vergangen. Daher wird der Task sofort ausgeführt.

Taskdetails – Update

Um das Programm von zwei Update-Servern aus zu aktualisieren, müssen zwei Update-Profile erstellt werden. Falls das Herunterladen der Update-Dateien von einem der Server fehlschlägt, wechselt das Programm automatisch zum anderen Server. Dies eignet sich z. B. für Notebooks, die normalerweise über einen Update-Server im lokalen Netzwerk aktualisiert werden, jedoch häufig über das Internet mit anderen Netzwerken verbunden sind. Falls das erste Profil nicht funktioniert, lädt das zweite automatisch die Update-Dateien von den ESET-Update-Servern herunter.

Taskdetails – Anwendung ausführen

Mit diesem Task können Sie die Ausführung einer externen Anwendung planen.



Ausführbare Datei - Wählen Sie eine ausführbare Datei aus dem Verzeichnis, klicken Sie auf die Option **...** oder geben Sie den Pfad per Hand ein.

Arbeitsverzeichnis - Legen Sie das Arbeitsverzeichnis der externen Anwendung fest. Alle temporären Dateien der

gewählten **Ausführbaren Datei** werden in diesem Verzeichnis gespeichert.

Parameter - Befehlszeilenparameter für die Anwendung (optional)

Klicken Sie auf **Fertig stellen**, um den Task zu übernehmen.

System Cleaner

System Cleaner ist ein Tool, mit dem Sie den Computer nach der Säuberung der Bedrohung auf einen nutzbaren Zustand wiederherstellen können. Schadsoftware kann Systemprogramme wie den Registrierungs-Editor, den Task-Manager oder Windows Update deaktivieren. System Cleaner stellt die Standardwerte und -Einstellungen für das jeweilige System mit einem Klick wieder her.

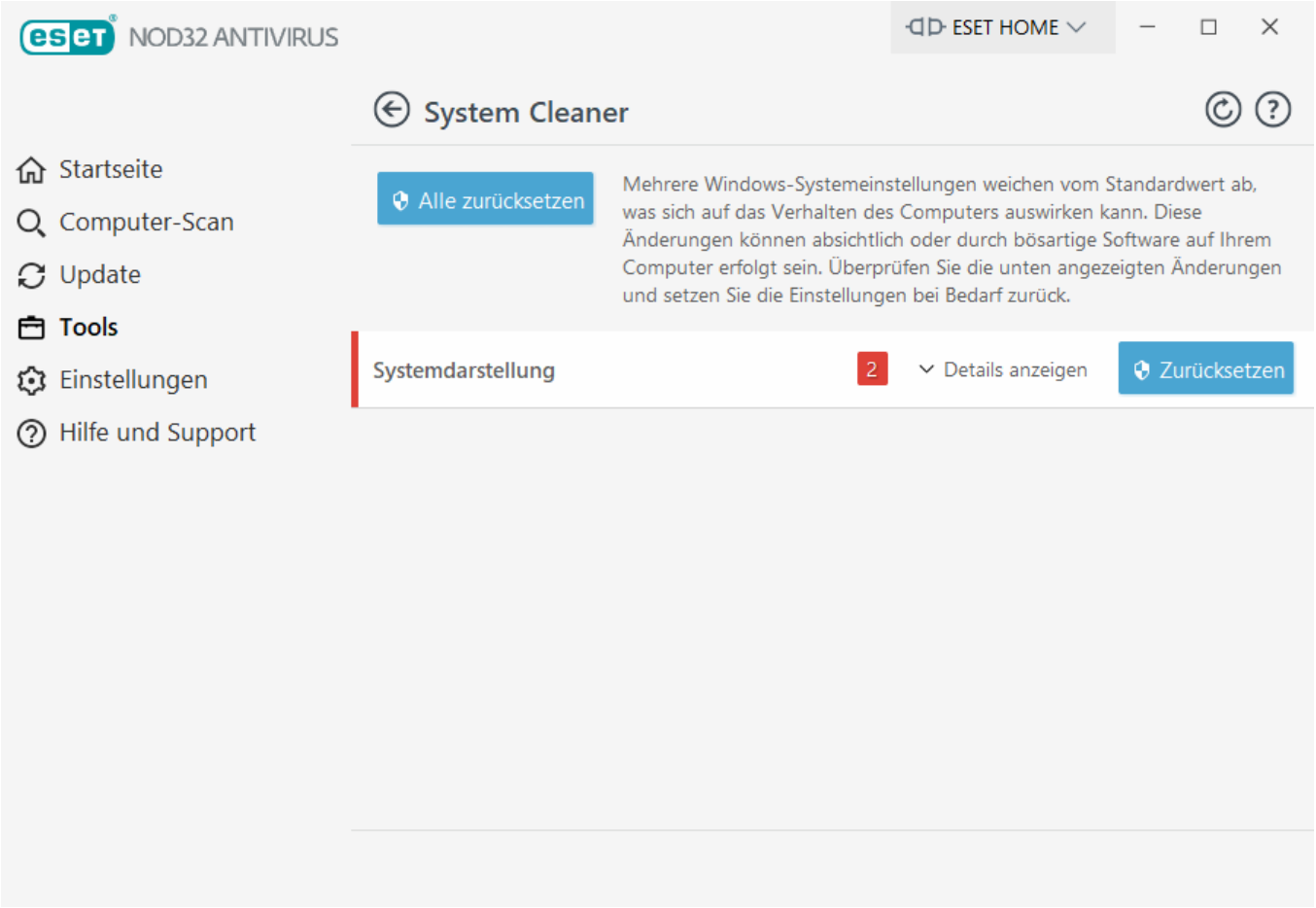
System Cleaner meldet Probleme aus fünf verschiedenen Einstellungskategorien:

- **Sicherheitseinstellungen**: Änderungen an Einstellungen, die sich auf die Anfälligkeit Ihres Computers auswirken können, z. B. Windows Update.
- **Systemeinstellungen**: Änderungen an Systemeinstellungen, die sich auf das Verhalten Ihres Computers auswirken können, z. B. Dateizuordnungen.
- **Systemdarstellung**: Einstellungen, die das Erscheinungsbild Ihres Systems bestimmen, z. B. Ihr Desktophintergrund.
- **Deaktivierte Funktionen**: Wichtige Funktionen und Anwendungen, die möglicherweise deaktiviert sind.
- **Windows-Systemwiederherstellung**: Einstellungen für die Windows-Systemwiederherstellung, mit der Sie Ihr System auf einen früheren Zeitpunkt zurücksetzen können.

Die Ausführung von System Cleaner wird in den folgenden Fällen angefordert:

- Wenn eine Bedrohung gefunden wird
- Wenn ein Benutzer auf **Zurücksetzen** klickt

Sie können die Änderungen überprüfen und die Einstellungen bei Bedarf zurücksetzen.



Die System Cleaner-Aktionen können nur von Benutzern mit Administratorrechten ausgeführt werden.

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

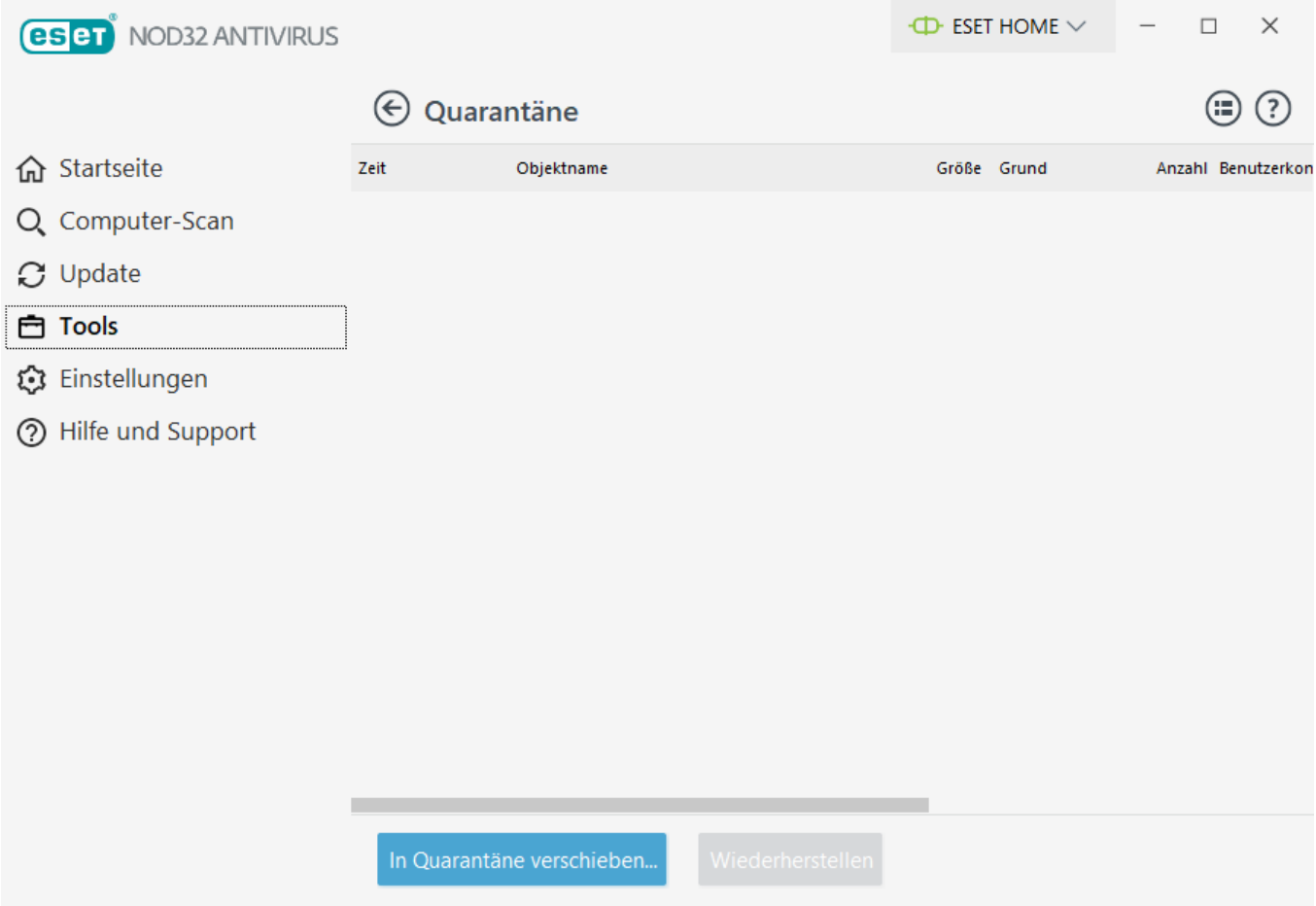
Quarantäne

Die Quarantäne dient hauptsächlich dazu, gemeldete Objekte (z. B. Malware, infizierte Dateien oder potenziell unerwünschte Anwendungen) sicher zu speichern.

Sie finden die Quarantäne im Hauptprogrammfenster von ESET NOD32 Antivirus unter **Tools** > **Quarantäne**.

Die im Quarantäneordner gespeicherten Dateien können in einer Tabelle zusammen mit den folgenden Daten angezeigt werden:

- Datum und Uhrzeit der Quarantäne
- Pfad zum ursprünglichen Speicherort der Datei
- Dateigröße in Byte
- Grund (z. B. Objekt hinzugefügt durch Benutzer)
- Verschiedene Ereignisse (z. B. duplizierte Ereignisse derselben Datei oder Archive mit mehreren Infiltrationen).



Quarantäne für Dateien

ESET NOD32 Antivirus verschiebt gelöschte Dateien automatisch in die Quarantäne (falls Sie diese Option im Warnungsfenster nicht deaktiviert haben).

Dateien sollten außerdem in die Quarantäne verschoben werden, wenn Folgendes zutrifft:

a.Dateien können nicht gesäubert werden

b.Es ist nicht sicher oder ratsam, die Dateien zu löschen

c.Die Dateien wurden fälschlicherweise von ESET NOD32 Antivirus erkannt

d.Eine Datei verhält sich verdächtig, wird jedoch vom Scanner nicht erkannt.

Sie haben mehrere Optionen, um eine Datei in die Quarantäne zu verschieben:

a.Per Ziehen und Ablegen können Sie Dateien manuell in die Quarantäne verschieben. Klicken Sie dazu auf die Datei, 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.

b.Klicken Sie mit der rechten Maustaste auf die Datei und dann auf **Erweiterte Einstellungen** > **Datei in Quarantäne verschieben**.

c.Klicken Sie im Fenster **Quarantäne** auf **In Quarantäne verschieben**.

d.Alternativ können Sie auch das Kontextmenü verwenden: Klicken Sie mit der rechten Maustaste in das Fenster **Quarantäne** und wählen Sie **Quarantäne** aus.

Wiederherstellen aus der Quarantäne

Die Dateien in der Quarantäne können an Ihrem ursprünglichen Speicherort wiederhergestellt werden:

- Verwenden Sie dazu die Funktion **Wiederherstellen** im Kontextmenü, indem Sie mit der rechten Maustaste auf eine Datei in der Quarantäne klicken.

- Wenn eine Datei als potenziell unerwünschte Anwendung markiert ist, wird die Option **Wiederherstellen und von Scans ausschließen** aktiviert. Siehe auch Ausschlüsse.

- Mit der Option **Wiederherstellen nach** im Kontextmenü können Sie eine Datei an einem anderen Ort als an ihrem ursprünglichen Speicherort wiederherstellen.

- Die Funktion zum Wiederherstellen ist nicht immer verfügbar, z. B. für Dateien in schreibgeschützten Netzwerkfreigaben.

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 die **Entf**-Taste auf der Tastatur drücken. Sie können auch mehrere Einträge gleichzeitig auswählen und gesammelt löschen. Die gelöschten Elemente werden permanent von Ihrem Gerät und aus der Quarantäne entfernt.

Einreichen einer Datei aus der Quarantäne

Wenn Sie eine verdächtige, nicht vom Programm erkannte Datei in die Quarantäne verschoben haben oder wenn eine Datei fälschlicherweise als infiziert eingestuft (etwa durch die heuristische Codeanalyse) und dadurch in den Quarantäneordner verschoben wurde, können Sie die Datei zur Analyse an das ESET-Virenlabor senden. Um eine Datei zu übermitteln, klicken Sie die Datei mit der rechten Maustaste an und wählen im Kontextmenü die Option **Zur Analyse einreichen** aus.

Ereignisbeschreibung

Klicken Sie mit der rechten Maustaste auf ein Element und klicken Sie auf **Ereignisbeschreibung**, um die ESET-Virenenzyklopädie mit detaillierten Informationen zu den Gefahren und Symptomen der aufgezeichneten Infiltration zu öffnen.

Illustrierte Anweisungen

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

- Wiederherstellen einer Datei aus der Quarantäne in ESET NOD32 Antivirus
- Löschen einer Datei aus der Quarantäne in ESET NOD32 Antivirus
- Mein ESET-Produkt hat mich über ein Ereignis benachrichtigt. Was kann ich tun?

Quarantäne fehlgeschlagen

Bestimmte Dateien können aus folgenden Gründen nicht in die Quarantäne verschoben werden:

- **Sie haben keine Leseberechtigungen** – Sie können den Inhalt einer Datei nicht anzeigen.
- **Sie haben keine Schreibberechtigungen** – Sie können den Inhalt der Datei nicht bearbeiten, also keine neuen Inhalte hinzufügen oder vorhandene Inhalte löschen.
- **Die Datei, die Sie in die Quarantäne verschieben möchten, ist zu groß** – Sie müssen die Dateigröße reduzieren.

Wenn die Fehlermeldung "Quarantäne fehlgeschlagen" angezeigt wird, klicken Sie auf **Weitere Informationen**. Das Fenster "Liste der Quarantänefehler" wird angezeigt, in dem der Name der Datei und der Grund angezeigt werden, warum die Datei nicht in die Quarantäne verschoben werden konnte.

Proxyserver

In großen LAN-Netzwerken wird die Verbindung zum Internet häufig über Proxyserver vermittelt. In einer solchen Konfiguration müssen die folgenden Einstellungen definiert werden. Andernfalls kann sich das Programm nicht automatisch aktualisieren. Die Proxyserver-Einstellungen in ESET NOD32 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 NOD32 Antivirus fest. Diese Parameter werden von allen Modulen verwendet, die eine Verbindung zum Internet benötigen.

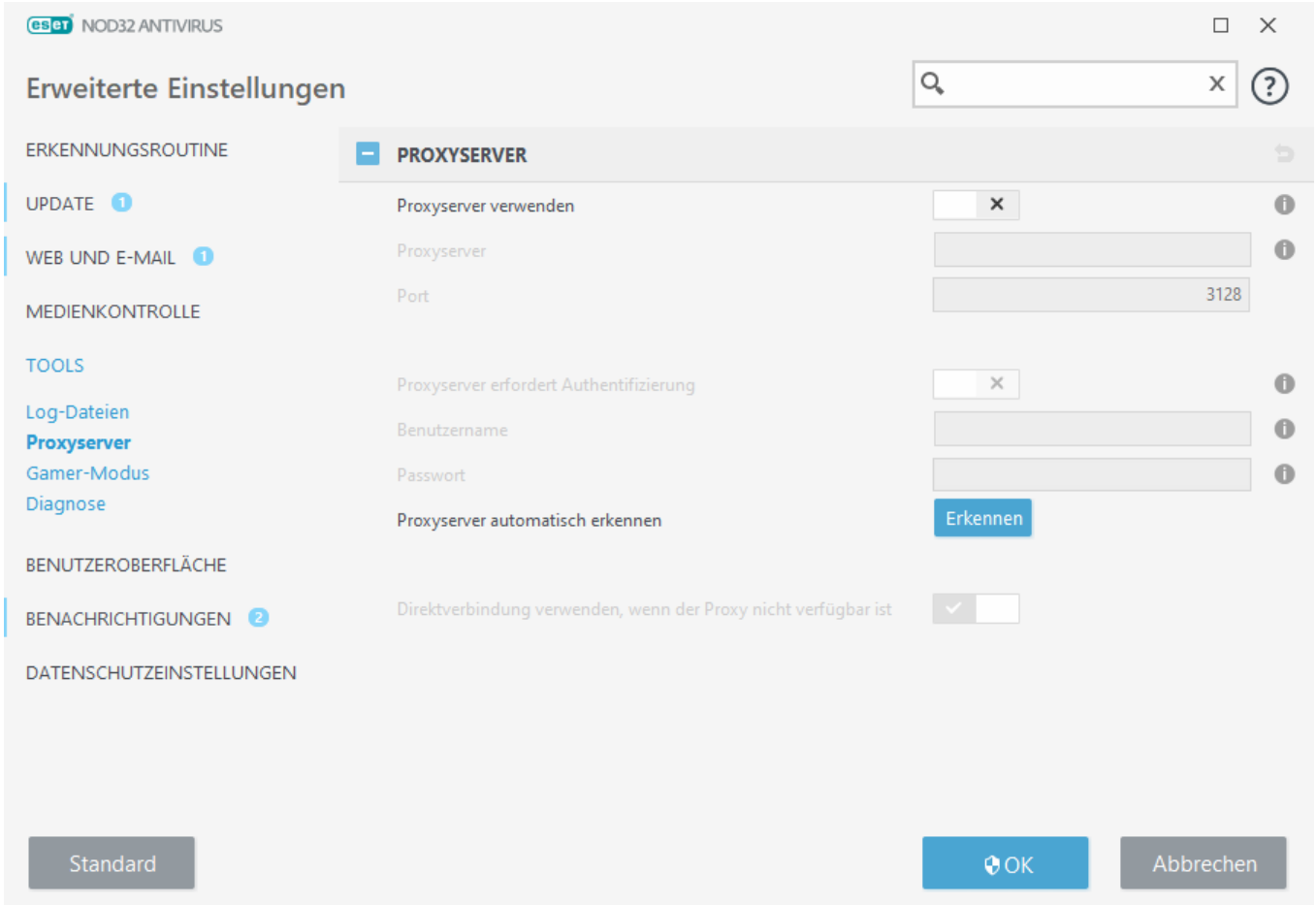
Um die Proxyserver-Einstellungen für diese Ebene festzulegen, aktivieren Sie die Option **Proxyserver verwenden** und geben im Feld **Proxyserver** die entsprechende Adresse zusammen mit dem **Port** des Proxyservers ein.

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.

Sie müssen den Benutzernamen und das Passwort manuell in den Einstellungen für den **Proxyserver** eingeben.

Direktverbindung verwenden, wenn Proxy nicht verfügbar ist – Wenn ESET NOD32 Antivirus für die Verwendung eines Proxys konfiguriert ist und der Proxy nicht erreichbar ist, umgeht ESET NOD32 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 remote beziehen. Weitere Informationen zu diesen Einstellungen finden Sie unter Erweiterte Einstellungen für Updates.



Probe für die Analyse auswählen

Wenn Sie eine verdächtige Datei auf Ihrem Computer oder eine verdächtige Webseite finden, können Sie sie zur Analyse an das ESET-Virenlabor senden (je nach Konfiguration von ESET LiveGrid® unter Umständen nicht verfügbar).

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 Sample (Dateien oder Webseiten) auf die folgenden Arten zur Analyse an ESET übermitteln:

1. Verwenden Sie das Übermittlungsformular für Sample in Ihrem Produkt. Sie finden es unter **Tools** > **Sample zur Analyse einreichen**. Die maximale Größe eines eingereichten Samples ist 256 MB.

2. Sie können Dateien auch per E-Mail einsenden. Komprimieren Sie in diesem Fall die Datei(en) mit WinRAR/WinZIP, verschlüsseln Sie das Archiv mit dem Passwort „infected“ und senden Sie es an samples@eset.com.

3. Falls Sie Spam oder einen Fehlalarm melden möchten, beachten Sie bitte unseren Artikel in der ESET-Knowledgebase.

Wählen Sie im Formular **Probe für die Analyse auswählen** im Dropdownmenü **Grund für Einreichen der Probe** die Beschreibung aus, die am besten auf den Zweck Ihrer Mitteilung zutrifft:

- Verdächtige Datei
- Verdächtige Website (eine Website, die mit Schadsoftware infiziert ist)
- Fehlalarm Webseite
- Fehlalarm Datei (als Bedrohung erkannte Datei, die jedoch nicht infiziert ist)
- 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**
> Beachten Sie, dass Sie nur dann eine Antwort von ESET erhalten, wenn weitere Informationen von Ihnen benötigt werden. Täglich gehen mehrere Zehntausend Dateien auf unseren Servern ein und wir können nicht jede Meldung individuell beantworten.
> 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.

> Das erste Feld - **Beobachtete Anzeichen und Symptome einer Malware-Infektion** - muss stets ausgefüllt werden, Zusatzangaben helfen dem Virenlabor jedoch erheblich bei der Identifizierung und Sampleauswertung.

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 Erkennungsroutine 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.

> 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 Verarbeitung der verdächtigen Website 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.

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 NOD32 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.

Dialogfenster – System-Updates

Falls Updates für Ihr Betriebssystem verfügbar sind, wird im Startfenster von ESET NOD32 Antivirus eine entsprechende Benachrichtigung angezeigt. Klicken Sie auf **Weitere Informationen**, um das Fenster mit den Systemupdates zu öffnen.

Das Fenster „System-Updates“ listet verfügbare Updates auf, die heruntergeladen und installiert werden können. Neben dem Namen des Updates wird der Updatetyp angezeigt.

Doppelklicken Sie auf ein beliebiges Update, um das Fenster Updateinformationen mit zusätzlichen Informationen zu öffnen.

Klicken Sie auf **System-Update durchführen**, um mit dem Herunterladen und Installieren zu beginnen.

Update-Informationen

Informationen über Windows-Updates. Name und Nummer des Updates werden oben im Fenster angezeigt, gefolgt von dessen Priorität und einer Beschreibung des Problems, welches durch das Update gelöst wird.

Benutzeroberfläche

Klicken Sie im Hauptprogrammfenster auf **Einstellungen** > **Erweiterte Einstellungen** (F5) **Grafische Benutzeroberfläche**, um das Verhalten der grafischen Benutzeroberfläche (GUI) zu konfigurieren.

Sie können das Erscheinungsbild und die Effekte des Programms in den erweiterten Einstellungen unter Elemente der Benutzeroberfläche anpassen.

Um Ihre Sicherheitssoftware bestmöglich vor Deinstallation und unerlaubten Änderungen zu schützen, können Sie mit der Funktion Einstellungen für den Zugriff einen Passwortschutz für Ihre Einstellungen einrichten.

> Im Abschnitt Benachrichtigungen können Sie das Verhalten von Systembenachrichtigungen, Ereigniswarnungen und Statusmeldungen konfigurieren.

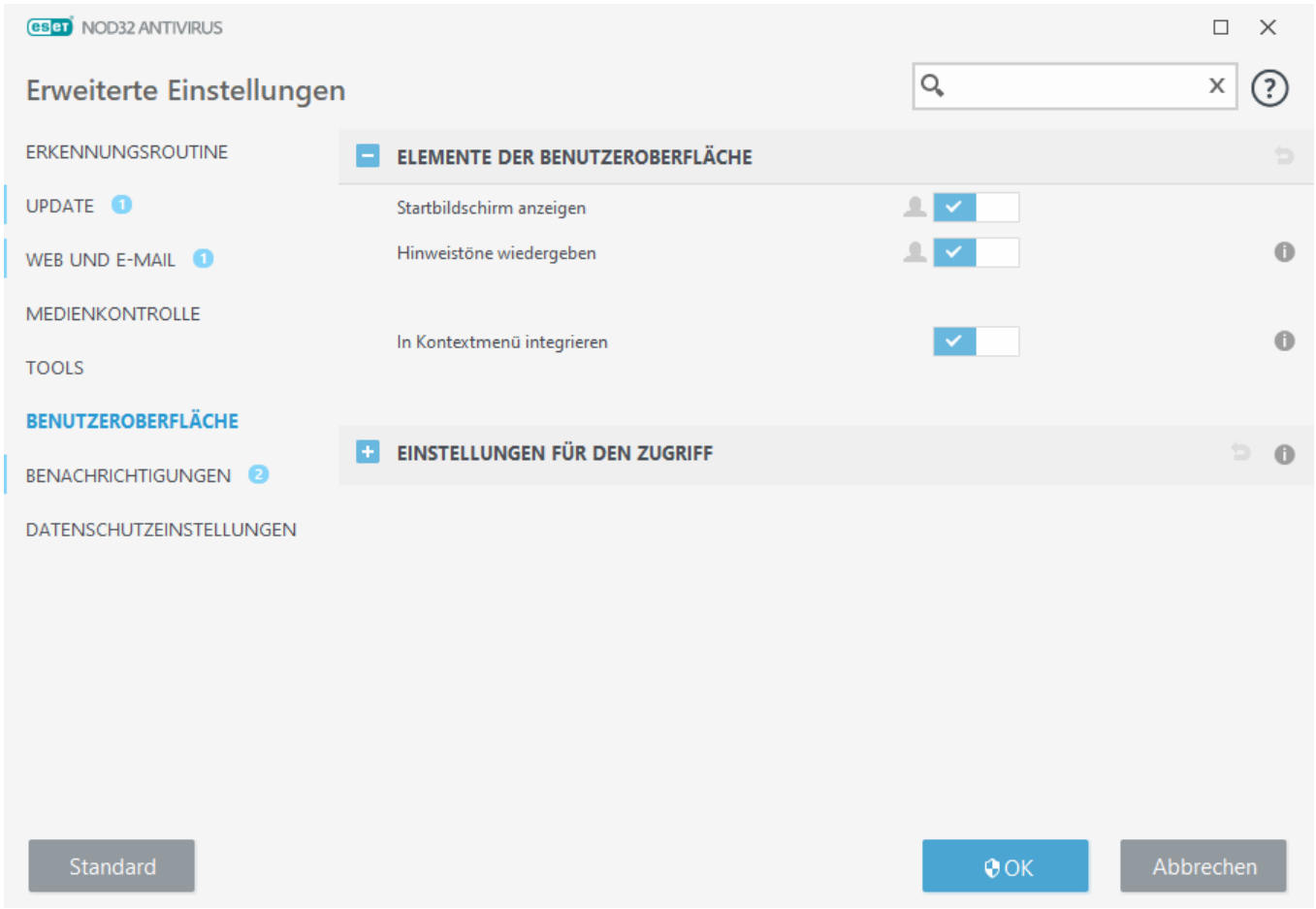
Elemente der Benutzeroberfläche

Über die Konfigurationsoptionen für die Benutzeroberfläche von ESET NOD32 Antivirus können Sie die Arbeitsumgebung an Ihre Anforderungen anpassen. Sie finden diese Konfigurationsoptionen unter **Erweiterte Einstellungen** (F5) > **Benutzeroberfläche** > **Elemente der Benutzeroberfläche**.

Wenn ESET NOD32 Antivirus ohne Anzeige des Startbilds gestartet werden soll, deaktivieren Sie die Option **Startbild anzeigen**.

Hinweistöne wiedergeben – ESET NOD32 Antivirus spielt bei wichtigen Ereignissen, wie z. B. bei erkannten Bedrohungen oder nach Abschluss von Scans, einen Warnton ab.

In Kontextmenü integrieren - ESET NOD32 Antivirus kann in das Kontextmenü integriert werden.



Einstellungen für den Zugriff

Die Einstellungen von ESET NOD32 Antivirus sind ein wichtiger Bestandteil Ihrer Sicherheitsrichtlinien. Unbefugte Änderungen können die Stabilität und den Schutz Ihres Systems gefährden. Um unberechtigte Änderungen zu verhindern, können Sie die Einstellungen von ESET NOD32 Antivirus mit einem Passwort schützen.

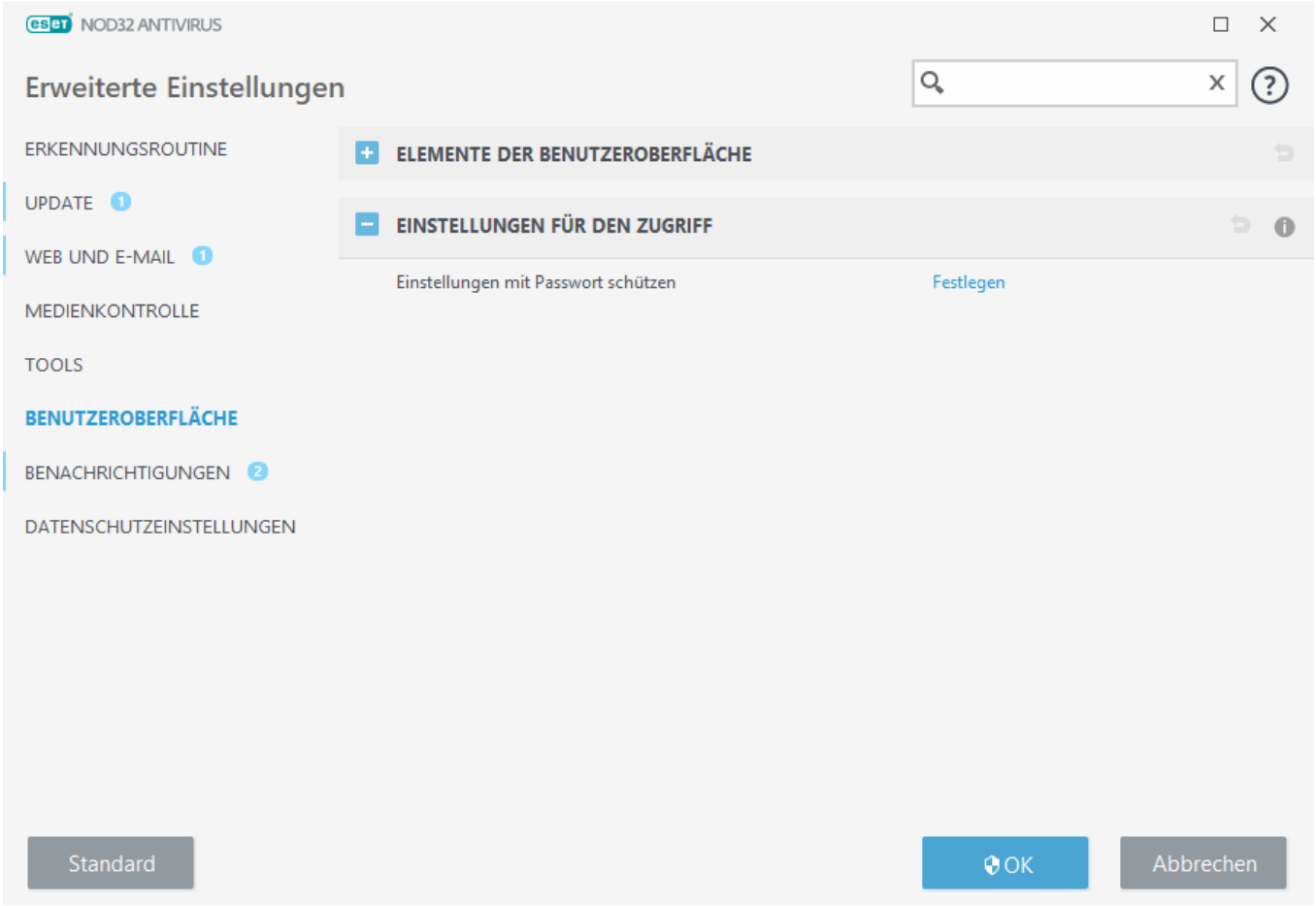
Klicken Sie neben **Einstellungen mit Passwort schützen** auf **Festlegen**, um ein Passwort für den Schutz der Einstellungen und als Deinstallationsschutz für ESET NOD32 Antivirus festzulegen.

Wenn Sie versuchen, die geschützten erweiterten Einstellungen zu öffnen, wird ein Fenster zur Eingabe des Passworts angezeigt. Falls Sie Ihr Passwort vergessen oder verloren haben, klicken Sie unten auf **Passwort wiederherstellen** und geben Sie die E-Mail-Adresse ein, die Sie bei der Registrierung dieser Lizenz verwendet haben. Sie erhalten eine E-Mail von ESET mit dem Überprüfungscode und einer Anleitung zum Zurücksetzen Ihres Passworts.

- So entsperren Sie die erweiterten Einstellungen

Klicken Sie auf **Passwort ändern** neben **Einstellungen mit Passwort schützen**, um Ihr Passwort zu ändern.

Klicken Sie auf **Entfernen** neben **Einstellungen mit Passwort schützen**, um Ihr Passwort zu entfernen.



Passwort für erweiterte Einstellungen

Zum Schutz der erweiterten Einstellungen in ESET NOD32 Antivirus vor unbefugten Änderungen müssen Sie ein neues Passwort festlegen.

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**.

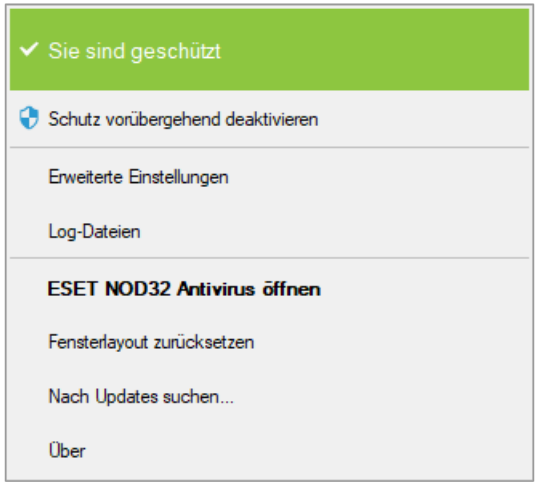
Dieses Passwort ist für alle zukünftigen Änderungen an ESET NOD32 Antivirus erforderlich.

Falls Sie Ihr Passwort vergessen haben, können Sie den Zugang zu den erweiterten Einstellungen mit der Methode „Passwort wiederherstellen“ zurückerlangen.

Wenn Sie Ihren verloren gegangenen ESET-Lizenzschlüssel wiederherstellen möchten oder Informationen zum Ablaufdatum Ihrer Lizenz oder andere Lizenzinformationen zu ESET NOD32 Antivirus benötigen, finden Sie diese Informationen in unserem Knowledgebase-Artikel.

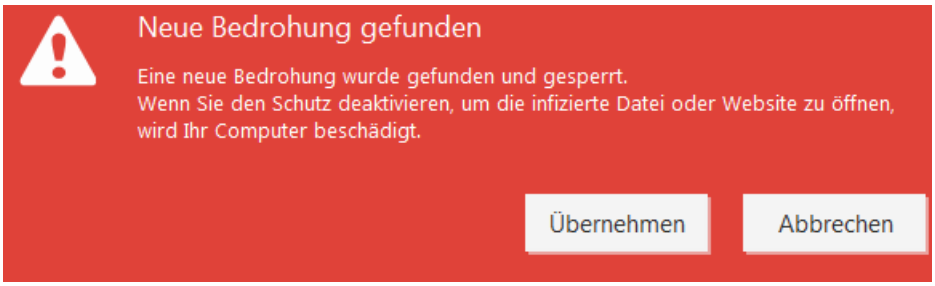
Symbol im Infobereich der Taskleiste

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 Bestätigungsdialogfeld an, dass die Erkennungsroutine deaktiviert wird, die Dateivorgänge sowie die Internet- und E-Mail-Kommunikation überwacht und Ihr System 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**. Alternativ können die erweiterten Einstellungen auch mit der Taste F5 oder unter **Einstellungen** > **Erweiterte Einstellungen** geöffnet werden.

Log-Dateien - Log-Dateien enthalten Informationen zu wichtigen aufgetretenen Programmereignissen und geben einen Überblick über erkannte Ereignisse.

ESET NOD32 Antivirus Öffnen – Öffnet das Hauptprogrammfenster von ESET NOD32 Antivirus über das Symbol im Infobereich der Taskleiste.

Fensterlayout zurücksetzen - Stellt die standardmäßige Fenstergröße von ESET NOD32 Antivirus und deren Standardposition auf dem Bildschirm wieder her.

Nach Updates suchen – Beginnt mit der Aktualisierung der Erkennungsroutine (bisher auch als „Signaturdatenbank“ bezeichnet), um den Schutz vor Schadcode zu gewährleisten.

Über - Zeigt Systeminformationen zur installierten Version von ESET NOD32 Antivirus und zu den installierten

Programmmodulen sowie das Ablaufdatum der Lizenz an. Hier finden Sie außerdem das Lizenzablaufdatum und Informationen zum Betriebssystem und zu den Systemressourcen.

Unterstützung für Sprachausgabeprogramme

ESET NOD32 Antivirus kann zusammen mit Sprachausgabeprogrammen verwendet werden, damit ESET-Benutzern mit Sehbehinderungen im Produkt navigieren oder die Einstellungen konfigurieren können. Die folgenden Bildschirmleser werden unterstützt: (JAWS, NVDA, Narrator).

Um sicherzustellen, dass das Sprachausgabeprogramm korrekt auf die GUI von ESET NOD32 Antivirus zugreifen kann, folgen Sie den Anweisungen in unserem Knowledgebase-Artikel.

Hilfe und Support

ESET NOD32 Antivirus enthält Tools für die Fehlerbehebung und Support-Informationen, die Ihnen bei der Lösung von möglichen Problemen behilflich sind.

Lizenz

- **Fehlerbehebung für Lizenzen** – Klicken Sie auf diesen Link, um Lösungen für Probleme bei der Aktivierung oder Änderung von Lizenzen zu finden.

- **Lizenz ändern** – Klicken Sie hier, um das Aktivierungsfenster zu öffnen und Ihr Produkt zu aktivieren. Falls Ihr Gerät mit ESET HOME verknüpft ist, wählen Sie eine Lizenz aus Ihrem ESET HOME-Konto aus oder fügen Sie eine neue Lizenz hinzu.

Installiertes Produkt

- **Neuerungen** - Klicken Sie auf diese Option, um das Informationsfenster für neue und verbesserte Funktionen zu öffnen.

- **Über ESET NOD32 Antivirus** – Informationen zu Ihrer Kopie von ESET NOD32 Antivirus.

- **Fehlerbehebung für das Produkt** – Klicken Sie auf diesen Link, um Lösungen für die häufigsten Probleme zu finden.

- **Produkt wechseln** – Klicken Sie hier, um herauszufinden, ob ESET NOD32 Antivirus mit der aktuellen Lizenz zu einer anderen Produktlinie geändert werden kann.

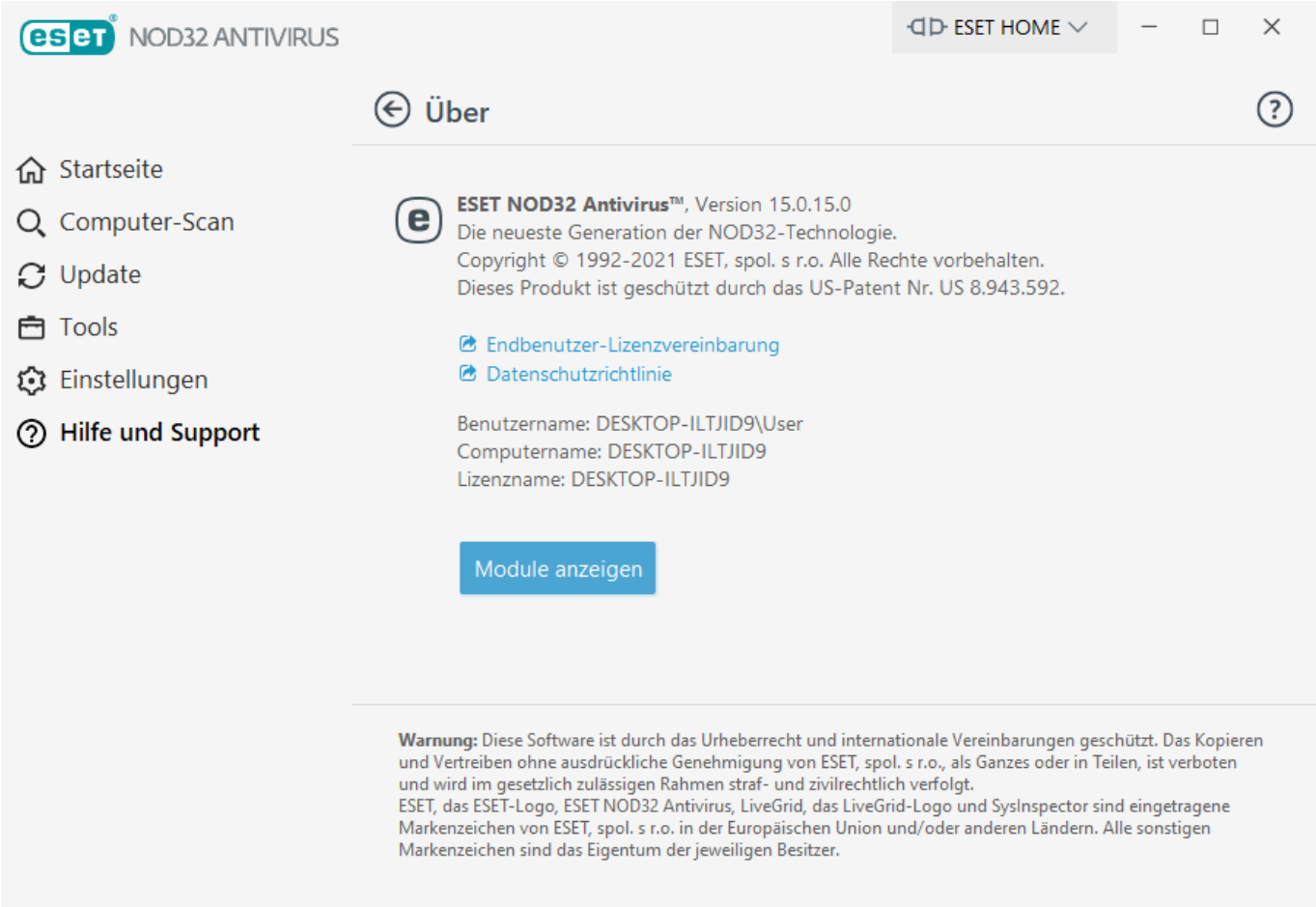
Hilfeseite - Mit diesem Link öffnen Sie die ESET NOD32 Antivirus-Hilfeseiten.

Technischer Support

Knowledgebase – 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.

Info zu ESET NOD32 Antivirus

Dieses Fenster enthält Details zur installierten Version von ESET NOD32 Antivirus und zu Ihrem Computer.



Klicken Sie auf **Module anzeigen**, um Informationen zur Liste der geladenen Programmmodule zu öffnen.

- Klicken Sie auf **Kopieren**, um Informationen zu den Modulen in die Zwischenablage zu kopieren. Dies kann für die Fehlerbehebung oder bei der Kontaktaufnahme zum technischen Support hilfreich sein.

- Klicken Sie im Fenster „Module“ auf **Erkennungsroutine**, um den ESET-Virusradar zu öffnen, der Informationen zu den einzelnen Versionen des ESET-Erkennungsmoduls enthält.

ESET-Ankündigungen

In diesem Fenster zeigt ESET NOD32 Antivirus regelmäßig Ankündigungen von ESET an.

Die produktinternen Nachrichten wurden entwickelt, um Benutzer über Neuigkeiten und Ankündigungen von ESET zu informieren. Für den Versand von Marketingnachrichten ist eine Zustimmung des Benutzers erforderlich. Marketingnachrichten werden daher standardmäßig nicht verschickt (als Fragezeichen angezeigt). Aktivieren Sie diese Option, um Marketingnachrichten von ESET zu erhalten. Deaktivieren Sie die **Marketing-Nachrichten anzeigen** Option, wenn Sie nicht an Marketingmaterial von ESET interessiert sind.

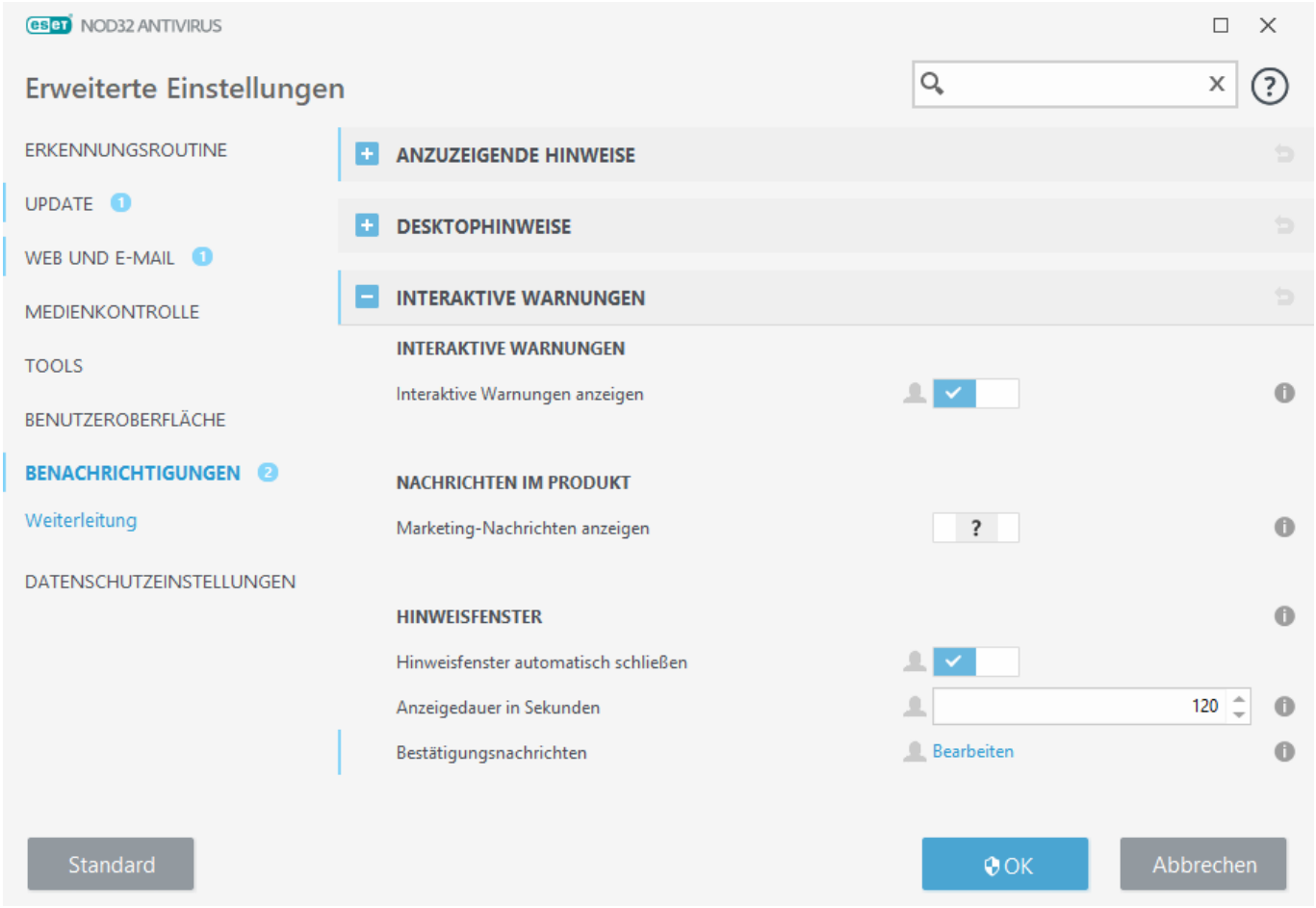
Führen Sie die folgenden Anweisungen aus, um den Empfang von Marketingnachrichten über ein Popupfenster zu aktivieren oder zu deaktivieren.

1. Öffnen Sie das Hauptfenster Ihres ESET-Produkts.

2. Drücken Sie die Taste **F5**, um **Erweiterte Einstellungen** zu öffnen.

3. Klicken Sie auf **Benachrichtigungen** > **Interaktive Warnungen**.

4. Passen Sie die Option **Marketing-Nachrichten anzeigen** an.



Systemkonfigurationsdaten senden

Um möglichst schnell und effizient helfen zu können, benötigt der ESET-Support Informationen zur Konfiguration von ESET NOD32 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.

Beim Senden des Webformulars *** 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 technischen Support von ESET über das Online-Supportformular erreichen.

Sie finden diese Einstellung auch unter **Erweiterte Einstellungen** > **Tools** > **Diagnose** > Technischer Support.

Wenn Sie Systemdaten einreichen möchten, müssen Sie das Webformular ausfüllen und einreichen. Andernfalls wird kein Ticket erstellt und die Systemdaten werden nicht übermittelt.

Technischer Support

Klicken Sie im Hauptprogrammfenster auf **Hilfe und Support** > **Technischer Support**.

Technischen Support kontaktieren

Support anfordern – Wenn Sie keine Lösung für Ihr Problem finden, können Sie sich über dieses Formular auf der ESET-Website schnell mit dem technischen ESET-Support in Verbindung setzen. Je nach Ihren Einstellungen wird das Fenster zum Senden der Systemkonfigurationsdaten angezeigt, bevor Sie das Webformular ausfüllen.

Informationen für den technischen Support abrufen

Details für den technischen Support – Wenn Sie dazu aufgefordert werden, können Sie Informationen für den technischen ESET-Support kopieren und senden (z. B. Lizenzdetails, Produktname, Produktversion, Betriebssystem und Computerdetails).

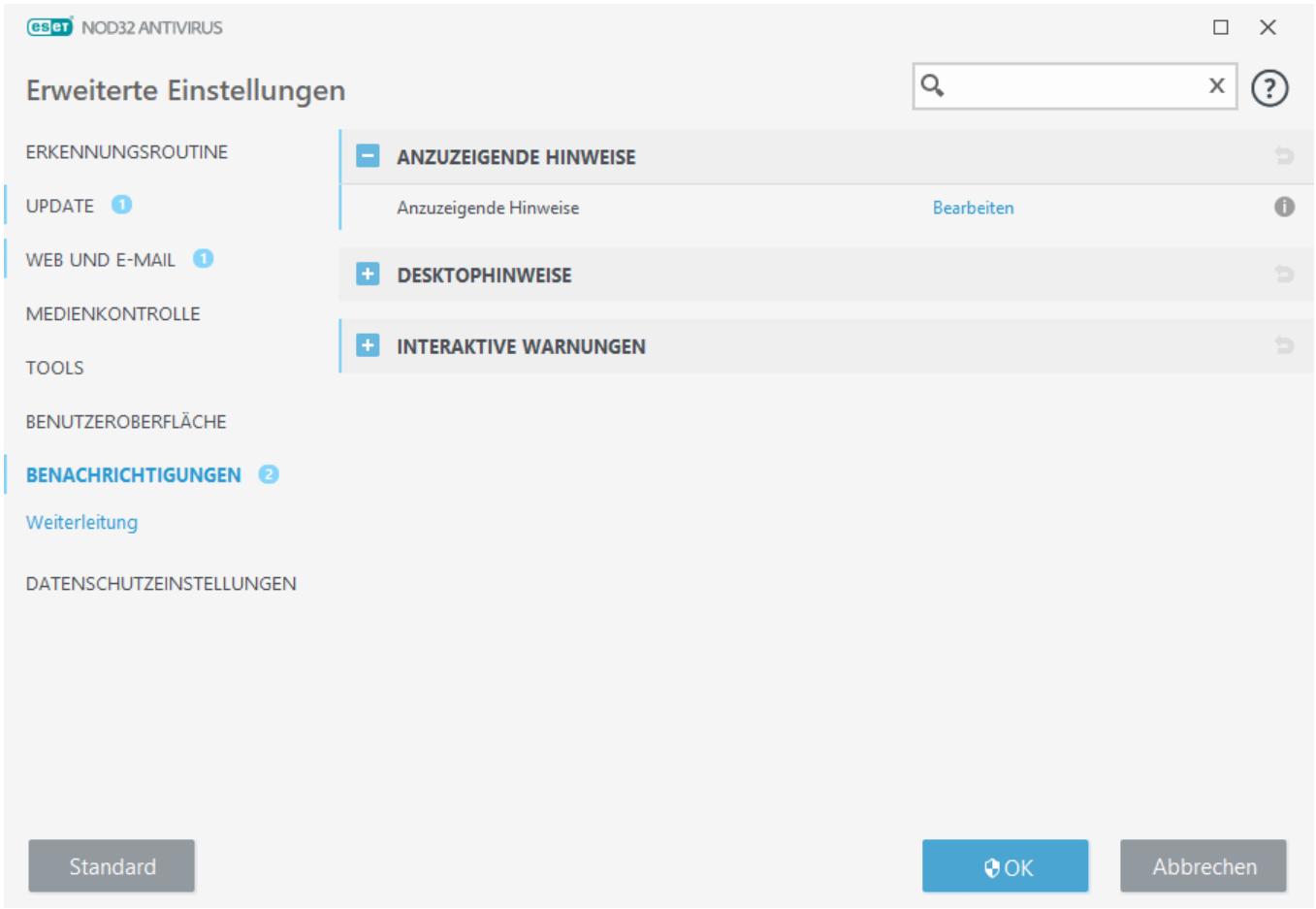
ESET Log Collector – Öffnet den Artikel in der ESET-Knowledgebase, in dem Sie das ESET Log Collector-Dienstprogramm herunterladen können. Diese Anwendung sammelt automatisch Informationen und Log-Dateien von einem Computer und ermöglicht somit eine schnellere Problemlösung. Weitere Informationen finden Sie online im ESET Log Collector-Benutzerhandbuch.

Aktivieren Sie das **erweiterte Logging**, um erweiterte Logs für alle verfügbaren Funktionen zu erstellen und den Entwicklern beim Diagnostizieren und Beheben der Probleme zu helfen. Die Mindestinformationen in den Logs werden auf die Stufe **Diagnose** festgelegt. Das erweiterte Logging wird automatisch nach zwei Stunden deaktiviert, wenn Sie die Funktion nicht vorher selbst mit der Option **Erweitertes Logging beenden** deaktivieren. Nachdem alle Logs erstellt wurden, wird ein Benachrichtigungsfenster mit dem Diagnoseordner und den erstellten Logs geöffnet.

Benachrichtigungen

Um die Benachrichtigungen in ESET NOD32 Antivirus zu verwalten, navigieren Sie zu **Erweiterte Einstellungen** (F5) > **Benachrichtigungen**. Dort können Sie die folgenden Arten von Benachrichtigungen verwalten:

- Anwendungsstatus – Benachrichtigungen, die im Startbereich des Hauptprogrammfensters angezeigt werden.
- Desktophinweise – Kleines Popupfenster neben der System-Taskleiste.
- Interaktive Warnungen – Fenster mit Warnungen und Hinweise, die ein Eingreifen des Benutzers erfordern.
- Weiterleitung (E-Mail-Benachrichtigungen) – E-Mail-Benachrichtigungen werden an die angegebene E-Mail-Adresse verschickt.



Anzuzeigende Hinweise

Anwendungsstatus – Klicken Sie auf **Bearbeiten**, um auszuwählen, welche Statusmeldungen im Startbereich des Hauptprogrammfensters angezeigt werden sollen.

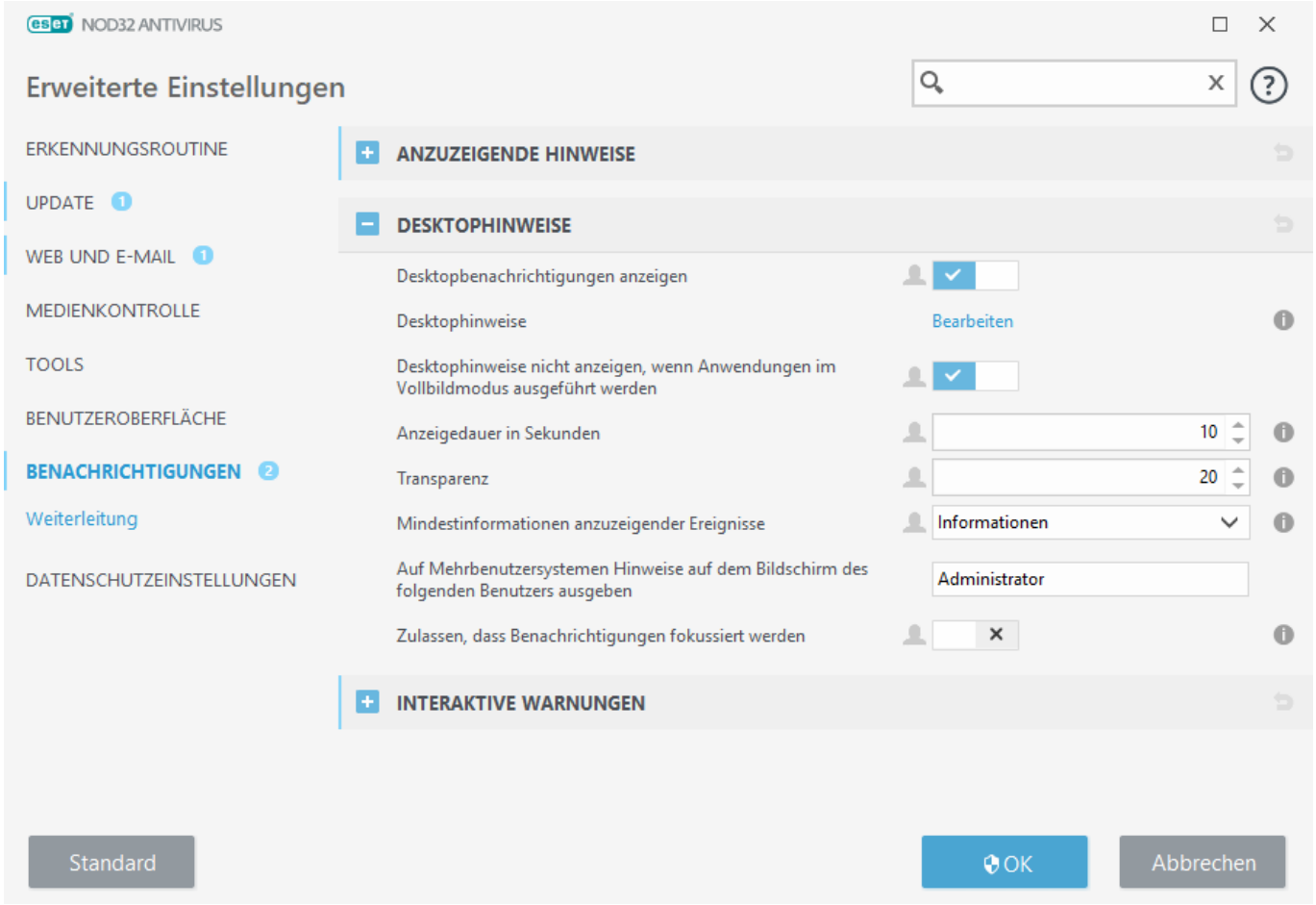
Dialogfenster – Anwendungsstatus

In diesem Dialogfenster können Sie auswählen, welche Statusmeldungen angezeigt werden sollen. Wenn Sie beispielsweise den Viren- und Spyware-Schutz anhalten oder den Gamer-Modus aktivieren.

Der Anwendungsstatus wird ebenfalls angezeigt, wenn Ihr Produkt nicht aktiviert ist oder Ihre Lizenz abgelaufen ist.

Desktophinweise

Desktopbenachrichtigungen werden als kleines Popupfenster neben der System-Taskleiste angezeigt. Standardmäßig werden sie 10 Sekunden lang angezeigt und verschwinden dann langsam. Zu Benachrichtigungen gehören erfolgreiche Produktupdates, neue verbundene Geräte, der Abschluss von Scans oder neu gefundene Bedrohungen.



Benachrichtigungen auf dem Desktop anzeigen – Wir empfehlen, diese Option aktiviert zu lassen, damit das Produkt Sie über neue Ereignisse informieren kann.

Desktophinweise – Klicken Sie auf **Bearbeiten**, um einzelne Desktophinweise zu aktivieren oder zu deaktivieren.

Desktophinweise nicht anzeigen, wenn Anwendungen im Vollbildmodus ausgeführt werden – Unterdrücken Sie alle nicht-interaktiven Benachrichtigungen, wenn Anwendungen im Vollbildmodus ausgeführt werden.

Zeitüberschreitung in Sekunden – Legen Sie die Anzeigedauer für Benachrichtigungen fest. Der Wert muss zwischen 3 und 30 Sekunden liegen.

Transparenz – Legen Sie die Prozentzahl für die Transparenz der Benachrichtigungen fest. Der unterstützte Bereich reicht von 0 (keine Transparenz) bis 80 (sehr hohe Transparenz).

Mindestinformationen anzuzeigender Ereignisse – Legen Sie den angezeigten anfänglichen Schweregrad der Benachrichtigung fest. Wählen Sie im Dropdownmenü eine der folgenden Optionen aus:

- **Diagnose** – Zeigt alle Informationen an, die für die Feinabstimmung des Programms und aller Meldungen höherer Stufen erforderlich sind.
- **Informationen** – Zeigt Informationsmeldungen an, z. B. nicht standardmäßige Netzwerkereignisse, Meldungen zu erfolgreichen Updates sowie alle Meldungen höherer Stufen.
- **Warnungen** – Zeigt Warnungen, Fehler und kritische Fehler (z. B. Anti-Stealth wird nicht ordnungsgemäß ausgeführt oder Update fehlgeschlagen) an.
- **Fehler** – Zeigt Fehler (z. B. nicht gestarteten Dokumentenschutz) und kritische Fehler an.

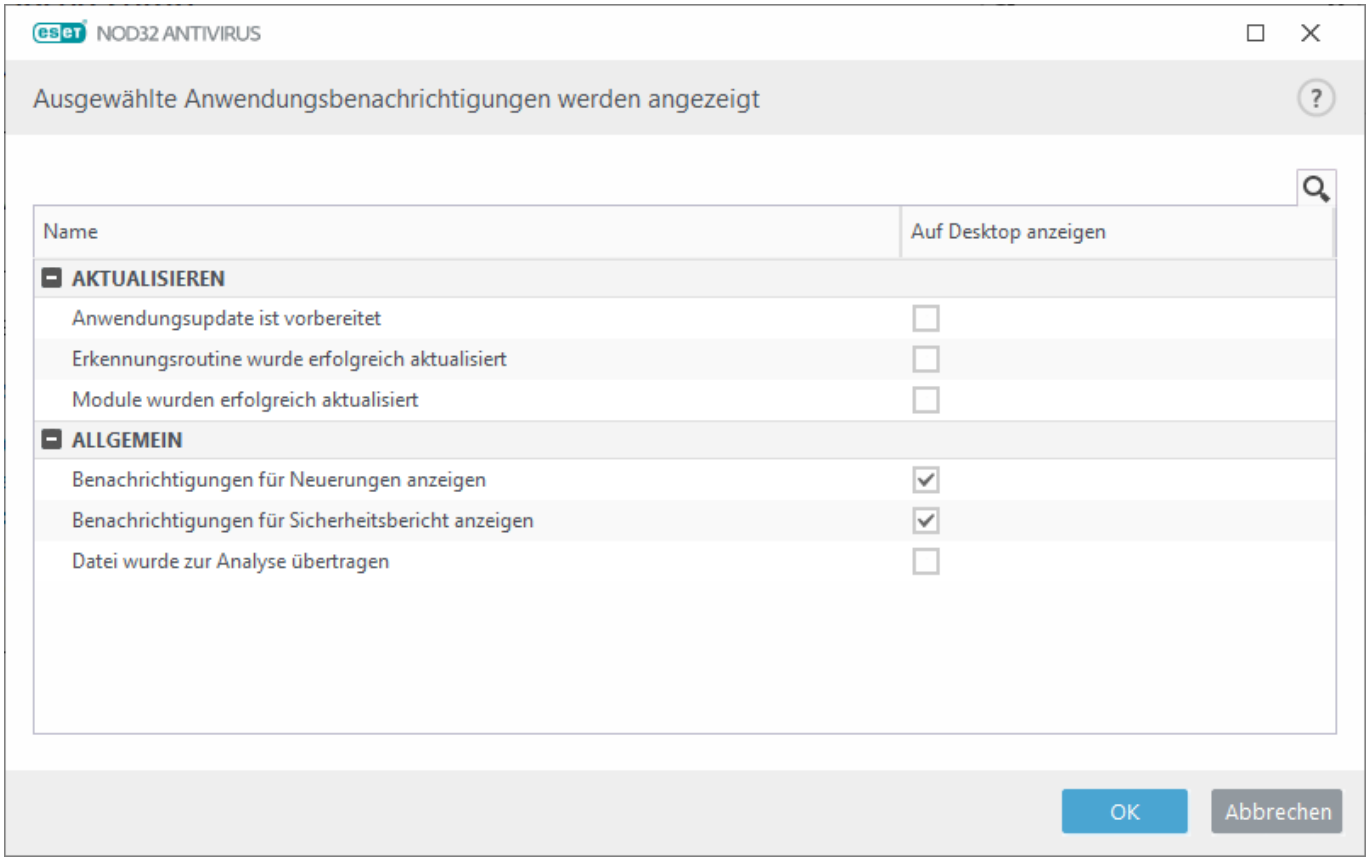
- **Kritische Warnungen** – Zeigt nur kritische Fehler an (z. B. Fehler beim Starten des Virenschutz-Moduls oder ein infiziertes System).

Auf Mehrbenutzersystemen Hinweise auf dem Bildschirm des folgenden Benutzers ausgeben – Ermöglicht den ausgewählten Konten den Empfang von Desktophinweisen. Wenn Sie z. B. das Administratorkonto nicht verwenden, können Sie den vollständigen Kontonamen eingeben, um Hinweise für das entsprechende Konto anzuzeigen. Nur ein Benutzerkonto kann die Desktophinweise erhalten.

Auf Mehrbenutzersystemen Hinweise auf dem Bildschirm des folgenden Benutzers ausgeben – Ermöglicht die Anzeige von Bildschirmbenachrichtigungen. Außerdem können die Hinweise über das Menü **ALT + Tab** aufgerufen werden.

Liste der Desktophinweise

Um die Sichtbarkeit von Desktophinweisen (rechts unten auf dem Bildschirm) zu ändern, navigieren Sie zu **Erweiterte Einstellungen** (F5) > **Benachrichtigungen** > **Desktophinweise**. Klicken Sie auf **Bearbeiten** neben **Desktophinweise** und aktivieren Sie das Kontrollkästchen neben **Anzeigen**.



Allgemein

Benachrichtigungen für Sicherheitsbericht anzeigen – Sie erhalten eine Benachrichtigung, wenn ein neuer Sicherheitsbericht erstellt wird.

Benachrichtigungen für Neuerungen anzeigen – Benachrichtigungen zu allen neuen und verbesserten Funktionen der neuesten Produktversion.

Datei wurde zur Analyse übertragen – Sie erhalten eine Benachrichtigung, wenn ESET NOD32 Antivirus eine Datei

zur Analyse überträgt.

Update

Anwendungsupdate ist vorbereitet – Sie erhalten eine Benachrichtigung, wenn ein Update für eine neue Version von ESET NOD32 Antivirus verfügbar ist.

Erkennungsroutine wurde erfolgreich aktualisiert – Sie erhalten eine Benachrichtigung, wenn das Produkt die Module der Erkennungsroutine aktualisiert.

Module wurden erfolgreich aktualisiert – Sie erhalten eine Benachrichtigung, wenn das Produkt die Programmkomponenten aktualisiert.

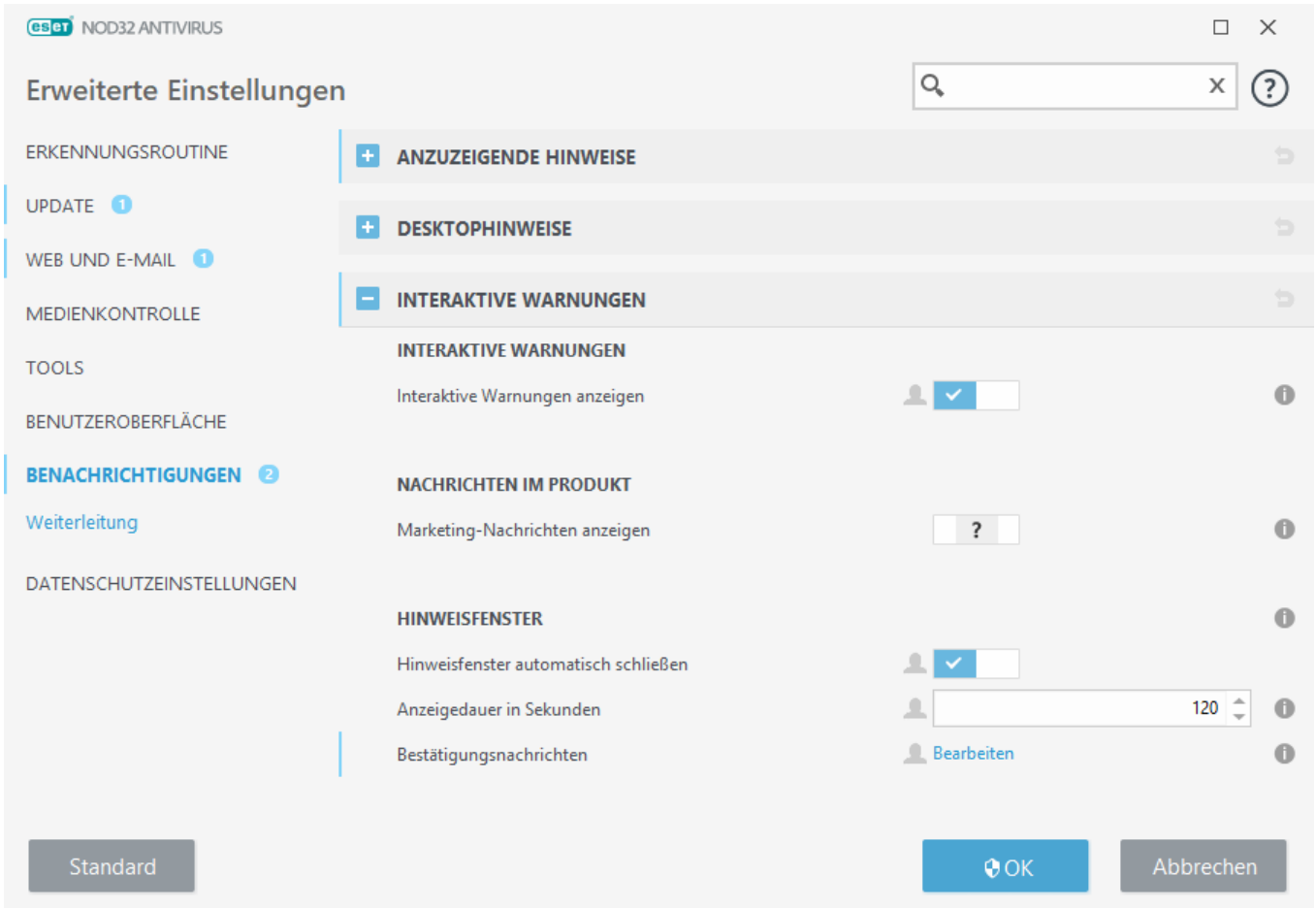
Allgemeine Einstellungen für Desktophinweise, wie etwa die Anzeigedauer für Benachrichtigungen und der Mindestinformationsumfang, können Sie unter **Erweiterte Einstellungen** (F5) > **Benachrichtigungen** > Desktophinweise anpassen.

Interaktive Warnungen

Suchen Sie nach Informationen zu allgemeinen Warnungen und Hinweisen?

- Bedrohung gefunden
- Adresse wurde blockiert
- Produkt nicht aktiviert
- Zu einem Produkt mit mehr Features wechseln
- Zu einem Produkt mit weniger Features wechseln
- Kostenloses Upgrade verfügbar
- Update-Daten sind nicht konsistent
- So beheben Sie das Problem „Modulupdate fehlgeschlagen“
- Fehler bei Modulupdates beheben
- Website-Zertifikat widerrufen

Im Abschnitt **Warnungen und Hinweisfenster** unter **Erweiterte Einstellungen** (F5) > **Benachrichtigungen** können Sie festlegen, wie ESET NOD32 Antivirus verschiedene Hinweisfenster und interaktive Warnungen verarbeiten soll, wenn eine Entscheidung von einem Benutzer erforderlich ist (z. B. potenzielle Phishing-Websites).



Interaktive Warnungen

Wenn Sie die Option **Interaktive Warnungen anzeigen** deaktivieren, werden alle Warnmeldungen und browserinternen Dialoge ausgeblendet. Diese Einstellung eignet sich nur für sehr spezielle Situationen. ESET empfiehlt, diese Option aktiviert zu lassen. ESET empfiehlt, diese Option aktiviert zu lassen.

Nachrichten im Produkt

Die produktinternen Nachrichten wurden entwickelt, um Benutzer über Neuigkeiten und Ankündigungen von ESET zu informieren. Für den Versand von Marketingnachrichten ist eine Zustimmung des Benutzers erforderlich. Marketingnachrichten werden daher standardmäßig nicht verschickt (als Fragezeichen angezeigt). Aktivieren Sie diese Option, um Marketingnachrichten von ESET zu erhalten. Deaktivieren Sie die **Marketing-Nachrichten anzeigen** Option, wenn Sie nicht an Marketingmaterial von ESET interessiert sind.

Hinweisfenster

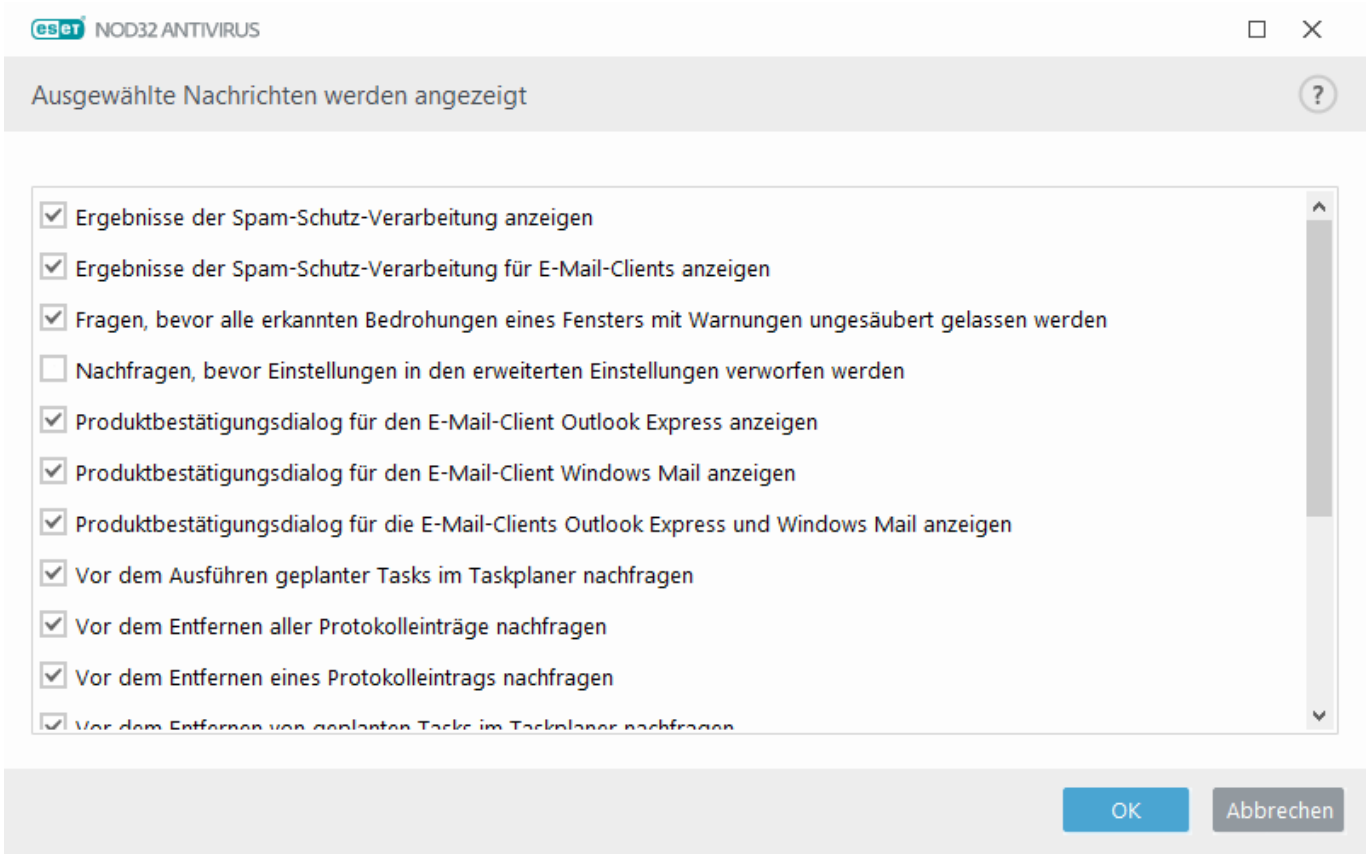
Um Hinweisfenster nach einer bestimmten Zeit automatisch zu schließen, aktivieren Sie die Option **Hinweisfenster automatisch schließen**. Die Hinweisfenster verschwinden nach Ablauf der festgelegten Zeit automatisch, wenn sie nicht manuell geschlossen wurden.

Zeitüberschreitung in Sekunden – Legen Sie die Anzeigedauer für Warnungen fest. Der Wert muss zwischen 10 und 999 Sekunden liegen.

Bestätigungsnachrichten – Klicken Sie auf **Bearbeiten**, um eine Liste mit Bestätigungsnachrichten anzuzeigen, die Sie ein- oder ausblenden können.

Bestätigungsnachrichten

Navigieren Sie zum Anpassen der Bestätigungsnachrichten zu **Erweiterte Einstellungen** (F5) > **Benachrichtigungen** > **Interaktive Warnungen**, und klicken Sie auf **Bearbeiten** neben **Bestätigungsnachrichten**.



In diesem Dialogfeld werden Bestätigungsmeldungen angezeigt, die von ESET NOD32 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.

Weitere Informationen zu bestimmten Funktionen in Bezug auf Bestätigungsnachrichten:

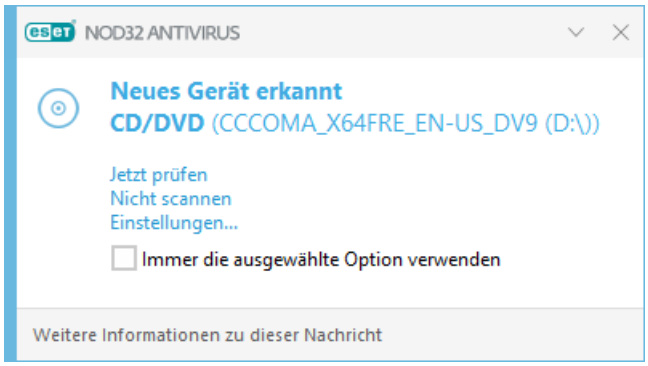
- Vor dem Löschen von ESET SysInspector-Log-Dateien nachfragen
- Vor dem Löschen aller ESET SysInspector-Log-Dateien nachfragen
- Vor dem Löschen von Objekten aus der Quarantäne nachfragen
- Nachfragen, bevor Einstellungen in den erweiterten Einstellungen verworfen werden
- Fragen, bevor alle erkannten Bedrohungen eines Fensters mit Warnungen ungesäubert gelassen werden
- Vor dem Entfernen eines Protokolleintrags nachfragen
- Vor dem Entfernen von geplanten Tasks im Taskplaner nachfragen
- Vor dem Entfernen aller Protokolleinträge nachfragen
- Vor dem Zurücksetzen von Statistiken nachfragen

- Vor dem Wiederherstellen eines Objekts aus der Quarantäne nachfragen
- Vor dem Wiederherstellen von Objekten aus der Quarantäne und dem Ausschluss von Scans nachfragen
- Vor dem Ausführen geplanter Tasks im Taskplaner nachfragen
- Produktbestätigungsdialog für die E-Mail-Clients Outlook Express und Windows Mail anzeigen
- Produktbestätigungsdialog für den E-Mail-Client Windows Mail anzeigen
- Produktbestätigungsdialog für den E-Mail-Client Outlook Express anzeigen

Wechselmedien

ESET NOD32 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 NOD32 Antivirus aktiviert ist und ein Wechselmedium eingelegt wird, wird der folgende Dialog angezeigt:



Optionen für dieses Dialogfeld:

- **Jetzt scannen** - Dies löst den Wechselmedienscan aus.
- **Nicht scannen** – Wechselmedien werden nicht gescannt.
- **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 NOD32 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.

Sie finden die Einstellungen für den Wechselmedien-Scan unter Erweiterte Einstellungen (**F5**) > **Erkennungsroutine** > **Malware-Scans** > **Wechselmedien**.

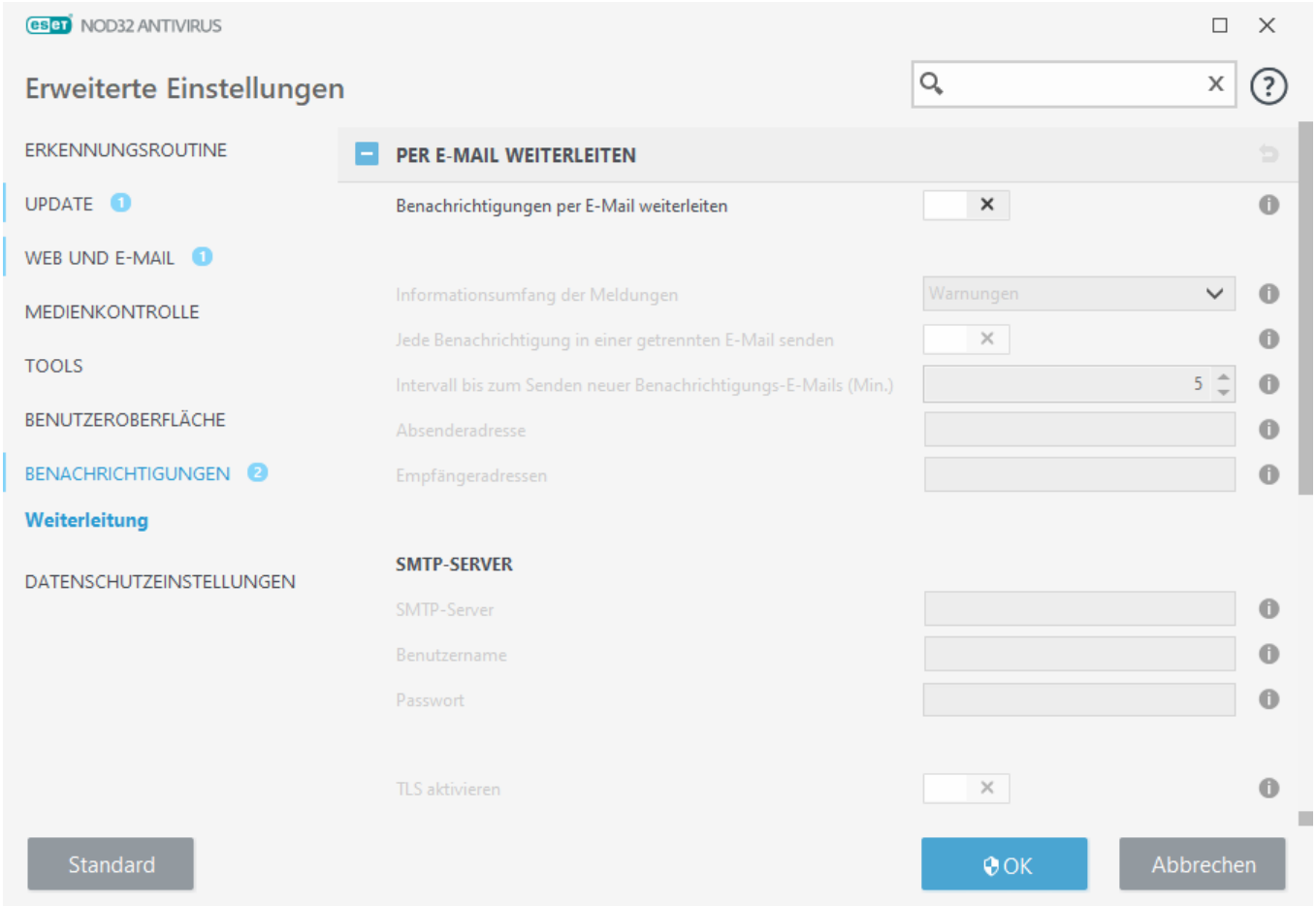
Aktion nach Einlegen von Wechselmedien - Wählen Sie die Aktion, die standardmäßig ausgeführt werden soll,

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**.

Weiterleitung

ESET NOD32 Antivirus kann automatisch Benachrichtigungs-E-Mails senden, wenn ein Ereignis mit dem ausgewählten Ausführlichkeitsgrad auftritt. Navigieren Sie zu **Erweiterte Einstellungen** (F5) > **Benachrichtigungen** > **Weiterleitung** und aktivieren Sie die Option **Benachrichtigungen per E-Mail weiterleiten**, um E-Mail-Benachrichtigungen zu erhalten.



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.

• **Kritisch** – Nur kritische Fehler (z. B. Fehler beim Start des Virenschutzes oder gefundene Bedrohungen) werden erfasst.

Jede Benachrichtigung in einer getrennten E-Mail senden – Wenn diese Option aktiviert ist, erhält der Empfänger für jede Benachrichtigung eine separate E-Mail. Dies kann dazu führen, dass innerhalb kurzer Zeit viele 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.

Absenderadresse – Geben Sie die Adresse an, die in Ereignismeldungen als Absender angezeigt werden sein soll.

Empfängeradressen – Geben Sie die Empfängeradressen an, die in Benachrichtigungs-E-Mailis als Empfänger angezeigt werden sein sollen. Sie können mehrere Werte eingeben. Sie können Semikolon „;“ als Trennzeichen benutzen.

SMTP server

SMTP-Server – Der SMTP-Server, über den Benachrichtigungen verschickt werden (z. B. smtp.provider.com:587, der Standardport ist 25).

ESET NOD32 Antivirus unterstützt SMTP-Server mit TLS-Verschlüsselung.

Benutzername und **Passwort** – Falls der SMTP-Server Authentifizierung erfordert, geben Sie hier einen gültigen Benutzernamen und das Passwort für den SMTP-Server ein.

TLS aktivieren - Warnungs- und Benachrichtigungs-E-Mails mit TLS-Verschlüsselung sichern.

SMTP-Verbindung testen - Eine Test-E-Mail wird an die E-Mail-Adresse des Empfängers gesendet. SMTP-Server, Benutzer, Passwort, Absenderadresse und Empfängeradressen müssen ausgefüllt werden.

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 verwenden ein vordefiniertes Standardformat. ESET empfiehlt, dieses Format nicht zu verändern. Unter bestimmten Umständen (wenn Sie beispielsweise ein automatisiertes E-Mail-Verarbeitungssystem verwenden) kann es jedoch erforderlich sein, 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 "?").

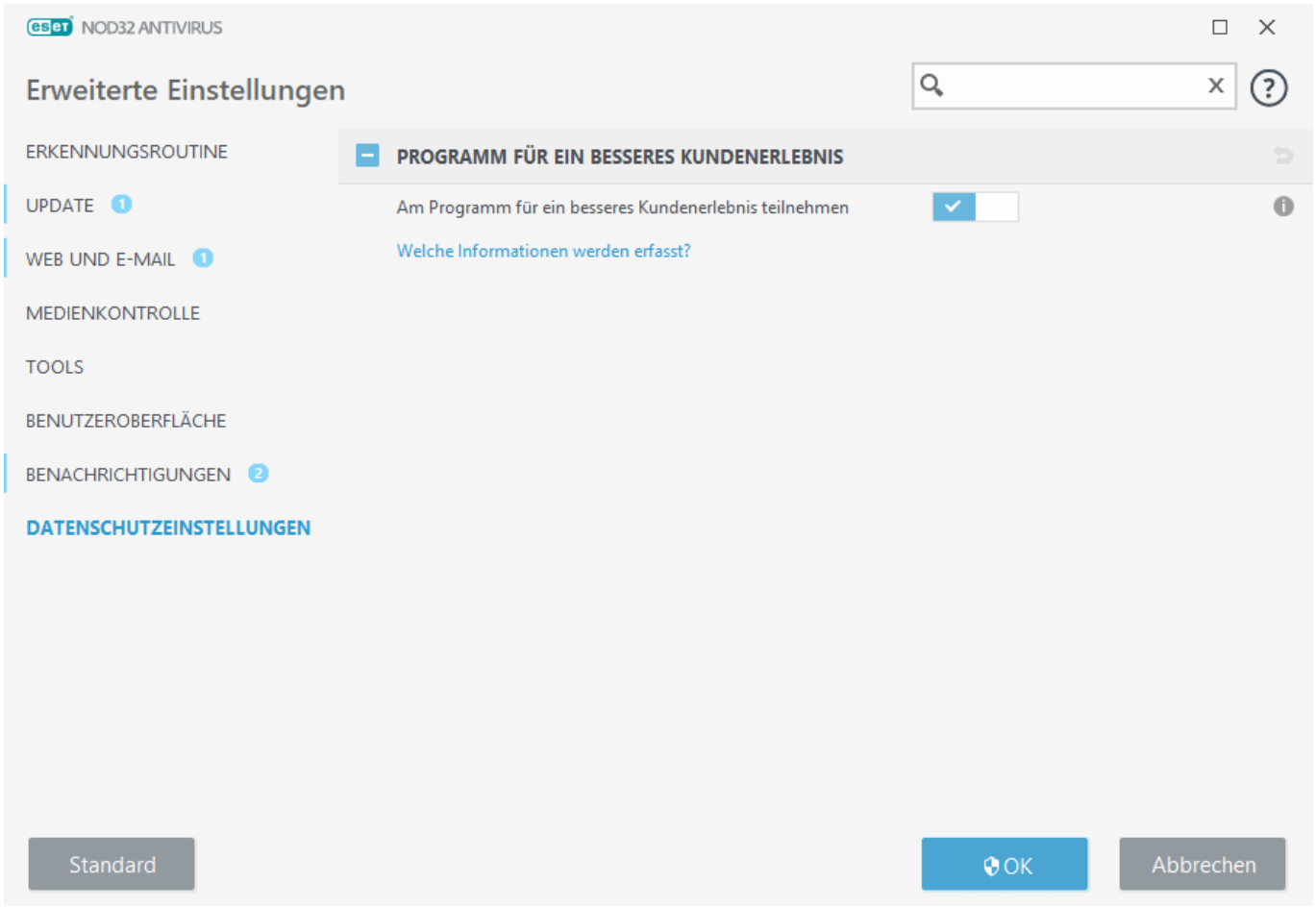
Quoted-Printable-Kodierung verwenden – Die E-Mail-Nachrichtenquelle wird in das Quoted-Printable-Format (QP) konvertiert, das ASCII-Zeichen verwendet und besondere regionale Zeichen in der E-Mail korrekt im 8-Bit-Format überträgt (áéíóú).

- **%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.

Datenschutzeinstellungen

Klicken Sie im Hauptprogrammfenster auf **Einstellungen** > **Erweiterte Einstellungen** (F5) > **Datenschutzeinstellungen**.



Programm für ein besseres Kundenerlebnis

Aktivieren Sie den Schieberegler neben **Am Programm für ein besseres Kundenerlebnis teilnehmen**, um dem Programm beizutreten. Mit Ihrer Teilnahme stellen Sie ESET anonyme Informationen zur Nutzung der ESET Produkte bereit. Die gesammelten Daten helfen uns, das Erlebnis für Sie zu verbessern, und werden niemals an Dritte weitergegeben. Welche Informationen werden erfasst?

Profile

Der Profilmanager wird an zwei Stellen in ESET NOD32 Antivirus verwendet: in den Bereichen **On-Demand-Prüfung** und **Update**.

Computer-Scan

In ESET NOD32 Antivirus sind vier vordefinierte Scan-Profile verfügbar:

- **Smart-Scan** – Dies ist das standardmäßig verwendete erweiterte Scan-Profil. Das Smart-Scan-Profil verwendet die Smart-Optimierungstechnologie, um Dateien auszuschließen, die bei einem vorherigen Scan als sauber eingestuft und seit dem Scan nicht mehr geändert wurden. Auf diese Weise können Sie schnellere Scans mit minimalen Auswirkungen auf die Systemsicherheit ausführen.

- **Scan via Kontextmenüs** – Im Kontextmenü können Sie bei Bedarf beliebige Dateien scannen. Mit dem Profil „Scan via Kontextmenüs“ können Sie definieren, welche Scan-Konfiguration für die auf diese Weise gestarteten Scans verwendet werden soll.

- **Tiefen-Scan** – Das Tiefen-Scan-Profil verwendet standardmäßig keine Smart-Optimierung, daher werden mit diesem Profil keine Dateien von der Prüfung ausgeschlossen.

- **Computer-Scan** – Dies ist das Standardprofil, das bei standardmäßigen Computer-Scans verwendet wird.

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.

Nehmen wir an, Sie möchten Ihr eigenes Prüfprofil erstellen. Die Option **Computerprüfung** eignet sich in gewissem Maße, aber Sie möchten keine laufzeitkomprimierten Dateien oder potenziell unsichere Anwendungen prüfen. Außerdem möchten Sie die Option **Ereignis immer beheben** 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

Für die Navigation in ESET NOD32 Antivirus können Sie die folgenden Tastaturbefehle verwenden:

Tastaturbefehle	Aktion
F1	öffnet die Hilfeseiten
F5	öffnen Sie die erweiterten Einstellungen.

Tastaturbefehle	Aktion
Pfeil nach oben / Pfeil nach unten	Navigation zwischen Elementen von Dropdownmenüs
TAB	Zum nächsten GUI-Element in einem Fenster springen
Shift+TAB	Zum vorherigen GUI-Element in einem Fenster springen
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
ALT + Pfeil nach links	Zurück
ALT + Pfeil nach rechts	Weiter
ALT+Home	Zum Anfang

Sie können auch die Zurück- und Weiter-Maustasten für die Navigation verwenden.

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 NOD32 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 in Marketing-Nachrichten aktivieren – Alle Ereignisse im Zusammenhang mit Marketing-Nachrichten im Produkt aufzeichnen.

Erweitertes Logging für Scanner aktivieren – Alle Ereignisse erfassen, die beim Scannen von Dateien und Ordnern

mit Computer-Scans.

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 Logging für die aktivieren – Alle Ereignisse aufzeichnen, die in ESET LiveGrid® auftreten. Diese Aufzeichnungen helfen Entwicklern bei der Diagnose und Behebung von Problemen mit ESET LiveGrid®.

Erweitertes Logging für Dokumentenschutz aktivieren – Alle aufgetretenen Ereignisse in Dokumentenschutz aufzeichnen, um Diagnose und Fehlerbehebung zu erleichtern.

Erweitertes Logging für E-Mail-Client-Schutz aktivieren – Alle Ereignisse aufzeichnen, die im E-Mail-Client-Schutz und im Plug-In für E-Mail-Clients auftreten, um Diagnose und Fehlerbehebung zu erleichtern

Erweitertes Kernel-Logging aktivieren – Alle Ereignisse aufzeichnen, die im ESET-Kernel (ekrn) auftreten.

Erweitertes Logging für Lizenzierung aktivieren – Sämtliche Produktkommunikation zwischen ESET-Aktivierung oder ESET License Manager Servern aufzeichnen.

Speicherablaufverfolgung aktivieren – Alle Ereignisse erfassen, um den Entwicklern bei der Diagnose von Speicherlecks zu helfen.

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 Push-Messaging aktivieren – Alle Ereignisse aufzeichnen, die beim Push-Messaging auftreten.

Erweiterte Logging für Echtzeit-Dateischutz aktivieren – Alle Ereignisse erfassen, die beim Scannen von Dateien und Ordnern mit dem Echtzeit-Dateischutz auftreten.

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.

Die Log-Dateien befinden sich in *C:\ProgramData\ESET\ESET Security\Diagnostics*.

Technischer Support

Wenn Sie sich über ESET NOD32 Antivirus an den technischen ESET-Support wenden, können Sie Systemkonfigurationsdaten senden. Wählen Sie **Immer senden** im Dropdownmenü **Systemkonfigurationsdaten senden** aus, um die Daten automatisch zu senden, oder auf **Vor dem Senden nachfragen**, um vor dem Senden der Daten aufgefordert zu werden.

Import-/Export-Einstellungen

Über das Menü **Einstellungen** können Sie die .xml-Datei mit Ihrer benutzerdefinierten Konfiguration von ESET NOD32 Antivirus importieren und exportieren.

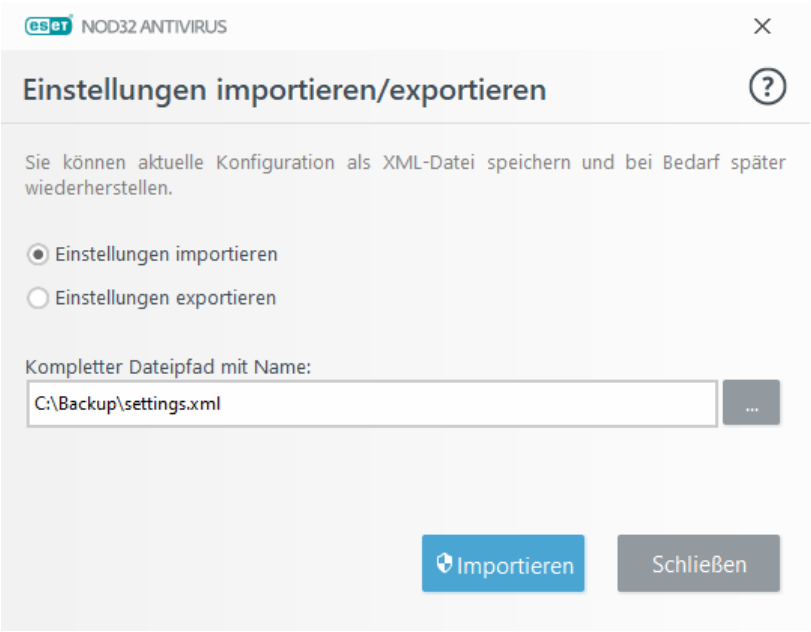
> **Illustrierte Anweisungen**
> Unter ESET-Konfigurationseinstellungen mit einer XML-Datei importieren oder exportieren finden Sie illustrierte Anweisungen in Englisch und weiteren Sprachen.

Das Importieren und Exportieren von Konfigurationsdateien ist sinnvoll, wenn Sie Ihre aktuelle ESET NOD32 Antivirus-Konfiguration für die Verwendung zu einem späteren Zeitpunkt sichern möchten. Die Option für die Exporteinstellungen eignet sich außerdem, wenn Sie Ihre vordefinierte Konfiguration auf mehreren Systemen verwenden möchten. Sie können eine .xml-Datei zum Übertragen dieser Einstellungen importieren.

Um eine Konfiguration zu importieren, klicken Sie im Hauptprogrammfenster auf **Einstellungen** > **Einstellungen importieren/exportieren** und wählen **Einstellungen importieren**. Geben Sie den Namen der Konfigurationsdatei ein, oder klicken Sie auf die Schaltfläche **...**, um nach der zu importierenden Datei zu suchen.

Um eine Konfiguration zu exportieren, klicken Sie im Hauptprogrammfenster auf **Einstellungen** > **Einstellungen importieren/exportieren**. Wählen Sie **Einstellungen exportieren**, und geben Sie den vollständigen Pfad mit dem Namen ein. Klicken Sie auf **...**, um zu einem Speicherort auf Ihrem Computer zu navigieren und die Konfigurationsdatei dort zu speichern.

> Beim Exportieren der Einstellungen kann ein Fehler auftreten, wenn Sie über unzureichende Berechtigungen für das angegebene Verzeichnis verfügen.



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.

Auf Standardeinstellungen zurücksetzen

Klicken Sie auf **Standard** in den **erweiterten Einstellungen** (F5), um die Programmeinstellungen für alle Module auf die Standardwerte zurückzusetzen. Alle Einstellungen werden auf die herstellerseitigen Standardwerte zurückgesetzt.

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.

Befehlszeilenscanner

Das Virenschutz-Modul von ESET NOD32 Antivirus kann über die Kommandozeile gestartet werden, entweder manuell (mit dem Befehl „ecls“) oder über eine Batch-Datei („.bat“).

Verwendung des ESET-Befehlszeilenscanners:

```
ecls [OPTIONS..] FILES..
```

Folgende Parameter und Switches stehen zur Verfügung, um die manuelle Prüfung über die Befehlszeile auszuführen:

Optionen

/base-dir=ORDNER	Module laden aus ORDNER
/quar-dir=ORDNER	Quarantäne-ORDNER
/exclude=MASK	Dateien, die mit der MASKE übereinstimmen, von Prüfungen ausschließen
/subdir	Unterordner scannen (Standard)
/no-subdir	Unterordner nicht scannen
/max-subdir-level=TIEFE	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

Option 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=MAXIMALE PRÜFDAUER	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` (Standard) – Es wird keine automatische Säuberung ausgeführt. • `standard` – „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

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 NOD32 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 NOD32 Antivirus-Konfigurationen über die Befehlszeile importieren und exportieren. Sie können diesen Vorgang manuell ausführen oder ein Skript für die Automatisierung erstellen.

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.

Befehl zum Exportieren von Einstellungen:
```
ecmd /getcfg c:\config\settings.xml
```

Befehl zum Importieren von Einstellungen:
```
ecmd /setcfg c:\config\settings.xml
```

Die erweiterten ecmd-Befehle können nur lokal ausgeführt werden.

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:

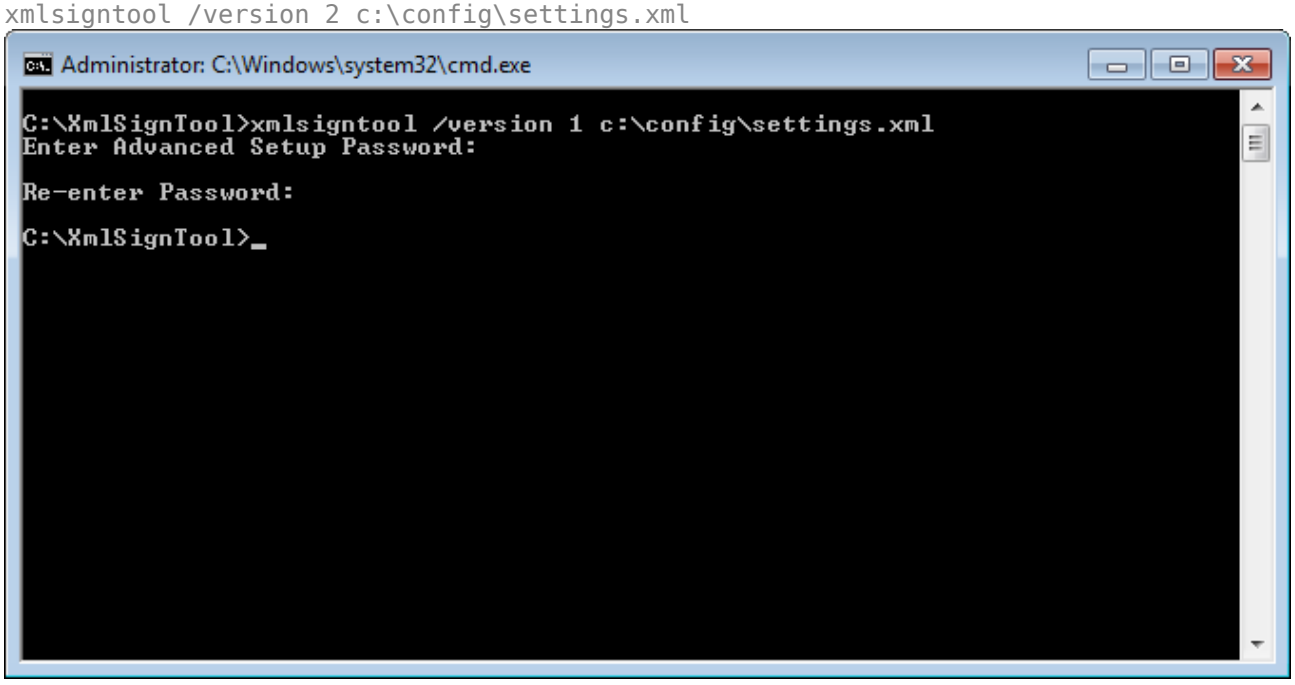
```
xmlsigntool /version 1|2 <xml_file_path>
```

Der Wert des Parameters `/version` hängt von Ihrer Version von ESET NOD32 Antivirus ab. Verwenden Sie `/version 1` für Versionen von ESET NOD32 Antivirus, die älter als 11.1 sind. Verwenden Sie `/version 2` für die aktuelle Version von ESET NOD32 Antivirus.

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 NOD32 Antivirus mit ESET CMD und der Passwortautorisierungsmethode importiert werden.

Befehl zum Signieren einer exportierten Konfigurationsdatei:

```
xmlsigntool /version 2 c:\config\settings.xml
```



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 NOD32 Antivirus erneut zu exportieren.

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.

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:

- **Bildschirm ausgeschaltet oder Bildschirmschoner**
- **Computersperre**
- **Benutzerabmeldung**

Aktivieren bzw. deaktivieren Sie die Auslöser für die Prüfung im Ruhezustand über die entsprechenden Schieberegler.

Häufig gestellte Fragen

Im folgenden Bereich werden einige der häufigsten Fragen und Probleme behandelt. Klicken Sie auf die jeweilige Themenüberschrift, um Hilfestellung bei der Lösung Ihres Problems zu erhalten:

- So aktualisieren Sie ESET NOD32 Antivirus
- So entfernen Sie einen Virus von Ihrem PC
- So erstellen Sie eine neue Aufgabe im Taskplaner
- So planen Sie einen regelmäßigen Scan-Task (wöchentlich)
- So entsperren Sie die erweiterten Einstellungen
- Beheben der Produktdeaktivierung in ESET HOME

Wenn Ihr Problem nicht in der obigen Liste aufgeführt ist, können Sie in der ESET NOD32 Antivirus Onlinehilfe danach suchen.

Wenn Sie keine Lösung für Ihr Problem bzw. Ihre Frage in der ESET NOD32 Antivirus Onlinehilfe finden, steht Ihnen auch unsere regelmäßig aktualisierte ESET Knowledgebase online zur Verfügung. Die folgende Liste enthält Links zu den beliebtesten Artikeln in unserer Knowledgebase:

- Lizenzverlängerung
- Bei der Installation meines ESET-Produkts ist ein Aktivierungsfehler aufgetreten. Was bedeutet das?
- Mein ESET Windows Home-Produkt mit Benutzernamen, Passwort oder Lizenzschlüssel aktivieren
- ESET Home-Produkt deinstallieren oder erneut installieren
- Ich wurde benachrichtigt, dass meine ESET-Installation vorzeitig abgebrochen wurde
- Was muss ich tun, nachdem ich meine Lizenz erneuert habe? (Benutzer der Home-Version)
- Was geschieht, wenn sich meine E-Mail-Adresse ändert?
- Mein ESET-Produkt auf einen neuen Computer oder ein neues Gerät übertragen
- Wie starte ich Windows im abgesicherten Modus bzw. abgesicherter Modus mit Netzwerk?
- Sichere Website von der Sperre ausschließen
- Zugriff auf die ESET GUI für Sprachausgabeprogramme erlauben

Bei Bedarf können Sie sich mit Ihren Fragen und Problemen auch direkt an unseren technischen Support wenden.

So aktualisieren Sie ESET NOD32 Antivirus

Die Aktualisierung von ESET NOD32 Antivirus kann manuell oder automatisch erfolgen. Um eine Aktualisierung zu starten, klicken Sie im Hauptprogrammfenster auf **Update** und dann auf **Jetzt aktualisieren**.

Bei der Standardinstallation wird stündlich ein automatisches Update ausgeführt. Wenn Sie diesen Zeitabstand ändern möchten, navigieren Sie zu **Tools** > **Taskplaner**.

So entfernen Sie einen Virus von Ihrem PC

Wenn Ihr Computer die Symptome einer Infektion mit Schadsoftware aufweist (Computer arbeitet langsamer als gewöhnlich, hängt sich oft auf usw.), sollten Sie folgendermaßen vorgehen:

1. Klicken Sie im Hauptfenster auf **Computer prüfen**.

2. Klicken Sie auf **Scannen Sie Ihren Computer**, 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

Um einen neuen Task zu erstellen, klicken Sie unter **Tools** > **Taskplaner** auf **Hinzufügen**, oder klicken Sie mit der rechten Maustaste und wählen Sie 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 (Stunden)** 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 eine regelmäßige Prüfung 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. Geben Sie einen Namen für den Task ein und wählen Sie im Dropdownmenü **Tasktyp** die Option **On-Demand-Computer-Scan** aus.
3. Wählen Sie **Wöchentlich** als 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 entsperren Sie die passwortgeschützten erweiterten Einstellungen

Wenn Sie versuchen, die geschützten erweiterten Einstellungen zu öffnen, wird ein Fenster zur Eingabe des Passworts angezeigt. Falls Sie Ihr Passwort vergessen oder verloren haben, klicken Sie unten auf **Passwort wiederherstellen**, und geben Sie die E-Mail-Adresse ein, die Sie bei der Registrierung dieser Lizenz verwendet haben. ESET schickt Ihnen eine E-Mail mit dem Überprüfungscode. Geben Sie den Überprüfungscode ein, geben Sie Ihr neues Passwort ein, und bestätigen Sie es anschließend. Der Überprüfungscode ist sieben Tage lang gültig.

Passwort über Ihr ESET HOME-Konto wiederherstellen – Verwenden Sie diese Option, wenn die Lizenz, die für die Aktivierung verwendet wird, mit Ihrem ESET HOME-Konto verknüpft ist. Geben Sie die E-Mail-Adresse ein, die Sie für die Anmeldung bei Ihrem ESET HOME-Konto verwenden.

Falls Sie Ihre E-Mail-Adresse vergessen oder Probleme beim Wiederherstellen des Passworts haben, klicken Sie auf **Technischen Support kontaktieren**. Sie werden zur ESET-Website weitergeleitet, um unseren technischen Support zu kontaktieren.

Code für den technischen Support generieren – Mit dieser Option wird ein Code für den technischen Support generiert. Kopieren Sie den durch den technischen Support bereitgestellten Code, und klicken Sie auf **Ich habe einen Überprüfungscode**. Geben Sie den Überprüfungscode ein, erstellen Sie ein neues Passwort, und bestätigen Sie es. Der Überprüfungscode ist sieben Tage lang gültig.

Weitere Informationen finden Sie unter Passwort für Einstellungen in ESET Windows Home-Produkten entsperren.

Beheben der Produktdeaktivierung in ESET HOME

Produkt nicht aktiviert

Diese Fehlermeldung wird angezeigt, wenn der Lizenzinhaber Ihr ESET NOD32 Antivirus im ESET HOME-Portal deaktiviert oder die mit Ihrem ESET HOME-Benutzerkonto geteilte Lizenz nicht mehr mit Ihnen geteilt wird. So beheben Sie dieses Problem:

- Klicken Sie auf **Aktivieren** und verwenden Sie eine der Aktivierungsmethoden, um ESET NOD32 Antivirus zu aktivieren.
- Wenden Sie sich an den Lizenzinhaber mit der Information, dass Ihr ESET NOD32 Antivirus vom Lizenzinhaber deaktiviert wurde oder dass die Lizenz nicht mehr mit Ihnen geteilt wird. Der Inhaber kann das Problem im ESET HOME beheben.

Produkt deaktiviert, Geräteverbindung getrennt

Diese Fehlermeldung wird angezeigt, wenn Sie ein Gerät aus dem ESET HOME entfernen. So beheben Sie dieses Problem:

- Klicken Sie auf **Aktivieren** und verwenden Sie eine der Aktivierungsmethoden, um ESET NOD32 Antivirus zu aktivieren.

• Wenden Sie sich an den Lizenzinhaber mit der Information, dass Ihr ESET NOD32 Antivirus deaktiviert und das Gerät von ESET HOME getrennt wurde.

• Falls Sie der Lizenzinhaber sind und Ihnen diese Änderungen nicht bekannt waren, überprüfen Sie Ihren Aktivitäts-Feed im ESET HOME. Falls Sie verdächtige Aktivitäten feststellen, ändern Sie das Passwort für Ihr ESET HOME-Benutzerkonto und wenden Sie sich an den technischen ESET-Support.

Produkt deaktiviert, Geräteverbindung getrennt

Diese Fehlermeldung wird angezeigt, wenn Sie ein Gerät aus dem ESET HOME entfernen. So beheben Sie dieses Problem:

• Klicken Sie auf **Aktivieren** und verwenden Sie eine der Aktivierungsmethoden, um ESET NOD32 Antivirus zu aktivieren.

• Wenden Sie sich an den Lizenzinhaber mit der Information, dass Ihr ESET NOD32 Antivirus deaktiviert und das Gerät von ESET HOME getrennt wurde.

• Falls Sie der Lizenzinhaber sind und Ihnen diese Änderungen nicht bekannt waren, überprüfen Sie Ihren Aktivitäts-Feed im ESET HOME. Falls Sie verdächtige Aktivitäten feststellen, ändern Sie das Passwort für Ihr ESET HOME-Benutzerkonto und wenden Sie sich an den technischen ESET-Support.

Produkt nicht aktiviert

Diese Fehlermeldung wird angezeigt, wenn der Lizenzinhaber Ihr ESET NOD32 Antivirus im ESET HOME-Portal deaktiviert oder die mit Ihrem ESET HOME-Benutzerkonto geteilte Lizenz nicht mehr mit Ihnen geteilt wird. So beheben Sie dieses Problem:

• Klicken Sie auf **Aktivieren** und verwenden Sie eine der Aktivierungsmethoden, um ESET NOD32 Antivirus zu aktivieren.

• Wenden Sie sich an den Lizenzinhaber mit der Information, dass Ihr ESET NOD32 Antivirus vom Lizenzinhaber deaktiviert wurde oder dass die Lizenz nicht mehr mit Ihnen geteilt wird. Der Inhaber kann das Problem im ESET HOME beheben.

Programm für ein besseres Kundenerlebnis

Mit Ihrer Teilnahme am Programm für ein besseres Kundenerlebnis stellen Sie ESET anonyme Informationen zur Nutzung unserer Produkte bereit. Weitere Informationen zur Datenverarbeitung finden Sie in unserer Datenschutzerklärung.

Ihre Zustimmung

Die Teilnahme am Programm ist freiwillig und erfolgt nur nach Ihrer Zustimmung. Nach der Zustimmung erfolgt die eigentliche Teilnahme passiv, Sie müssen also keine weiteren Aktionen ausführen. Sie können Ihre Zustimmung in den Produkteinstellungen jederzeit widerrufen. Wenn Sie Ihre Zustimmung widerrufen, dürfen wir Ihre anonymen Daten nicht weiter verarbeiten.

Sie können Ihre Zustimmung in den Produkteinstellungen jederzeit widerrufen:

- Ändern der Einstellung für das Programm für ein besseres Kundenerlebnis in ESET Windows Home-Produkten

Welche Arten von Informationen erfassen wir?

Daten zur Interaktion mit dem Produkt

Diese Informationen teilen uns mit, wie unsere Produkte verwendet werden. Wir können beispielsweise erkennen, welche Funktionen häufig verwendet werden, welche Einstellungen die Benutzer anpassen und wie viel Zeit sie mit der Nutzung des Produkts verbringen.

Daten zu Geräten

Anhand dieser Informationen können wir erkennen, wo und auf welchen Geräten unsere Produkte eingesetzt werden. Typische Beispiele sind Gerätemodell, Land, Version und Name des Betriebssystems.

Fehlerdiagnosedaten

Informationen zu Fehlern und Abstürzen werden ebenfalls gesammelt. Mögliche Beispiele sind die Art des Fehlers und die Aktionen, die ihn verursacht haben.

Warum erfassen wir diese Informationen?

Mit diesen anonymen Informationen können wir das Produkt für Sie, unsere Benutzer, verbessern. Wir möchten Ihnen ein möglichst relevantes, benutzerfreundliches und fehlerfreies Produkt anbieten.

Wer verarbeitet diese Informationen?

Die bei diesem Programm gesammelten Daten werden ausschließlich durch ESET, spol. s r.o. verarbeitet. Die Informationen werden nicht an externe Parteien weitergegeben.

Endbenutzer-Lizenzvereinbarung

Gültig ab dem 19. Oktober 2021.

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 ERKENNEN DIE DATENSCHUTZERKLÄRUNG AN.**

Endbenutzer-Lizenzvereinbarung

Diese Endbenutzer-Lizenzvereinbarung (die "Vereinbarung") zwischen ESET, spol. s r. o., mit Sitz in Einsteinova 24, 85101 Bratislava, Slovak Republic, Handelsregistereintrag 3586/B in der Rubrik Sro beim Amtsgericht Bratislava I, Firmennummer 31333532, ("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 und akzeptieren die Datenschutzerklärung. Wenn Sie mit einer der Bestimmungen dieser Vereinbarung und/oder der Datenschutzerklärung 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 sich mit dieser Vereinbarung einverstanden erklärt 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; oder (ii) wenn sich der Umfang einer Lizenz nach der Anzahl von Postfächern richtet, ist ein Endbenutzer ein Computerbenutzer, der E-Mails 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) **Home/Business Edition.** Die Home Edition der Software darf ausschließlich in privaten und/oder nichtkommerziellen Umgebungen für den Haus- und Familiengebrauch eingesetzt werden. Für die Verwendung der Software in kommerziellen Umgebungen sowie 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.** Als „OEM“ klassifizierte Software darf ausschließlich auf dem Computer genutzt werden, mit dem sie ausgeliefert wurde. 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“) oder Upgrades bereitzustellen, ist dazu 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 Datenschutzerklärung.

Die Bereitstellung von Updates unterliegt möglicherweise der End-of-Life-Richtlinie („EOL-Richtlinie“), die auf https://go.eset.com/eol_home verfügbar ist. Nachdem die Software oder eine ihrer Funktionen das in der EOL-Policy festgelegte End-of-Life-Datum erreicht hat, werden keine Aktualisierungen mehr bereitgestellt.

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 ("Infiltrationen"). Diese Daten werden zusammen mit Informationen über den Installationsprozess, den Computer und/oder die Plattform, auf der die Software installiert ist und Informationen über Betrieb und Funktionsweise der Software ("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.

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. Ihr Recht zur Nutzung der Software und deren Funktionen unterliegt möglicherweise einer EOL-Richtlinie. Wenn die Software oder deren Funktionen das in der EOL-Richtlinie definierte Ende des Lebenszyklus erreichen, erlischt Ihr Nutzungsrecht für die Software. 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 INSTALLATION, 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. Nachdem die Software oder eine ihrer Funktionen das in der EOL-Policy festgelegte End-of-Life-Datum erreicht hat, wird kein technischer Support mehr bereitgestellt. 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 („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

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.

(die in den Punkten i und ii genannten Gesetze zusammengefasst als „Handelskontrollgesetze“).

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, 85101 Bratislava, Slovak Republic. ESET behält sich das Recht vor, Sie über alle Änderungen an dieser Vereinbarung, der Datenschutzerklärung, der EOL-Richtlinie und der Dokumentation gemäß Art. 22 der Vereinbarung zu informieren. ESET kann Ihnen E-Mails oder In-App-Benachrichtigungen über die Software schicken oder die Kommunikation auf unserer Website veröffentlichen. Sie stimmen zu, rechtliche Mitteilungen von ESET in elektronischer Form zu erhalten, inklusive Mitteilungen zu Änderungen an Bedingungen, Sonderbedingungen oder Datenschutzerklärungen, Benachrichtigungen oder Einladungen zu Vertragsverlängerungen, Kündigungen oder andere rechtliche Mitteilungen. Diese elektronische Kommunikation gilt als schriftlich empfangen, sofern nicht durch geltendes Recht eine andere Kommunikationsform vorgeschrieben ist.

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. Diese Vereinbarung wird auf Englisch getroffen. Falls eine Übersetzung der Vereinbarung aus Gründen der Annehmlichkeit bereitgestellt wird, sind die Bestimmungen der englischen Version maßgeblich, falls Abweichungen bestehen.

ESET behält sich das Recht vor, Änderungen an der Software vorzunehmen und die Bestimmungen dieser Vereinbarung, deren Anhänge und Ergänzungen, die Datenschutzerklärung, die EOL-Richtlinie und die Dokumentation ganz oder in Teilen jederzeit zu ändern, indem das entsprechende Dokument aktualisiert wird, (i) um Änderungen an der Software oder der Funktionsweise von ESET zu berücksichtigen, (ii) aus rechtlichen, regulatorischen oder Sicherheitsgründen oder (iii) um Missbrauch oder Schaden zu verhindern. Bei Änderungen an dieser Vereinbarung werden Sie per E-Mail, per In-App-Benachrichtigung oder über andere elektronische Kommunikationsformen informiert. Wenn Sie den Änderungen der Vereinbarung nicht zustimmen, können Sie diese gemäß Artikel 10 innerhalb von 30 Tagen nach Erhalt der Änderungsbenachrichtigung kündigen. Sofern Sie die Vereinbarung nicht innerhalb dieser Frist kündigen, gelten die Änderungen als von Ihnen akzeptiert und wirksam ab dem Tag, an dem Sie die Änderungsbenachrichtigung erhalten haben.

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.

ANHANG ZUR VEREINBARUNG

Sicherheitsanalyse für mit dem Netzwerk verbundene Geräte. Zur Sicherheitsanalyse für mit dem Netzwerk verbundene Geräte gelten die folgenden zusätzlichen Bestimmungen:

Die Software enthält eine Funktion zum Überprüfen der Sicherheit des lokalen Netzwerks des Endbenutzers und der Sicherheit der Geräte im lokalen Netzwerk. Diese Funktion benötigt den Namen des lokalen Netzwerks und Informationen über die Geräte im Netzwerk, inklusive Vorhandensein, Typ, Name, IP-Adresse und MAC-Adresse der Geräte im lokalen Netzwerk zusammen mit Lizenzinformationen. Diese Informationen umfassen außerdem dem drahtlosen Sicherheitstyp und den Verschlüsselungstyp für Routergeräte. Diese Funktion liefert unter Umständen auch Informationen zur Verfügbarkeit von Sicherheitssoftwarelösungen zum Schutz von Geräten im lokalen Netzwerk.

Schutz vor dem Missbrauch von Daten. Zum Schutz vor dem Missbrauch von Daten gelten die folgenden zusätzlichen Bestimmungen:

Die Software enthält eine Funktion, die im direkten Zusammenhang mit dem Diebstahl eines Computers vor dem Verlust oder Missbrauch kritischer Daten schützt. Diese Funktion ist in den Standardeinstellungen der Software deaktiviert. Sie müssen ein ESET HOME-Konto erstellen, um die Funktion aktivieren und bei einem Diebstahl des Computers die Datensammlung aktivieren zu können. Wenn Sie diese Funktion der Software aktivieren, willigen Sie ein, dass Daten über den gestohlenen Computer an den Anbieter gesendet werden. Diese Daten (nachfolgend zusammenfassend als „die Daten“ bezeichnet) können Folgendes umfassen: Angaben zum Netzwerkstandort des Computers; Daten zu den auf dem Bildschirm angezeigten Inhalten; Daten zur Konfiguration des Computers; Daten, die mit einer an den Computer angeschlossenen Kamera aufgezeichnet werden. Der Endbenutzer darf Daten, die mithilfe dieser Funktion erhalten und über das ESET HOME-Konto zur Verfügung gestellt werden, ausschließlich zur Schadensminderung nach dem Diebstahl des Computers nutzen. Weiterhin erteilt er dem Anbieter alle gemäß der Datenschutzerklärung und gemäß geltendem Recht erforderlichen Zustimmungen zur Verarbeitung der Daten. Der Anbieter gestattet dem Endbenutzer, auf die Daten so lange zuzugreifen, wie dies zur Erreichung des Erfassungszwecks erforderlich ist. Dieser Zeitraum darf die in der Datenschutzrichtlinie genannte Aufbewahrungsfrist nicht überschreiten. Der Schutz vor dem Missbrauch von Daten darf ausschließlich für Computer und Konten verwendet werden, auf die der Endbenutzer rechtmäßigen Zugriff hat. Jegliche unrechtmäßige Verwendung wird den zuständigen Behörden gemeldet. Der Anbieter befolgt die entsprechenden anwendbaren Vorschriften und unterstützt die Behörden im Falle eines Missbrauchs. Sie erkennen an, dass Sie für den Schutz des Passworts für das ESET HOME-Konto verantwortlich sind, und stimmen zu, das Passwort nicht an Drittparteien weiterzugeben. Der Endbenutzer ist für sämtliche autorisierten und nicht autorisierten Aktivitäten im Zusammenhang mit der Funktion zum Schutz vor dem Missbrauch von Daten und dem ESET HOME-Konto verantwortlich. Benachrichtigen Sie den Anbieter unverzüglich, falls Ihr ESET HOME-Konto kompromittiert wurde. Die zusätzlichen Bestimmungen zum Schutz vor dem Missbrauch von Daten gelten ausschließlich für Endbenutzer von ESET Internet Security und ESET Smart Security Premium.

ESET Secure Data. Für ESET Secure Data gelten die folgenden zusätzlichen Bestimmungen:

1. Definitionen. In diesen zusätzlichen Bestimmungen für ESET Secure Data haben die nachstehenden Begriffe die folgende Bedeutung:

a) "Informationen" Alle Informationen oder Daten, die mit der Software ver- oder entschlüsselt werden;

b) „Produkte“ESET Secure Datadie Software und die Dokumentation;

"ESET Secure Data" Die Software, die zum Ver- und Entschlüsseln elektronischer Daten verwendet wird;

Bei Verwendung des Plurals ist auch der Singular eingeschlossen und bei Verwendung des Maskulinums sind auch das Femininum und das Neutrum eingeschlossen und umgekehrt. Worte ohne spezifische Definition werden gemäß der Definitionen in der Vereinbarung verwendet.

2. Zusätzliche Endbenutzer-Erklärung. Sie bestätigen und akzeptieren Folgendes:

a) Sie sind für Schutz, Erhalt und Sicherung von Daten verantwortlich;

b) Sie sollten alle Informationen und Daten (insbesondere solche von kritischer Natur) vor der Installation von ESET Secure Data auf Ihrem Computer komplett sichern;

c) Sie müssen Passwörter und andere für Einrichtung und Nutzung von ESET Secure Data erforderliche Daten sicher aufbewahren und Sicherungskopien aller Verschlüsselungsschlüssel, Lizenzcodes, Schlüsseldateien und anderer Daten auf separaten Speichermedien erstellen;

d) Sie sind für die Nutzung der Produkte verantwortlich. Der Anbieter übernimmt keinerlei Haftung für Verluste, Forderungen oder Schäden durch die unbefugte oder fälschliche Verschlüsselung oder Entschlüsselung von Informationen und Daten, ganz gleich, wo und auf welche Weise diese Informationen oder Daten gespeichert wurden;

e) Obwohl der Anbieter alle angemessenen Schritte unternommen hat, um die Integrität und Sicherheit von ESET Secure Data zu gewährleisten, dürfen die Produkte nicht in Bereichen verwendet werden, die von einem ausfallsicheren Sicherheitsniveau abhängen oder potenziell gefährlich oder riskant sind. Dazu gehören insbesondere kerntechnische Anlagen, Flugzeugnavigations-, -steuerungs- oder -kommunikationssysteme, Waffen- oder Verteidigungssysteme und Lebenserhaltungs- oder Überwachungssysteme;

f) Der Endbenutzer muss sicherstellen, dass die von den Produkten bereitgestellte Sicherheits- und Verschlüsselungsebene den jeweiligen Anforderungen entspricht;

g) Sie sind für die Verwendung aller oder eines Teils der Produkte und insbesondere dafür verantwortlich, sicherzustellen, dass die Verwendung im Rahmen aller geltenden Gesetze und Bestimmungen der Slowakischen Republik bzw. des jeweiligen Landes, der Region bzw. des Staats erfolgt, in dem das Produkt verwendet wird; Sie müssen sich vor Verwendung der Produkte vergewissern, dass Sie gegen kein von einer Regierung (in der Slowakischen Republik oder am jeweiligen Einsatzort) verhängtes Embargo verstoßen;

h) ESET Secure Data kontaktiert die Server des Anbieters in regelmäßigen Abständen, um Lizenzinformationen, verfügbare Patches, Service Packs und andere Updates zu überprüfen, mit denen der allgemeine Betrieb von ESET Secure Data verbessert, gewartet, modifiziert oder erweitert wird, und kann dabei allgemeine Systeminformationen im Zusammenhang mit der Funktionsweise der Software gemäß der Datenschutzrichtlinie übertragen.

i) Der Anbieter ist nicht verantwortlich für Verlust, Schäden, Kosten oder Forderungen, die infolge von Verlust, Diebstahl, Missbrauch, Zerstörung oder Beschädigung von Passwörtern, Setupdaten, Verschlüsselungsschlüsseln, Lizenzaktivierungscodes und anderer bei der Nutzung der Software generierten oder gespeicherten Daten entstehen.

Die zusätzlichen Bestimmungen für ESET Secure Data gelten ausschließlich für Endbenutzer von ESET Smart Security Premium.

Password Manager Software. Zur Password Manager-Software gelten die folgenden zusätzlichen Bestimmungen:

1. Zusätzliche Endbenutzer-Erklärung. Sie bestätigen und akzeptieren, dass Sie nicht dazu berechtigt sind:

a) Einsatz der Password Manager-Software für den Betrieb missionskritischer Anwendungen, bei denen

Menschenleben oder Besitztümer auf dem Spiel stehen. Sie erkennen an, dass die Password Manager-Software nicht für solche Zwecke geeignet ist und dass ein Defekt in diesen Fällen zu Tod, Verletzungen oder schweren Eigentums- oder Umweltschäden führen kann, für die der Anbieter nicht verantwortlich ist.

DIE PASSWORD MANAGER-SOFTWARE WURDE NICHT FÜR GEFÄHRLICHE UMGEBUNGEN ENTWICKELT, AUSGERICHTET ODER LIZENZIERT, IN DENEN AUSFALLSCHUTZMASSNAHMEN ERFORDERLICH SIND. DAZU GEHÖREN OHNE EINSCHRÄNKUNG TÄTIGKEITEN WIE PLANUNG, BAU, WARTUNG ODER BETRIEB NUKLEARER EINRICHTUNGEN, NAVIGATIONS- ODER KOMMUNIKATIONSSYSTEME IM FLUGVERKEHR, IN DER LUFTFAHRTKONTROLLE, SOWIE LEBENSERHALTUNGS- ODER WAFFENSYSTEME. DER ANBIETER LEHNT AUSDRÜCKLICH JEGLICHE IMPLIZITE GARANTIE ODER ZWECKTAUGLICHKEIT FÜR DIESE ANWENDUNGEN AB.

b) Die Password Manager-Software auf eine Art und Weise zu nutzen, die diese Vereinbarung, die Gesetze der Slowakischen Republik bzw. des jeweiligen Einsatzorts verletzt. Die Password Manager-Software darf insbesondere nicht dazu eingesetzt werden, illegale Aktivitäten durchzuführen oder zu bewerben, inklusive des Uploads von Daten oder schädlichen Inhalten oder Inhalten, die für illegale Aktivitäten genutzt werden können oder die Gesetze oder die Rechte von Drittparteien (inklusive des Rechts am geistigen Eigentum) verletzen. Dazu gehören (jedoch nicht ausschließlich) Versuche, Zugriff auf Speicherkonten zu erlangen („Speicher“ bezieht sich in diesen zusätzlichen Bestimmungen für die Password Manager-Software auf den vom Anbieter oder einem Drittanbieter und dem Benutzer zur Bereitstellung der Synchronisierung und Sicherung von Benutzerdaten verwalteten Datenspeicher) oder anderen Konten und Daten von anderen Benutzern der Password Manager-Software oder des Speichers. Wenn Sie eine dieser Bestimmungen verletzen, kann der Anbieter diese Vereinbarung unverzüglich beenden und die Kosten für Abhilfemaßnahmen an Sie weitergeben und kann alle notwendigen Schritte ergreifen, um zu verhindern, dass Sie die Password Manager-Software weiterhin verwenden, ohne dass daraus ein Anrecht auf eine Rückerstattung entsteht.

2. HAFTUNGSAUSSCHLUSS. DIE PASSWORD MANAGER-SOFTWARE WIRD IM IST-ZUSTAND UND OHNE AUSDRÜCKLICHE ODER KONKLUDENTE GEWÄHRLEISTUNG BEREITGESTELLT. DIE NUTZUNG DER SOFTWARE ERFOLGT AUF IHR EIGENES RISIKO. DER ANBIETER HAFTET NICHT FÜR DATENVERLUSTE, SCHÄDEN, EINGESCHRÄNKTE DIENSTVERFÜGBARKEIT INKLUSIVE ALLER DATEN, DIE VON DER PASSWORD MANAGER-SOFTWARE FÜR SYNCHRONISIERUNG ODER SICHERUNG AN EXTERNE SPEICHERMEDIEN GESCHICKT WERDEN. DIE VERSCHLÜSSELUNG DER DATEN MIT DER PASSWORD MANAGER-SOFTWARE IMPLIZIERT KEINERLEI HAFTUNG DES ANBIETERS HINSICHTLICH DER SICHERHEIT DIESER DATEN. SIE STIMMEN AUSDRÜCKLICH ZU, DASS DIE MIT DER PASSWORD MANAGER-SOFTWARE ERFASSTEN, VERWENDETEN, VERSCHLÜSSELTEN, GESPEICHERTEN, SYNCHRONISIERTEN ODER VERSCHICKTEN DATEN AUCH AUF EXTERNEN SERVERN GESPEICHERT WERDEN DÜRFEN (GILT NUR FÜR DIE NUTZUNG DER PASSWORD MANAGER-SOFTWARE MIT AKTIVIERTEN SYNCHRONISIERUNGS- UND SICHERUNGSDIENSTEN). WENN DER ANBIETER NACH EIGENEM ERMESSEN EINEN SOLCHEN EXTERNEN DATENSPEICHER, EINE WEBSEITE, EIN WEBPORTAL, EINEN SERVER ODER EINEN DIENST AUSWÄHLT, HAFTET DER ANBIETER NICHT FÜR QUALITÄT, SICHERHEIT ODER VERFÜGBARKEIT DIESER EXTERNEN DIENSTE ODER FÜR VERTRAGS- ODER RECHTSVERLETZUNGEN DURCH DIE EXTERNEN ANBIETER ODER FÜR SCHÄDEN, ENTGANGENE PROFITE, FINANZIELLE ODER NICHTFINANZIELLE SCHÄDEN ODER SONSTIGE ARTEN VON VERLUSTEN BEIM EINSATZ DIESER SOFTWARE. DER ANBIETER HAFTET NICHT FÜR DEN INHALT VON DATEN, DIE MIT DER PASSWORD MANAGER-SOFTWARE ODER IM SPEICHER ERFASST, VERWENDET, VERSCHLÜSSELT, GESPEICHERT, SYNCHRONISIERT ODER VERSCHICKT WERTEN. SIE ERKENNEN AN, DASS DER ANBIETER KEINEN ZUGANG ZUM INHALT DER GESPEICHERTEN DATEN HAT UND DAHER GESETZLICH VERBOTENE INHALTE NICHT ÜBERWACHEN ODER ENTFERNEN KANN.

Sämtliche Verbesserungen, Upgrades und Fehlerkorrekturen an der Password MANAGER-Software ("Verbesserungen") sind das alleinige Eigentum des Anbieters, selbst wenn diese Verbesserungen anhand von Feedback, Ideen oder Vorschlägen erstellt wurden, die in irgendeiner Form von Ihnen eingereicht wurden. Sie haben keinerlei Anspruch auf Vergütung, inklusive Lizenzgebühren für diese Verbesserungen.

ENTITÄTEN UND LIZENZGEBER DES ANBIETERS HAFTEN IHNEN GEGENÜBER NICHT FÜR ANSPRÜCHE UND

FORDERUNGEN JEGLICHER ART, DIE IN IRGENDEINEM ZUSAMMENHANG MIT DER NUTZUNG DER PASSWORD MANAGER-SOFTWARE, DER BEAUFTRAGUNG ODER NICHT-BEAUFTRAGUNG VON BROKERUNTERNEHMEN ODER HÄNDLERN, ODER DEM KAUF ODER VERKAUF VON SICHERHEITEN DURCH SIE ODER DURCH EXTERNE PARTEIEN ENTSTEHEN, EGAL OB DIESE ANSPRÜCHE UND FORDERUNGEN EINEM URTEIL ODER EINEM VERGLEICH ENTSTAMMEN.

ENTITÄTEN UND LIZENZGEBER DES ANBIETERS HAFTEN IHNEN GEGENÜBER NICHT FÜR IRGENDWELCHE DIREKTEN, NEBEN-, VERMÖGENS- ODER FOLGESCHÄDEN, DIE AUS DER SOFTWARE ODER IM ZUSAMMENHANG MIT EXTERNER SOFTWARE ENTSTEHEN, FÜR IRGENDWELCHE DATEN, AUF DIE MIT DER PASSWORD MANAGER-SOFTWARE ZUGEGRIFFEN WIRD, IHRE NUTZUNG BZW. DIE UNMÖGLICHKEIT DER NUTZUNG DER PASSWORD MANAGER-SOFTWARE ODER FÜR DATEN, DIE ÜBER DIE PASSWORD MANAGER-SOFTWARE BEREITGESTELLT WERDEN, EGAL OB DIESE ANSPRÜCHE UND FORDERUNGEN EINEM URTEIL ODER EINEM VERGLEICH ENTSTAMMEN. VON DIESER KLAUSEL AUSGESCHLOSSENE SCHÄDEN SIND, OHNE EINSCHRÄNKUNG, ENTGANGENE GESCHÄFTSPROFITE, PERSONEN- UND EIGENTUMSSCHÄDEN, GESCHÄFTSUNTERBRECHUNGEN, VERLUST VON PERSÖNLICHEN ODER GESCHÄFTLICHEN INFORMATIONEN. DA IN MANCHEN LÄNDERN KEINE EINSCHRÄNKUNG VON NEBEN- ODER FOLGESCHÄDEN ZULÄSSIG IST, GILT DIESE EINSCHRÄNKUNG UNTER UMSTÄNDEN NICHT FÜR SIE. IN DIESEN FÄLLEN ERSTRECKT SICH DIE HAFTUNG DES ANBIETERS AUF DAS GESETZLICH FESTGESCHRIEBENE MINIMUM.

DIE ÜBER DIE PASSWORD MANAGER-SOFTWARE BEREITGESTELLTEN INFORMATIONEN INKLUSIVE AKTIENKURSE, ANALYSEN, MARKTINFORMATIONEN, NACHRICHTEN UND FINANZDATEN KÖNNEN VERZÖGERT ODER UNGENAU SEIN ODER FEHLER ODER AUSLASSUNGEN ENTHALTEN. DIE ENTITÄTEN UND LIZENZGEBER DES ANBIETERS HAFTEN IN DIESEN FÄLLEN NICHT. DER ANBIETER KANN BELIEBIGE FUNKTIONEN DER PASSWORD MANAGER-SOFTWARE ODER DIE NUTZUNG SÄMTLICHER FUNKTIONEN ODER TECHNOLOGIEN IN DER PASSWORD MANAGER-SOFTWARE ÄNDERN ODER AUSSER BETRIEB NEHMEN, OHNE SIE VORAB IN KENNTNIS ZU SETZEN.

FALLS DIE BESTIMMUNGEN IN DIESEM ARTIKEL AUS IRGENDEINEM GRUND UNGÜLTIG SEIN SOLLTEN ODER DER ANBIETER FÜR VERLUSTE, SCHÄDEN USW. UNTER GELTENDEM RECHT HAFTET, VEREINBAREN DIE PARTEIEN, DASS DIE HAFTUNG DES ANBIETERS IHNEN GEGENÜBER AUF DEN GESAMTPREIS DER VON IHNEN BEZAHLTEN LIZENZGEBÜHREN BESCHRÄNKT IST.

SIE WERDEN DEN ANBIETER UND DESSEN MITARBEITER, NIEDERLASSUNGEN, PARTNER, REBRANDING UND ANDERE PARTNER GEGENÜBER SÄMTLICHEN EXTERNEN (INKLUSIVE EIGENTÜMER DER GERÄTE ODER PARTEIEN, DEREN RECHTE VON DEN IN DER PASSWORD MANAGER-SOFTWARE ODER IM SPEICHER VERWENDETEN DATEN VERLETZT WURDEN) SCHÄDEN, ANSPRÜCHEN, VERLUSTEN, KOSTEN, AUSGABEN ODER GEBÜHREN SCHADLOS HALTEN, DIE DIESEN EXTERNEN PARTEIEN DURCH IHRE NUTZUNG DER PASSWORD MANAGER-SOFTWARE ENTSTEHEN.

3. Daten in der Password Manager-Software. Sofern nicht anderweitig und ausdrücklich von Ihnen ausgewählt, werden alle von Ihnen eingegebenen und in einer Datenbank der Password Manager-Software gespeicherten Daten in einem verschlüsselten Format auf Ihrem Computer oder einem anderen von Ihnen definierten Speichergerät abgelegt. Sie erkennen an, dass im Fall einer Löschung oder Beschädigung der Password Manager-Datenbank oder anderer Dateien alle enthaltenen Daten unwiederbringlich verloren gehen und akzeptieren das Risiko eines solchen Verlusts. Die Tatsache, dass Ihre persönlichen Daten in verschlüsselter Form auf dem Computer gespeichert sind, bedeutet nicht, dass die Daten nicht von einer Person gestohlen oder missbraucht werden können, die in den Besitz des Master-Passworts gelangt oder sich Zugang zu dem vom Kunden definierten Aktivierungsgerät zum Öffnen der Datenbank verschafft. Sie sind für die Sicherheit all dieser Zugriffsmethoden selbst verantwortlich.

4. Übertragung persönlicher Daten an den Anbieter oder ein Speichermedium. Wenn Sie dies auswählen, überträgt die Password Manager-Software persönliche Daten aus der Datenbank der Password Manager-Software - Passwörter, Anmeldeinformationen, Konten und Identitäten - zum alleinigen Zweck der zeitnahen Datensynchronisierung und -sicherung über das Internet an ein Speichermedium. Die Daten werden

ausschließlich in verschlüsselter Form übertragen. Die Password Manager-Software dient zum Ausfüllen von Onlineformularen mit Passwörtern, Anmeldeinformationen oder anderen Daten, die über das Internet an von Ihnen ausgewählte Websites übertragen werden müssen. Diese Datenübertragung wird nicht von der Password Manager-Software ausgelöst, daher haftet der Anbieter nicht für die Sicherheit dieser Interaktionen mit den Webseiten andere Anbieter. Sämtliche Transaktionen über das Internet, ob mit oder ohne Verwendung der Password Manager-Software, erfolgen auf Ihre eigene Gefahr, und Sie sind allein verantwortlich für Schäden an Ihrem Computersystem oder für Datenverluste, die aus dem Download oder der Nutzung solcher Materialien oder Dienste entstehen. Um das Risiko eines Verlusts wertvoller Daten zu reduzieren, sollten Sie regelmäßige Sicherungen der Datenbank und anderer wichtiger Dateien auf externe Laufwerke anfertigen. Der Anbieter ist nicht in der Lage, Sie bei der Wiederherstellung verlorener oder beschädigter Daten zu unterstützen. Wenn der Anbieter Sicherungsdienste für Datenbankdateien des Benutzers für den Fall von Schäden oder Verlusten der Dateien auf dem PC des Benutzers bereitstellt, gilt für diese Sicherungsdienste keinerlei Gewährleistung oder Haftung des Anbieters Ihnen gegenüber.

Mit der Nutzung der Password Manager-Software stimmen Sie zu, dass die Software in regelmäßigen Abständen Kontakt mit den Servern des Anbieters aufnimmt, um Lizenzinformationen, verfügbare Patches, Service Packs und andere Updates zu überprüfen, um den Betrieb der Password Manager-Software zu verbessern, zu erweitern oder um Wartungsvorgänge durchzuführen. Die Software darf allgemeine Systeminformationen im Zusammenhang mit der Funktionsweise der Password Manager-Software gemäß der Datenschutzrichtlinie übertragen.

5. Informationen und Anweisungen zur Deinstallation. Alle Informationen, die Sie behalten möchten, müssen vor der Deinstallation der Password Manager-Software aus der Datenbank exportiert werden.

Die zusätzlichen Bestimmungen für die Password Manager-Software gelten ausschließlich für Endbenutzer von ESET Smart Security Premium.

ESET LiveGuard. Für ESET LiveGuard gelten die folgenden zusätzlichen Bestimmungen:

Die Software enthält eine Funktion zur zusätzlichen Analyse der von Endbenutzern übermittelten Dateien. Der Anbieter nutzt die von Endbenutzern übermittelten Dateien und die Analyseergebnisse ausschließlich im Rahmen der Datenschutzerklärung und unter Einhaltung der relevanten gesetzlichen Vorgaben.

Die zusätzlichen Bestimmungen für ESET LiveGuard gelten ausschließlich für Endbenutzer von ESET Smart Security Premium.

EULAID: EULA-PRODUCT-LG-EHSW; 3537.0

Datenschutzerklärung

Der Schutz personenbezogener Daten genießt absolute Priorität bei ESET, spol. s r. o. mit eingetragenem Firmensitz in Einsteinova 24, 851 01 Bratislava, Slovak Republic, dem Handelsregistereintrag 3586/B vor dem Bezirksgericht Bratislava I, Rubrik Sro und der eingetragenen Unternehmensnummer 31333532 als Datenverantwortlicher („ESET“ oder „wir“). Wir möchten die Transparenzanforderungen erfüllen, die in der Datenschutz-Grundverordnung (DSGVO) der Europäischen Union gesetzlich festgelegt sind. Aus diesem Grund veröffentlichen wir diese Datenschutzerklärung mit dem ausschließlichen Ziel, unsere Kunden („Endbenutzer“ oder „Sie“) als betroffene Person über die folgenden Themen im Hinblick auf den Schutz personenbezogener Daten zu informieren:

- Rechtliche Grundlage der Verarbeitung personenbezogener Daten
- Datenweitergabe und Vertraulichkeit

- Datensicherheit
- Ihre Rechte als betroffene Person
- Verarbeitung personenbezogener Daten
- Kontaktinformationen.

Rechtliche Grundlage der Verarbeitung personenbezogener Daten

Es gibt nur wenige rechtliche Grundlagen für die Datenverarbeitung, die wir gemäß dem geltenden rechtlichen Rahmen für den Schutz personenbezogener Daten verwenden. Die Verarbeitung personenbezogener Daten bei ESET dient hauptsächlich der Erfüllung der Endbenutzer-Lizenzvereinbarung („EULA“) im Hinblick auf den Endbenutzer (Art. 6 (1) (b) der DSGVO, die für die Bereitstellung von ESET-Produkten oder -Diensten gilt, sofern nicht ausdrücklich anders angegeben. Beispiele für rechtliche Grundlagen sind:

- Rechtliche Grundlage aufgrund legitimer Interessen (Art. 6 (1) (f) der DSGVO), mit der wir Daten zur Nutzung unserer Dienste und zur Zufriedenheit von Kunden verarbeiten, um Benutzer bestmöglich schützen, unterstützen und bedienen zu können. Sogar Marketing ist im geltenden Recht ebenfalls als legitimes Interesse anerkannt, daher verwenden wir es in Bezug auf die Marketingkommunikation mit unseren Kunden.
- Zustimmung (Art. 6 (1) (a) der DSGVO), die wir ggf. in bestimmten Situationen von Ihnen erbitten, wenn wir diese Rechtsgrundlage für besonders geeignet halten oder wenn dies gesetzlich erforderlich ist.
- Einhaltung einer gesetzlichen Verpflichtung (Art. 6 (1) (c) der DSGVO), z. B. die Anforderungen bei elektronischer Kommunikation, Rechnungsstellung oder Abrechnungsdokumenten.

Datenweitergabe und Vertraulichkeit

Wir geben Ihre Daten nicht an Dritte weiter. Allerdings ist ESET ein internationales Unternehmen, das weltweit durch angeschlossene Unternehmen oder Partner im Rahmen unseres Vertriebs-, Dienstleistungs- und Supportnetzwerks vertreten ist. Die von ESET verarbeiteten Informationen zu Lizenzierung, Abrechnung und technischem Support können zur Einhaltung der EULA an angeschlossene Unternehmen oder Partner übertragen und von diesen weitergeleitet werden, beispielsweise zur Bereitstellung von Diensten und zur Erbringung von Supportleistungen.

ESET bevorzugt die Verarbeitung seiner Daten in der Europäischen Union (EU). Je nach Ihrem Standort (Nutzung unserer Produkte und/oder Dienste außerhalb der EU) und/oder der von Ihnen ausgewählten Dienste kann es jedoch erforderlich sein, die Daten in ein Land außerhalb der EU zu übertragen. Im Zusammenhang mit Cloud-Computing nehmen wir beispielsweise Dienste von Drittanbietern in Anspruch. In diesen Fällen wählen wir unsere Dienstanbieter sorgfältig aus und gewährleisten durch vertragliche sowie technische und organisatorische Maßnahmen einen angemessenen Datenschutz. In der Regel werden EU-Standardvertragsklauseln vereinbart, bei Bedarf ergänzt durch vertragliche Bestimmungen.

In einigen Ländern außerhalb der EU, z. B. dem Vereinigten Königreich und der Schweiz, hat die EU bereits ein vergleichbares Datenschutzniveau beschlossen. Aufgrund dieses vergleichbaren Datenschutzstandards bedarf es zur Übertragung von Daten in diese Länder keiner besonderen Genehmigung oder Vereinbarung.

Datensicherheit

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. Sollten Ihre Rechte und Freiheiten durch einen Datenangriff gefährdet sein, informieren wir die Aufsichtsbehörden sowie die Endbenutzer als die betroffenen Personen.

Rechte betroffener Personen

Die Rechte aller Endbenutzer liegen uns am Herzen, und wir möchten Ihnen versichern, dass ESET allen Endbenutzern (aus einem EU-Land oder anderen Nicht-EU-Ländern) die nachstehenden Rechte garantiert. Zur Ausübung Ihrer Rechte als betroffene Person kontaktieren Sie uns mithilfe des Supportformulars, oder schreiben Sie eine E-Mail an dpo@eset.sk. Zu Identifizierungszwecken bitten wir Sie um die folgenden Informationen: Name, E-Mail-Adresse und, sofern vorhanden, Lizenzschlüssel oder Kundennummer sowie Firmenmitgliedschaft. Bitte senden Sie uns keine anderen personenbezogenen Daten wie beispielweise Ihr Geburtsdatum. Wir weisen zudem darauf hin, dass wir zur Abwicklung Ihrer Anfrage sowie zu Identifizierungszwecken Ihre personenbezogenen Daten verarbeiten.

Recht auf Widerruf der Zustimmung: Das Recht auf Widerruf der Zustimmung gilt nur im Falle einer Verarbeitung auf Grundlage einer Zustimmung. Wenn wir Ihre personenbezogenen Daten auf Grundlage Ihrer Zustimmung verarbeiten, können Sie Ihre Zustimmung jederzeit und ohne Angabe von Gründen widerrufen. Der Widerruf der Zustimmung gilt nur für die Zukunft und hat keinen Einfluss auf die Rechtmäßigkeit der vor dem Widerruf verarbeiteten Daten.

Recht auf Einspruch: Das Recht auf Einspruch gilt im Falle einer Verarbeitung auf Grundlage eines berechtigten Interesses von ESET oder eines Dritten. Wenn wir Ihre personenbezogenen Daten verarbeiten, um ein legitimes Interesse zu schützen, haben Sie als betroffene Person jederzeit das Recht, dem von uns angegebenen legitimen Interesse und der Verarbeitung Ihrer personenbezogenen Daten zu widersprechen. Ihr Einspruch gilt nur für die Zukunft und hat keinen Einfluss auf die Rechtmäßigkeit der vor dem Einspruch verarbeiteten Daten. Sofern wir Ihre personenbezogenen Daten zu Direktwerbungszwecken verarbeiten, müssen Sie Ihren Einspruch nicht begründen. Dies gilt auch für die Profilerstellung, insofern diese mit einer solchen Direktvermarktung in Zusammenhang steht. In allen anderen Fällen bitten wir Sie, uns die Beschwerde bezüglich des legitimen Interesses von ESET an der Verarbeitung Ihrer personenbezogenen Daten unverzüglich zukommen zu lassen.

Beachten Sie, dass wir in manchen Fällen trotz des Widerrufs Ihrer Zustimmung berechtigt sind, Ihre personenbezogenen Daten auf einer anderen rechtlichen Grundlage weiter zu verarbeiten, z. B. zur Erfüllung eines Vertrags.

Recht auf Auskunft: Als betroffene Person haben Sie das Recht, jederzeit kostenlos Informationen über Ihre bei ESET gespeicherten Daten zu verlangen.

Recht auf Berichtigung: Sollten wir versehentlich falsche personenbezogene Daten über Sie verarbeiten, haben Sie das Recht, diese berichtigen zu lassen.

Recht auf Löschung und auf Einschränkung der Verarbeitung: Als betroffene Person haben Sie das Recht, die Löschung Ihrer personenbezogenen Daten oder die Einschränkung der Verarbeitung dieser zu verlangen. Wenn wir Ihre personenbezogenen Daten verarbeiten, z. B. mit Ihrer Zustimmung, Sie diese Zustimmung widerrufen und keine andere gesetzliche Grundlage wie beispielsweise ein Vertrag vorliegt, löschen wir Ihre personenbezogenen Daten umgehend. Ihre personenbezogenen Daten werden auch gelöscht, sobald sie zum Ende der Aufbewahrungsdauer zu den genannten Zwecken nicht mehr benötigt werden.

Wenn wir Ihre personenbezogenen Daten ausschließlich für Direktmarketing verwenden und Sie Ihre Zustimmung widerrufen oder Einspruch gegen das berechtigte Interesse von ESET erheben, schränken wir die Verarbeitung Ihrer personenbezogenen Daten soweit ein, dass wir Ihre Kontaktdaten in unsere interne Negativliste aufnehmen, um derartige unerwünschte Kontaktaufnahmen zu vermeiden. Andernfalls werden Ihre personenbezogenen

Daten gelöscht.

Beachten Sie, dass wir unter Umständen verpflichtet sind, Ihre Daten bis zum Ablauf der von Gesetzgeber und Aufsichtsbehörden vorgegebenen Aufbewahrungsdauer zu speichern. Aufbewahrungspflichten und Aufbewahrungsdauer können sich auch aus der slowakischen Gesetzgebung ergeben. Anschließend werden die entsprechenden Daten routinemäßig gelöscht.

Das Recht auf Übertragbarkeit der Daten. Als betroffene Person stellen wir Ihnen gerne die von ESET verarbeiteten personenbezogenen Daten im XLS-Format zur Verfügung.

Recht auf Beschwerde: Betroffene Personen haben das Recht, jederzeit Beschwerde bei einer Aufsichtsbehörde einzulegen. ESET unterliegt slowakischem Recht und ist als Teil der Europäischen Union an die Datenschutzgesetze gebunden. Die zuständige Aufsichtsbehörde ist das Büro für den Schutz personenbezogener Daten der Slowakischen Republik mit Sitz in Hraničná 12, 82007 Bratislava 27, Slovak Republic.

Verarbeitung personenbezogener Daten

Die von ESET angebotenen und in unserem Produkt implementierten Dienste werden gemäß den Bestimmungen der Endbenutzer-Lizenzvereinbarungangeboten, bedürfen jedoch mitunter zusätzlicher Maßnahmen. Wir möchten Ihnen weitere Details zur Datensammlung im Zusammenhang mit der Bereitstellung unserer Dienste liefern. Wir bieten verschiedene in der EULA und der Dokumentation. Für die Erbringung dieser Dienste erfassen wir die folgenden Informationen:

Lizenzierungs- und Abrechnungsdaten: Der Name, die E-Mail-Adresse, der Lizenzschlüssel und ggf. die Adresse, die Mitgliedschaft in der Firma und die Zahlungsdaten werden von ESET erfasst und verarbeitet, um die Aktivierung der Lizenz, die Zustellung von Lizenzschlüsseln, Erinnerungen bei Ablauf, Supportanfragen, die Überprüfung der Echtheit der Lizenz, die Bereitstellung unserer Dienste sowie die Zustellung sonstiger Benachrichtigungen einschließlich Marketingnachrichten nach geltendem Gesetz oder gemäß Ihrer Zustimmung zu ermöglichen. ESET ist gesetzlich verpflichtet, die Abrechnungsdaten zehn Jahre lang aufzubewahren. Die Lizenzinformationen hingegen werden spätestens zwölf Monate nach Ablauf der Lizenz anonymisiert.

Update- und andere Statistiken: Zu den Informationen, die verarbeitet werden, gehören Informationen zu Installationsprozess und Computer, z. B. die Plattform, auf der unser Produkt installiert wird, sowie Informationen zum Betrieb und Funktionsumfang der Produkte, darunter Betriebssystem, Hardwareinformationen, Installations- und Lizenz-IDs, IP-Adresse, MAC-Adresse und Konfigurationseinstellungen des Produkts. Zweck der Verarbeitung dieser Informationen sind die Bereitstellung von Update- und Upgrade-Diensten, Wartung, Sicherheit und Verbesserung unserer Back-End-Struktur.

Die Informationen werden getrennt von den für Lizenzierungs- und Abrechnungszwecke erforderlichen Identifikationsinformationen aufbewahrt, weil hierzu keine Identifizierung des Endbenutzers erforderlich ist. Der Aufbewahrungszeitraum beträgt bis zu vier Jahre.

ESET LiveGrid®-Reputationssystem: Einweg-Hashes im Zusammenhang mit Infiltrationen werden zum Zweck unseres ESET LiveGrid®-Reputationssystems verarbeitet, das die Wirksamkeit unserer Sicherheitslösungen verbessert, indem es gescannte Dateien mit Positiv- und Negativlisten in einer Datenbank in der Cloud vergleicht. Bei diesem Vorgang wird der Endbenutzer nicht identifiziert.

ESET LiveGrid®-Feedbacksystem: 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:

- Eingedrungene 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;

- Informationen zur Internetnutzung wie IP-Adresse und geografische Informationen, IP-Pakete, URLs und Ethernet-Frames;

- Absturzabbilder 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.

Alle im ESET LiveGrid®-Feedbacksystem eingegangenen und verarbeiteten Informationen werden ohne Identifizierung des Endbenutzers verwendet.

Sicherheitsanalyse für mit dem Netzwerk verbundene Geräte. Zur Bereitstellung der Funktion zur Sicherheitsanalyse verarbeiten wir den Namen des lokalen Netzwerks sowie Angaben zu Geräten in Ihrem lokalen Netzwerk, wie Vorhandensein, Typ, Name, IP-Adresse und MAC-Adresse des Netzwerkgeräts in Zusammenhang mit Ihren Lizenzinformationen. Diese Informationen umfassen außerdem dem drahtlosen Sicherheitstyp und den Verschlüsselungstyp für Routergeräte. Die Lizenzinformationen, die Aufschluss über den Endbenutzer geben, werden spätestens zwölf Monate nach Ablauf der Lizenz anonymisiert.

Technischer Support. Kontaktinformationen und andere Daten aus Ihren Supportanfragen werden unter Umständen für Supportleistungen benötigt. Je nachdem, über welchen Kanal Sie uns kontaktieren, speichern wir möglicherweise Ihre E-Mail-Adresse, Telefonnummer, Lizenzinformationen, Produktdetails und eine Beschreibung Ihres Supportfalls. Unter Umständen werden Sie nach weiteren Informationen gefragt, um die Erbringung der Supportleistung zu erleichtern. Die im Rahmen des technischen Supports verarbeiteten Daten werden vier Jahre lang aufbewahrt.

Schutz vor dem Missbrauch von Daten. Wenn das ESET HOME-Konto auf https://home.eset.com vom Endbenutzer erstellt und die Funktion im Zusammenhang mit einem Diebstahl des Computers aktiviert wird, werden folgende Informationen erfasst und verarbeitet: Standortdaten, Screenshots, Daten zur Konfiguration des Computers sowie von der Computerkamera aufgezeichnete Daten. Die erfassten Daten werden auf unseren oder den Servern unserer Dienstanbieter drei Monate lang gespeichert.

Password Manager. Wenn Sie den Password Manager aktivieren, werden Daten im Zusammenhang mit Ihren Anmeldedaten verschlüsselt nur auf Ihrem Computer oder einem anderen zugewiesenen Gerät gespeichert. Wenn Sie den Synchronisierungsdienst aktivieren, werden die verschlüsselten Daten auf unseren Servern oder den Servern unserer Dienstanbieter gespeichert, um den Dienst zu erbringen. Weder ESET noch die Dienstanbieter haben Zugang zu den verschlüsselten Daten. Nur Sie sind in der Lage, die Daten zu entschlüsseln. Nach Deaktivierung der Funktion werden die Daten entfernt.

ESET LiveGuard. Wenn Sie die ESET LiveGuard-Funktion aktivieren, müssen Sie Proben mit den vordefinierten und vom Endbenutzer ausgewählten Dateien einsenden. Die für die Remoteanalyse auswählen Proben werden an den ESET-Dienst hochgeladen, und das Analyseergebnis wird an Ihren Computer gesendet. Verdächtige Proben werden genauso verarbeitet wie die vom ESET LiveGrid®-Feedbacksystem erfassten Informationen.

Programm für ein besseres Kundenerlebnis. Falls Sie das Programm für ein besseres Kundenerlebnis aktiviert haben, werden anonyme Telemetrieinformationen im Zusammenhang mit der Nutzung unserer Produkte gemäß Ihrer Zustimmung gesammelt und verwendet.

Hinweis: Ist die Person, die unsere Produkte und Dienste in Anspruch nimmt, nicht mit dem Endbenutzer

identisch, der das Produkt oder den Dienst erworben und die EULA mit uns geschlossen hat (beispielsweise ein Mitarbeiter des Endbenutzers, ein Familienmitglied oder eine vom Endbenutzer bevollmächtigte und im Einklang mit der EULA anderweitig zur Nutzung des Produkts oder Dienstes berechtigte Person), so erfolgt die Datenverarbeitung im legitimen Interesse von ESET gemäß Auslegung von Art. 6 (1) (f) der DSGVO, damit der vom Endbenutzer bevollmächtigte Benutzer die von uns bereitgestellten Produkte und Dienste im Einklang mit der EULA verwenden kann.

Kontaktinformationen

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