

ESET Security for Microsoft SharePoint

Benutzerhandbuch

[Klicken Sie hier um die Hilfe-Version dieses Dokuments anzuzeigen](#)

Copyright ©2023 by ESET, spol. s r.o.

ESET Security for Microsoft SharePoint wurde entwickelt von ESET, spol. s r.o.

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

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

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

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

REV. 19.03.2023

1 Einleitung	1
2 Übersicht	2
2.1 Hauptfunktionen	2
2.2 Neuerungen	4
2.3 Bereitstellung	4
2.3 SharePoint Farm-Bereitstellung	4
2.3 Installation in einer Cluster-Umgebung	5
2.4 SharePoint-Schutzarten	6
2.4 SharePoint-Integration	6
2.4 Zugriffsfilter	6
2.4 On-Demand-Datenbank-Scan	7
3 Vorbereiten für die Installation	8
3.1 Systemanforderungen	10
3.2 SHA-2-Kompatibilität erforderlich	11
3.3 ESET Security for Microsoft SharePoint Installationsschritte	12
3.3 Vorhandene Installation bearbeiten	15
3.4 Stille/unbeaufsichtigte Installation	17
3.4 Installation über die Kommandozeile	18
3.5 Produktaktivierung	21
3.5 ESET Business Account	22
3.5 Aktivierung erfolgreich	22
3.5 Aktivierungsfehler	22
3.5 Lizenz	23
3.6 Auf neuere Version aktualisieren	23
3.6 Upgrades über ESMC	24
3.6 Upgrades per ESET-Cluster	27
3.7 Terminalserver	30
4 Erste Schritte	30
4.1 Verwaltung über ESET Security Management Center	31
4.2 Überwachung	31
4.2 Status	33
4.2 Windows-Update verfügbar	35
4.2 Netzwerkisolierung	36
5 Arbeiten mit ESET Security for Microsoft SharePoint	37
5.1 Prüfung	37
5.1 Scanfenster und Scan-Log	39
5.2 Log-Dateien	42
5.2 Log-Filter	45
5.3 Update	47
5.4 Einstellungen	49
5.4 Server	50
5.4 Computer	51
5.4 Netzwerk	52
5.4 Fehlerbehebungsassistent für das Netzwerk	53
5.4 Web und E-Mail	54
5.4 Tools - Diagnose-Logging	54
5.4 Einstellungen importieren/exportieren	55
5.5 Tools	56
5.5 Ausgeführte Prozesse	57
5.5 Aktivität beobachten	59

5.5 Schutzstatistiken	60
5.5 Cluster	62
5.5 Clusterassistent – Knoten auswählen	64
5.5 Clusterassistent – Clustereinstellungen	65
5.5 Clusterassistent - Einstellungen für die Clustereinrichtung	66
5.5 Clusterassistent – Knotenprüfung	66
5.5 Clusterassistent - Knoteninstallation	68
5.5 ESET-Shell	71
5.5 Nutzung	73
5.5 Befehle	78
5.5 Batchdateien / Skripts	81
5.5 ESET SysInspector	82
5.5 ESET SysRescue Live	83
5.5 Taskplaner	84
5.5 Taskplaner - Task hinzufügen	85
5.5 Tasktyp	87
5.5 Task-Zeitplanung	87
5.5 Durch Ereignis ausgelöst	88
5.5 Anwendung starten	88
5.5 Übersprungener Task	88
5.5 Übersicht über geplante Tasks	89
5.5 Datei zur Analyse einreichen	89
5.5 Verdächtige Datei	90
5.5 Verdächtige Webseite	90
5.5 Fehlalarm Datei	91
5.5 Fehlalarm Webseite	91
5.5 Sonstige	91
5.5 Quarantäne	92
6 Server-Schutzeinstellungen	93
6.1 Leistungsindikatoren	95
6.2 Echtzeitfilter	96
6.2 Viren- und Spyware-Schutz	97
6.3 On-Demand-Datenbankprüfung	99
6.3 Prüfziele für die On-Demand-Datenbankprüfung	99
6.3 Viren- und Spyware-Schutz	100
6.4 Regeln	101
6.4 Regelliste	101
6.4 Regelassistent	103
6.4 Regelbedingung	104
6.4 Regelaktionen	106
7 Allgemeine Einstellungen	107
7.1 Computer	108
7.1 Erkennung durch Machine Learning	110
7.1 Ausschlussfilter	113
7.1 Leistungsausschlüsse	113
7.1 Ereignisausschlüsse	115
7.1 Assistent zum Erstellen von Ausschlüssen	116
7.1 Erweiterte Einstellungen	117
7.1 Automatische Ausschlüsse	117
7.1 Shared local cache	118
7.1 Eindringene Schadsoftware wurde erkannt	118

7.1 Echtzeit-Dateischutz	119
7.1 ThreatSense-Parameter	120
7.1 Zusätzliche ThreatSense-Parameter	124
7.1 Von der Prüfung ausgeschlossene Dateiendungen	125
7.1 Ausgeschlossene Prozesse	125
7.1 Cloudbasierter Schutz	126
7.1 Ausschlussfilter	128
7.1 Malware-Prüfungen	129
7.1 Profilmanager	131
7.1 Profil-Ziele	131
7.1 Scanziele	133
7.1 Scan im Leerlaufbetrieb	135
7.1 Prüfung der Systemstartdateien	135
7.1 Prüfung Systemstartdateien	135
7.1 Wechselmedien	136
7.1 Dokumentenschutz	137
7.1 Hyper-V-Scan	137
7.1 HIPS	139
7.1 HIPS-Regeleinstellungen	141
7.1 Erweiterte HIPS-Einstellungen	144
7.2 Update-Konfiguration	144
7.2 Update-Rollback	148
7.2 Geplanter Task - Update	149
7.2 Update-Mirror	149
7.3 Netzwerk-Schutz	151
7.3 IDS-Ausnahmen	153
7.3 Vorübergehende Negativliste der IP-Adressen	153
7.4 Web und E-Mail	154
7.4 Protokollprüfung	154
7.4 Webbrowser und E-Mail-Programme	155
7.4 SSL/TLS	155
7.4 Liste bekannter Zertifikate	157
7.4 Verschlüsselte SSL-Kommunikation	157
7.4 E-Mail-Client-Schutz	158
7.4 E-Mail-Protokolle	159
7.4 Warnungen und Hinweise	160
7.4 Symbolleiste für MS Outlook	161
7.4 Symbolleisten für Outlook Express und Windows Mail	161
7.4 Bestätigungsfenster	162
7.4 E-Mails erneut prüfen	162
7.4 Web-Schutz	162
7.4 URL-Adressverwaltung	163
7.4 Neue Liste erstellen	164
7.4 Phishing-Schutz	166
7.5 Gerätesteuerung	167
7.5 Geräteregeeln	168
7.5 Gerätegruppen	170
7.6 Tool-Konfiguration	171
7.6 Zeitfenster	172
7.6 Microsoft Windows Update	172
7.6 ESET CMD	172

7.6 ESET RMM	174
7.6 Lizenz	175
7.6 WMI-Anbieter	175
7.6 Bereitgestellte Daten	176
7.6 Zugriff auf die bereitgestellten Daten	183
7.6 Scan-Ziele für ERA/ESMC	184
7.6 Override-Modus	184
7.6 Log-Dateien	188
7.6 Proxyserver	189
7.6 Benachrichtigungen	190
7.6 Anwendungsbenachrichtigungen	191
7.6 Desktophinweise	191
7.6 E-Mail-Benachrichtigungen	192
7.6 Anpassen	193
7.6 Präsentationsmodus	194
7.6 Diagnose	194
7.6 Technischer Support	196
7.6 Cluster	196
7.7 Benutzeroberfläche	197
7.7 Warnungen und Hinweifenster	198
7.7 Einstellungen für den Zugriff	199
7.7 ESET-Shell	200
7.7 Deaktivieren der Benutzeroberfläche auf Terminalserver	200
7.7 Deaktivierte Nachrichten und Statusmeldungen	201
7.7 Anwendungsstatuseinstellungen	201
7.7 Symbol im Infobereich der Taskleiste	202
7.8 Auf Standardeinstellungen zurücksetzen	203
7.9 Hilfe und Support	204
7.9 Supportanfrage senden	205
7.9 Über ESET Security for Microsoft SharePoint	206
7.10 Glossar	206
8 Endbenutzer-Lizenzvereinbarung	206
9 Datenschutzerklärung	213

Einleitung

Dieses Handbuch unterstützt Sie dabei, ESET Security for Microsoft SharePoint optimal einzusetzen. Drücken Sie jederzeit die Taste **F1** auf Ihrer Tastatur, um die Hilfeseite zum aktuell geöffneten Fenster anzuzeigen.

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

HINWEIS

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

WICHTIG

Diese Abschnitte erfordern Ihre Aufmerksamkeit und sollten nicht übersprungen werden. Wichtige Hinweise umfassen nicht-kritische, jedoch wichtige Informationen.

WARNUNG

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

BEISPIEL

Dieser praktische Anwendungsfall veranschaulicht, wie Sie sich mit einer Funktion oder einem Feature vertraut machen können.

Wenn das folgende Element oben rechts in einer Hilfeseite angezeigt wird, bezieht sich die Information auf die Navigation in der grafischen Benutzeroberfläche (GUI) von ESET Security for Microsoft SharePoint. Folgen Sie diesen Anweisungen, um zum Fenster zu gelangen, das auf der jeweiligen Hilfeseite beschrieben wird.


ESET Security for Microsoft SharePoint Öffnen

Klicken Sie auf *Einstellungen* > *Server* > *OneDrive-Scan einrichten* > *Registrieren*



Formatierungskonventionen:

Konvention	Bedeutung
Fettdruck	Abschnittsüberschriften, Featurenamen oder Elemente der Benutzeroberfläche, z. B. Schaltflächen.
<i>Kursivdruck</i>	Platzhalter für Informationen, die Sie eingeben. Dateiname oder Pfad bedeutet z. B., dass Sie den tatsächlichen Pfad oder den Namen einer Datei angeben.

Konvention	Bedeutung
Courier New-Schriftart	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 installierte Windows-Programme und andere Anwendungen gespeichert werden.

Die Seiten der ESET Security for Microsoft SharePoint-Onlinehilfe sind in Kapitel und Unterkapitel unterteilt. Im Inhalt der Hilfeseiten können Sie schnell nach einer bestimmten Information suchen. Alternativ können Sie Wörter oder Sätze eingeben, um die Volltextsuche zu verwenden.

Übersicht

ist eine integrierte Lösung und wurde speziell für die Microsoft SharePoint-Produktfamilie auf Microsoft Windows Server in einer Standalone- oder Farm-Konfiguration entwickelt. Die Lösung bietet einen wirksamen und zuverlässigen Schutz vor verschiedenen Arten von Schadsoftware, Viren und anderem Schadcode. ESET Security for Microsoft SharePoint schützt Dateien, die in SharePoint-Inhaltsdatenbanken gespeichert sind. Dabei werden sowohl die von Benutzern abgelegten Dateien in Dokumentbibliotheken, Objektbibliotheken, Wiki-Seiten usw. geschützt sowie ASP-Seiten, (JavaScript)-Skripts, Bilder usw., aus denen die eigentliche SharePoint-Site besteht.

ESET Security for Microsoft SharePoint schützt Ihre Inhalte:

- Durch Filterung beim Dateizugriff (Echtzeitschutz)
- Mit der On-Demand-Datenbankprüfung (On-Demand-Prüfung)

Der Echtzeitfilter wird nach dem Ermessen von SharePoint ausgeführt, und die Funktionsweise hängt zum Teil von der eingesetzten SharePoint-Generation ab (2010 oder 2007). Normalerweise wird der Echtzeitfilter beim ersten Zugriff auf eine Datei ausgeführt. Das Prüfergebnis wird zwischengespeichert, bis sich die Version der Virusdatenbank ändert oder bis eine gewisse Zeit vergangen ist.

Die On-Demand-Prüfung durchläuft alle Dateien und Verzeichnisse einer vom Administrator ausgewählten Website hierarchisch. Die Dateien werden mit dem SharePoint-Objektmodell (.NET based) geöffnet, das eine einheitliche Sicht aller Inhalte in einer SharePoint-Farm ermöglicht und die tatsächlich verwendete Datenbankserver-Technologie abstrahiert.

Sowohl Echtzeitfilter als auch On-Demand-Scan verwenden die folgenden Prüfungen:

- Viren- und Spyware-Schutz
- Benutzerdefinierte Regeln mit unterschiedlichen Arten von Bedingungen


Hauptfunktionen

Die folgende Tabelle enthält eine Liste der in ESET Security for Microsoft SharePoint verfügbaren Funktionen. ESET Security for Microsoft SharePoint [unterstützt](#) die meisten Editionen von Microsoft Windows Server 2008 R2 SP1, 2012, 2016 und 2019 in eigenständigen oder geclusterten Umgebungen. Mit [ESET Security Management Center](#) können Sie ESET Security for Microsoft SharePoint in größeren Netzwerken zentral verwalten.

Echter 64-Bit-Produktkern	Mehr Leistung und Stabilität für die wichtigsten Produktkomponenten.
Leistungsindikatoren	Mit den ESET Security for Microsoft SharePoint-Leistungsindikatoren können Sie die Gesamtleistung von ESET Security for Microsoft SharePoint überwachen.
Echtzeitfilter	Dateischutz durch Filterung beim Dateizugriff.
On-Demand-Scan	Dateischutz durch eine Datenbankprüfung, die entweder durch den Benutzer oder zu einem bestimmten Zeitpunkt ausgelöst wird.
Benutzerdefinierte Regeln	Administratoren können benutzerdefinierte Regeln für Dateien erstellen und verwalten, indem sie Bedingungen und Aktionen für gefilterte Dateien festlegen.
Automatische Ausschlüsse	Automatische Erkennung und anschließender Ausschluss von kritischen Anwendungen und Serverdateien zur Aufrechterhaltung eines reibungslosen Betriebs.
Selbstschutz	Verhindert, dass ESET-Sicherheitslösungen manipuliert oder deaktiviert werden.
Hilfreiche Fehlerbehebung	Integrierte Tools zur Behebung verschiedener Probleme: ESET SysInspector für die Systemdiagnose und ESET SysRescue Live zum Erstellen eines bootfähigen Rettungsmediums (CD oder USB).
ESET-Cluster	Mit dieser Infrastruktur können ESET-Serverprodukte miteinander kommunizieren, Konfigurationsdaten und Benachrichtigungen austauschen und die für den ordnungsgemäßen Betrieb einer Gruppe von Produktinstanzen erforderlichen Daten synchronisieren. Dies gewährleistet eine einheitliche Konfiguration des Produkts im gesamten Cluster. ESET Security for Microsoft SharePoint unterstützt Windows-Failover-Cluster und Network Load Balancing (NLB)-Cluster. Außerdem können Sie manuell ESET-Clustermitglieder hinzufügen, ohne dass ein bestimmtes Windows-Cluster erforderlich ist. ESET-Cluster funktionieren in Domänen- und Arbeitsgruppenumgebungen.
Komponentenbasierte Installation	Wählen Sie aus, welche Komponenten Sie hinzufügen oder entfernen möchten.
Speicher prüfen	Scannt alle freigegebenen Dateien auf dem lokalen Server. Auf diese Weise können Sie beispielsweise nur Benutzerdaten auf dem Dateiserver scannen.
Ausgeschlossene Prozesse	Die Prozesse werden nur von der Virenschutz-Echtzeitprüfung ausgeschlossen. Aufgrund der entscheidenden Rolle wichtiger Server (Anwendungsserver, Speicherserver usw.) müssen unbedingt regelmäßig Sicherungen angelegt werden, um die Server bei einer schweren Störung wiederherstellen zu können. Zur Verbesserung von Sicherungsgeschwindigkeit, Prozessintegrität und Dienstverfügbarkeit werden bei Sicherungen bestimmte Techniken verwendet, die zu Konflikten mit Virenschutzlösungen auf der Dateiebene führen können. Bei Live-Migrationen virtueller Computer können ähnliche Probleme auftreten. Die einzig effektive Lösung zur Vermeidung dieser beiden Situationen ist eine Deaktivierung der Virenschutzsoftware. Wenn Sie Prozesse ausschließen (z. B. die Prozesse der Sicherungssoftware), werden alle Dateioperationen dieser Prozesse ignoriert und als sicher betrachtet, um Wechselwirkungen mit dem Sicherungsprozess zu minimieren. Wir empfehlen Vorsicht beim Ausschließen von Prozessen, da ausgeschlossene Sicherungssoftware zum Beispiel auf infizierte Dateien zugreifen kann, ohne einen Alarm auszulösen. Aus diesem Grund sind erweiterte Berechtigungen nur für den Echtzeitschutz erlaubt.
eShell (ESET-Shell)	eShell 2.0 ist jetzt in ESET Security for Microsoft SharePoint verfügbar. eShell ist eine neue Kommandozeilen-Schnittstelle mit zusätzlichen Optionen für die Verwaltung von ESET-Serverprodukten für erfahrene Benutzern und Administratoren.
ESET Security Management Center	Bessere Integration mit ESET Security Management Center inklusive der Möglichkeit zur Planung von On-Demand-Scans . Weitere Informationen zu ESMC finden Sie in der ESET Security Management Center- Onlinehilfe ↗ .
Hyper-V-Scan	Beim Hyper-V-Scan werden virtuelle Computerlaufwerke auf Microsoft Hyper-V Servern ↗ geprüft, ohne auf der jeweiligen VM einen Agenten installieren zu müssen.

Neuerungen

ESET Security for Microsoft SharePoint enthält die folgenden neuen Features:

- Echter 64-Bit-Produktkern
- [Direktzugriff auf die SQL-Datenbank](#)
- [Leistungsindikatoren](#)
- [ESET Enterprise Inspector](#)  Unterstützung
- [ESET RMM](#)
- Netzwerkisolierung
- [Erkennung durch Machine Learning](#)

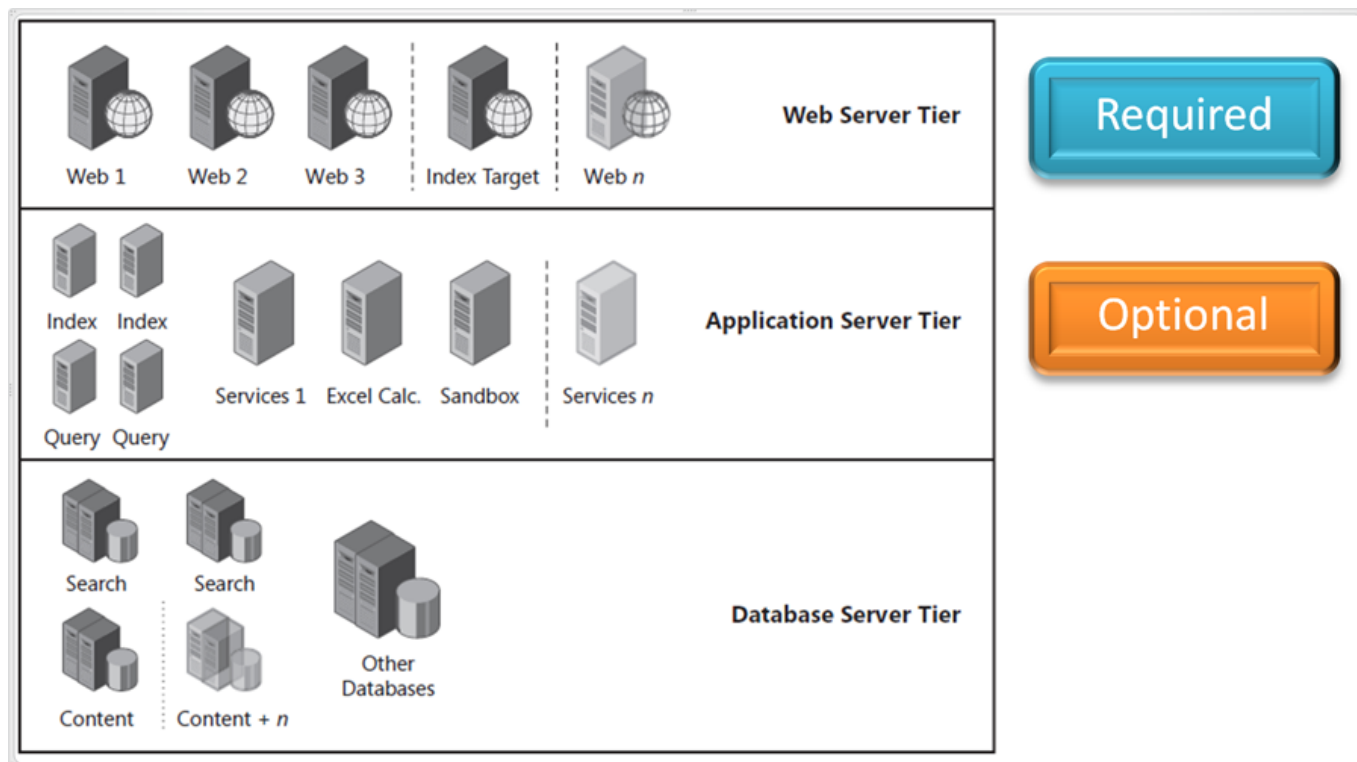
Bereitstellung

Die nächsten Kapitel unterstützen Sie bei der Planung der Bereitstellung von ESET Security for Microsoft SharePoint in Ihrer SharePoint-Infrastruktur, insbesondere wenn Sie eine [SharePoint-Serverfarm](#) oder eine [Cluster-Umgebung](#) verwenden.

SharePoint Farm-Bereitstellung

ESET Security for Microsoft SharePoint muss auf allen SharePoint-Computern mit der Webserver-Rolle installiert werden, um sicherzustellen, dass die Benutzer durch den [Echtzeit-Dateifilter](#) geschützt sind. Eine [On-Demand-Datenbankprüfung](#) kann von jedem dieser Computer aus gestartet werden. Optional kann ESET Security for Microsoft SharePoint auf SharePoint-Computern mit der Anwendungsserverrolle installiert werden. Von solchen Computern aus kann zwar keine On-Demand-Datenbankprüfung der SharePoint-Inhaltsdatenbank gestartet werden, sie können jedoch als Echtzeitfilter verwendet werden.

In der nachstehenden Abbildung ist die Serverumgebung in solche Bereiche unterteilt, die einen ESET-Schutz erfordern, und solche, für die dieser Schutz optional ist.



HINWEIS

In einer SharePoint-Farmumgebung reicht es aus, die On-Demand-Datenbankprüfung von einem Computer aus zu starten. Die gesamte SharePoint-Farmdatenbank wird gescannt.

Die On-Demand-Prüfung ist ein ressourcenintensiver Vorgang und sollte daher auf einem Computer ausgeführt werden, auf dem eine erhöhte Last keine Probleme verursacht. Aus funktionaler Sicht kann die On-Demand-Datenbankprüfung von einem beliebigen SharePoint-Farmcomputer gestartet werden, der Zugriff auf die Inhaltsdatenbank hat, unabhängig von dessen Rolle.

Die Geschwindigkeit der On-Demand-Datenbankprüfung hängt zum Großteil vom Durchsatz des Datenbankservers und des verwendeten Netzwerks ab. Um den Durchsatz bei der Datenbankprüfung in großen SharePoint-Farmen zu steigern, können Sie die On-Demand-Datenbankprüfung auf mehr als einem Computer ausführen und die einzelnen Computer für unterschiedliche (nicht überlappende) Teile der Inhaltsdatenbank konfigurieren. Dabei wird jedoch die Last auf dem Datenbankserver erhöht, und die Vorteile dieses Vorgehens sollten vom Farmadministrator geprüft werden.

Installation in einer Cluster-Umgebung

Sie können ESET Security for Microsoft SharePoint in einer Cluster-Umgebung bereitstellen (z. B. in einem Failover-Cluster). Dabei sollten Sie ESET Security for Microsoft SharePoint nach Möglichkeit auf einem aktiven Knoten installieren und die Installation anschließend mit der [ESET Cluster](#)-Funktion von ESET Security for Microsoft SharePoint auf die passiven Knoten verteilen. Neben der Installation dient ESET Cluster auch als Replikation für die ESET Security for Microsoft SharePoint-Konfiguration, um sicherzustellen, dass die Clusterknoten für den korrekten Betrieb einheitlich konfiguriert sind.

SharePoint-Schutzarten

Es gibt zwei ESET Security for Microsoft SharePoint-Sharepoint-Schutzarten:

- Virenschutz
- Spyware-Schutz

Dieser Schutz wird ermöglicht durch:

- Filterung beim Dateizugriff (Echtzeitschutz)
- On-Demand-Datenbankprüfung (On-Demand-Prüfung)

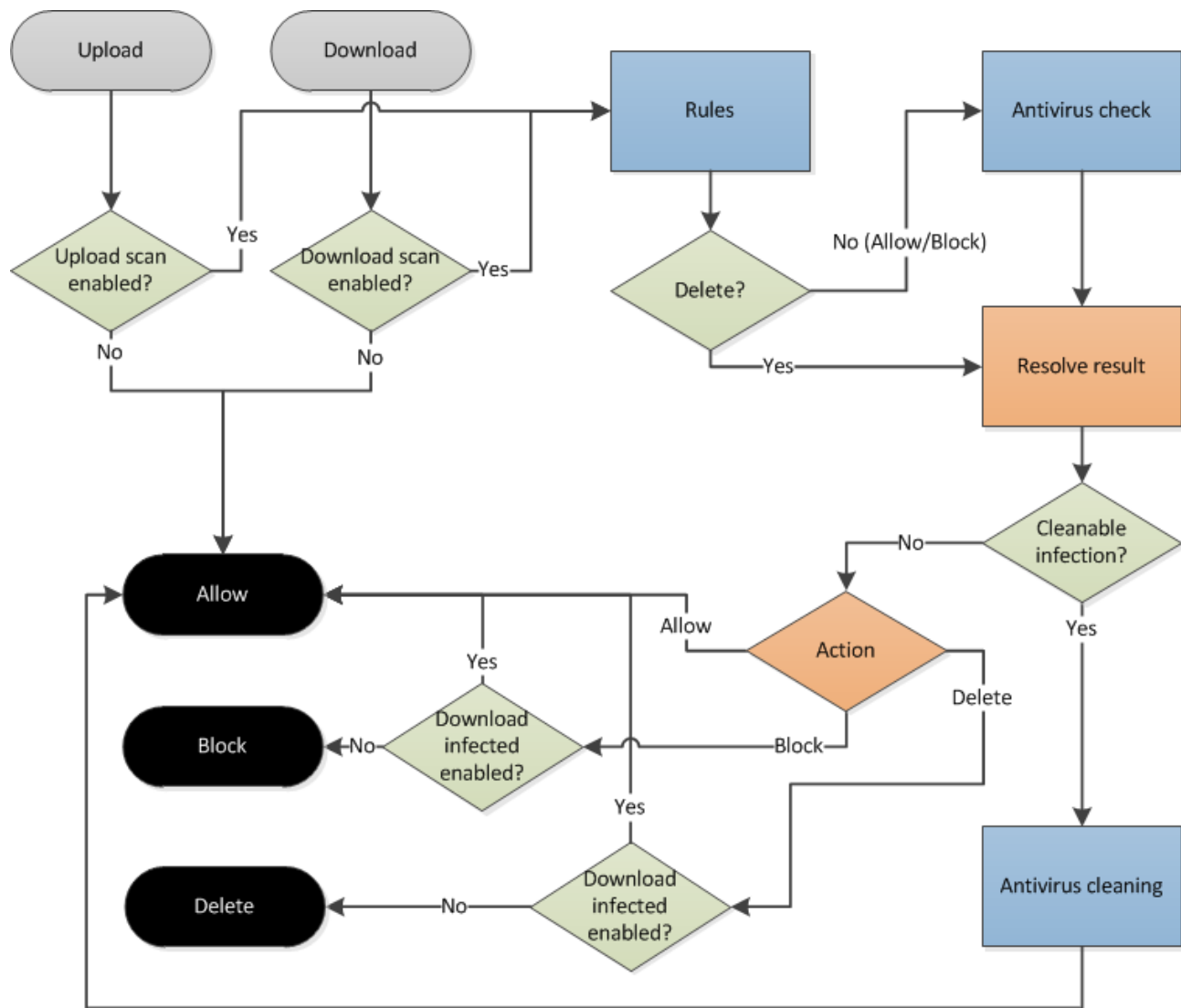
SharePoint-Integration

Dieser Abschnitt beschreibt den [Echtzeitfilter](#) und die [On-Demand-Datenbankprüfung](#) sowie die Integration dieser Funktionen in SharePoint.

Echtzeitfilter

Der Echtzeitfilter prüft alle Dateien gemäß der SharePoint-Schutzeinstellungen. Es werden zum Beispiel alle in SharePoint gespeicherten MS Office-Dokumente, Bilder, .aspx-Dateien (die eigentlichen SharePoint-Seiten), css-Styles und zugehörige Symboldateien zu den Dokumenten geprüft. Die SharePoint-Einstellungen legen den Umfang der Dateien fest, die via VSAPI zum Scannen gesendet werden. ESET Security for Microsoft SharePoint kann nicht aktiv auswählen, welche Dateien gescannt werden. Wenn eine Datei zur Prüfung oder zur Säuberung übermittelt wird, erkennt ESET Security for Microsoft SharePoint deren Dateiname und Größe. Details zur Datei, wie der Eigentümer, der Speicherort oder ob die Datei beim Hoch- oder Herunterladen gescannt wird, können nicht von ESET festgelegt werden. Wenn die Option **Dokumentversionen scannen** aktiviert ist, wird nur der Dateiname der aktuellen Version angezeigt. Für ältere Versionen wird ein alternativer Text verwendet.

Der Prozess für die Prüfung durch den Echtzeitfilter wird im folgenden Diagramm dargestellt. Dieses Diagramm zeigt die möglichen Aktionen im Rahmen der Prüfung durch den Echtzeitfilter:



On-Demand-Datenbankprüfung

Die On-Demand-Datenbankprüfung dient zur Überprüfung der SharePoint-Inhaltsdatenbank, die SharePoint-Websites und -Dateien enthält. ESET Security scannt die Datei- und Ordnerstrukturen der einzelnen zu scannenden Websites.

Wenn eine Infektion gefunden wird, kann eine von drei möglichen Aktionen (beibehalten, säubern oder löschen) ausgeführt werden. Bei einer Löschung aus irgendeinem Grund, inklusive einer Säuberung, wird die Datei in den Papierkorb verschoben. Wenn der Papierkorb deaktiviert ist, wird die Datei unwiederbringlich gelöscht.

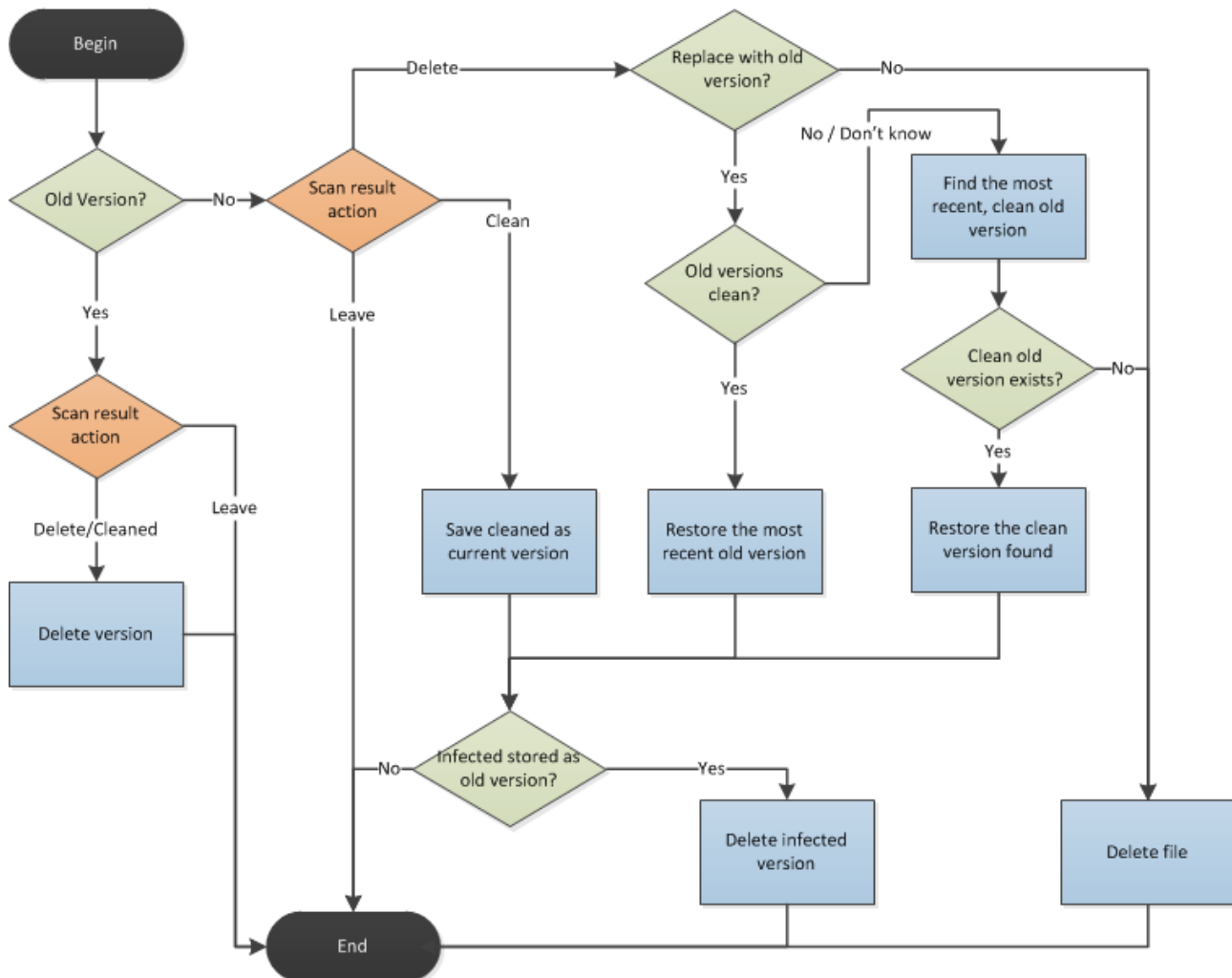
Wenn ältere Versionen einer Datei vorhanden sind und die Funktion **Dokumentversionen prüfen** aktiviert ist, werden die älteren Versionen des Dokuments zuerst überprüft.

Hinweise zur Überprüfung von Dokumentversionen:

- Sie können die Überprüfung älterer Dokumentversionen in den ESET Security for Microsoft SharePoint-Einstellungen aktivieren (Dokumentversionen prüfen).
- Wenn ein Dokument gesäubert werden muss, wird eine neue Version des Dokuments erstellt. Die infizierte Version wird in den Papierkorb verschoben.
- Ältere Versionen von Dokumenten können nicht gesäubert werden, nur gelöscht.
- Wenn die aktuelle Version eines Dokuments gelöscht wird, werden die älteren Versionen beibehalten.

Die neueste nicht infizierte Version wird anschließend als aktuelles Dokument deklariert. Dieses Verhalten kann in den Einstellungen aktiviert werden (Beim Löschen des Dokuments die letzte saubere Version wiederherstellen) und funktioniert auch, wenn die Option Dokumentversionen prüfen deaktiviert ist.

Dieses Diagramm zeigt die Verarbeitung der Prüfergebnisse und die nachfolgenden Aktionen bei der On-Demand-Datenbankprüfung:







Vorbereiten für die Installation

Bevor Sie Ihr Produkt installieren, sollten Sie einige Schritte ausführen:

- Laden Sie nach dem Kauf von ESET Security for Microsoft SharePoint das .msi-Installationspaket von der [ESET-Website](#) herunter.
- Vergewissern Sie sich, dass der Server, auf dem Sie ESET Security for Microsoft SharePoint installieren werden, die [Systemanforderungen](#) erfüllt.
- Melden Sie sich mit einem Administratorkonto beim Server an.

HINWEIS

Führen Sie das Installationsprogramm mit dem integrierten Administratorkonto oder einem Domänenadministratorkonto aus (falls das lokale Administratorkonto deaktiviert ist). Andere Benutzer haben nicht die erforderlichen Zugriffsrechte (auch dann nicht, wenn sie der Gruppe „Administratoren“ angehören). Verwenden Sie also immer das integrierte Administratorkonto, da die Installation nur mit einem lokalen oder Domänenadministratorkonto abgeschlossen werden kann.

- Falls Sie ein [Upgrade](#) von einer vorhandenen Installation von ESET Security for Microsoft SharePoint durchführen, sollten Sie die aktuelle Konfiguration mit der Funktion [Einstellungen exportieren](#) sichern.
- Entfernen /deinstallieren Sie bei Bedarf sämtliche Virenschutzlösungen von Drittanbietern von Ihrem System. Dazu empfehlen wir den [ESET AV Remover](#) . Eine Liste der Virenschutz-Software von Drittanbietern, die mit dem ESET AV Remover entfernt werden können, finden Sie in diesem [KB-Artikel](#) .
- Falls Sie ESET Security for Microsoft SharePoint unter Windows Server 2016 installieren, [empfiehlt](#)  Microsoft die [Deinstallation](#)  der Windows Defender-Funktionen und das Aufheben der Windows Server ATP-Registrierung, um Probleme zu vermeiden, die durch mehrere parallel installierte Virenschutzprodukte verursacht werden können.

Sie können das ESET Security for Microsoft SharePoint-Installationsprogramm in zwei verschiedenen Modi ausführen:

- [Grafische Benutzeroberfläche](#)

Die empfohlene Installationsart in Form eines Installationsassistenten.

- [Stille/unbeaufsichtigte Installation](#)

Sie können ESET Security for Microsoft SharePoint anstatt mit dem Assistenten auch unbeaufsichtigt über die Befehlszeile installieren.

WICHTIG

Installieren Sie ESET Security for Microsoft SharePoint nach Möglichkeit unbedingt auf einem neu installierten und konfigurierten Betriebssystem. Bei der Installation auf einem vorhandenen System sollten Sie die vorherige Version von ESET Security for Microsoft SharePoint deinstallieren, den Server neu starten und danach die neue Version von ESET Security for Microsoft SharePoint installieren.

- [Auf neuere Version aktualisieren](#)

Falls Sie eine ältere Version von ESET Security for Microsoft SharePoint verwenden, können Sie eine passende Upgrademethode auswählen.

Nachdem Sie Ihr ESET Security for Microsoft SharePoint erfolgreich installiert bzw. aktualisiert haben, können Sie zwischen den folgenden Aktivitäten wählen:

- [Produktaktivierung](#)

Die Verfügbarkeit einer bestimmten Aktivierungsmöglichkeit im Aktivierungsfenster hängt vom Land und vom Vertriebsweg ab.

- [Serverschutz konfigurieren](#)

Nehmen Sie Feineinstellungen an Ihrem ESET Security for Microsoft SharePoint vor, indem Sie die erweiterten Einstellungen der einzelnen Funktionen an Ihre Anforderungen anpassen.

WICHTIG

Wenn möglich, wird die Installation von ESET Security for Microsoft SharePoint auf einem neu installierten und konfigurierten Betriebssystem dringend empfohlen. Wenn Sie die Installation auf einem vorhandenen System vornehmen, sollten Sie die alte Version von ESET Security for Microsoft SharePoint deinstallieren, den Server neu starten und danach die neue Version von ESET Security for Microsoft SharePoint installieren.

- [Auf neuere Version aktualisieren](#) – Falls Sie eine ältere Version von ESET Security for Microsoft SharePoint verwenden, können Sie eine Upgrademethode auswählen.
- [Produktaktivierung](#) - Die Verfügbarkeit einer bestimmten Aktivierungsmöglichkeit im Aktivierungsfenster hängt vom Land und vom Vertriebsweg ab.
- [Verwaltung und Konfiguration](#) - Verwaltungs- und Konfigurationsoptionen

Systemanforderungen

Unterstützte Betriebssysteme:

- Microsoft Windows Server 2019
- Microsoft Windows Server 2016
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2008 R2 SP1 mit [KB4474419](#) und [KB4490628](#) installiert

HINWEIS

Falls Sie Microsoft Windows Server 2008 R2 SP1 verwenden, lesen Sie den Artikel [erforderliche Kompatibilität mit SHA-2](#) und stellen Sie sicher, dass auf Ihrem Betriebssystem alle erforderlichen Patches installiert sind.

Small Business Server:

- Microsoft Windows Server 2019 Essentials
- Microsoft Windows Server 2016 Essentials
- Microsoft Windows Server 2012 R2 Essentials
- Microsoft Windows Server 2012 Essentials
- Microsoft Windows Small Business Server 2011 SP1 (x64) mit [KB4474419](#) und [KB4490628](#) installiert

sowie die folgenden Anwendungsserver:

- Microsoft SharePoint Server 2019 (x64) - alle Editionen
- Microsoft SharePoint Server 2016 (x64) - alle Editionen
- Microsoft SharePoint Server 2013 (x64) - alle Editionen
- Microsoft SharePoint Server 2010 (x64) - alle Editionen
- Microsoft SharePoint Server 2007 (x86 und x64) - alle Editionen

Unterstützte Hyper-V-Hostbetriebssysteme:

- Microsoft Windows Server 2019
- Microsoft Windows Server 2016
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012
- [Microsoft Windows Server 2008 R2 SP1](#) - Virtuelle Computer können nur im Offlinebetrieb geprüft

werden

Die Hardware-Anforderungen sind abhängig von der verwendeten Version des Betriebssystems. Beachten Sie die Produktdokumentation für Microsoft Windows Server und Microsoft SharePoint Server für ausführliche Informationen zu Hardwareanforderungen.

HINWEIS

Installieren Sie unbedingt das neueste Service Pack für Ihr Microsoft Server-Betriebssystem und die jeweilige Serveranwendung, bevor Sie irgendein ESET-Sicherheitsprodukt installieren. Installieren Sie außerdem stets die neuesten verfügbaren Windows Updates und Hotfixes.

SHA-2-Kompatibilität erforderlich

Microsoft hat den Secure Hash Algorithm 1 (SHA-1) als veraltet markiert und Anfang 2019 mit dem Migrationsprozess zu SHA-2 begonnen. Daher werden alle mit dem SHA-1-Algorithmus signierten Zertifikate nicht mehr anerkannt und verursachen Sicherheitswarnungen. Leider hat die Sicherheit des SHA-1-Hashalgorithmus aufgrund von Schwachstellen im Algorithmus, zunehmender Prozessorleistung und dem Aufkommen von Cloud-Computing im Lauf der Zeit abgenommen.

Der SHA-2-Hashalgorithmus (als Nachfolger von SHA-1) ist jetzt die bevorzugte Methode, um die Zuverlässigkeit der SSL-Sicherheit zu gewährleisten. Weitere Details finden Sie im Microsoft Docs-Artikel über [Hash- und Signaturalgorithmen](#).

HINWEIS

Diese Änderung bedeutet, dass Ihre ESET-Sicherheitslösung auf Betriebssystemen ohne SHA-2-Unterstützung die Module, inklusive der Erkennungsroutine, nicht mehr aktualisieren kann. Dies bedeutet letztendlich, dass ESET Security for Microsoft SharePoint nicht vollständig funktioniert ist und Ihr Schutz unvollständig ist.

Falls Sie **Microsoft Windows 2008 R2 SP1**, **Microsoft Windows Small Business Server 2011 SP1** verwenden, stellen Sie sicher, dass Ihr System mit SHA-2 kompatibel ist. Installieren Sie die passenden Patches für Ihre Betriebssystemversion:

- **Microsoft Windows Server 2008 R2 SP1:** Installieren Sie [KB4474419](#) und [KB4490628](#) (möglicherweise ist ein zusätzlicher Systemneustart erforderlich)
- **Microsoft Windows Small Business Server 2011 SP1 (x64):** Installieren Sie [KB4474419](#) und [KB4490628](#) (möglicherweise ist ein zusätzlicher Systemneustart erforderlich)

WICHTIG

Nachdem Sie die Updates installiert und Ihr System neu gestartet haben, öffnen Sie die ESET Security for Microsoft SharePoint-Benutzeroberfläche, um den Status zu überprüfen. Falls der Status in Orange angezeigt wird, starten Sie das System noch einmal neu. Wenn der Status in Grün angezeigt wird, sind Sie optimal geschützt.

HINWEIS

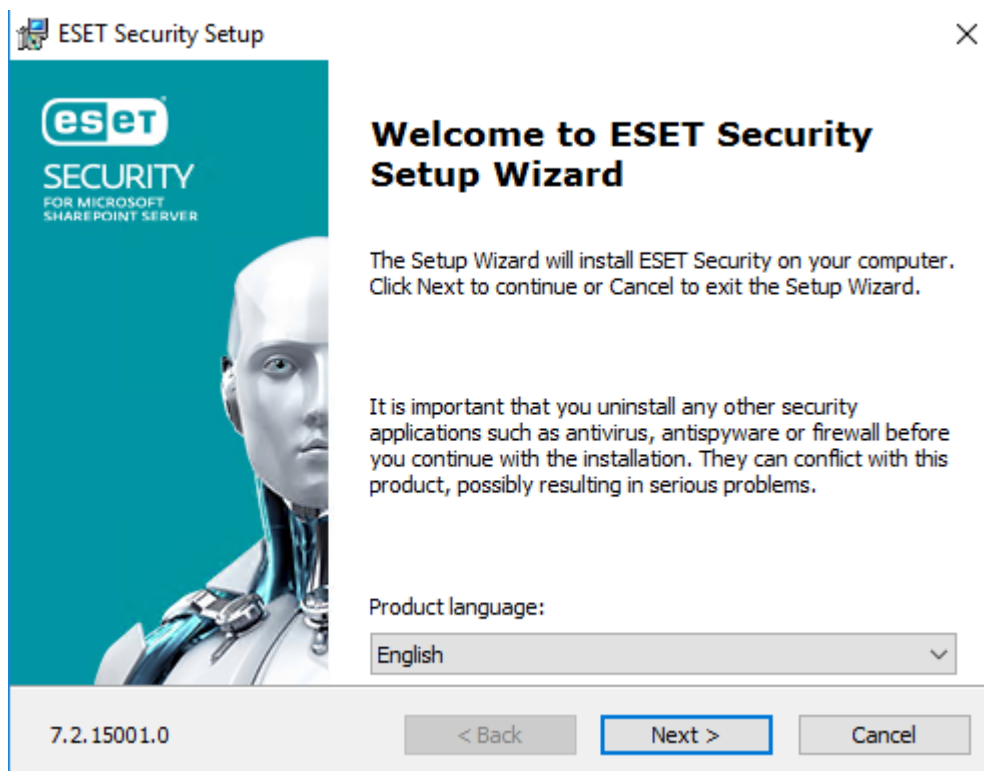
Installieren Sie unbedingt das neueste Service Pack für Ihr Microsoft Server-Betriebssystem und die jeweilige Serveranwendung. Installieren Sie außerdem stets die neuesten verfügbaren Windows Updates und Hotfixes.

ESET Security for Microsoft SharePoint

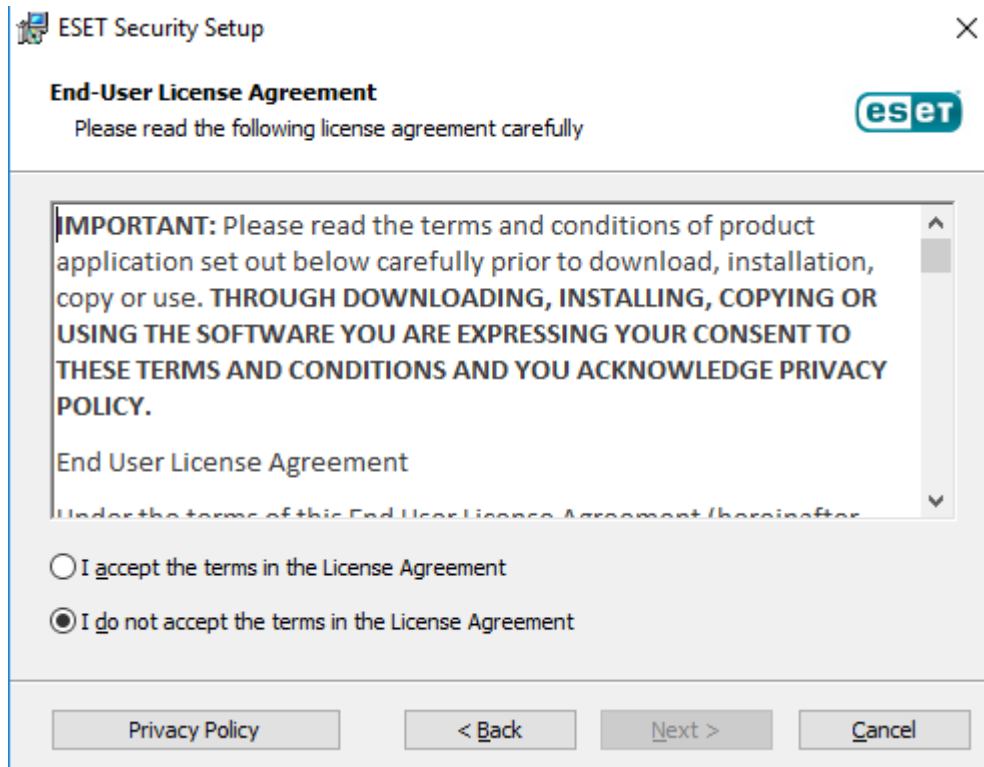
Installationsschritte

Dies ist eine typische Installation in Form eines grafischen Assistenten. Doppelklicken Sie auf das .msi-Paket und folgen Sie den Schritten, um ESET Security for Microsoft SharePoint zu installieren:

1. Klicken Sie auf **Weiter**, um fortzufahren, oder auf **Abbrechen**, um die Installation abzubrechen.
2. Der Installationsassistent wird in der Sprache ausgeführt, die in der Einstellung **Standort** unter **Region > Standort** in Ihrem Betriebssystem (oder **Aktueller Ort** unter **Region und Sprache > Standort** in älteren Systemen) festgelegt ist. Wählen Sie im Dropdownmenü eine **Produktsprache** aus, in der Sie Ihr ESET Security for Microsoft SharePoint installieren möchten. Die Sprachauswahl für ESET Security for Microsoft SharePoint ist unabhängig von der Anzeigesprache im Installationsassistenten.



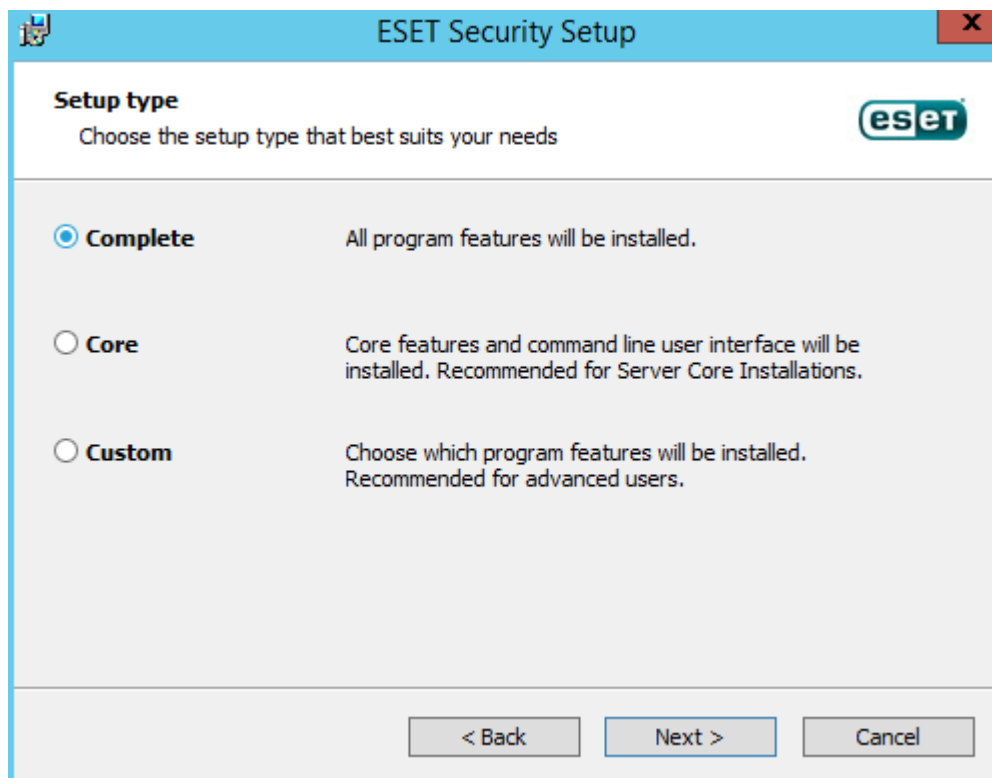
3. Wenn Sie auf **Weiter** klicken, wird die Endbenutzer-Lizenzvereinbarung angezeigt. Bestätigen Sie, dass Sie die Endbenutzer-Lizenzvereinbarung und die Datenschutzerklärung akzeptieren, und klicken Sie auf **Weiter**.



4. Wählen Sie eine der verfügbaren Installationsarten aus (Die Verfügbarkeit hängt von Ihrem Betriebssystem ab):

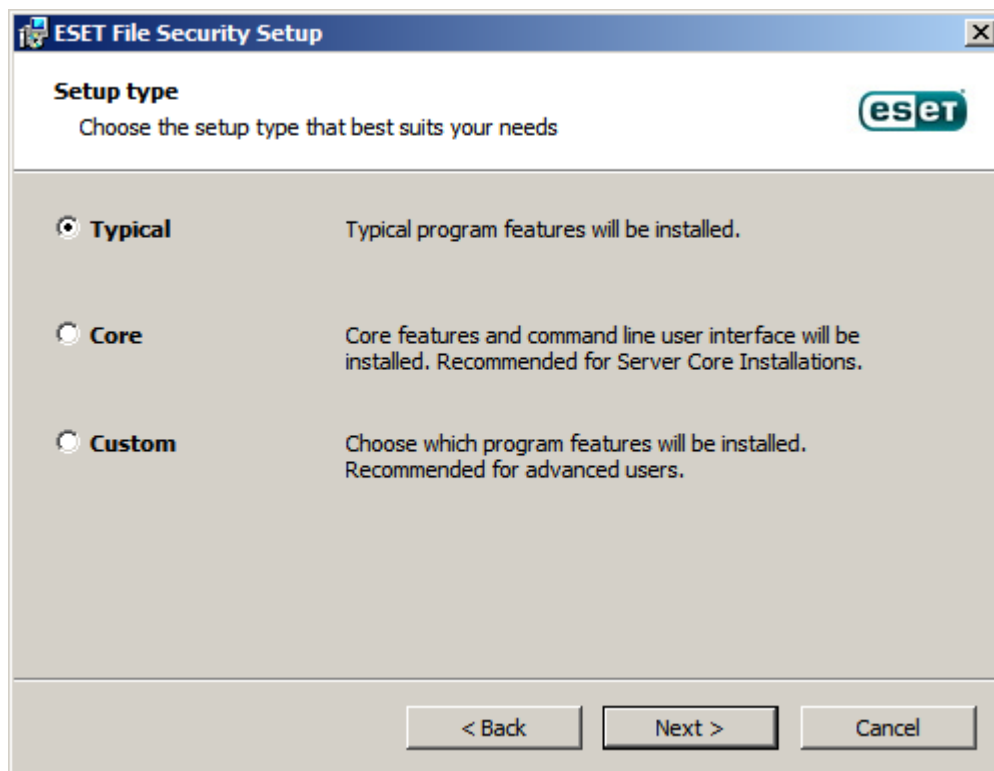
Vollständig

Installiert alle Funktionen von ESET Security for Microsoft SharePoint. Wird auch als vollständige Installation bezeichnet. Dies ist die empfohlene Installationsart, verfügbar für **Windows Server 2012, 2012 R2, 2016, 2019, Windows Server 2012 Essentials, 2012 R2 Essentials, 2016 Essentials und 2019 Essentials**.



Typisch

Installiert die empfohlenen Funktionen von ESET Security for Microsoft SharePoint. Verfügbar für **Windows Server 2008 R2 SP1, Windows Small Business Server 2011**.



Kern

Diese Installationsart ist für Windows Server Core-Editionen geeignet. Die Installationsschritte entsprechen denen der vollständigen Installation, es werden jedoch nur die Kernfunktionen und die Befehlszeilen-Benutzeroberfläche installiert. Die Kerninstallation ist hauptsächlich für Windows Server Core geeignet, kann jedoch bei Bedarf auch für normale Windows-Server verwendet werden. Mit der Core-Installation werden die ESET-Sicherheitsprodukte ohne grafische Benutzeroberfläche installiert. In diesem Fall können Sie also für die Arbeit mit ESET Security for Microsoft SharePoint nur die Befehlszeile verwenden. Weitere Informationen und sonstige Parameter finden Sie im Abschnitt [Installation über die Kommandozeile](#).

BEISPIEL

Führen Sie den folgenden Befehl aus, um die Core-Installation über die Befehlszeile zu starten:

```
msiexec /qn /i efs_w_nt64.msi ADDLOCAL=_Base
```

Benutzerdefiniert

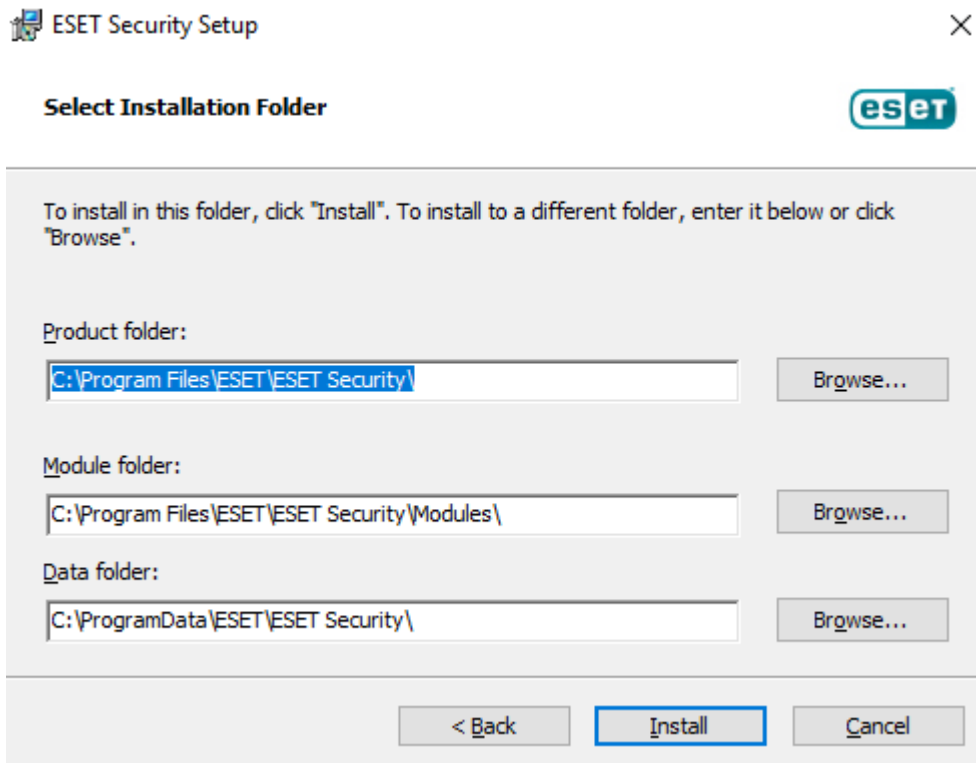
Wählen Sie aus, welche Programmfunktionen von ESET Security for Microsoft SharePoint auf dem System installiert werden. Vor der Installation wird eine Liste von Produktmodulen und Features angezeigt. Diese Installationsart ist hilfreich, wenn Sie nur die gewünschten Komponenten von ESET Security for Microsoft SharePoint installieren möchten.


HINWEIS

Unter Windows Server 2008 R2 SP1 ist die Installation der Komponente **Netzwerkschutz** standardmäßig deaktiviert (Installationsart **Typisch**). Wählen Sie den Installationstyp **Benutzerdefiniert** aus, um diese Komponente zu installieren.

5. Sie werden aufgefordert, einen Zielordner für die Installation von ESET Security for Microsoft SharePoint auszuwählen. Standardmäßig schlägt das Programm den Speicherort `C:\Program Files\ESET\ESET Security`

for Microsoft SharePoint vor. Klicken Sie auf **Durchsuchen**, um diesen Speicherort zu ändern (nicht empfohlen).

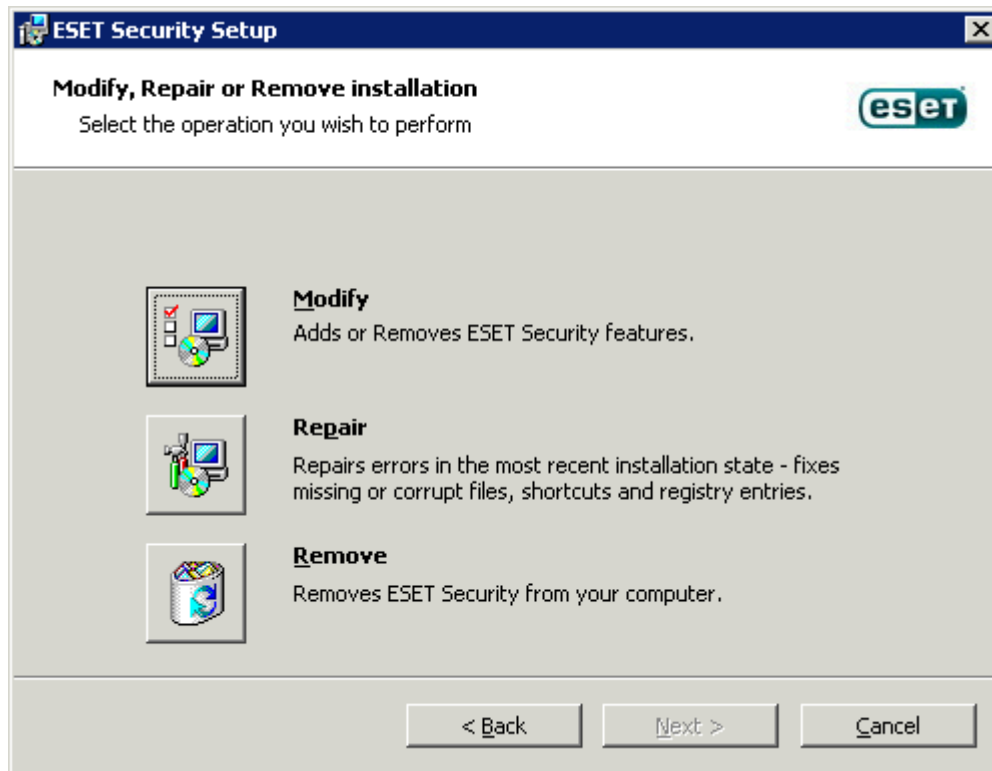


6. Klicken Sie auf **Installieren**, um die Installation zu starten. Nach Abschluss der Installation wird ein [Symbol im Infobereich](#)  angezeigt (in der Taskleiste).

Vorhandene Installation bearbeiten

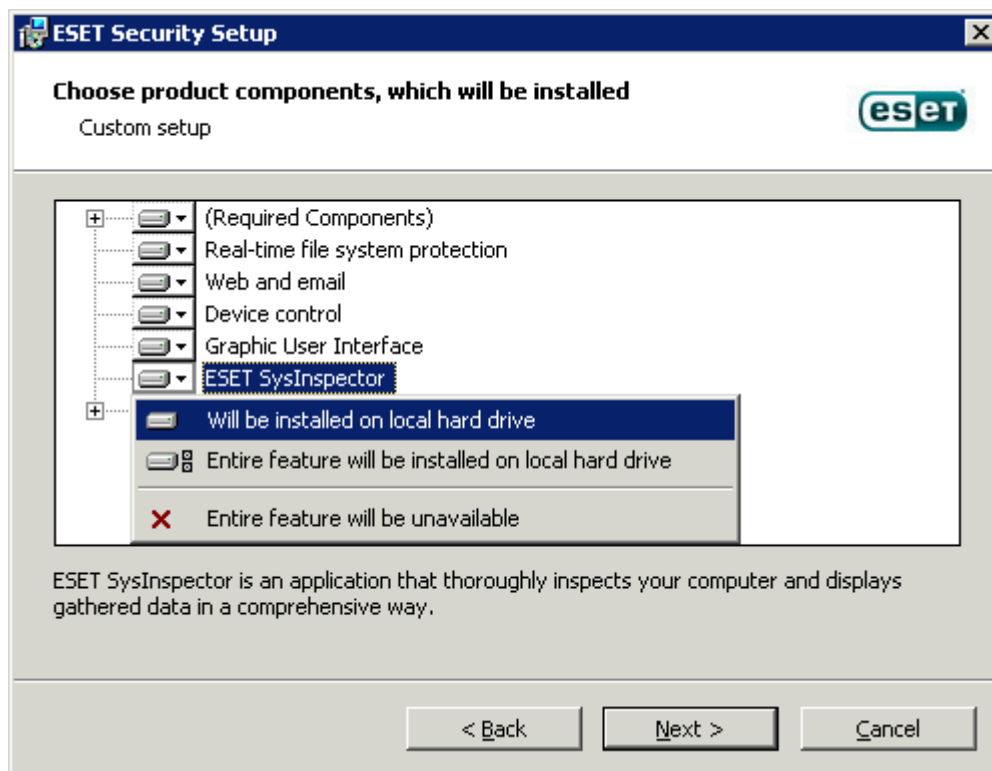
Sie können Komponenten zur vorhandenen Installation hinzufügen oder aus der Installation entfernen. Führen Sie dazu entweder das .msi-Installationspaket aus, das Sie für die ursprüngliche Installation verwendet haben, oder öffnen Sie **Programme und Funktionen** in der Windows-Systemsteuerung. Klicken Sie mit der rechten Maustaste auf ESET Security for Microsoft SharePoint und wählen Sie **Ändern** aus. Befolgen Sie die nachstehenden Schritte, um Komponenten hinzuzufügen oder zu entfernen.

Sie haben 3 Optionen zur Auswahl: **Ändern** der installierten Komponenten, **Reparieren** der Installation von ESET Security for Microsoft SharePoint oder **Entfernen** bzw. vollständiges Deinstallieren.



Wenn Sie **Ändern** auswählen, wird eine Liste der verfügbaren Programmkomponenten angezeigt.

Wählen Sie aus, welche Komponenten hinzugefügt oder entfernt werden sollen. Sie können mehrere Komponenten gleichzeitig hinzufügen/entfernen. Klicken Sie auf die Komponente und wählen Sie im Dropdownmenü eine Option aus:



Nachdem Sie eine Option ausgewählt haben, klicken Sie auf **Ändern**, um die Änderungen vorzunehmen.

HINWEIS

Sie können installierte Komponenten jederzeit ändern, indem Sie das Installationsprogramm ausführen. Für die meisten Komponenten ist kein Serverneustart erforderlich, um die Änderungen zu übernehmen. Die grafische Benutzeroberfläche wird neu gestartet, und es werden nur die zur Installation ausgewählten Komponenten angezeigt. Falls ein Serverneustart erforderlich ist, werden Sie vom Windows-Installationsprogramm dazu aufgefordert, und die Komponenten sind verfügbar, sobald der Server wieder online ist.

Stille/unbeaufsichtigte Installation

Führen Sie den folgenden Befehl aus, um die Installation über die Befehlszeile zu starten: `msiexec /i <packagename> /qn /l*xv msi.log`

HINWEIS


Unter Windows Server 2008 R2 SP1 wird die Funktion **Netzwerkschutz** nicht installiert.

Um zu überprüfen, ob die Installation erfolgreich war, oder falls Probleme bei der Installation auftreten, öffnen Sie die Windows-Ereignisansicht und überprüfen Sie das **Anwendungsprotokoll** (suchen Sie nach Einträgen von der Quelle MsiInstaller).

BEISPIEL

Vollständige Installation auf einem 64-Bit-System:

```
msiexec /i eshp_nt64.msi /qn /l*xv msi.log ADDLOCAL=NetworkProtection,RealtimeProtection,^
DeviceControl,DocumentProtection,Cluster,GraphicUserInterface,SysInspector,SysRescue,Rmm,eula
```

Nach Abschluss der Installation wird die ESET-GUI gestartet und ein [Symbol im Infobereich](#)  angezeigt (in der Taskleiste).

BEISPIEL

Installation des Produkts in der **angegebenen Sprache** (Deutsch):

```
msiexec /i eshp_nt64.msi /qn ADDLOCAL=NetworkProtection,RealtimeProtection,^
DeviceControl,DocumentProtection,Cluster,GraphicUserInterface,^
SysInspector,SysRescue,Rmm,eula PRODUCT_LANG=1031 PRODUCT_LANG_CODE=de-de
```

Siehe **Sprachparameter** unter [Installation über die Kommandozeile](#) für weitere Details und eine Liste der Sprachcodes.

WICHTIG

Wenn Sie Werte für den Parameter **REINSTALL** angeben, müssen Sie die restlichen Features auflisten, die nicht als Werte für die Parameter **ADDLOCAL** bzw. **REMOVE** verwendet werden. Bei der Installation über die Kommandozeile müssen Sie alle Funktionen als Werte für die Parameter **REINSTALL**, **ADDLOCAL** und **REMOVE** angeben. Wenn Sie den Parameter **REINSTALL** nicht verwenden, können werden die Features möglicherweise nicht hinzugefügt oder entfernt werden.

Im Abschnitt [Installation über die Kommandozeile](#) finden Sie eine vollständige Liste der Features.

BEISPIEL

Vollständige Deinstallation auf einem 64-Bit-System:

```
msiexec /x eshp_nt64.msi /qn /l*xv msi.log
```

Ihr Server wird nach der erfolgreichen Deinstallation automatisch neu gestartet.

Installation über die Kommandozeile

Die folgenden Einstellungen sind nur mit den Einstellungen **reduziert**, **einfach** und **keine** der Benutzeroberfläche geeignet. Weitere Informationen zur **msiexec**-Version für die Befehlszeilenschalter finden Sie in der [Dokumentation](#).

Unterstützte Parameter:

APPDIR=<Pfad>

- Pfad – gültiger Verzeichnispfad
- Installationsverzeichnis der Anwendung
- Beispiel: `eshp_nt64.msi /qn APPDIR=C:\ESET\ ADDLOCAL=DocumentProtection`

APPDATADIR=<Pfad>

- Pfad – gültiger Verzeichnispfad
- Installationsverzeichnis der Anwendungsdaten

MODULEDIR=<Pfad>

- Pfad: gültiger Verzeichnispfad
- Installationsverzeichnis des Moduls

ADDLOCAL=<Liste>

- Komponenteninstallation: Liste nicht obligatorischer Funktionen, die lokal installiert werden sollen.
- Verwendung mit `.msi`-Paketen von ESET: `eshp_nt64.msi /qn ADDLOCAL=<list>`
- Weitere Informationen zur `ADDLOCAL`-Eigenschaft finden Sie unter <https://docs.microsoft.com/en-gb/windows/desktop/Msi/addlocal>
- Die `ADDLOCAL`-Liste ist eine kommasetrennte Liste der Namen aller zu installierenden Funktionen.
- Wenn Sie eine Funktion für die Installation auswählen, muss der gesamte Pfad (alle übergeordneten Funktionen) explizit in der Liste aufgeführt werden.

REMOVE=<Liste>

- Komponenteninstallation – Übergeordnetes Feature, das Sie nicht lokal installieren möchten.
- Verwendung mit `.msi` -Paketen von ESET: `eshp_nt64.msi /qn REMOVE=<list>`
- Weitere Informationen zur `REMOVE`-Eigenschaft finden Sie unter <https://docs.microsoft.com/en-gb/windows/desktop/Msi/remove>
- Die `REMOVE`-Liste ist eine kommasetrennte Liste der übergeordneten Features, die nicht installiert bzw. entfernt werden, falls sie bereits installiert sind.
- Es reicht aus, das übergeordnete Feature anzugeben. Sie müssen nicht jedes untergeordnete Feature einzeln zur Liste hinzufügen.

ADDEXCLUDE=<Liste>

- Die `ADDEXCLUDE`-Liste ist eine kommasetrennte Liste der Namen aller Features, die nicht installiert werden sollen.
- Wenn Sie eine Funktion auswählen, die nicht installiert werden soll, müssen der gesamte Pfad (alle untergeordneten Features) sowie verwandte unsichtbare Features ausdrücklich in der Liste aufgeführt

werden.

- Beispiel: `eshp_nt64.msi /qn ADDEXCLUDE=<list>`

HINWEIS

ADDEXCLUDE kann nicht zusammen mit ADDLOCAL verwendet werden.

Vorhandensein der Funktion

- **Obligatorisch** – Die Funktion wird immer installiert.
- **Optional** – Die Installation der Funktion kann abgewählt werden.
- **Unsichtbar** – logische Funktion, die für das Funktionieren anderer Funktionen erforderlich ist

Liste der ESET Security for Microsoft SharePoint-Features:

WICHTIG

Die Namen der Features unterscheiden zwischen Groß- und Kleinschreibung. `RealtimeProtection` ist nicht gleich `REALTIMEPROTECTION`.

Funktionsname	Vorhandensein der Funktion
SERVER	Obligatorisch
RealtimeProtection	Optional
WMIProvider	Obligatorisch
HIPS	Obligatorisch
Updater	Obligatorisch
eShell	Obligatorisch
UpdateMirror	Obligatorisch
DeviceControl	Optional
DocumentProtection	Optional
WebAndEmail	Optional
ProtocolFiltering	Unsichtbar
NetworkProtection	Optional
IdsAndBotnetProtection	Optional
Rmm	Optional
WebAccessProtection	Optional
EmailClientProtection	Optional
MailPlugins	Unsichtbar
Cluster	Optional
_Base	Obligatorisch
eula	Obligatorisch
ShellExt	Optional
_FeaturesCore	Obligatorisch
GraphicUserInterface	Optional
SysInspector	Optional
SysRescue	Optional

Funktionsname	Vorhandensein der Funktion
EnterpriseInspector	Optional

Falls Sie eines der folgenden Features entfernen möchten, müssen Sie die gesamte Gruppe entfernen, indem Sie alle Features in der Gruppe einzeln angeben. Andernfalls wird das Feature nicht entfernt. Hier sehen Sie zwei Gruppen (jede Zeile steht für eine Gruppe):

GraphicUserInterface,ShellExt

NetworkProtection,WebAccessProtection,IdsAndBotnetProtection^
ProtocolFiltering,MailPlugins,EmailClientProtection

BEISPIEL

Schließen Sie den Bereich **NetworkProtection** (inklusive der untergeordneten Features mit dem Parameter REMOVE von der Installation aus und geben Sie nur das übergeordnete Feature an:

```
msiexec /i eshp_nt64.msi /qn ADDLOCAL=ALL REMOVE=NetworkProtection
```

Alternativ können Sie den Parameter ADDEXCLUDE verwenden, in diesem Fall müssen Sie jedoch alle untergeordneten Features angeben:

```
msiexec /i eshp_nt64.msi /qn ADDEXCLUDE=NetworkProtection,WebAccessProtection^  
IdsAndBotnetProtection,ProtocolFiltering,MailPlugins,EmailClientProtection
```

BEISPIEL

Beispiel für **Kerninstallation**:

```
msiexec /qn /i eshp_nt64.msi /l*xv msi.log ADDLOCAL=RealtimeProtection,Rmm
```

Sie können einfache Konfigurationsparameter im Installationsbefehl angeben, um Ihr ESET Security for Microsoft SharePoint nach der Installation automatisch zu konfigurieren.

BEISPIEL



ESET Security for Microsoft SharePoint installieren und ESET LiveGrid® deaktivieren:

```
msiexec /qn /i eshp_nt64.msi ADDLOCAL=RealtimeProtection,Rmm,GraphicUserInterface CFG_LIVEGRID_ENABLED=0
```

Liste aller Konfigurationseigenschaften:

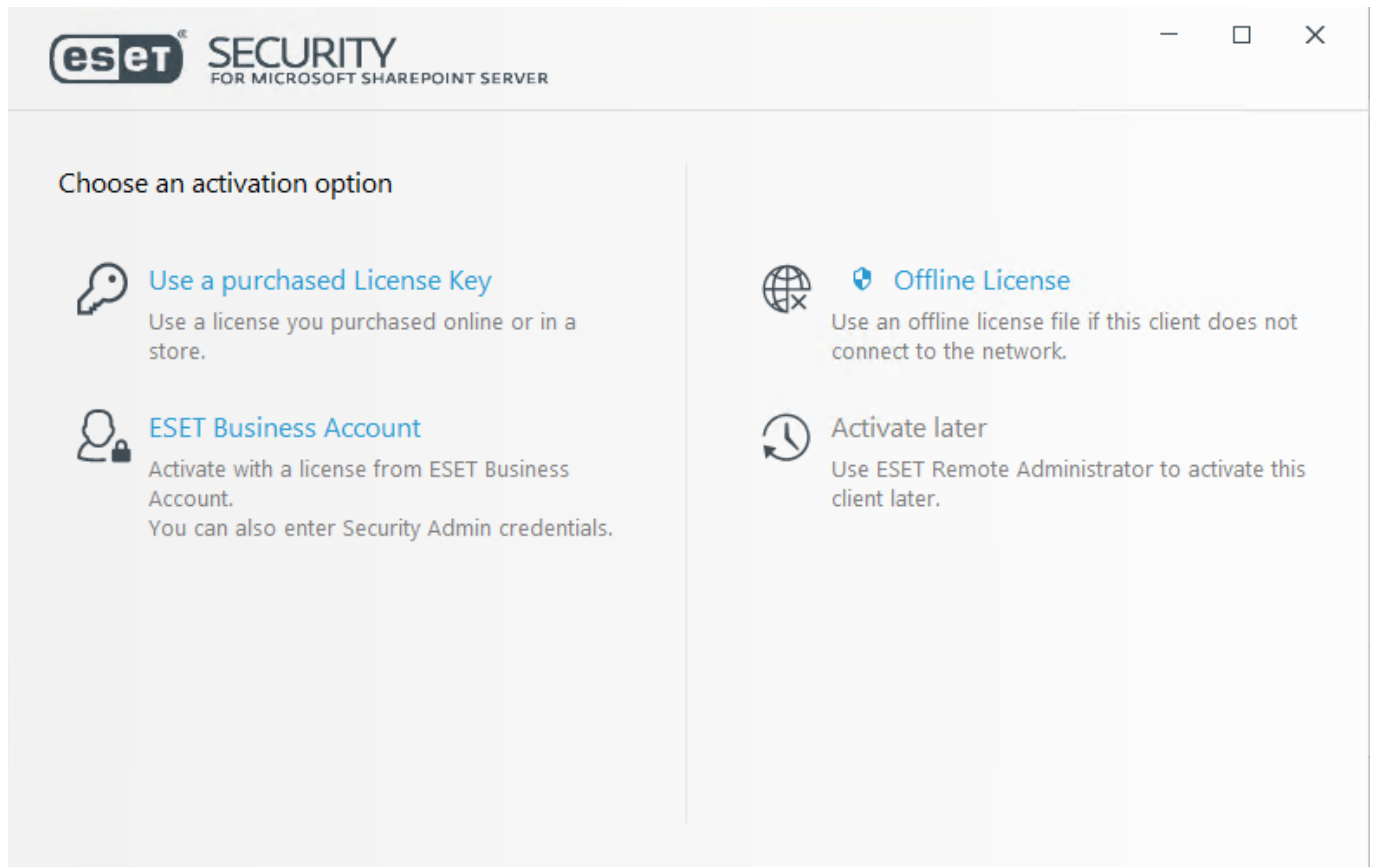
Schalter	Wert
CFG_POTENTIALLYUNWANTED_ENABLED=1/0	0 – deaktiviert, 1 – aktiviert
CFG_LIVEGRID_ENABLED=1/0	0 – deaktiviert, 1 – aktiviert
FIRSTSCAN_ENABLE=1/0	0 – deaktiviert, 1 – aktiviert
CFG_PROXY_ENABLED=0/1	0 – deaktiviert, 1 – aktiviert
CFG_PROXY_ADDRESS=<ip>	IP-Adresse des Proxyservers
CFG_PROXY_PORT=<port>	Proxy-Portnummer
CFG_PROXY_USERNAME=<user>	Benutzername für die Authentifizierung
CFG_PROXY_PASSWORD=<pass>	Passwort für die Authentifizierung

Sprachparameter: Produktsprache (beide Parameter müssen angegeben werden)

Schalter	Wert
PRODUCT_LANG=	LCID-Dezimalzahl (Gebietsschema-ID), zum Beispiel 1033 für <i>English - United States</i> (siehe auch Liste der Sprachcodes  .
PRODUCT_LANG_CODE=	LCID-Zeichenfolge in Kleinbuchstaben, zum Beispiel en-us für <i>English - United States</i> (siehe auch Liste der Sprachcodes  .

Produktaktivierung

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



Sie können ESET Security for Microsoft SharePoint mit einer der folgenden Methoden aktivieren:

Lizenzschlüssel eingeben

Eine eindeutige Zeichenfolge im Format XXXX-XXXX-XXXX-XXXX-XXXX zur Identifizierung des Lizenzinhabers und der Aktivierung der Lizenz.


ESET Business Account

Verwenden Sie diese Option, wenn Sie bereits registriert sind und über ein [ESET Business Account \(EBA\)](#) verfügen, in das Sie Ihre ESET Security for Microsoft SharePoint-Lizenz importiert haben. Sie können auch die Anmeldeinformationen eines **Sicherheitsadministrators** eingeben, die Sie im [ESET Lizenzadministrator-Portal](#) verwenden.

Offline-Lizenzdatei

Eine automatisch generierte Datei, die zur Bereitstellung von Lizenzinformationen in das ESET-Produkt übertragen wird. Die Offline-Lizenzdatei wird im Lizenzportal generiert und in Umgebungen verwendet, in denen die Anwendung keine Verbindung zur Lizenzierungsstelle herstellen kann.

Klicken Sie auf **Später mit ESET Security Management Center aktivieren**, wenn der Computer Teil eines verwalteten Netzwerks ist und der Administrator die Aktivierung remote über [ESET Security Management Center](#) ausführt. Wählen Sie diese Option nur, wenn der Client später aktiviert werden soll.

Sie können jederzeit im Hauptprogrammfenster auf **Hilfe und Support** > **Lizenz verwalten** klicken, um Ihre Lizenzinformationen zu verwalten. Hier wird die öffentliche Lizenz-ID angezeigt, mit der Ihr Produkt von ESET identifiziert werden kann und die Lizenzinformationen enthält. Ihr Benutzername, unter dem der Computer registriert ist, befindet sich im Bereich [Über](#), den Sie per Rechtsklick auf das Symbol  im Infobereich der Taskleiste erreichen.

Nach der erfolgreichen Aktivierung von ESET Security for Microsoft SharePoint wird das Hauptprogrammfenster geöffnet. Auf der Seite [Überwachung](#) wird der aktuelle Status angezeigt. Bei der ersten Verwendung sind möglicherweise einige Eingaben erforderlich, beispielsweise müssen Sie angeben, ob Sie an ESET LiveGrid® teilnehmen möchten.

Im Hauptprogrammfenster werden außerdem Benachrichtigungen zu anderen Elementen wie System-Updates (Windows Update) oder Updates der Erkennungsroutine angezeigt. Wenn alle Elemente, die Ihre Aufmerksamkeit erfordern, aufgelöst sind, wird der Überwachungsstatus in grün zusammen mit der Statusmeldung **Sie sind geschützt** angezeigt.

Sie können das Produkt auch im Hauptmenü unter **Hilfe und Support** > **Produkt aktivieren** oder **Schutzstatus** > **Produkt ist nicht aktiviert** aktivieren.


HINWEIS

ESET Security Management Center kann Clientcomputer mithilfe von Lizenzen, die der Administrator bereitstellt, im Hintergrund aktivieren.

ESET Business Account

Mit einem ESET Business Account können Sie mehrere Lizenzen verwalten. Wenn Sie noch keinen ESET Business Account haben, klicken Sie auf **Konto erstellen**. Anschließend werden Sie zum ESET Business Account Portal weitergeleitet und können sich registrieren.

HINWEIS

Weitere Informationen finden Sie im Benutzerhandbuch zum [ESET Business Account \(EBA\)](#) .

Falls Sie Sicherheitsadmin-Anmeldeinformationen verwenden und Ihr Passwort vergessen haben, klicken Sie auf **Ich habe mein Passwort vergessen**. Daraufhin werden Sie zum ESET License Administrator-Portal weitergeleitet. Geben Sie Ihre E-Mail-Adresse ein und klicken Sie auf **Senden**. Sie erhalten in Kürze eine Nachricht mit Anweisungen zum Zurücksetzen Ihres Passworts.

Erfolgreiche Aktivierung

Die Aktivierung erfolgreich und ESET Security for Microsoft SharePoint ist nun aktiviert. Ab jetzt erhält ESET Security for Microsoft SharePoint regelmäßige Updates, um die neuesten Bedrohungen zu erkennen und Ihren Computer zu schützen. Klicken Sie auf **Fertig**, um die Produktaktivierung abzuschließen.

Aktivierungsfehler

Die Aktivierung von ESET Security for Microsoft SharePoint war nicht erfolgreich. Vergewissern Sie sich, dass Sie den richtigen **Lizenzschlüssel** eingegeben oder eine **Offline-Lizenz** angehängt haben. Wenn Sie über eine andere

Offline-Lizenz verfügen, geben Sie sie erneut ein. Um den eingegebenen Lizenzschlüssel zu überprüfen, klicken Sie auf **Lizenzschlüssel erneut prüfen** oder **geben Sie eine andere Lizenz** ein.

Lizenz

Sie werden aufgefordert, eine mit Ihrem Konto verknüpfte Lizenz auszuwählen, die für ESET Security for Microsoft SharePoint verwendet wird. Klicken Sie auf **Weiter**, um die Aktivierung fortzusetzen.

Auf neuere Version aktualisieren

Neuere Versionen von ESET Security for Microsoft SharePoint werden veröffentlicht, um Verbesserungen bereitzustellen oder Probleme zu korrigieren, die mit einem automatischen Update der Programmmodule nicht behoben werden können.

Upgrademethoden:

- **Deinstallation / Installation** – Bei dieser Methode wird die zunächst die alte Version entfernt und anschließend die neue Version installiert. Laden Sie die neueste Version von ESET Security for Microsoft SharePoint herunter. [Exportieren Sie die Einstellungen](#) aus Ihrem aktuellen ESET Security for Microsoft SharePoint, falls Sie die Konfiguration beibehalten möchten. Deinstallieren Sie ESET Security for Microsoft SharePoint und starten Sie den Server neu. Führen Sie eine [frische Installation](#) mit dem heruntergeladenen Installationsprogramm durch. [Importieren Sie die Einstellungen](#), um Ihre Konfiguration zu laden. Wir empfehlen diesen Vorgang, falls Sie einen einzigen Server mit ESET Security for Microsoft SharePoint verwenden.
- **Vor Ort** – Bei dieser Upgrademethode wird die neue Version von ESET Security for Microsoft SharePoint über die vorhandene Version installiert, ohne diese zu entfernen.

WICHTIG

Achten Sie darauf, dass auf Ihrem Server **keine Windows Updates ausstehen** und kein **Neustart** aufgrund von Windows Updates oder aus anderen Gründen geplant ist. Wenn Sie versuchen, ein Vor-Ort-Upgrade auf einem Computer mit ausstehendem Windows Update oder Neustart auszuführen, wird die vorhandene Version von ESET Security for Microsoft SharePoint möglicherweise nicht korrekt entfernt. Außerdem können Probleme auftreten, wenn Sie anschließend versuchen, die alte Version von ESET Security for Microsoft SharePoint manuell zu entfernen.

HINWEIS

Während des Upgrades von ESET Security for Microsoft SharePoint muss der Server neu gestartet werden.

- [Remote](#) - Für große Netzwerkumgebungen, die mit ESET Security Management Center verwaltet werden. Dies ist eine saubere Upgrademethode, die remote ausgeführt wird. Dieses Verfahren ist hilfreich, wenn Sie mehrere Server mit ESET Security for Microsoft SharePoint betreiben.
- [ESET-Clusterassistent](#) - Kann auch als Upgrademethode verwendet werden. Verwenden Sie dieses Verfahren, falls Ihre Umgebung mindestens zwei Server mit ESET Security for Microsoft SharePoint enthält. Dies ist eine Vor-Ort-Upgrademethode, die über das ESET-Cluster ausgeführt wird. Außerdem können Sie das [ESET-Cluster](#) nach der Aktualisierung beibehalten und dessen Funktionen weiterhin nutzen.

WICHTIG

Beim Upgrade von Version 4.x werden nicht alle Einstellungen beibehalten. Insbesondere Regeln können nicht migriert werden. Der Grund hierfür sind Änderungen an der Regelfunktion, die in späteren Versionen eingeführt wurden. Notieren Sie sich daher Ihre Regeleinstellungen, bevor Sie ein Upgrade von einer 4.x-Version durchführen. Nach Abschluss des Upgrades können Sie [Regeln](#) einrichten. Die neuen Regeln bieten mehr Flexibilität und mehr Möglichkeiten im Vergleich zu den Regeln in früheren Versionen von ESET Security for Microsoft SharePoint.

HINWEIS

Nach der Aktualisierung von ESET Security for Microsoft SharePoint sollten Sie die Einstellungen überprüfen, um sicherzustellen, dass die Software korrekt nach Ihren Anforderungen konfiguriert ist.

Upgrades über ESMC

[ESET Security Management Center](#) ermöglicht Upgrades für mehrere Server, auf denen ältere Versionen von ESET Security for Microsoft SharePoint laufen. Mit dieser Methode können Sie eine große Anzahl an Servern gleichzeitig aktualisieren und dabei sicherstellen, dass alle Instanzen von ESET Security for Microsoft SharePoint identisch konfiguriert sind (falls gewünscht).

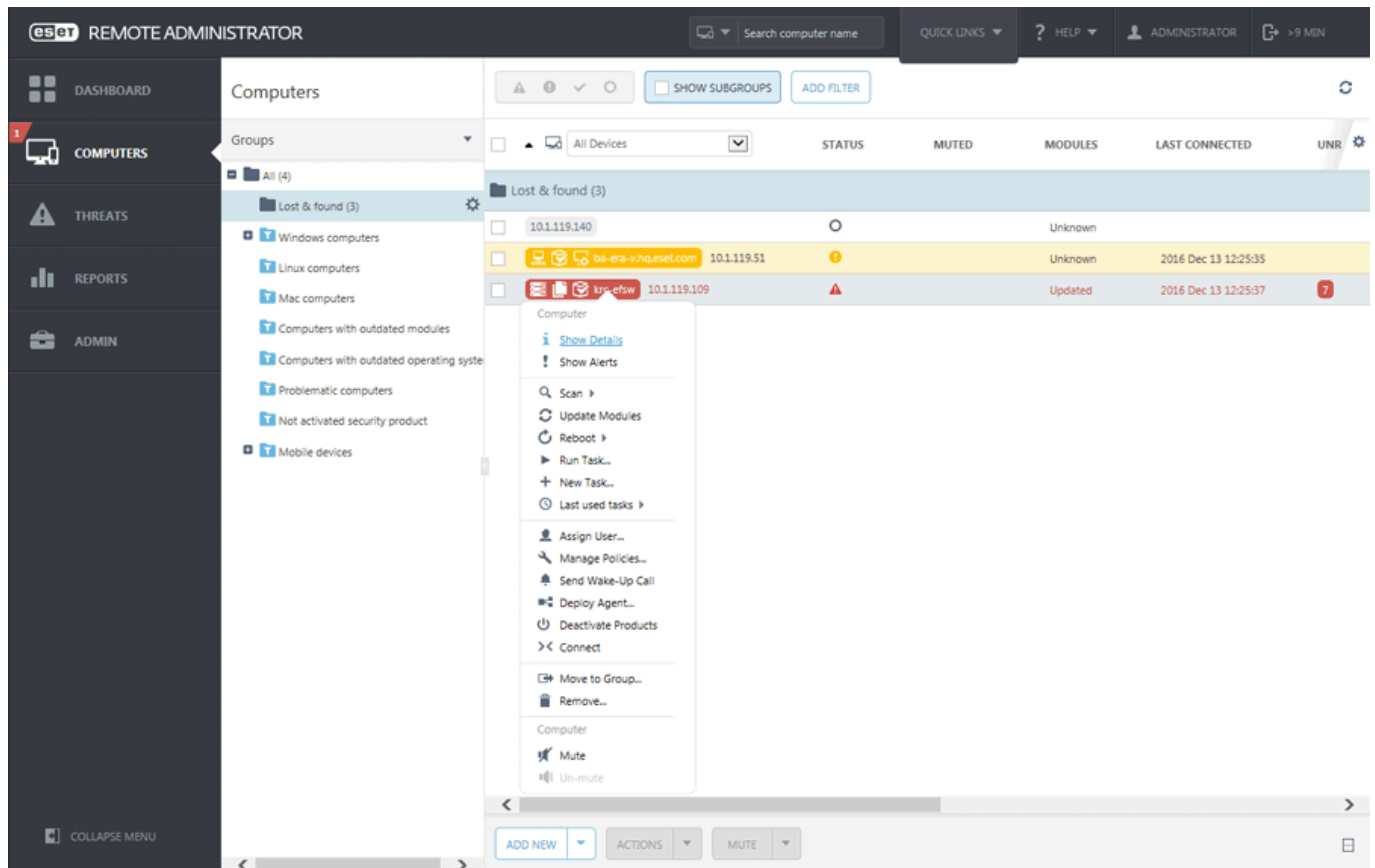
Das Verfahren umfasst die folgenden Phasen:

- **Aktualisieren Sie den ersten Server** manuell, indem Sie die aktuelle Version von ESET Security for Microsoft SharePoint über ihre vorhandene Version installieren, um sämtliche Konfigurationselemente beizubehalten, inklusive Regeln, verschiedene Positiv- und Negativlisten usw. Dieser Schritt wird lokal auf dem Server ausgeführt, auf dem ESET Security for Microsoft SharePoint läuft.
- **Fordern Sie die Konfiguration** des auf Version 7.x aktualisierten ESET Security for Microsoft SharePoint an und **konvertieren Sie die Konfiguration** in ESET Security Management Center zu einer Policy, die später auf alle aktualisierten Server angewendet wird. Dieser und die folgenden Schritte werden remote mithilfe von ESMC ausgeführt.
- **Führen Sie den Task Software-Deinstallation** auf allen Servern aus, auf denen eine alte Version von ESET Security for Microsoft SharePoint läuft.
- **Führen Sie den Task Software-Installation** auf allen Servern aus, die Sie auf die aktuelle Version von ESET Security for Microsoft SharePoint aktualisieren möchten.
- **Weisen Sie die Konfigurationsrichtlinie** zu allen Servern zu, auf denen die aktuelle Version von ESET Security for Microsoft SharePoint läuft.
- **Legen Sie das Administratorkonto für die SharePoint-Farm** auf jedem Server manuell fest. Dieser Schritt wird lokal ausgeführt.

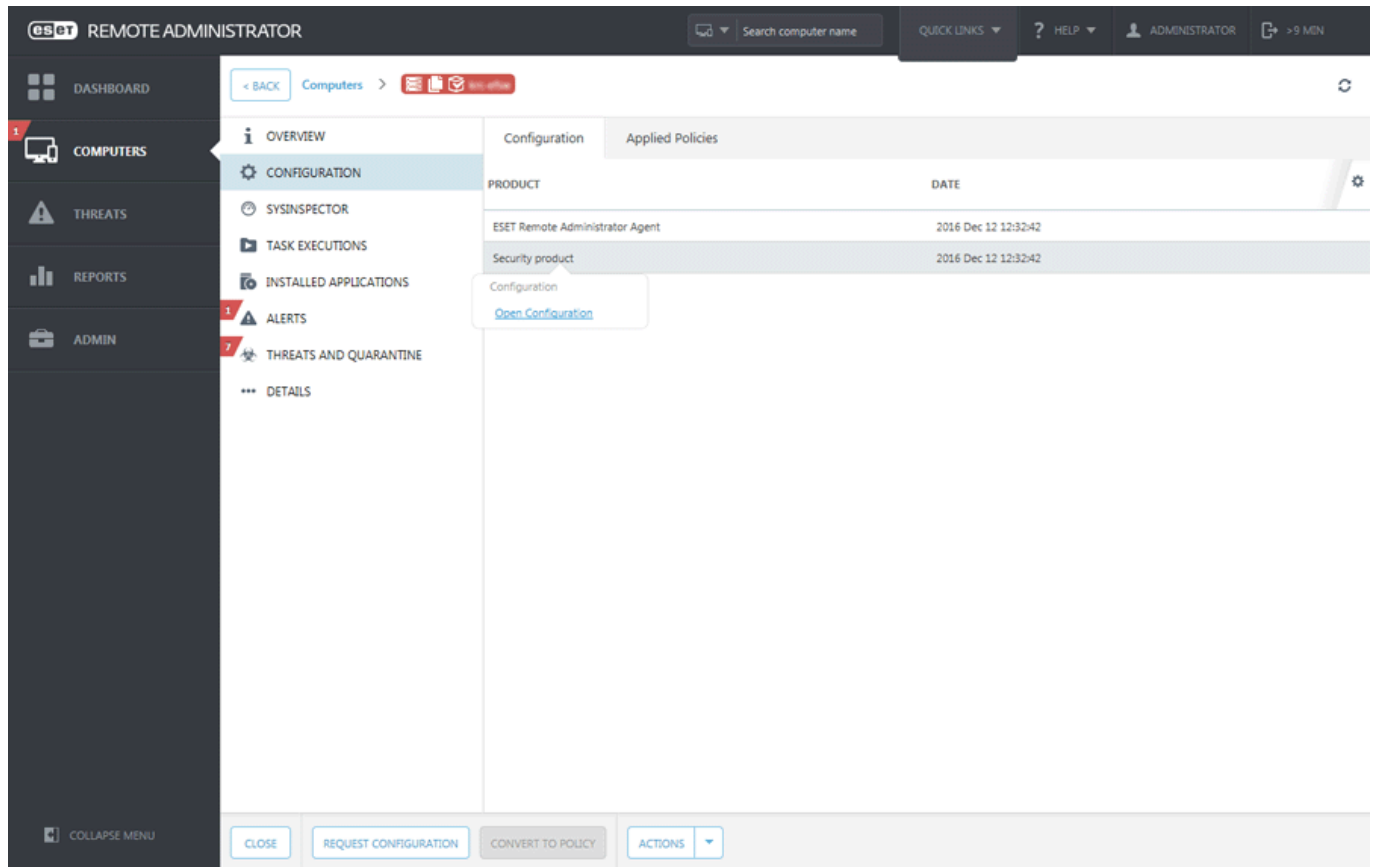
Schritt-für-Schritt-Anleitung:

1. Melden Sie sich bei einem der Server an, auf denen ESET Security for Microsoft SharePoint läuft, und führen Sie ein Upgrade durch, indem Sie die aktuelle Version herunterladen und über die vorhandene Version installieren. Führen Sie die [Schritte für eine normale Installation](#) durch. Die gesamte Konfiguration Ihrer alten ESET Security for Microsoft SharePoint-Version bleibt bei der Installation erhalten.

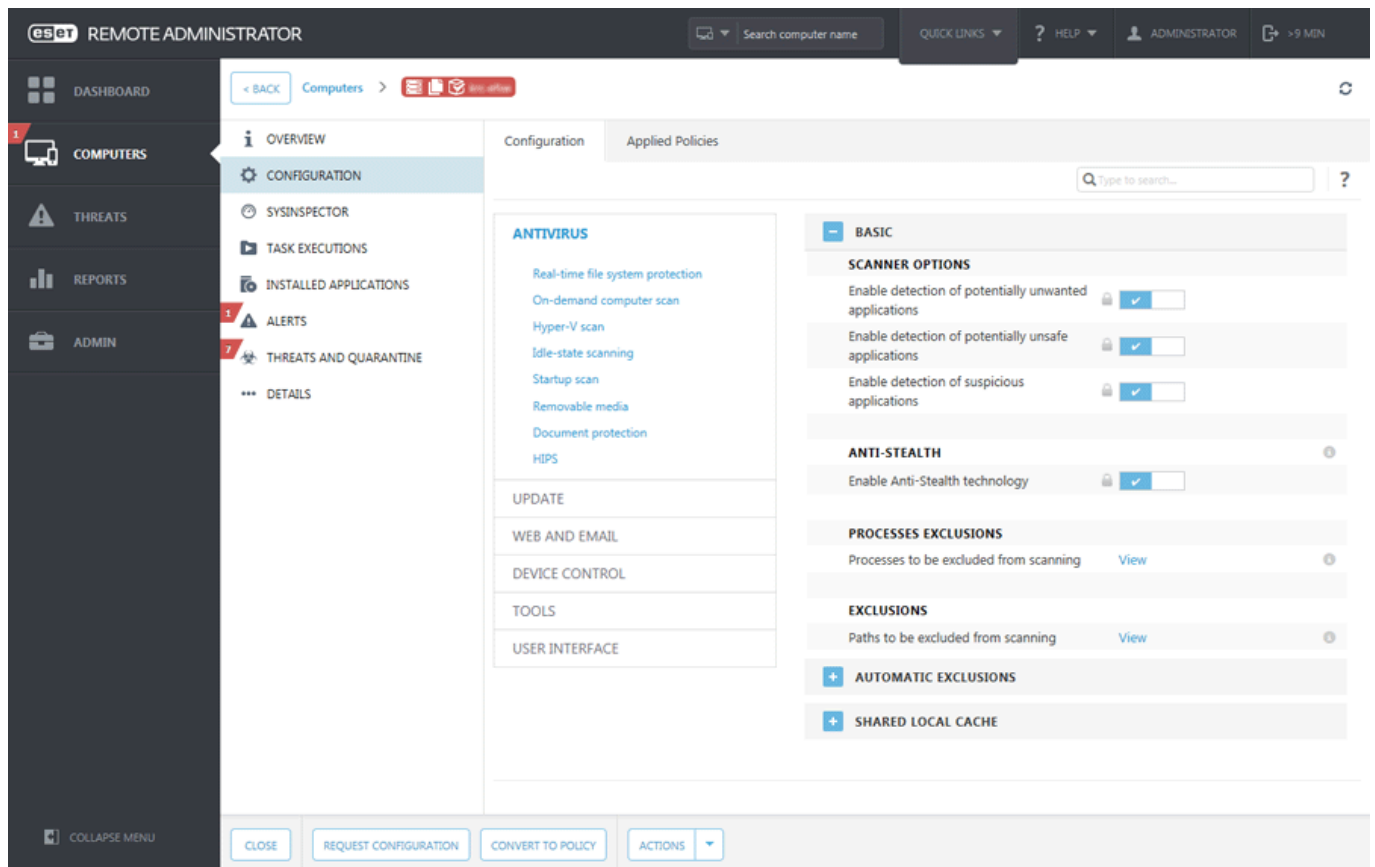
2. Öffnen Sie die **ESET Security Management Center-Web-Konsole**, wählen Sie einen Clientcomputer in einer statischen oder dynamischen Gruppe aus, und klicken Sie auf **Details anzeigen**.



3. Navigieren Sie zur Registerkarte [Konfiguration](#) und klicken Sie auf die Schaltfläche **Konfiguration anfordern**, um die gesamte Konfiguration des verwalteten Produkts zu erfassen. Warten Sie einen Moment, bis die Konfiguration abgerufen wurde. Nachdem die aktuelle Konfiguration in der Liste angezeigt wird, klicken Sie auf **Sicherheitsprodukt** und wählen Sie **Konfiguration öffnen** aus.




4. Klicken Sie auf **In Richtlinie umwandeln**, um eine Konfigurationsrichtlinie zu erstellen. Geben Sie einen **Namen** für die neue Richtlinie ein und klicken Sie auf **Fertig stellen**.



5. Navigieren Sie zu **Clienttasks** und wählen Sie den Task [Software-Deinstallation](#) aus. Achten Sie beim Erstellen des Deinstallationstasks darauf, den Server nach der Deinstallation neu zu starten, indem Sie das

Kontrollkästchen **Bei Bedarf automatisch neu starten** markieren. Erstellen Sie den Task und fügen Sie alle gewünschten Zielcomputer für die Deinstallation aus.

6. Vergewissern Sie sich, dass ESET Security for Microsoft SharePoint von allen Zielen deinstalliert wurde.

7. Erstellen Sie einen Task [Software-Installation](#) , um die aktuelle Version von ESET Security for Microsoft SharePoint auf allen Zielen zu installieren.

8. **Weisen Sie die Konfigurationsrichtlinie** zu allen Servern zu, auf denen ESET Security for Microsoft SharePoint läuft, idealerweise in einer Gruppe.

9. Melden Sie sich lokal auf den einzelnen Servern an und öffnen Sie ESET Security for Microsoft SharePoint. Daraufhin wird eine rote [Warnung](#) mit der folgenden Meldung angezeigt: *ESET SharePoint Helper Service is not running*. Legen Sie das **Administratorkonto für die SharePoint-Farm** unter [Erweiterte Einstellungen](#) fest.

WICHTIG

Dieser Schritt muss auf jedem Server ausgeführt werden, auf dem ESET Security for Microsoft SharePoint läuft. Dies ist aus Sicherheitsgründen erforderlich. ESET-Produkte speichern die Anmeldeinformationen des SharePoint-Administrators nicht. Daher sind die Anmeldeinformationen nicht in der Konfigurationsrichtlinie enthalten und können nicht an andere Server weitergegeben werden.

Upgrades per ESET-Cluster

Mit einem [ESET-Cluster](#) können Sie mehrere Server aktualisieren, auf denen ältere Versionen von ESET Security for Microsoft SharePoint laufen. Dieses Verfahren ist eine Alternative zum [Upgrade über ESMC](#). Wir empfehlen das Cluster-Upgradeverfahren, wenn Ihre Umgebung mindestens zwei Server mit ESET Security for Microsoft SharePoint enthält. Außerdem können Sie mit dieser Upgrademethode weiterhin Ihr [ESET-Cluster](#) verwenden, um die Konfiguration von ESET Security for Microsoft SharePoint auf allen Mitglieds-knoten zu synchronisieren.

Führen Sie die folgenden Schritte aus, um ein Upgrade mit dieser Methode durchzuführen:

1. Melden Sie sich bei einem der Server an, auf denen ESET Security for Microsoft SharePoint läuft, und führen Sie ein Upgrade durch, indem Sie die aktuelle Version herunterladen und über die vorhandene Version installieren. Führen Sie die [Schritte für eine normale Installation](#) durch. Die gesamte Konfiguration Ihrer alten ESET Security for Microsoft SharePoint-Version bleibt bei der Installation erhalten.

2. Führen Sie den [ESET-Clusterassistenten](#) aus und fügen Sie Clusterknoten hinzu (Server, auf denen Sie ESET Security for Microsoft SharePoint aktualisieren möchten). Bei Bedarf können Sie weitere Server hinzufügen, auf denen ESET Security for Microsoft SharePoint noch nicht läuft. Auf diesen Servern wird eine Neuinstallation durchgeführt. Verwenden Sie bei der Angabe von [Clustername und Installationstyp](#) die Standardeinstellungen (aktivieren Sie die Option **Lizenz auf Knoten ohne aktiviertes Produkt übertragen**).

3. Überprüfen Sie den Bildschirm **Knotenprüfungs-Log**. Dort werden Server angezeigt, auf denen ältere Produktversionen laufen und auf denen eine Neuinstallation durchgeführt wird. ESET Security for Microsoft SharePoint wird auch auf allen hinzugefügten Servern installiert, auf denen das Produkt noch nicht installiert ist.

Node check log

[13:39:36] Node check started
[13:39:36] PING test:
[13:39:36] OK
[13:39:36] Administration share access test:
[13:39:36] OK
[13:39:36] Service manager access test:
[13:39:39] OK
[13:39:39] Checking installed product version and features:
[13:39:42] -2003-SHAREPOINT_2: Older version of the product detected. Product will be reinstalled.
[13:39:43] -2003-CLEAN: Install will be performed.
[13:39:45] OK
[13:39:45]
[13:39:45] Warning: The product needs to be reinstalled on some machines before creating the cluster. This may cause those machines to be automatically restarted.

Check

< Previous

Next >

Cancel

4. Auf dem Bildschirm **Knoteninstallation und Clusteraktivierung** wird der Installationsfortschritt angezeigt. Nach dem erfolgreichen Abschluss der Installation sollte in etwa das folgende Ergebnis angezeigt werden:



Product install log

[15:53:58] Generating certificates for cluster nodes...
[15:54:01] All certificates created.
[15:54:01] Copying files to remote machines:
[15:54:05] All files have been copied to remote machines.
[15:54:05] Installing product:
[15:55:00] ESET solutions are installed on all remote machines.
[15:55:00] Enrolling certificates:
[15:55:02] All certificates have been enrolled to remote machines.
[15:55:02] Activating cluster feature:
[15:55:03] Cluster feature has been activated on all machines.
[15:55:03] Pushing license to the nodes:
[15:55:05] License has been successfully pushed to the nodes.
[15:55:05] Synchronizing settings:
[15:55:06] Settings have been synchronized.

Install

< Previous

Finish

Cancel

5. Melden Sie sich lokal auf den einzelnen Servern an und öffnen Sie ESET Security for Microsoft SharePoint. *ESET SharePoint Helper Service is not running will be displayed*. Geben Sie Ihr **Administratorkonto** für die **SharePoint Farm** in den [erweiterten Einstellungen](#) an.

WICHTIG

Dieser Schritt muss auf jedem Server ausgeführt werden, auf dem ESET Security for Microsoft SharePoint läuft. Dies ist aus Sicherheitsgründen erforderlich. ESET-Produkte speichern die Anmeldeinformationen des SharePoint-Administrators nicht. Daher können die Anmeldeinformationen nicht an andere Server weitergegeben werden.

Falls Ihr Netzwerk oder Ihr DNS nicht korrekt konfiguriert ist, wird möglicherweise die Nachricht **Fehler beim Abrufen des Aktivierungs-Tokens vom Server** angezeigt. Führen Sie in diesem Fall den [ESET-Clusterassistenten](#) erneut aus. Dabei wird das Cluster gelöscht und ein neues erstellt, ohne das Produkt neu zu installieren. Anschließend sollte die Aktivierung funktionieren. Überprüfen Sie Ihre Netzwerk- und DNS-Einstellungen, falls das Problem weiterhin auftritt.



Product install log

[18:06:59] Generating certificates for cluster nodes...
[18:07:01] All certificates created.
[18:07:01] Copying files to remote machines:
[18:07:01] All files have been copied to remote machines.
[18:07:01] Enrolling certificates:
[18:07:03] All certificates have been enrolled to remote machines.
[18:07:03] Activating cluster feature:
[18:07:04] Cluster feature has been activated on all machines.
[18:07:04] Pushing license to the nodes:
[18:07:04] Failed to obtain activation token from the server.
[18:07:04] There were errors pushing license to the nodes.
[18:07:04] Synchronizing settings:
[18:07:05] There were errors synchronizing settings in the cluster.

Install

< Previous

Finish

Cancel

Terminalserver

Wenn Sie ESET Security for Microsoft SharePoint auf einem Windows-Server installieren, der als Terminalserver eingerichtet ist, empfehlen wir Ihnen, die grafische Benutzeroberfläche von ESET Security for Microsoft SharePoint zu deaktivieren, da diese sonst bei jeder Anmeldung eines Benutzers gestartet wird. Nähere Informationen hierzu finden Sie im Abschnitt [Deaktivieren der Benutzeroberfläche auf Terminalserver](#).

Erste Schritte

Der folgende Abschnitt unterstützt Sie bei Ihren ersten Schritten mit ESET Security for Microsoft SharePoint.

[Überwachung](#)

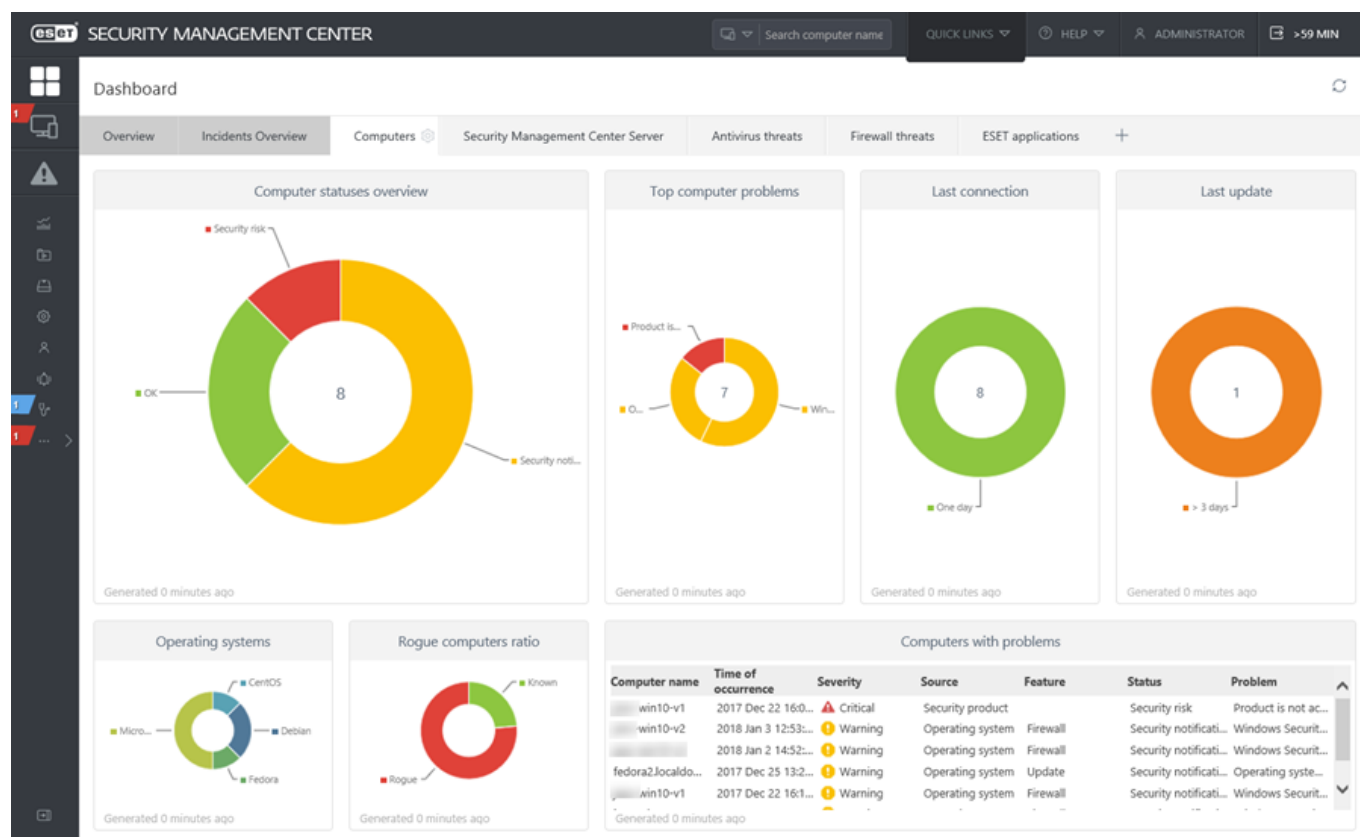
Hier finden Sie eine praktische Übersicht über den aktuellen Status von ESET Security for Microsoft SharePoint und erkennen auf einen Blick, ob irgendwelche Probleme Ihre Aufmerksamkeit erfordern.

[Verwaltung über ESET Security Management Center](#)

Sie können ESET Security Management Center verwenden, um ESET Security for Microsoft SharePoint remote zu verwalten.

Verwaltung über ESET Security Management Center

ESET Security Management Center (ESMC) ist eine Anwendung, mit der Sie ESET-Produkte in einer Netzwerkumgebung von einem zentralen Standort aus verwalten können. Das Task-Management-System von ESET Security Management Center ermöglicht das Installieren von ESET-Sicherheitslösungen auf Remotecomputern und eine schnelle Reaktion auf neue Probleme und Bedrohungen. ESET Security Management Center bietet keinen Schutz vor Schadcode selbst, sondern stützt sich hierzu auf die auf jedem Client installierte ESET-Sicherheitslösung. ESET-Sicherheitslösungen unterstützen Netzwerke, die verschiedene Plattformtypen umfassen. Ihr Netzwerk kann eine Kombination aus aktuellen Microsoft-, Linux-basierten, Mac OS- und mobilen Betriebssystemen enthalten.



Weitere Informationen zu ESMC finden Sie in der [ESET Security Management Center-Onlinehilfe](#).

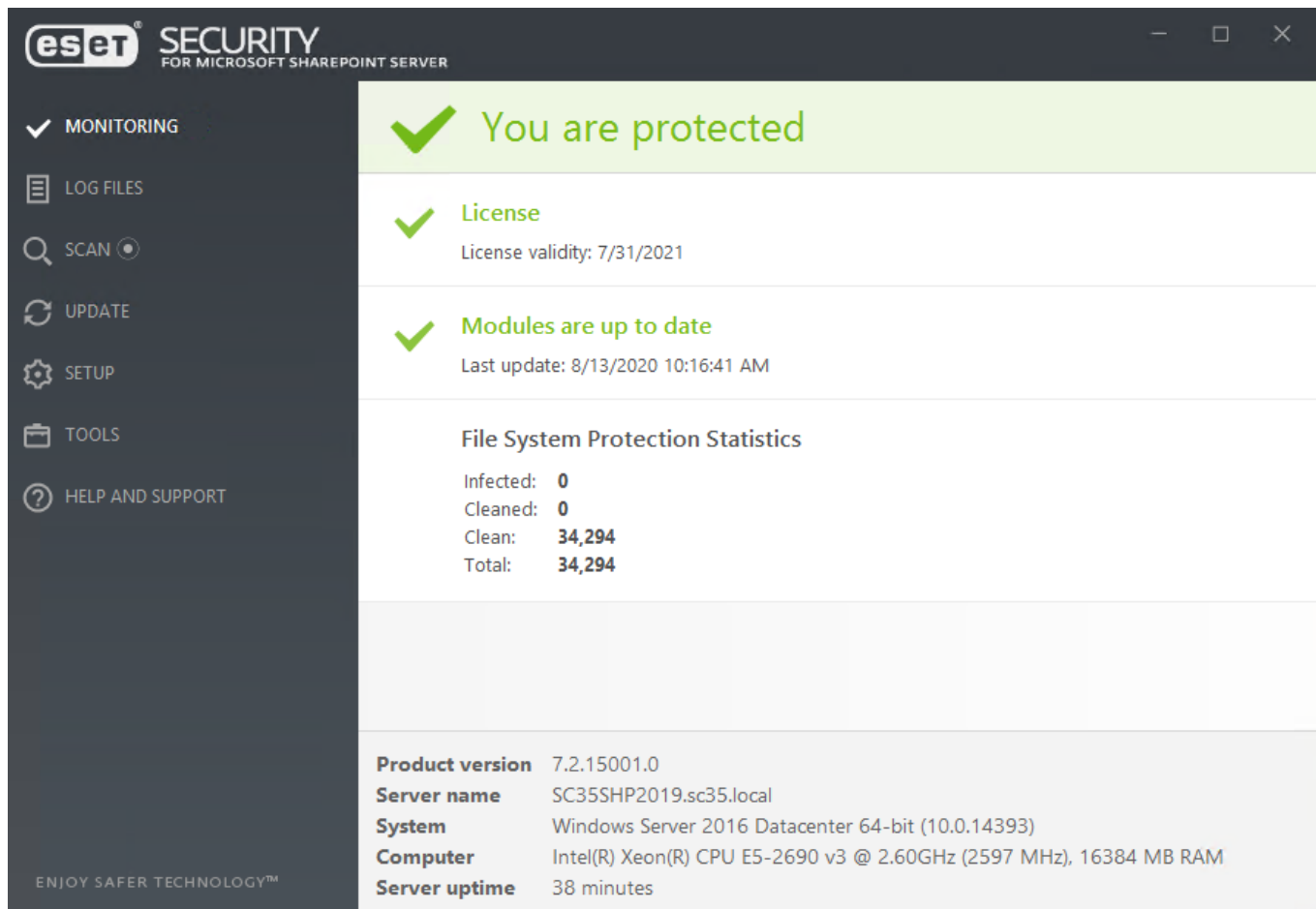
Überwachung

Der Bildschirm Schutzstatus im Bereich **Überwachung** enthält Informationen über die aktuelle Schutzstufe Ihres Computers. Im primären Fenster wird eine Darstellung des aktuellen Betriebszustands von ESET Security for Microsoft SharePoint angezeigt.

✓ Das grüne Schutzstatussymbol und die Meldung **Sie sind geschützt** zeigen an, dass der maximale Schutz gewährleistet ist.

! Das rote Symbol weist auf kritische Probleme hin. Der maximale Schutz Ihres Computers ist nicht gewährleistet. Eine Liste der möglichen Schutzstatusmeldungen finden Sie im Bereich [Status](#).

! Das orangefarbene Symbol weist auf ein nicht-kritisches Problem in Ihrem ESET-Produkt hin.



Richtig funktionierende Module sind mit einem grünen Häkchen gekennzeichnet. Nicht vollständig funktionsfähige Module werden mit einem roten Ausrufezeichen oder einem orangen Benachrichtigungssymbol gekennzeichnet. Weitere Informationen zum Modul werden im oberen Teil des Fensters eingeblendet. Unter anderem finden Sie dort einen Vorschlag zur Behebung des Problems. Um den Status einzelner Module zu ändern, klicken Sie im Hauptmenü auf [Einstellungen](#) und wählen das gewünschte Modul aus.

Die Überwachungsseite enthält Informationen zu Ihrem System, darunter:

- **Produktversion** - Versionsnummer von ESET Security for Microsoft SharePoint.
- **Servername** - Hostname oder FQDN des Computers.
- **System** - Details zum Betriebssystem.
- **Computer** - Hardwaredetails.
- **Betriebszeit des Servers** - Zeigt an, wie lange das System bereits läuft.

Benutzeranzahl

ESET Security for Microsoft SharePoint erkennt die Anzahl der Benutzer, die SharePoint verwenden. Dieser Wert wird zu Lizenzierungszwecken verwendet. Dabei wird zwischen zwei Arten von Benutzern unterschieden:

- **Domäne** – Anzahl der Benutzer in der SharePoint-Datenbank, die sich per Windows-Authentifizierung bei SharePoint anmelden. Die Anwesenheit wird auch direkt in Active Directory überprüft. Bei einer Übereinstimmung werden die Benutzer gezählt. Diese Überprüfung verhindert, dass Benutzer gezählt werden, die nicht mehr in Active Directory existieren, jedoch immer noch in der SharePoint-Liste vorhanden sind. Diese Benutzer werden nicht gezählt.
- **Sonstige** – Anzahl der Benutzer, die andere Authentifizierungsformen verwenden (unabhängig vom Vorhandensein in Active Directory), z. B. eine formularbasierte oder anspruchsbasierte Authentifizierung.

Diese Anzahl basiert außerdem auf der Benutzerliste in der SharePoint-Datenbank.

HINWEIS

Die Benutzer werden 5 Minuten nach dem Systemstart bzw. alle 6 Stunden neu gezählt. Sie müssen gültige SharePoint-[Administratoranmeldeinformationen](#) eingeben, um die Benutzeranzahl anzeigen zu können.

Wenn Sie ein Problem mit den vorgeschlagenen Lösungen nicht beseitigen können, klicken Sie auf **Hilfe und Support**, um die Hilfedateien zu öffnen, oder durchsuchen Sie die [ESET-Knowledgebase](#). Falls Sie weitere Unterstützung benötigen, können Sie eine [Supportanfrage senden](#). Der ESET-Support wird sich umgehend mit Ihnen in Verbindung setzen, um Ihre Fragen zu beantworten und Lösungen für Ihr Problem zu finden.

Status



Im Hauptfenster wird eine Statusmeldung für ESET Security for Microsoft SharePoint mit ausführlichen Informationen zu Ihrem System angezeigt. Wenn alle Module problemlos funktionieren, wird der Schutzstatus

🟢 Grün angezeigt. Der Schutzstatus kann sich jedoch in bestimmten Situationen ändern. Der Schutzstatus wechselt zu 🟡 Orange oder 🔴 Rot, und eine Warnmeldung wird angezeigt, wenn eines der folgenden Ereignisse eintritt:

HINWEIS

Dies ist eine Liste der SharePoint-Plugin-Meldungen. Außerdem können weitere Meldungen in Bezug auf den Dateiserverschutz angezeigt werden (nicht in der nachfolgenden Tabelle enthalten).

Warnmeldung	Ausführliche Warnmeldung
SharePoint nicht installiert	Es wurde keine Installation von Microsoft SharePoint Server gefunden, oder eine nicht unterstützte Version ist installiert. Installieren Sie eine der unterstützten Serverversionen .
SharePoint-Server ist nicht unterstützt	Die installierte Version wird nicht von ESET Security for Microsoft SharePoint unterstützt. Installieren Sie eine der unterstützten Serverversionen .
SharePoint-Echtzeitschutz ist vorübergehend deaktiviert	Microsoft SharePoint Server ist nicht vor Bedrohungen geschützt, und keine Regeln werden angewendet.
SharePoint-Echtzeitschutz wird nicht verwendet	Der Microsoft SharePoint Server-Echtzeitschutz scannt keine Dokumente beim Hoch- oder Herunterladen.
SharePoint-Echtzeitschutz ist deaktiviert	Microsoft SharePoint Server ist nicht vor Bedrohungen geschützt, und keine Regeln werden angewendet.
Zugriff auf SharePoint-Konfiguration nicht möglich	SharePoint-Administratorkonto hat keinen Zugriff auf SharePoint-Konfigurationsobjekte. Stellen Sie sicher, dass das SharePoint-Administratorkonto richtig konfiguriert ist.
Fehler beim Zugriff auf SharePoint-Webseiten-Objekte	SharePoint-Administratorkonto hat keinen Zugriff auf SharePoint-Website-Objekte. Die On-Demand-Datenbankprüfung kann nicht durchgeführt werden. Stellen Sie sicher, dass das SharePoint-Administratorkonto richtig konfiguriert ist.
Zugriff auf manche SharePoint-Webseitenobjekte nicht möglich	SharePoint-Administratorkonto hat keinen Zugriff auf einen Teil der SharePoint-Website-Objekte. Die On-Demand-Datenbankprüfung für diese Websites kann nicht durchgeführt werden.
Warte auf Microsoft SharePoint	ESET Security for Microsoft SharePoint wartet auf die Verfügbarkeit der Microsoft SharePoint Services. Unter Umständen werden nicht alle SharePoint-bezogenen Fehler angezeigt.

Warnmeldung	Ausführliche Warnmeldung
Erforderliche SharePoint-Dienste werden nicht ausgeführt	SharePoint-Administrationsdienst oder SharePoint-Timerdienst läuft nicht. Diese Dienste werden für eine korrekte Funktionsweise der Update-Benachrichtigungen benötigt.
Ungültiges SharePoint-Administratorkonto.	Das angegebene SharePoint-Administratorkonto existiert nicht. Klicken Sie auf Konto ändern .
SharePoint-Administratorkonto ist nicht konfiguriert	Klicken Sie auf Zugriffsfilter aktivieren .
Der SharePoint-Helferdienst läuft nicht	Der ESET SharePoint-Helferdienst wurde beendet oder kann nicht gestartet werden. Das SharePoint-Administratorkonto wird benötigt, um den ESET SharePoint-Helferdienst auszuführen. Überprüfen Sie, ob die Anmeldeinformationen für das Konto korrekt sind und ob das Konto über die Berechtigung "Als Dienst anmelden" verfügt.
Das Betriebssystem ist veraltet	Das Fenster „System-Updates“ enthält verfügbare Updates, die heruntergeladen und installiert werden können.
Ihr Gerät verliert seinen Schutz demnächst	Klicken Sie auf Optionen anzeigen , um Details zum Aktualisieren Ihrer Microsoft Windows-Version anzuzeigen. Falls Sie Microsoft Windows Server 2008 R2 SP1 verwenden, stellen Sie sicher, dass Ihr System mit SHA-2 kompatibel ist. Installieren Sie die passenden Patches für Ihre Betriebssystemversion.
Computerneustart erforderlich	Klicken Sie auf Computer neu starten , falls Sie Ihr System sofort neu starten möchten, oder auf Verwerfen , falls Sie das System später neu starten möchten.
Die Erkennung evtl. unerwünschter Anwendungen ist nicht konfiguriert 	Potenziell unerwünschte Anwendungen sind Programme, die Adware enthalten, Toolbars installieren oder andere unklare Zwecke verfolgen. Möglicherweise sind Sie jedoch der Ansicht, dass die Vorteile der potenziell unerwünschten Anwendung gegenüber den Risiken überwiegen.
Der Echtzeit-Dateischutz ist angehalten	Klicken Sie auf Echtzeit-Dateischutz aktivieren in der Registerkarte Überwachung oder aktivieren Sie die Option Echtzeit-Dateischutz in der Registerkarte Einstellungen im Hauptprogrammfenster.
Produkt ist nicht aktiviert oder Lizenz abgelaufen	In diesen Fällen ist das Schutzstatussymbol rot. Bei abgelaufener Lizenz kann das Programm keine Updates mehr durchführen. Führen Sie die in der Warnung angezeigten Anweisungen zur Verlängerung Ihrer Lizenz aus.
Policy außer Kraft setzen ist aktiv	Die von der Policy festgelegte Konfiguration wurde vorübergehend außer Kraft gesetzt, möglicherweise bis zum Abschluss der Problembehandlung. Falls Sie ESET Security for Microsoft SharePoint mit ESMC verwalten und eine Policy  zugewiesen haben, ist der Status-Link je nach Konfiguration der Policy möglicherweise gesperrt (ausgegraut).
Netzwerkangriffsschutz (IDS) ist angehalten	Klicken Sie auf Netzwerkangriffsschutz (IDS) aktivieren , um dieses Feature erneut zu aktivieren.
Botnet-Erkennung ist angehalten	Klicken Sie auf Botnet-Erkennung aktivieren , um dieses Feature erneut zu aktivieren.
Web-Schutz ist angehalten	Klicken Sie auf Web-Schutz aktivieren in der Registerkarte Überwachung oder aktivieren Sie den Web-Schutz in der Registerkarte Einstellungen im Hauptprogrammfenster.

Warnmeldung	Ausführliche Warnmeldung
Policy außer Kraft setzen ist aktiv	Die von der Policy festgelegte Konfiguration wurde vorübergehend außer Kraft gesetzt, möglicherweise bis zum Abschluss der Problembehandlung. Falls Sie ESET Security for Microsoft SharePoint mit ESMC verwalten und eine Policy zugewiesen haben, ist der Status-Link je nach Konfiguration der Policy möglicherweise gesperrt (ausgegraut).



HINWEIS

Die letzten beiden Statusnachrichten werden nach dem Serverstart für bis zu 5 Minuten zurückgestellt. In diesem Zeitraum wird der ESET SharePoint-Helferdienst gestartet und wartet darauf, dass SharePoint verfügbar wird. Dieser Vorgang dauert normalerweise wenige Sekunden, kann jedoch unter hoher Last bis zu 5 Minuten dauern. Das Ende dieser anfänglichen Verzögerung wird durch die folgende Meldung im Ereignisprotokoll gemeldet: Wartezeit auf SharePoint Services ist abgeschlossen.








Wenn Sie ein Problem nicht beseitigen können, durchsuchen Sie die [ESET-Knowledgebase](#). Falls Sie weitere Unterstützung benötigen, können Sie eine [Supportanfrage senden](#). Der ESET-Support wird sich umgehend mit Ihnen in Verbindung setzen, um Ihre Fragen zu beantworten und Lösungen für Ihr Problem zu finden.

Windows-Update verfügbar

Im Fenster „System-Updates“ werden verfügbare Updates aufgelistet, die Sie herunterladen und installieren können. Neben dem Namen des Updates wird die Update-Priorität angezeigt. Klicken Sie mit der rechten Maustaste auf ein beliebiges Update und klicken Sie auf **Mehr Informationen**, um ein Fenster mit zusätzlichen Informationen zu öffnen:

System updates



Total number of available updates: 7

Name	Type
 2019-02 Security Monthly Quality Rollup for Windows Server 2012 R2 for x64-based Systems (KB4487000)	Critical
 2018-12 Cumulative Security Update for Internet Explorer 11 for Windows Server 2012 R2 for x64-based systems (KB4...	Important
 Update for Microsoft Silverlight (KB4481252)	Important
 Windows Malicious Software Removal Tool x64 - February 2019 (KB890830)	Important
 2019-02 Security and Quality Rollup for .NET Framework 3.5, 4.5.2, 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, 4.7.2 for Windows 8.1 a...	Important
 Update for Windows Server 2012 R2 (KB4033428)	Recommended
 Microsoft .NET Framework 4.7.2 for Windows Server 2012 R2 for x64 (KB4054566)	Recommended

Run system update
Cancel

Klicken Sie auf **System-Update durchführen**, um das Fenster **Windows Update** zu öffnen und die System-Updates zu installieren.

Netzwerkisolierung

Mit ESET Security for Microsoft SharePoint können Sie die Netzwerkverbindung Ihres Servers blockieren. Dies wird auch als Netzwerkisolation bezeichnet. In bestimmten extremen Situationen kann es sinnvoll sein, einen Server vorbeugend vom Netzwerk zu isolieren, zum Beispiel wenn der Server mit Malware infiziert ist oder auf eine andere Art und Weise kompromittiert wurde.

Wenn Sie die Netzwerkisolation aktivieren, wird der gesamte Netzwerkdatenverkehr blockiert, mit den folgenden Ausnahmen:

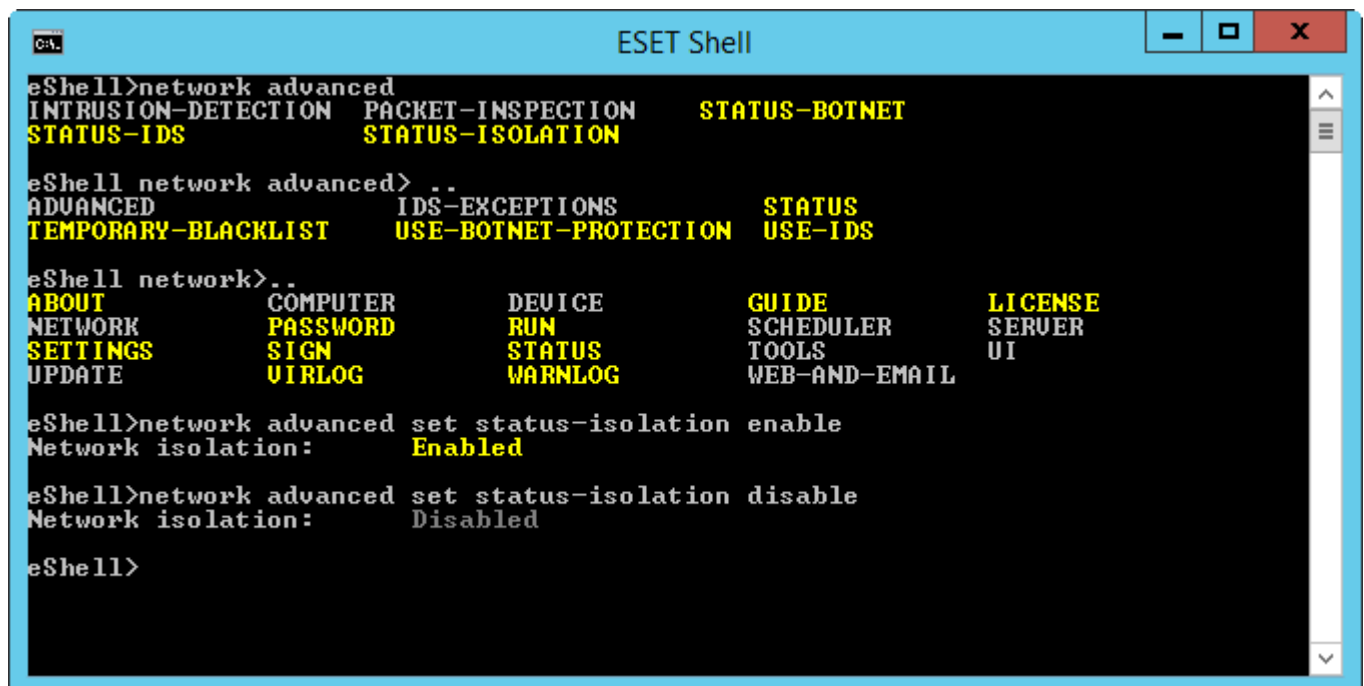
- Die Verbindung zum Domänencontroller bleibt erhalten
- ESET Security for Microsoft SharePoint kann weiterhin kommunizieren
- Falls vorhanden, können der ESET Management Agent und der ESET Enterprise Inspector Agent über das Netzwerk kommunizieren.

Aktivieren und deaktivieren Sie die Netzwerkisolation mit dem Befehl [eShell](#) oder dem Clienttask [ESET Security Management Center](#).

eShell

Im interaktiven Modus:

- Netzwerkisolation aktivieren: `network advanced set status-isolation enable`
- Netzwerkisolation deaktivieren: `network advanced set status-isolation disable`



```
ESET Shell
eShell>network advanced
INTRUSION-DETECTION  PACKET-INSPECTION  STATUS-BOTNET
STATUS-IDS          STATUS-ISOLATION

eShell network advanced> ..
ADVANCED             IDS-EXCEPTIONS      STATUS
TEMPORARY-BLACKLIST  USE-BOTNET-PROTECTION  USE-IDS

eShell network>..
ABOUT              COMPUTER          DEVICE          GUIDE          LICENSE
NETWORK            PASSWORD          RUN             SCHEDULER      SERVER
SETTINGS           SIGN             STATUS          TOOLS          UI
UPDATE             VIRLOG           WARNLOG         WEB-AND-EMAIL



eShell>network advanced set status-isolation enable
Network isolation:    Enabled

eShell>network advanced set status-isolation disable
Network isolation:    Disabled

eShell>
```

Alternativ können Sie eine Batch-Datei mit dem [Batch-/Skriptmodus](#) erstellen und ausführen.

ESET Security Management Center

- Netzwerkisolation aktivieren per [Client-Task](#) .
- Netzwerkisolation deaktivieren per [Client-Task](#) .

Wenn die Netzwerkisolation aktiviert ist, wird der Status von ESET Security for Microsoft SharePoint in rot angezeigt, zusammen mit der Nachricht **Netzwerkzugriff blockiert**.

Arbeiten mit ESET Security for Microsoft SharePoint

Dieser Abschnitt enthält eine ausführliche Beschreibung der Benutzeroberfläche des Programms und erklärt die Verwendung von ESET Security for Microsoft SharePoint.

In der Benutzeroberfläche können Sie schnell auf häufig verwendete Features zugreifen:

- [Überwachung](#)
- [Log-Dateien](#)
- [Prüfen](#)
- [Update](#)
- [Einstellungen](#)
- [Tools](#)

Prüfen

On-Demand-Scans sind ein wichtiger Teil von ESET Security for Microsoft SharePoint und dienen zur Prüfung von Dateien und Ordnern auf dem Computer. Um Ihr Netzwerk optimal zu schützen, sollten Sie Ihren Computer nicht nur bei Infektionsverdacht prüfen, sondern diese Prüfung in die allgemeinen Sicherheitsroutinen integrieren. Führen Sie regelmäßig eine gründliche Prüfung des Computers durch, um mögliche Viren zu entdecken, die nicht vom [Echtzeit-Dateischutz](#) erfasst wurden. Dies kommt z. B. vor, wenn der Echtzeit-Dateischutz deaktiviert oder die Erkennungsroutine nicht auf dem neuesten Stand ist, oder wenn die Datei beim Speichern auf dem Datenträger nicht als Virus erkannt wird.

Wählen Sie verfügbare On-Demand-Scans für ESET Security for Microsoft SharePoint aus:

[SharePoint-Datenbankprüfung](#)

Sie können die gewünschten SharePoint-Websites auswählen und den Scanvorgang ausführen.

Speicher prüfen

Prüft alle freigegebenen Ordner auf dem lokalen Server. Wenn die Option Speicher prüfen nicht verfügbar ist, bedeutet dies, dass auf dem Server keine freigegebenen Ordner vorhanden sind.

Scannen Sie Ihren Computer

Mit dem Smart-Scan können Sie schnell den Computer scannen und infizierte Dateien entfernen, ohne eingreifen zu müssen. Ihr Vorteil ist die einfache Bedienung, ohne detaillierte Prüfeinstellungen festlegen zu müssen. Beim Smart-Scan werden alle Dateien auf lokalen Laufwerken geprüft, und erkannte eingedrungene Schadsoftware wird automatisch entfernt. Als Säuberungsstufe wird automatisch der Standardwert festgelegt. Weitere Informationen zu den Säuberungstypen finden Sie unter [Säubern](#).

HINWEIS

Sie sollten mindestens einmal im Monat eine Prüfung des Computers vornehmen. Sie können die Prüfung als [geplanten Task](#).


Benutzerdefinierter Scan

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

Wechselmedienscan

Dieser Scan ähnelt dem Smart-Scan und ermöglicht ein schnelles Scannen der aktuell an den Computer angeschlossenen Wechselmedien (wie CD/DVD/USB). Diese Prüfung 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 starten, indem Sie auf **Benutzerdefinierter Scan** klicken, die Option **Wechselmedien** im Dropdownmenü **Prüfziele** auswählen und auf **Scannen** klicken.

Hyper-V-Scan

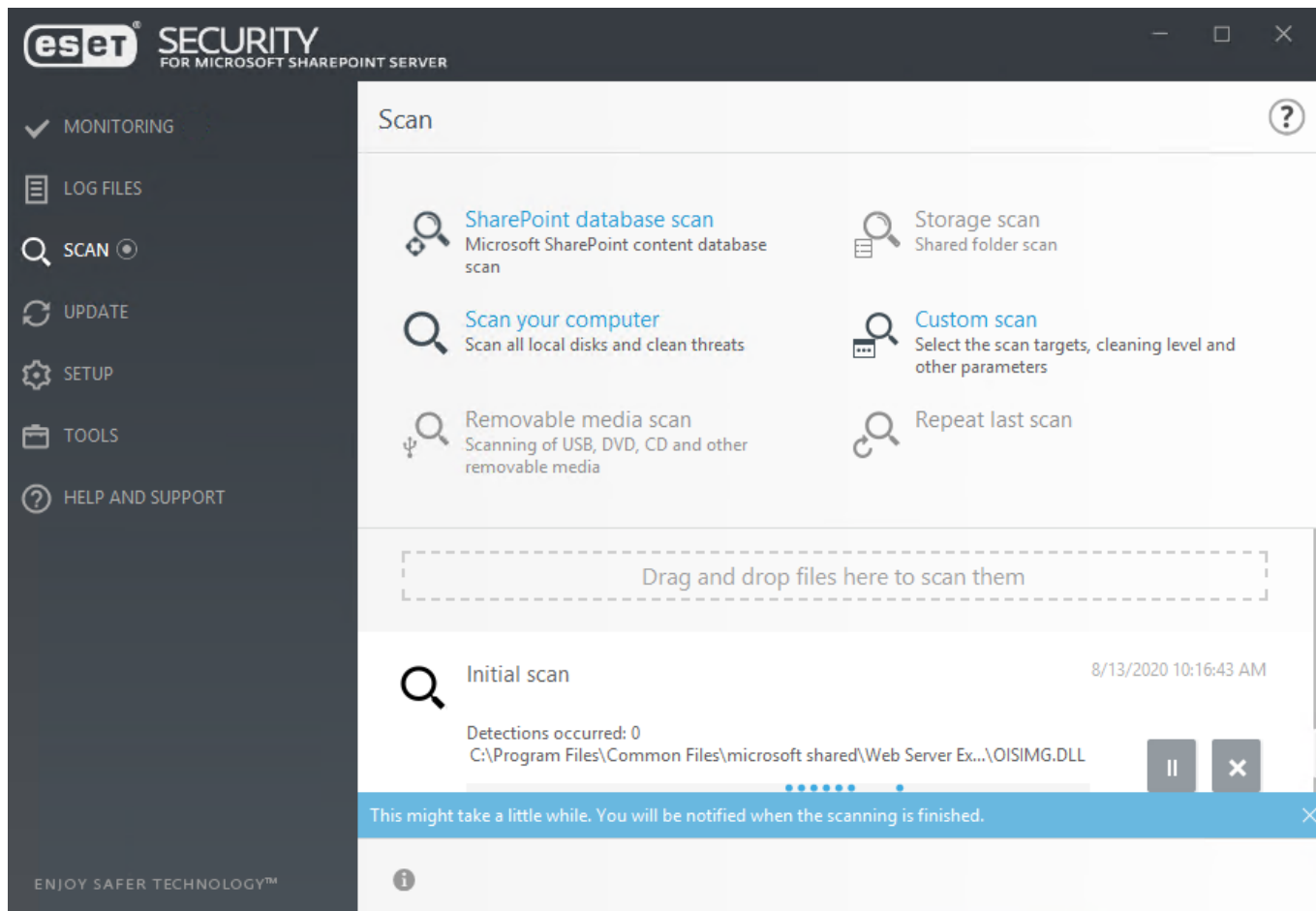
Diese Option ist nur sichtbar, wenn Hyper-V Manager auf dem Server installiert ist, auf dem ESET Security for Microsoft SharePoint ausgeführt wird. Mit dem Hyper-V-Scan können virtuelle Computerlaufwerke auf [Microsoft Hyper-V-Servern](#)  geprüft werden, ohne auf der jeweiligen VM einen „Agent“ installieren zu müssen.

Letzte Prüfung wiederholen

Wiederholt Ihren letzten Scanvorgang mit denselben Einstellungen.

HINWEIS

Die Funktion zum Wiederholen der letzten Prüfung ist nicht verfügbar, wenn eine On-Demand-Datenbankprüfung ausgeführt wird.



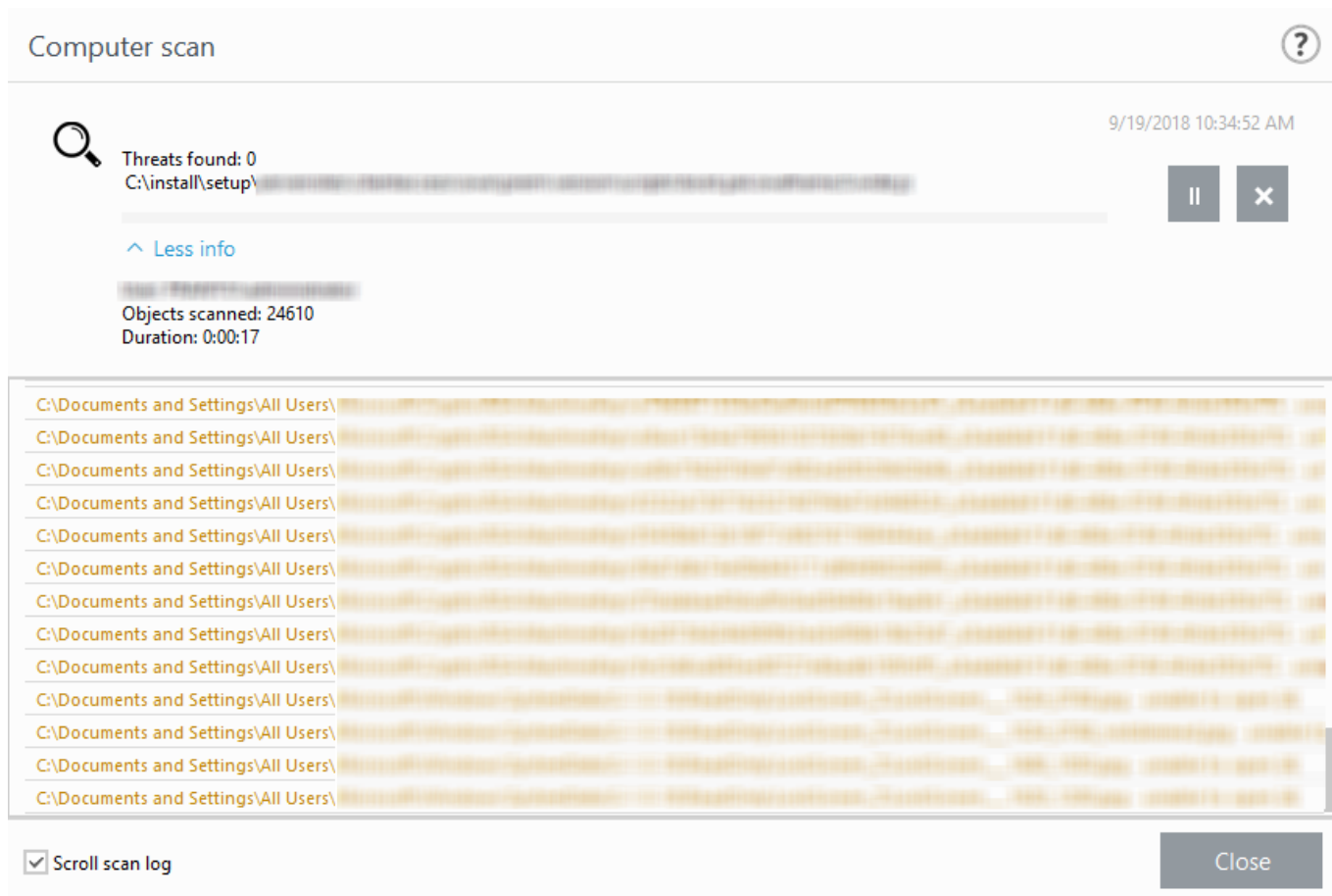
Sie können Optionen verwenden und weitere Informationen zum Scanstatus anzeigen:

Dateien ziehen und Ablegen	Sie können Dateien mit der Maus ziehen und im ESET Security for Microsoft SharePoint-Scanfenster ablegen, um sie sofort nach Viren zu scannen.
Verwerfen/Alle verwerfen	Angezeigte Nachrichten werden verworfen.
Scanstatus	Zeigt den Status des Erstscans an. Dieser Scan wurde entweder abgeschlossen oder vom Benutzer unterbrochen.
Log anzeigen	Zeigt ausführlichere Informationen an.
Weitere Informationen	Während eines Scans können Sie zusätzliche Details anzeigen, z. B. den Benutzer , der den Scanvorgang ausgeführt hat, die geprüften Objekte und die Scandauer .
Scanfenster öffnen	Die Fortschrittsanzeige enthält den aktuellen Stand der Prüfung und die Anzahl der bisher gefundenen infizierten Dateien.

Scanfenster und Scan-Log

Das Scanfenster enthält die aktuell gescannten Objekte zusammen mit ihrem Speicherort, die Anzahl der gefundenen Bedrohungen (falls vorhanden), die Anzahl gescannter Objekte und die Scandauer. Der untere Teil des Fensters enthält ein Scan-Log mit der Versionsnummer der Erkennungsroutine, den Zeitpunkt, zu dem der Scan gestartet wurde, und die Zielauswahl.

Wenn ein Scan ausgeführt wird, können Sie auf **Anhalten** klicken, um den Scan vorübergehend zu unterbrechen. Wenn ein Scan angehalten wurde, ist die Option **Fortsetzen** verfügbar.



Bildlauf in Log-Anzeige aktivieren

Wenn diese Option aktiv ist, wandern alte Logs automatisch aus der Anzeige, sodass im Fenster der Log-Dateien die neuesten Einträge sichtbar sind.

HINWEIS

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

Nach Abschluss des Scans wird das Scan-Log mit allen relevanten Informationen zum Scanvorgang angezeigt.

Computer scan



Scan Log

Version of detection engine: 18075 (20180919)

Date: 9/19/2018 Time: 10:34:23 AM

Scanned disks, folders and files: C:\Program Files\Microsoft

C:\Users\All Users\Microsoft\

C:\Users\All Users\Microsoft\

C:\Users\All Users\Microsoft\

C:\Users\All Users\Microsoft\

C:\Users\All Users\Microsoft\

C:\Users\All Users\Microsoft\

C:\Users\All Users\Microsoft\

C:\Users\All Users\Microsoft\

C:\Users\All Users\Microsoft\

C:\Users\All Users\Microsoft\

C:\Users\All Users\Microsoft\

C:\Users\All Users\Microsoft\

C:\Users\All Users\Microsoft\

C:\Users\All Users\Microsoft\

C:\Users\All Users\Microsoft\

C:\Users\All Users\Microsoft\

C:\Users\All Users\Microsoft\

☐ Filtering

Klicken Sie auf das Schaltersymbol ☐ **Filter**, um das Fenster [Log-Filter](#) zu öffnen, in dem Sie Filter- oder Suchkriterien definieren können. Klicken Sie mit der rechten Maustaste auf einen Logeintrag, um das Kontextmenü zu öffnen:

Aktion	Nutzung	Verknüpfung	Siehe auch
Gleiche Datensätze filtern	Diese Option aktiviert die Log-Filterung, sodass nur Einträge vom gleichen Typ wie der ausgewählte Eintrag angezeigt werden.	Strg + Umsch + F	
Filter ...	Wenn Sie auf diese Option klicken, können Sie im Fenster „Log-Filterung“ Filterkriterien für bestimmte Log-Einträge festlegen.		Log-Filter
Filter aktivieren	Aktiviert die Filtereinstellungen. Wenn Sie die Filterung zum ersten Mal aktivieren, müssen Sie einige Einstellungen festlegen.		
Filter deaktivieren	Deaktiviert die Filterung (gleiche Funktion wie der Schalter am unteren Rand).		
Kopieren	Kopiert die Informationen der ausgewählten/hervorgehobenen Datensätze in die Zwischenablage.	Strg + C	
Alle kopieren	Kopiert die Informationen aller im Fenster angezeigten Einträge.		
Exportieren...	Exportiert die Informationen der ausgewählten/hervorgehobenen Datensätze in eine XML-Datei.		
Alle exportieren ...	Exportiert sämtliche Informationen aus dem Fenster in eine XML-Datei.		

Log-Dateien

Die Log-Dateien enthalten Informationen zu allen wichtigen aufgetretenen Programmereignissen sowie einen Überblick über Scanergebnisse, erkannte Bedrohungen usw. Logs sind unabdingbar für die Systemanalyse, die Erkennung von Problemen oder Risiken sowie die Fehlerbehebung. Die Logs werden im Hintergrund ohne Eingriffe des Benutzers erstellt. Welche Informationen aufgezeichnet werden, hängt von den aktuellen Einstellungen für die Mindestinformation ab. Textnachrichten und Logs können direkt in ESET Security for Microsoft SharePoint angezeigt oder exportiert werden.

Wählen Sie im Dropdownmenü den gewünschten Log-Typ aus. Folgende Logs sind verfügbar:

Ereignisse

Das Ereignis-Log enthält detaillierte Informationen zu Infiltrationen, die von den ESET Security for Microsoft SharePoint-Modulen erkannt wurden. Die Informationen umfassen Erkennungszeitpunkt, Name der Infiltration, Speicherort, ausgeführte Aktion und Name des Benutzers, der zum Zeitpunkt der Erkennung der Infiltration angemeldet war. Doppelklicken Sie auf einen Log-Eintrag, um die Details in einem separaten Fenster anzuzeigen. Erstellen Sie einen [Ereignisausschluss](#), indem Sie mit der rechten Maustaste auf einen Log-Eintrag (Ereignis) klicken und auf **Ausschluss erstellen** klicken. Daraufhin wird der [Ausschluss-Assistent](#) mit vordefinierten Kriterien geöffnet. Wenn neben einer ausgeschlossenen Datei der Name eines Ereignisses angezeigt wird, bedeutet dies, dass die Datei nur für das jeweilige Ereignis ausgeschlossen wird. Wenn die Datei später mit einer anderen Malware infiziert wird, wird Sie erneut erkannt.

Ereigniss

Alle von ESET Security for Microsoft SharePoint ausgeführten wichtigen Aktionen werden im Ereignis-Log aufgezeichnet. Das Ereignis-Log enthält Informationen über Ereignisse und im Programm aufgetretene Fehler. Es unterstützt Systemadministratoren und Benutzer bei der Fehlerbehebung. Die hier aufgeführten Informationen sind oftmals hilfreich, um ein im Programm aufgetretenes Problem zu beheben.

Computer prüfen

Alle Scanergebnisse werden in diesem Fenster angezeigt. Jede Zeile entspricht der Überprüfung eines einzelnen Computers. Doppelklicken Sie auf einen Eintrag, um Einzelheiten zum entsprechenden Scanvorgang anzuzeigen.

Gesperrte Dateien

Enthält Einträge für die Dateien, die gesperrt waren und auf die nicht zugegriffen werden konnte. Das Log enthält den Grund für die Sperrung und das Quellmodul, das die Datei gesperrt hat, sowie die Anwendung und den Benutzer, der die Datei ausgeführt hat.

Versickte Dateien

Enthält Einträge der cloudbasierten Schutzmodule ESET Dynamic Threat Defense und ESET LiveGrid®.

HIPS

Enthält Einträge spezifischer Regeln, die zum Aufzeichnen markiert wurden. Das Log enthält die Anwendung, die den Vorgang angefordert hat, das Ergebnis (zugelassen oder blockiert) sowie den Namen der erstellten Regel.

Netzwerkschutz

Enthält Einträge zu den Dateien, die vom Botnet-Schutz und dem IDS (Netzwerkangriffsschutz) blockiert wurden.

Gefilterte Websites

Diese Liste enthält die vom [Web-Schutz](#) gesperrten Websites. Die Logs enthalten die Uhrzeit, die URL, den Benutzer und die Anwendung, die eine Verbindung zur gegebenen Website hergestellt hat.

Gerätesteuerung

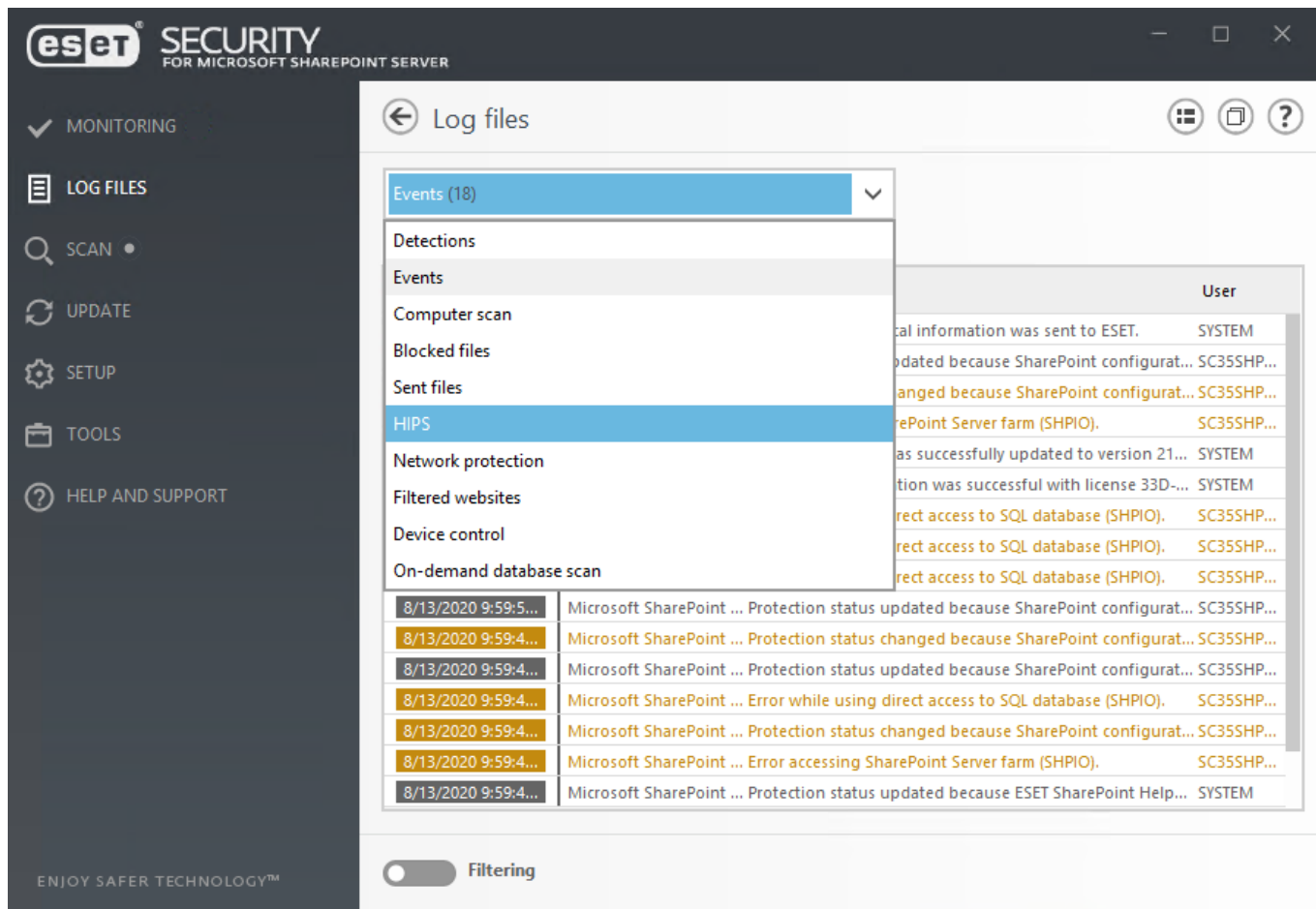
Enthält Datensätze zu Wechselmedien oder externen Geräten, die an den Computer angeschlossen wurden. Nur Geräte mit einer Regel für die Gerätesteuerung werden in die Log-Datei aufgenommen. Wenn auf ein angeschlossenes Gerät keine Regel zutrifft, wird für das Gerät kein Log-Eintrag erstellt. Hier finden Sie außerdem Details wie Gerätetyp, Seriennummer, Herstellername und Mediengröße (je nach Verfügbarkeit der Informationen).

On-Demand-Datenbankprüfung

Enthält eine Liste der Scans von SharePoint-Inhaltsdatenbanken. Für jeden Scanvorgang werden die folgenden Informationen angezeigt: Version der Erkennungsroutine, Datum, gescannter Ort, Anzahl gescannter Objekte, Anzahl erkannter Bedrohungen, Anzahl Regeltreffer und Abschlusszeitpunkt.

Hyper-V-Scan

Enthält eine Liste aller Hyper-V-Scanergebnisse. Durch Doppelklicken auf einen Eintrag können Sie Einzelheiten zum entsprechenden Scanvorgang anzeigen.



Im Kontextmenü (Rechtsklick) können Sie eine Aktion für den ausgewählten Logeintrag auswählen:


Aktion	Nutzung	Verknüpfung	Siehe auch
Anzeigen	Zeigt ausführlichere Informationen zum ausgewählten Log in einem neuen Fenster an (gleiche Aktion wie durch Doppelklicken).		
Gleiche Datensätze filtern	Diese Option aktiviert die Log-Filterung, sodass nur Einträge vom gleichen Typ wie der ausgewählte Eintrag angezeigt werden.	Strg + Umsch + F	
Filter ...	Wenn Sie auf diese Option klicken, können Sie im Fenster „Log-Filterung“ Filterkriterien für bestimmte Log-Einträge festlegen.		Log-Filter
Filter aktivieren	Aktiviert die Filtereinstellungen. Wenn Sie die Filterung zum ersten Mal aktivieren, müssen Sie einige Einstellungen festlegen.		
Filter deaktivieren	Deaktiviert die Filterung (gleiche Funktion wie der Schalter am unteren Rand).		
Kopieren	Kopiert die Informationen der ausgewählten/hervorgehobenen Datensätze in die Zwischenablage.	Strg + C	
Alle kopieren	Kopiert die Informationen aller im Fenster angezeigten Einträge.		
Löschen	Löscht die ausgewählten/hervorgehobenen Datensätze. Für diese Aktion sind Administratorberechtigungen erforderlich.		
Alle löschen	Löscht alle Datensätze im Fenster. Für diese Aktion sind Administratorberechtigungen erforderlich.		
Exportieren...	Exportiert die Informationen der ausgewählten/hervorgehobenen Datensätze in eine XML-Datei.		

Aktion	Nutzung	Verknüpfung	Siehe auch
Alle exportieren ...	Exportiert sämtliche Informationen aus dem Fenster in eine XML-Datei.		
Suchen...	Öffnet das Fenster „Im Log suchen“, in dem Sie Suchkriterien festlegen können. Dort können Sie nach Einträgen suchen, auch während die Filterung aktiviert ist.	Strg + F	In Log suchen
Weitersuchen	Sucht den nächsten Eintrag für die zuvor definierten Suchkriterien.	F3	
Rückwärts suchen	Sucht den vorherigen Eintrag.	Umsch + F3	
Ausschluss erstellen	Um Objekte anhand von Erkennungsname, Pfad oder Hash von der Säuberung auszuschließen.		Ausschluss erstellen

Log-Filter

Mit dem Log-Filter finden Sie die gesuchten Informationen auch in großen Mengen von Datensätzen. Sie können Log-Datensätze eingrenzen, wenn Sie beispielsweise nach einem bestimmten Ereignistyp, Status oder Zeitraum suchen. Wenn Sie Log-Datensätze nach Suchoptionen filtern, werden nur relevante Datensätze (gemäß der Suchoptionen) im Fenster „Log-Dateien“ angezeigt.

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. Definieren Sie den **Zeitraum**, aus dem Sie Datensätze anzeigen möchten. Außerdem haben Sie weitere Suchoptionen wie **Nur ganze Wörter** oder **Groß-/Kleinschreibung beachten** zur Auswahl.

Log filtering


Find text:

Search in columns:
Time; Module; Event; User

Record types:
Diagnostic; Informative; Warnings; Errors; Critical

Time period:
Not specified

From:
05/20/2018
11:00:00 AM

To:
05/21/2018
11:00:00 AM

Search options
☐ Match whole words only
☐ Case sensitive

Default
OK
Close

Suchen nach

Geben Sie eine Zeichenfolge ein (ein Wort oder einen Teil eines Wortes). Es werden nur Einträge angezeigt, die diese Zeichenfolge enthalten. Andere Einträge werden nicht berücksichtigt.

In Spalten

Wählen Sie die Spalten aus, die bei der Suche berücksichtigt werden sollen. Sie können mehr als eine Spalte für die Suche markieren.

Eintragstypen

Wählen Sie einen oder mehrere Log-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.
- **Kritisch** - Nur kritische Fehler werden protokolliert.

Zeitraum

Legen Sie fest, aus welchem Zeitraum die Suchergebnisse stammen sollen:

- **Keine Angabe** (Standardeinstellung) - Begrenzt die Suche nicht auf einen Zeitraum, sondern durchsucht das gesamte Log.
- **Gestern**
- **Letzte Woche**
- **Letzter Monat**
- **Zeitraum** - Sie können einen genauen Zeitraum angeben (Von: und Bis:), um nur Einträge aus diesem Zeitraum zu suchen.

Nur ganze Wörter

Aktivieren Sie dieses Kontrollkästchen, wenn Sie mit ganzen Wörtern genauere Suchergebnisse erzielen möchten.

Groß-/Kleinschreibung beachten

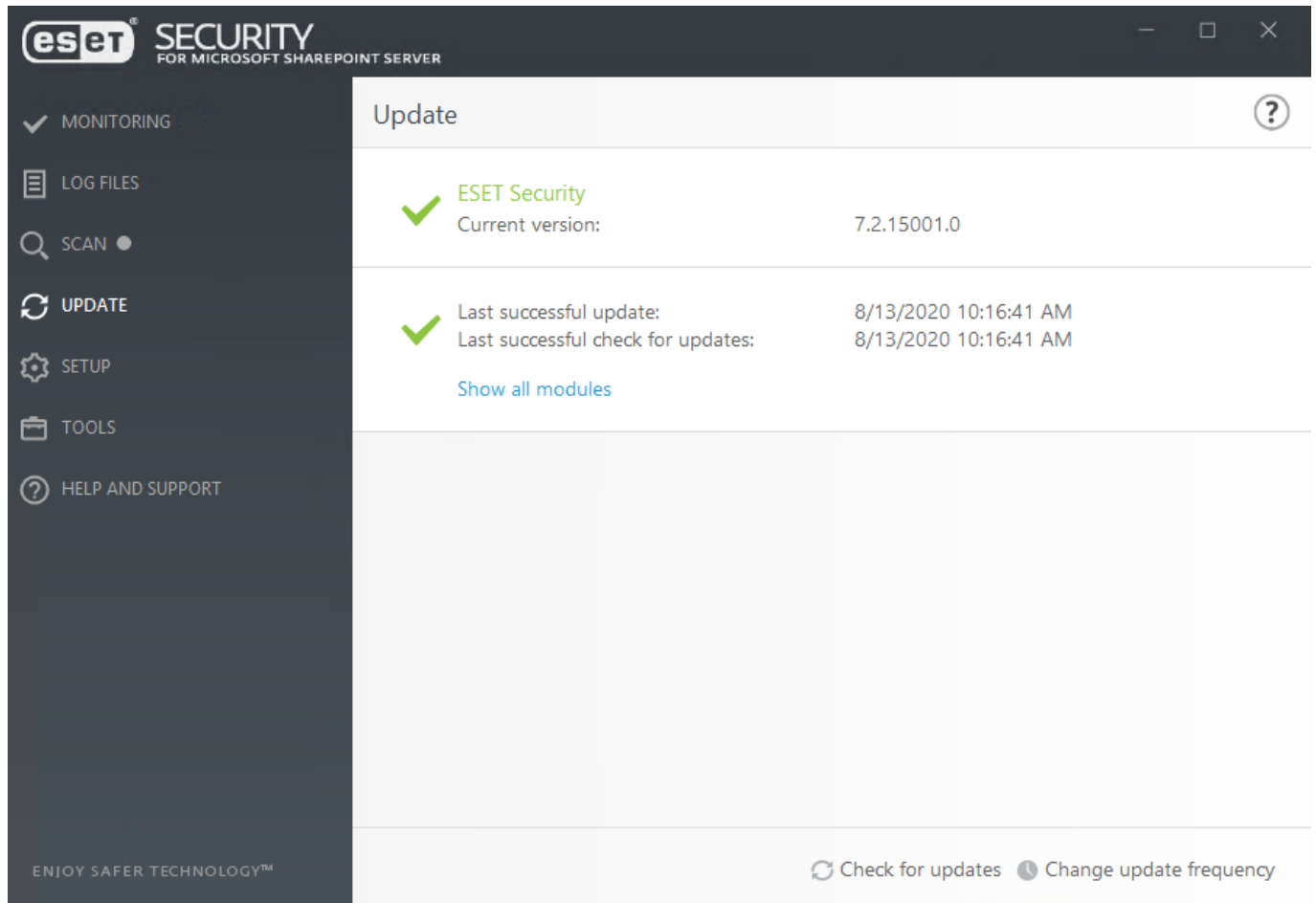
Aktivieren Sie diese Option, wenn die Groß- oder Kleinschreibung der Suchwörter beachtet werden soll. Wenn Sie Ihre Filter- und Suchoptionen konfiguriert haben, klicken Sie auf **OK**, um die gefilterten Log-Datensätze anzuzeigen, oder auf **Suchen**, um die Suche zu starten. Die Log-Dateien werden von oben nach unten ab der aktuellen (hervorgehobenen) Position durchsucht. Die Suche wird gestoppt, sobald der erste übereinstimmende Eintrag gefunden wurde. Drücken Sie **F3**, um den nächsten Datensatz zu suchen, oder klicken Sie mit der rechten Maustaste und wählen Sie **Suchen** aus, um Ihre Suchoptionen zu verfeinern.

Update

Im Bereich „Update“ wird der aktuelle Updatestatus Ihres ESET Security for Microsoft SharePoint angezeigt, inklusive Datum und Uhrzeit der letzten erfolgreichen Aktualisierung. Den optimalen Schutz Ihres Computers gewährleisten Sie, indem Sie ESET Security for Microsoft SharePoint regelmäßig aktualisieren. Das Updatemodul hält das Programm fortlaufend auf dem neuesten Stand, indem die Erkennungsroutine und die Systemkomponenten aktualisiert werden. Die Aktualisierungen von Erkennungsroutine und Programmkomponenten sind entscheidend für einen vollständigen Schutz vor Schadcode.

HINWEIS

Falls Sie noch keinen [License Lizenzschlüssel](#) eingegeben haben, erhalten Sie keine Updates und werden aufgefordert, Ihr Produkt zu aktivieren. Navigieren Sie dazu zu **Hilfe und Support > Produkt aktivieren**.



Aktuelle Version

Die Buildversion von ESET Security for Microsoft SharePoint.

Letztes erfolgreiches Update

Das Datum des letzten Updates. Hier sollte ein aktuelles Datum angezeigt werden, was auf eine kürzlich vorgenommene Aktualisierung hinweist.

Letzte erfolgreiche Prüfung auf Updates

Das Datum der letzten Überprüfung auf Modulupdates.

Alle Module anzeigen

Öffnet die Liste der installierten Module.

Nach Updates suchen

Updates der Module sind entscheidend für einen möglichst umfassenden Schutz vor Schadcode.

Updatehäufigkeit ändern

Sie können das Timing für den Taskplaner-Task [Automatische Updates in festen Zeitabständen](#) bearbeiten.

Wenn Sie nicht so schnell wie möglich nach Updates suchen, wird eine der folgenden Nachrichten angezeigt:

Fehlermeldung	Beschreibung
Die Module sind veraltet	Dieser Fehler wird angezeigt, wenn die Module trotz wiederholter Versuche nicht aktualisiert werden konnten. Überprüfen Sie in diesem Fall die Update-Einstellungen. Die häufigste Fehlerursache sind falsch eingegebene Lizenzdaten oder fehlerhaft konfigurierte Verbindungseinstellungen .
Modul-Update fehlgeschlagen - Produkt ist nicht aktiviert	Der Lizenzschlüssel wurde falsch in den Update-Einstellungen eingegeben. Wir empfehlen eine Überprüfung Ihrer Lizenzdaten. Das Fenster Erweiterte Einstellungen (F5) enthält zusätzliche Update-Optionen. Klicken Sie im Hauptmenü auf Hilfe und Support > Lizenzen verwalten , um einen neuen Lizenzschlüssel einzugeben.
Beim Herunterladen der Update-Dateien ist ein Fehler aufgetreten	Eine mögliche Fehlerursache sind die Internetverbindungseinstellungen . 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. Wenden Sie sich in diesem Fall an Ihren Internetdienstanbieter.
Modulupdate fehlgeschlagen Fehler 0073	Klicken Sie auf Update > Nach Updates suchen . Weitere Informationen finden Sie in diesem Knowledgebase-Artikel ↗ .

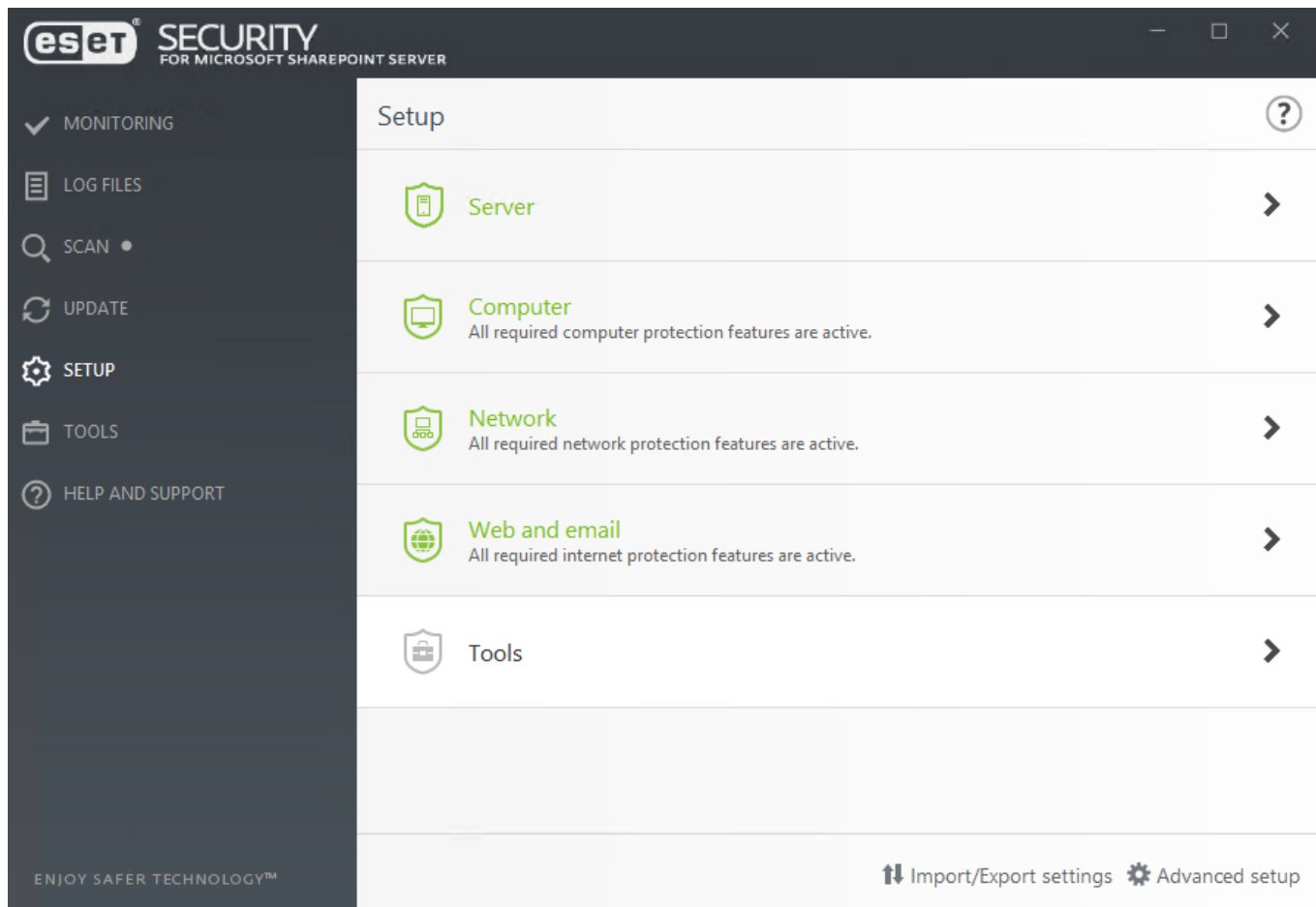
HINWEIS


Die Proxyserver-Optionen können für verschiedene Update-Profile abweichen. Konfigurieren Sie in diesem Fall die verschiedenen Update-Profile in den **Erweiterten Einstellungen (F5)**, indem Sie auf **Update** > [Profil](#) klicken.


Einstellungen


Folgende Abschnitte stehen im Menü „Einstellungen“ zur Verfügung:

- [Server](#)
- [Computer](#)
- [Netzwerk](#)
- [Web und E-Mail](#)
- [Tools - Diagnose-Logging](#)



Um einzelne Module vorübergehend zu deaktivieren, klicken Sie neben dem entsprechenden Modul auf den grünen Schieberegler . Dabei wird möglicherweise die Schutzebene Ihres Servers reduziert.

Klicken Sie auf den roten Schieberegler , um eine deaktivierte Sicherheitskomponente erneut zu aktivieren. Die Komponente wird daraufhin erneut aktiviert.

Klicken Sie auf das Zahnradsymbol , um die ausführlichen Einstellungen für eine bestimmte Sicherheitskomponente zu öffnen.



[Import-/Export-Einstellungen](#)

Mit dieser Option können Sie die Einstellungen aus einer *.xml*-Konfigurationsdatei laden oder die aktuellen Einstellungen in einer Konfigurationsdatei speichern.


[Erweiterten Einstellungen](#)

In den erweiterten Einstellungen können Sie Einstellungen und Funktionen an Ihre Anforderungen anpassen. Drücken Sie die Taste **F5** an einer beliebigen Stelle im Programm, um die **erweiterten Einstellungen** zu öffnen.

Server

Hier wird eine Liste der Komponenten angezeigt, die Sie mit dem Schieberegler  aktivieren/deaktivieren können. Um die Einstellungen für ein bestimmtes Element zu konfigurieren, klicken Sie auf das Zahnradsymbol .

Echtzeit-SharePoint-Serverschutz


Dieser Echtzeitfilter kann bei Bedarf weiter konfiguriert werden. Klicken Sie auf das Zahnradsymbol , um das Fenster [SharePoint-Schutzeinstellungen](#) zu öffnen.


[Automatische Ausschlüsse](#)


Diese Funktion identifiziert Anwendungen und Betriebssystemdateien, die für den Serverbetrieb erforderlich sind und übernimmt sie automatisch in die Liste der [Ausschlüsse](#). Auf diese Weise wird das Risiko von Konflikten durch die Bedrohungserkennungssoftware minimiert und die Gesamtleistung des Servers verbessert.

[Cluster](#)

Hier können Sie den ESET-Cluster konfigurieren und aktivieren.

Um einzelne Module vorübergehend zu deaktivieren, klicken Sie neben dem entsprechenden Modul auf den grünen Schieberegler . Dabei wird möglicherweise die Schutzebene Ihres Servers reduziert.

Klicken Sie auf den roten Schieberegler , um eine deaktivierte Sicherheitskomponente erneut zu aktivieren. Die Komponente wird daraufhin erneut aktiviert.

Klicken Sie auf das Zahnradsymbol , um die ausführlichen Einstellungen für eine bestimmte Sicherheitskomponente zu öffnen.

[Import-/Export-Einstellungen](#)

Mit dieser Option können Sie die Einstellungen aus einer *.xml*-Konfigurationsdatei laden oder die aktuellen Einstellungen in einer Konfigurationsdatei speichern.

[Erweiterten Einstellungen](#)

In den erweiterten Einstellungen können Sie Einstellungen und Funktionen an Ihre Anforderungen anpassen. Drücken Sie die Taste **F5** an einer beliebigen Stelle im Programm, um die **erweiterten Einstellungen** zu öffnen.

Computer

ESET Security for Microsoft SharePoint enthält alle erforderlichen Komponenten, um den Server als Computer zu schützen. In diesem Modul können Sie die folgenden Komponenten aktivieren, deaktivieren und konfigurieren:

[Echtzeit-Dateischutz](#)

Alle Dateien werden beim Öffnen, Erstellen oder Ausführen auf Ihrem Computer auf Schadcode geprüft. Für den Echtzeit-Dateischutz können Sie Ausschlüsse **konfigurieren** oder **bearbeiten**. Über diese Option können Sie das Fenster zum Einrichten der [Ausschlüsse](#) öffnen, in dem Sie Dateien und Ordner vom Scannen ausschließen können.

[Medienkontrolle](#)

Mit diesem Modul können Sie Medien bzw. Geräte prüfen oder sperren oder erweiterte Filter- und

Berechtigungseinstellungen anpassen und definieren, wie Benutzer auf diese Geräte zugreifen und mit ihnen arbeiten dürfen.

[Host Intrusion Prevention System \(HIPS\)](#)

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


- [Erweiterte Speicherprüfung](#) 
- [Exploit-Blocker](#) 
- [Ransomware-Schutz](#) 


[Präsentationsmodus](#)


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

Viren- und Spyware-Schutz anhalten

Bei der vorübergehenden Deaktivierung des Viren- und Spyware-Schutzes können Sie im entsprechenden Dropdownmenü den Zeitraum wählen, in dem die jeweilige Komponente deaktiviert werden soll. Klicken Sie anschließend auf **Übernehmen**, um die Sicherheitskomponente zu deaktivieren. Klicken Sie auf **Viren- und Spyware-Schutz aktivieren** oder verwenden Sie den Schieberegler, um den Schutz wieder zu aktivieren.

Um einzelne Module vorübergehend zu deaktivieren, klicken Sie neben dem entsprechenden Modul auf den grünen Schieberegler . Dabei wird möglicherweise die Schutzebene Ihres Servers reduziert.

Klicken Sie auf den roten Schieberegler , um eine deaktivierte Sicherheitskomponente erneut zu aktivieren. Die Komponente wird daraufhin erneut aktiviert.

Klicken Sie auf das Zahnradsymbol , um die ausführlichen Einstellungen für eine bestimmte Sicherheitskomponente zu öffnen.

[Import-/Export-Einstellungen](#)

Mit dieser Option können Sie die Einstellungen aus einer *.xm*-Konfigurationsdatei laden oder die aktuellen Einstellungen in einer Konfigurationsdatei speichern.

[Erweiterten Einstellungen](#)

In den erweiterten Einstellungen können Sie Einstellungen und Funktionen an Ihre Anforderungen anpassen. Drücken Sie die Taste **F5** an einer beliebigen Stelle im Programm, um die **erweiterten Einstellungen** zu öffnen.

Netzwerk


Sie können einzelne Netzwerkverbindungen anhand Ihrer Filterregeln erlauben oder ablehnen, um sich vor Angriffen von Remotecomputern zu schützen oder potenziell gefährliche Dienste zu blockieren.

Im Netzwerk-Modul können Sie folgende Komponenten aktivieren oder deaktivieren:

Netzwerkangriffsschutz (IDS)

Analysiert den Netzwerkdatenverkehr und schützt Sie vor Netzwerkangriffen. Als schädlich erkannter Datenverkehr wird blockiert.

Botnetz-Schutz


Erkennung und Sperrung von [Botnet](#) -Kommunikation. Schadsoftware im System wird schnell und akkurat identifiziert.


Vorübergehende Negativliste der IP-Adressen (blockierte Adressen)


Zeigt eine Liste von IP-Adressen an, die als Angriffsquellen identifiziert und zur Negativliste hinzugefügt wurden, um die Verbindung für einen bestimmten Zeitraum zu unterbinden.

Fehlerbehebungsassistent (kürzlich gesperrte Anwendungen oder Geräte)

Hilfreich zur Behebung von Verbindungsproblemen, die durch den Netzwerkangriffsschutz wurden.

Um einzelne Module vorübergehend zu deaktivieren, klicken Sie neben dem entsprechenden Modul auf den grünen Schieberegler . Dabei wird möglicherweise die Schutzebene Ihres Servers reduziert.

Klicken Sie auf den roten Schieberegler , um eine deaktivierte Sicherheitskomponente erneut zu aktivieren. Die Komponente wird daraufhin erneut aktiviert.

Klicken Sie auf das Zahnradsymbol , um die ausführlichen Einstellungen für eine bestimmte Sicherheitskomponente zu öffnen.

Import-/Export-Einstellungen

Mit dieser Option können Sie die Einstellungen aus einer *.xml*-Konfigurationsdatei laden oder die aktuellen Einstellungen in einer Konfigurationsdatei speichern.

Erweiterten Einstellungen

In den erweiterten Einstellungen können Sie Einstellungen und Funktionen an Ihre Anforderungen anpassen. Drücken Sie die Taste **F5** an einer beliebigen Stelle im Programm, um die **erweiterten Einstellungen** zu öffnen.

Fehlerbehebungsassistent für das Netzwerk

Der Fehlerbehebungsassistent überwacht alle blockierten Verbindungen und führt Sie durch den Fehlerbehebungsprozess, um Probleme im Zusammenhang mit dem Netzwerkangriffsschutz und bestimmten Anwendungen oder Geräten zu beheben. Anschließend empfiehlt der Assistent bestimmte Regeln, die Sie genehmigen können.

Web und E-Mail

In diesem Modul können Sie folgende Komponenten aktivieren oder deaktivieren:

[Web-Schutz](#)


Wenn diese Option aktiviert ist, werden alle Daten auf Schadsoftware geprüft, die über HTTP oder HTTPS übertragen werden.


[E-Mail-Schutz](#)


Überwacht eingehende E-Mails, die mit dem POP3- oder dem IMAP-Protokoll übertragen werden.

[Phishing-Schutz](#)

Schützt Sie vor Versuchen unseriöser Webseiten, an Passwörter, Bankdaten und andere sicherheitsrelevante Informationen zu gelangen, indem sie sich als seriöse Webseiten ausgeben.

Um einzelne Module vorübergehend zu deaktivieren, klicken Sie neben dem entsprechenden Modul auf den grünen Schieberegler . Dabei wird möglicherweise die Schutzebene Ihres Servers reduziert.

Klicken Sie auf den roten Schieberegler , um eine deaktivierte Sicherheitskomponente erneut zu aktivieren. Die Komponente wird daraufhin erneut aktiviert.

Klicken Sie auf das Zahnradsymbol , um die ausführlichen Einstellungen für eine bestimmte Sicherheitskomponente zu öffnen.


[Import-/Export-Einstellungen](#)

Mit dieser Option können Sie die Einstellungen aus einer *.xml*-Konfigurationsdatei laden oder die aktuellen Einstellungen in einer Konfigurationsdatei speichern.

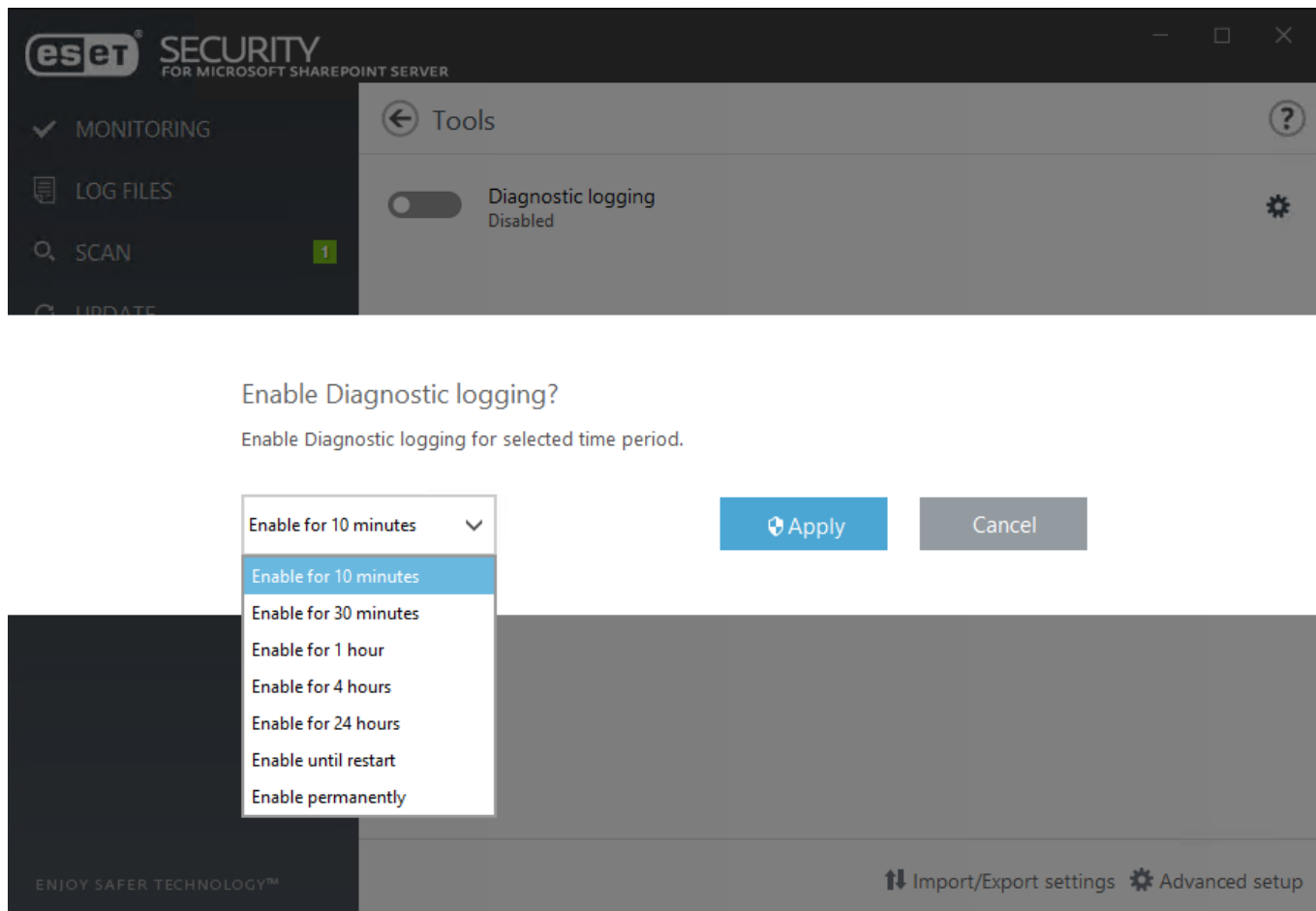
[Erweiterten Einstellungen](#)


In den erweiterten Einstellungen können Sie Einstellungen und Funktionen an Ihre Anforderungen anpassen. Drücken Sie die Taste **F5** an einer beliebigen Stelle im Programm, um die **erweiterten Einstellungen** zu öffnen.


Tools - Diagnose-Logging


Aktivieren Sie das [Diagnose-Logging](#), wenn Sie ausführliche Informationen zum Verhalten einer bestimmten ESET Security for Microsoft SharePoint-Funktion benötigen, z. B. für die Fehlerbehebung. Wenn Sie auf das Zahnradsymbol  klicken, können Sie festlegen, für welche [Funktionen](#) Diagnose-Logs gesammelt werden sollen.

Wählen Sie aus, für welchen Zeitraum dieses Feature aktiviert werden soll (10 Minuten, 30 Minuten, 1 Stunde, 4 Stunden, 24 Stunden, bis zum nächsten Serverneustart oder permanent). Nachdem Sie das Diagnose-Logging aktiviert haben, sammelt ESET Security for Microsoft SharePoint ausführliche Logs für die ausgewählten Funktionen.



Um einzelne Module vorübergehend zu deaktivieren, klicken Sie neben dem entsprechenden Modul auf den grünen Schieberegler . Dabei wird möglicherweise die Schutzebene Ihres Servers reduziert.

Klicken Sie auf den roten Schieberegler , um eine deaktivierte Sicherheitskomponente erneut zu aktivieren. Die Komponente wird daraufhin erneut aktiviert.

Klicken Sie auf das Zahnradsymbol , um die ausführlichen Einstellungen für eine bestimmte Sicherheitskomponente zu öffnen.

[Import-/Export-Einstellungen](#)

Mit dieser Option können Sie die Einstellungen aus einer *.xml*-Konfigurationsdatei laden oder die aktuellen Einstellungen in einer Konfigurationsdatei speichern.

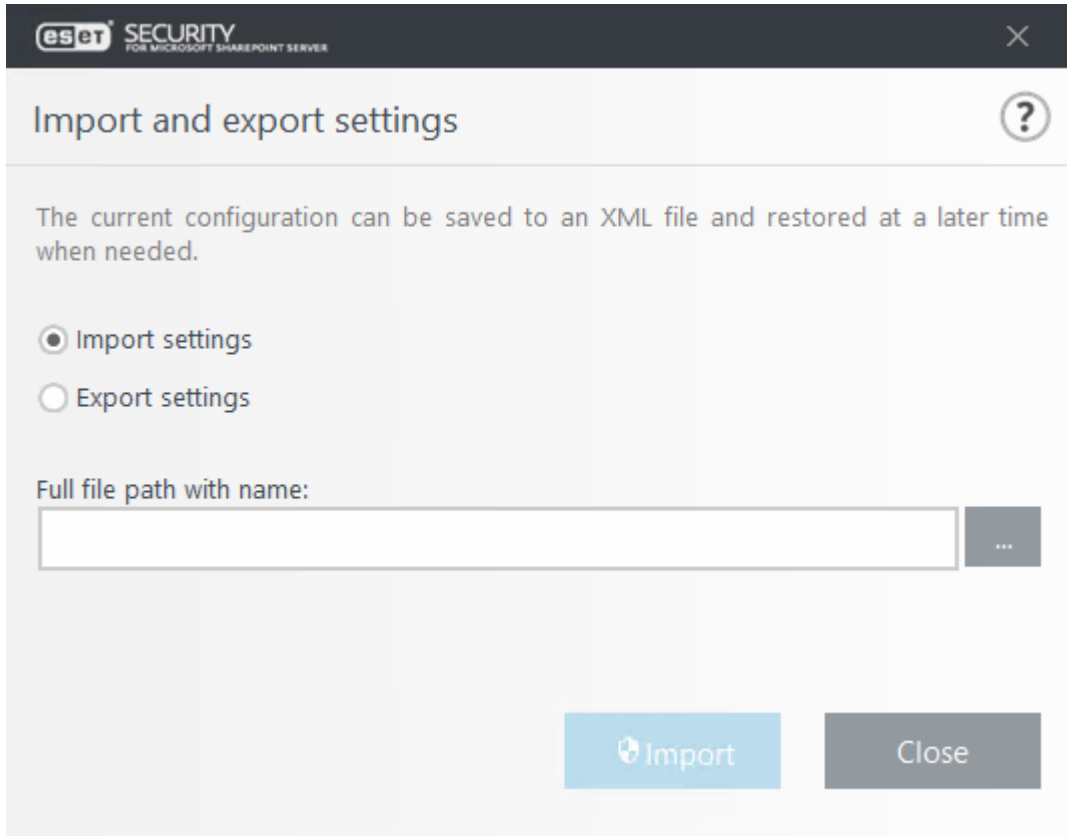
[Erweiterten Einstellungen](#)

In den erweiterten Einstellungen können Sie Einstellungen und Funktionen an Ihre Anforderungen anpassen. Drücken Sie die Taste **F5** an einer beliebigen Stelle im Programm, um die **erweiterten Einstellungen** zu öffnen.

Einstellungen importieren/exportieren

Mit der Funktion zum Importieren und Exportieren von Einstellungen können Sie Ihre aktuelle ESET Security for Microsoft SharePoint-Konfiguration sichern. Außerdem können Sie diese Funktion verwenden, um dieselben

Einstellungen auf anderen Servern mit ESET Security for Microsoft SharePoint zu verteilen oder anzuwenden. Die Einstellungen werden in eine *.xml*-Datei exportiert.



The screenshot shows a dialog box titled "Import and export settings" with a question mark icon in the top right corner. Below the title bar, there is a message: "The current configuration can be saved to an XML file and restored at a later time when needed." Below this message, there are two radio buttons: "Import settings" (which is selected) and "Export settings". Below the radio buttons, there is a text input field labeled "Full file path with name:" followed by a browse button (three dots). At the bottom of the dialog, there are two buttons: "Import" and "Close".

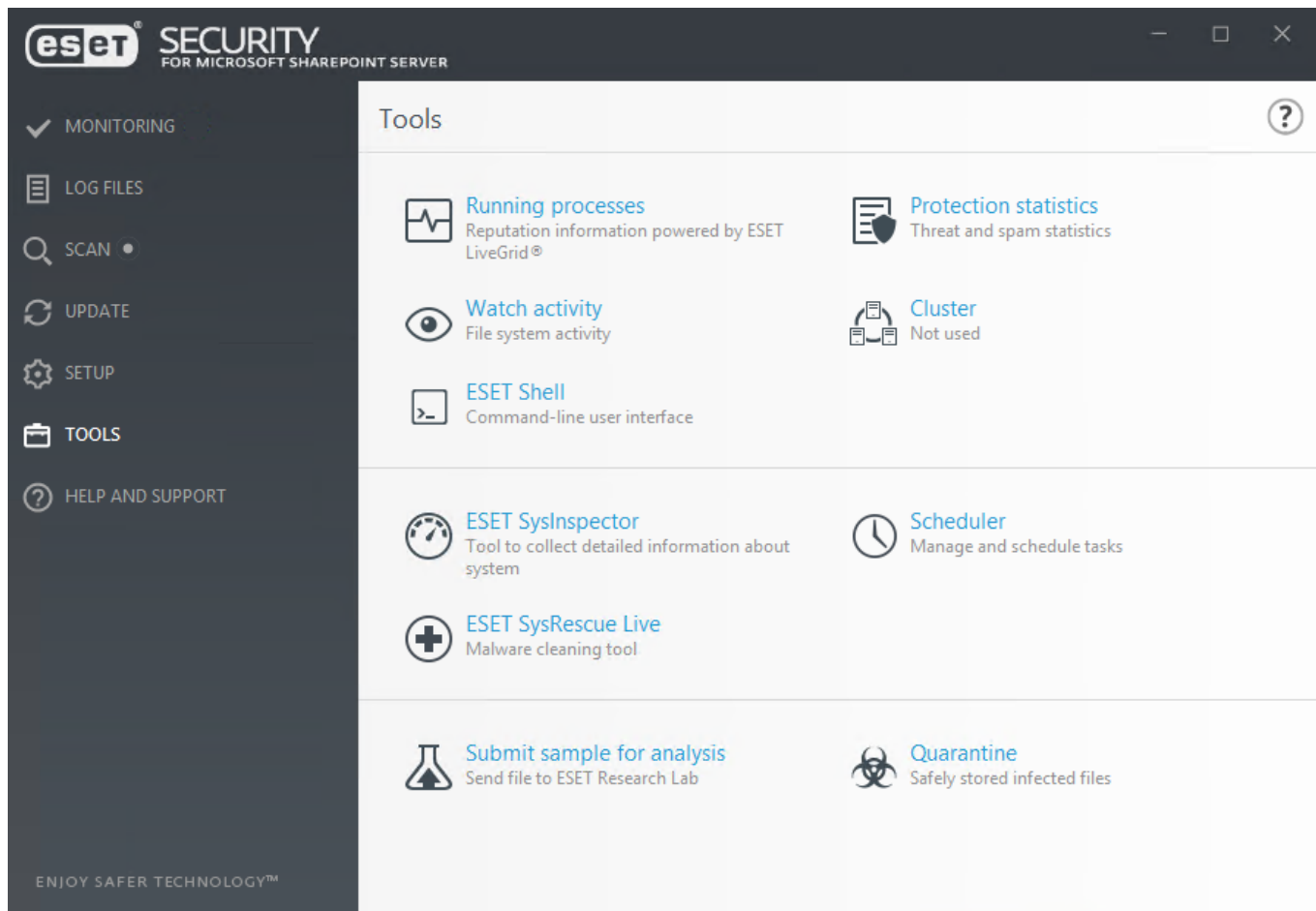
HINWEIS

Beim Exportieren der Einstellungen kann ein Fehler auftreten, wenn Sie keine Berechtigung zum Schreiben der Datei in das angegebene Verzeichnis haben.

Tools

Für die ESET Security for Microsoft SharePoint-Verwaltung sind die folgenden Funktionen verfügbar:

- [Ausgeführte Prozesse](#)
- [Aktivität beobachten](#)
- [Schutzstatistiken](#)
- [Cluster](#)
- [ESET-Shell](#)
- [ESET SysInspector](#)
- [ESET SysRescue Live](#)
- [Taskplaner](#)
- [Datei zur Analyse einreichen](#)
- [Quarantäne](#)



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 Security for Microsoft SharePoint bietet ausführliche Informationen zu ausgeführten Prozessen, um den Benutzern den Schutz der [ESET LiveGrid®](#)-Technologie zu bieten.

SECURITY
FOR MICROSOFT SHAREPOINT SERVER

MONITORING
LOG FILES
SCAN
UPDATE
SETUP
TOOLS
HELP AND SUPPORT

Running processes

This window displays a list of selected files with additional information from ESET LiveGrid®. The reputation of each is indicated, along with the number of users and time of first discovery.

Reputation	Process	PID	Number of users	Time of disc...	Application name
★★★★★	smss.exe	304	Unavailable	Unavailable	Microsoft® Windows® Op...
★★★★★	csrss.exe	412	Unavailable	Unavailable	Microsoft® Windows® Op...
★★★★★	wininit.exe	500	Unavailable	Unavailable	Microsoft® Windows® Op...
★★★★★	winlogon.exe	560	Unavailable	Unavailable	Microsoft® Windows® Op...
★★★★★	services.exe	636	Unavailable	Unavailable	Microsoft® Windows® Op...
★★★★★	lsass.exe	652	Unavailable	Unavailable	Microsoft® Windows® Op...
★★★★★	svchost.exe	748	Unavailable	Unavailable	Microsoft® Windows® Op...
★★★★★	dwm.exe	928	Unavailable	Unavailable	Microsoft® Windows® Op...
★★★★★	spoolsv.exe	1592	Unavailable	Unavailable	Microsoft® Windows® Op...
★★★★★	sqlwriter.exe	1880	Unavailable	Unavailable	Microsoft SQL Server
★★★★★	smsvchost.exe	1896	Unavailable	Unavailable	Microsoft® .NET Framework
★★★★★	wssadmin.exe	1960	Unavailable	Unavailable	Microsoft SharePoint Foun...
★★★★★	wsstracing.exe	1980	Unavailable	Unavailable	Microsoft SharePoint Foun...
★★★★★	vmtoolsd.exe	1360	Unavailable	Unavailable	VMware Tools
★★★★★	vgauthservice.exe	1348	Unavailable	Unavailable	VMware Workstation
★★★★★	dllhost.exe	2856	Unavailable	Unavailable	Microsoft® Windows® Op...

[Show details](#)

ENJOY SAFER TECHNOLOGY™

HINWEIS

Bekannte Anwendungen, die als „Beste Reputation“ (grün) markiert sind, sind sauber (Whitelist) und werden vom Scannen ausgenommen. Dadurch wird der On-Demand-Scan bzw. der Echtzeit-Dateischutz auf Ihrem Computer beschleunigt.

Reputation	Normalerweise bestimmen ESET Security for Microsoft SharePoint und die ESET LiveGrid®-Technologie die Reputation von Objekten mit einer Reihe heuristischer Regeln, bei denen die Eigenschaften der einzelnen Objekte (Dateien, Prozesse, Registrierungsschlüssel) untersucht und deren Potenzial für böswärtige Aktivitäten eingeschätzt wird. Auf Basis dieser Heuristik wird den Objekten eine Reputationsstufe von 0 - Beste Reputation (grün) bis 9 - Schlechteste Reputation (rot) zugewiesen.
Prozess	Zeigt den Namen des Programms oder Prozesses an, das/der derzeit auf dem Computer ausgeführt wird. Sie können alle auf Ihrem Computer ausgeführten Prozesse auch über den Windows-Taskmanager anzeigen. Öffnen Sie den Taskmanager, indem Sie mit der rechten Maustaste auf einen leeren Bereich auf der Taskleiste und dann auf „Taskmanager“ klicken oder indem Sie Strg+Umschalt+Esc auf Ihrer Tastatur drücken.
PID	Eine ID der in Windows-Betriebssystemen ausgeführten Prozesse.
Anzahl Benutzer	Die Anzahl der Benutzer, die eine bestimmte Anwendung verwenden. Diese Informationen werden von der ESET LiveGrid®-Technologie gesammelt.
Erkennungszeit	Die Zeitspanne seit der Erkennung der Anwendung durch die ESET LiveGrid®-Technologie.
Anwendungsname	Der festgelegte Name des Programms, zu dem der Prozess gehört.

HINWEIS

Eine als unbekannt (orange) 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 [Datei zur Analyse einreichen](#) an ESET übermitteln. Wenn sich herausstellt, dass die Datei Schadcode enthält, werden entsprechende Erkennungsfunktionen in zukünftigen Updates der Erkennungsroutine berücksichtigt.

Details anzeigen

Unten im Fenster werden die folgenden Informationen angezeigt:

- **Pfad** - Speicherort einer Anwendung auf Ihrem Computer.
- **Größe** - Dateigröße entweder in KB (Kilobyte) oder MB (Megabyte).
- **Beschreibung** - Dateieigenschaften auf Basis der Beschreibung des Betriebssystems.
- **Firma** - Name des Herstellers oder des Anwendungsprozesses.
- **Version** - Information vom Herausgeber der Anwendung.
- **Produkt** - Name der Anwendung und/oder Firmenname.
- **Erstellt** - Datum und Uhrzeit der Erstellung einer Anwendung.
- **Geändert** - Datum und Uhrzeit der letzten Änderung einer Anwendung.

[Zu ausgeschlossenen Prozessen hinzufügen](#)

Klicken Sie mit der rechten Maustaste auf einen Prozess im Fenster „Ausgeführte Prozesse“, um den Pfad zur Liste der [ausgeschlossenen Prozesse](#) hinzuzufügen und vom Scannen auszuschließen.

Aktivität beobachten

Wählen Sie die folgende Aktivität im Dropdownmenü aus, um die Aktivität als Grafik anzuzeigen:

Systemaktivität

Menge der gelesenen oder geschriebenen Daten. Die vertikale Achse des Diagramms enthält die gelesenen (blau) und geschriebenen (grün) Daten.

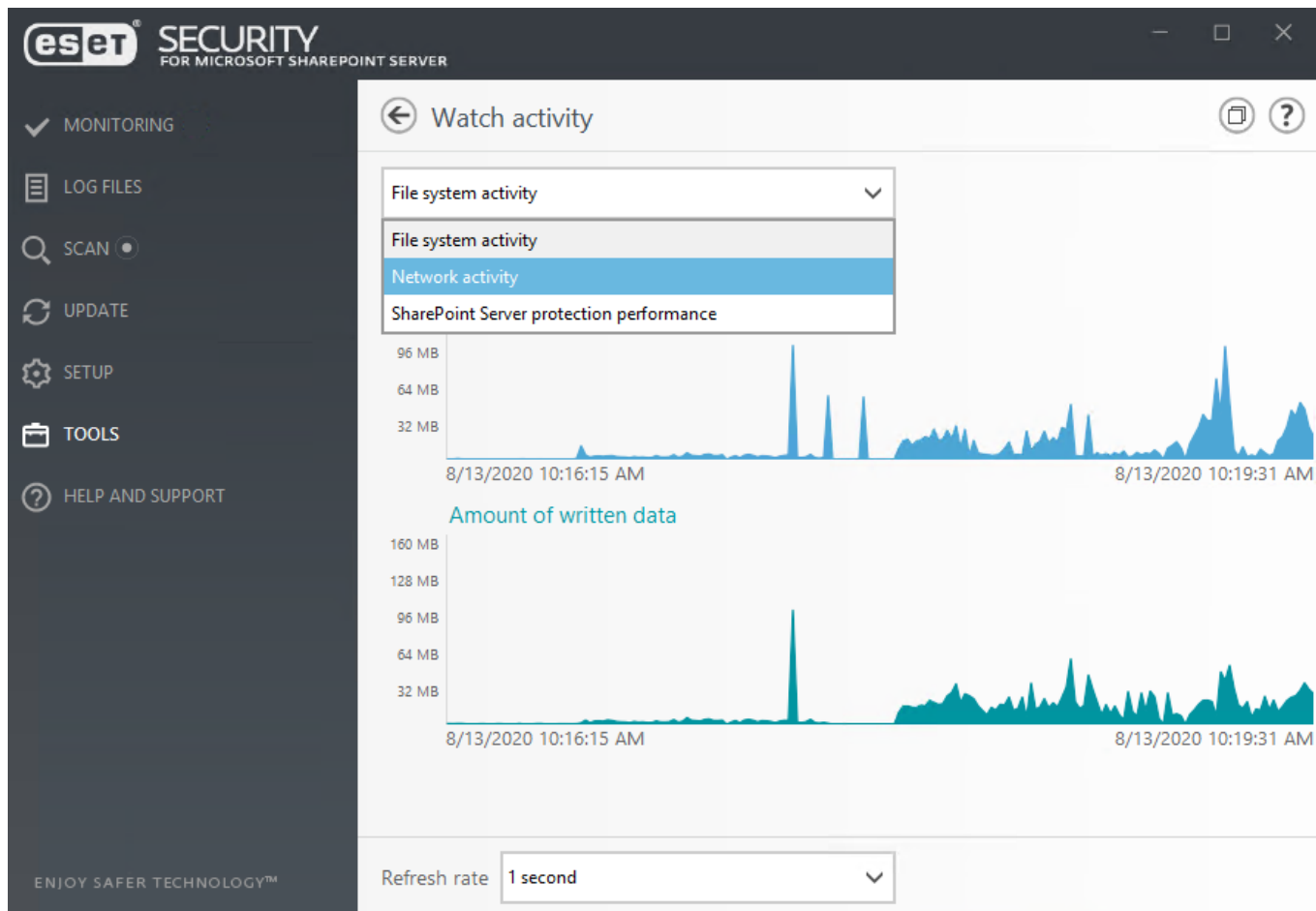
Netzwerkaktivität

Menge der empfangenen oder gesendeten Daten. Die vertikale Achse des Diagramms enthält die empfangenen (blau) und gesendeten (grün) Daten.

SharePoint-Serverschutz: Leistung

Die aktuelle Leistung (B/s, in blau) und die durchschnittliche Leistung (B/s, grün).

Im unteren Bereich des Diagramms befindet sich eine Zeitleiste, welche die Systemaktivität in Echtzeit innerhalb des gewählten Zeitraums aufzeichnet. Mit dem Dropdownmenü **Bildwiederholrate** können Sie die Aktualisierungsrate ändern.

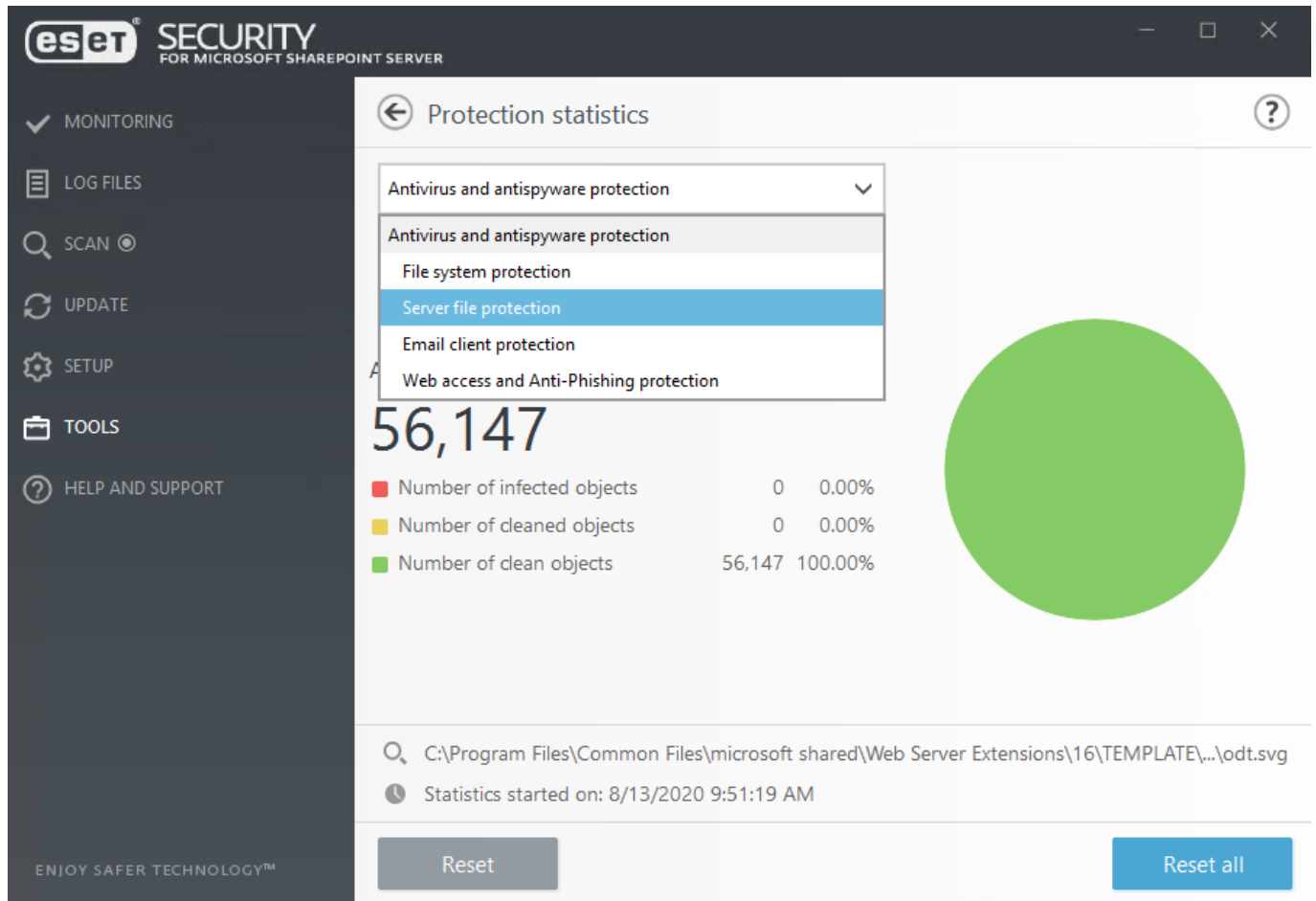


Folgende Optionen stehen zur Verfügung:

1 Sekunde	Das Diagramm wird jede Sekunde aktualisiert, und die Zeitleiste umfasst die letzten 10 Minuten.
1 Minute (letzte 24 Stunden)	Das Diagramm wird jede Minute aktualisiert, und die Zeitleiste umfasst die letzten 24 Stunden.
1 Stunde (letzter Monat)	Das Diagramm wird jede Stunde aktualisiert. Die Zeitleiste umfasst den letzten Monat.
1 Stunde (ausgewählter Monat)	Das Diagramm wird jede Stunde aktualisiert. Die Zeitleiste umfasst den letzten Monat. Wählen Sie einen Monat und ein Jahr im Dropdownmenü aus, um die Aktivität anzuzeigen. Klicken Sie auf Ändern .

Schutzstatistiken

Wählen Sie das entsprechende Schutzmodul im Dropdownmenü aus, um Statistiken zu den Schutzmodulen von ESET Security for Microsoft SharePoint anzuzeigen. Neben dem Statistik-Diagramm wird die Gesamtanzahl der geprüften, infizierten, gesäuberten und sauberen Objekte angezeigt. Bewegen Sie den Mauszeiger über ein Objekt neben dem Diagramm, um nur die Daten für das jeweilige Objekt im Diagramm anzuzeigen. Klicken Sie auf **Zurücksetzen**, um die Statistiken für das aktuelle Schutzmodul zurückzusetzen. Klicken Sie auf **Alle zurücksetzen**, um die Daten für alle Module zu löschen.



Folgende Statistikdiagramme stehen in ESET Security for Microsoft SharePoint zur Auswahl:

Viren- und Spyware-Schutz

Anzeige der Anzahl infizierter und gesäuberter Objekte.

Dateischutz

Anzeige von Objekten, die aus dem Dateisystem gelesen oder in das Dateisystem geschrieben wurden.

Hyper-V-Schutz

Anzeige der Anzahl infizierter, gesäuberter und sauberer Objekte (nur auf Systemen mit Hyper-V).

E-Mail-Schutz

Anzeige von Objekten, die von E-Mail-Programmen gesendet oder empfangen wurden.

Web- und Phishing-Schutz

Anzeige von Objekten, die von einem Webbrowser heruntergeladen wurden.

Server-Dateischutz

Zeigt hoch- und heruntergeladene SharePoint-Objekte an.

Cluster

Der **ESET-Cluster** ist eine P2P-Kommunikationsinfrastruktur aus der ESET-Produktlinie für Microsoft Windows Server.

Mit dieser Infrastruktur können ESET-Serverprodukte miteinander kommunizieren, Daten wie Konfigurationsdaten und Benachrichtigungen austauschen, ordnungsgemäßen Betrieb einer Gruppe von Produktinstanzen erforderlichen Daten synchronisieren. Ein Beispiel einer solchen Gruppe ist eine Knotengruppe in einem Windows-Failover-Cluster oder einem Network Load Balancing (NLB)-Cluster mit installiertem ESET-Produkt, bei der das Produkt im gesamten Cluster gleich konfiguriert sein muss. ESET Cluster garantiert diese Einheitlichkeit zwischen den Instanzen.

HINWEIS

Die Einstellungen für die [Benutzeroberfläche](#) werden nicht zwischen ESET-Clusterknoten synchronisiert.

Sie finden die Statusseite für ESET-Cluster im Hauptmenü unter **Tools > Cluster**. Bei korrekter Konfiguration sieht die Statusseite wie folgt aus:

The screenshot shows the ESET Security for Microsoft SharePoint Server interface. The left sidebar contains navigation options: MONITORING, LOG FILES, SCAN, UPDATE, SETUP, TOOLS, and HELP AND SUPPORT. The main area displays the 'Cluster' status page. At the top of this page is a 'Cluster' header with a back arrow, a refresh icon, and a help icon. Below this is a table with two columns: 'Name' and 'State'. The table lists three nodes: W2012R2-NODE1, W2012R2-NODE2, and W2012R2-NODE3, all with a state of 'Online'. At the bottom of the main area are three buttons: 'Cluster wizard...', 'Import certificates...', and 'Destroy cluster'.

Name	State
W2012R2-NODE1	Online
W2012R2-NODE2	Online
W2012R2-NODE3	Online

HINWEIS

Das Erstellen von ESET-Clustern zwischen ESET Security for Microsoft SharePoint und ESET File Security für Linux wird nicht unterstützt.

Beim Einrichten des ESET-Cluster können Sie Knoten auf zwei Arten hinzufügen:

Autom. erkennen

Falls Sie ein vorhandenes Windows-Failovercluster oder NLB-Cluster haben, werden dessen Mitglieds-knoten automatisch zum ESET-Cluster hinzugefügt.

Durchsuchen

Sie können Knoten manuell durch Eingeben der Servernamen hinzufügen (entweder Mitglieder der gleichen Arbeitsgruppe oder der gleichen Domäne).

HINWEIS

Server müssen nicht Mitglieder des Windows-Failoverclusters/NLB-Clusters sein. Zur Verwendung eines ESET-Clusters ist kein Windows-Failovercluster oder NLB-Cluster erforderlich.

Nachdem Sie Knoten zum ESET-Cluster hinzugefügt haben, muss auf jedem Knoten ESET Security for Microsoft SharePoint installiert werden. Dies erfolgt automatisch während der Einrichtung des ESET-Cluster. Folgende Anmeldedaten sind für die Remote-Installation von ESET Security for Microsoft SharePoint auf anderen Clusterknoten erforderlich:

In einer Domäne

Anmeldedaten des Domänenadministrators.

In einer Arbeitsgruppe

Vergewissern Sie sich, dass alle Knoten die Anmeldedaten des gleichen lokalen Administratorkontos verwenden.

In einem ESET-Cluster können Sie auch eine Kombination aus automatisch hinzugefügten Knoten (Mitglieder eines Windows-Failover-Cluster oder NLB-Cluster) und manuell hinzugefügten Knoten verwenden, sofern die Knoten sich in der gleichen Domäne befinden.

WICHTIG

Domänenknoten und Arbeitsgruppenknoten können nicht kombiniert werden.

In einem ESET-Cluster muss außerdem die **Datei- und Druckerfreigabe** in der Windows-Firewall aktiviert werden, bevor ESET Security for Microsoft SharePoint auf die ESET-Clusterknoten verteilt wird.

Sie können jederzeit neue Knoten zu einem vorhandenen ESET-Cluster hinzufügen, indem Sie den [Clusterassistenten](#) ausführen.

Zertifikate importieren

Zertifikate ermöglichen eine sichere Computerauthentifizierung, wenn HTTPS verwendet wird. Jedes ESET-Cluster verwendet eine unabhängige Zertifikathierarchie. Die Hierarchie enthält ein Stammzertifikat und eine Reihe von Knotenzertifikaten, die mit dem Stammzertifikat signiert wurden. Der private Schlüssel des Stammzertifikats wird vernichtet, nachdem alle Knotenzertifikate erstellt wurden. Wenn Sie einen neuen Knoten zum Cluster hinzufügen, wird eine neue Zertifikathierarchie erstellt. Navigieren Sie zum Ordner, der die Zertifikate enthält, die vom Clusterassistenten erstellt wurden. Wählen Sie die Zertifikatdatei aus und klicken Sie auf **Öffnen**.

Cluster zerstören

ESET-Cluster können gelöscht werden. Jeder Knoten schreibt einen Eintrag zur Zerstörung des ESET-Clusters das eigene Ereignis-Log. Anschließend werden alle ESET-Firewall-Regeln aus der Windows-Firewall entfernt.

Die ehemaligen Knoten werden in ihren vorherigen Zustand zurückversetzt und können bei Bedarf erneut in einem anderen ESET-Cluster verwendet werden.

Clusterassistent – Knoten auswählen

Der erste Schritt zur Einrichtung eines ESET-Clusters ist das Hinzufügen von Knoten. Verwenden Sie entweder die Option **Automatisch erkennen** oder fügen Sie die Knoten über die Funktion **Durchsuchen** manuell hinzu. Alternativ können Sie den Servernamen in das Textfeld eingeben und auf **Hinzufügen** klicken.

Autom. erkennen

Fügt Knoten eines vorhandenen Windows-Failover-Clusters/Network Load Balancing(NLB)-Clusters automatisch hinzu. Der Server, über den Sie den ESET-Cluster erstellen möchten, muss Mitglied eines Windows-Failover-Clusters/NLB-Clusters sein, damit die Knoten automatisch hinzugefügt werden. Auf dem NLB-Cluster muss in den Clustereigenschaften die Option **Remotesteuerung zulassen** aktiviert sein, damit der ESET-Cluster die Knoten richtig erkennt. Nachdem die Liste der neu hinzugefügten Knoten erstellt wurde, können Sie unerwünschte Knoten entfernen.


Durchsuchen

Klicken Sie auf „Durchsuchen“, um Computer innerhalb einer Domäne oder Arbeitsgruppe zu suchen und auszuwählen. Mit dieser Methode können Sie Knoten manuell zum ESET-Cluster hinzufügen. Eine weitere Methode zum Hinzufügen von Knoten ist die Eingabe des Hostnamens des hinzuzufügenden Servers. Bestätigen Sie die Eingabe durch Klicken auf **Hinzufügen**.

Laden

Importiert eine Liste von Knoten aus einer Datei.

Select nodes



Machine to add to the list of cluster nodes

Add
Remove
Remove all
Autodetect
Browse...
Load...

Cluster nodes

ESFW_NODE1
ESFW_NODE2
ESFW_NODE3

Next
Cancel

Um **Clusterknoten** in der Liste zu ändern, wählen Sie einen zu entfernenden Knoten aus und klicken Sie auf **Entfernen**. Klicken Sie alternativ auf **Alle entfernen**, um die Liste vollständig zu löschen.

Sie können jederzeit Knoten zu einem bereits vorhandenen ESET-Cluster hinzufügen. Die Schritte entsprechen der oben beschriebenen Vorgehensweise.

HINWEIS

Alle in der Liste verbleibenden Knoten müssen online und erreichbar sein. Localhost wird standardmäßig zu den Clusterknoten hinzugefügt.

Clusterassistent – Clustereinstellungen

Definieren Sie einen Clusternamen und Netzwerkeinstellungen (falls erforderlich).

Clustername

Wählen Sie einen Namen für den Cluster aus und klicken Sie auf **Weiter**.

Listening Port - (Der Standardport ist 9777)

Falls Port 9777 in Ihrer Netzwerkumgebung bereits verwendet wird, geben Sie eine andere, nicht verwendete Portnummer ein.

Port in Windows-Firewall öffnen

Wenn diese Option aktiviert ist, wird in der Windows-Firewall eine Regel erstellt.

Clusterassistent - Einstellungen für die Clustereinrichtung

Legen Sie einen Zertifikatverteilungsmodus fest und geben Sie an, ob das Produkt auf den anderen Knoten installiert werden soll oder nicht.

Zertifikatverteilung

- **Automatisch remote** - Das Zertifikat wird automatisch installiert.
- **Manuell** - Klicken Sie auf **Erstellen** und wählen Sie den Ordner aus, in dem die Zertifikate gespeichert werden sollen. Es werden ein Stammzertifikat und ein Zertifikat für jeden Knoten erstellt, einschließlich für den Knoten (lokaler Computer), auf dem Sie den ESET-Cluster einrichten. Klicken Sie auf **Ja**, um das Zertifikat auf dem lokalen Computer zu registrieren.

Produktinstallation an anderen Knoten

- **Automatisch remote** - ESET Security for Microsoft SharePoint wird auf jedem Knoten automatisch installiert (sofern die Betriebssysteme der Knoten dieselbe Architektur haben).
- **Manuell** - Manuelle Installation von ESET Security for Microsoft SharePoint (beispielsweise falls einige der Knoten eine andere Betriebssystemarchitektur aufweisen).

Lizenz auf Knoten ohne aktiviertes Produkt übertragen

ESET Security aktiviert die auf Knoten ohne Lizenzen installierten ESET-Lösungen automatisch.

HINWEIS

Wenn Sie einen ESET-Cluster mit gemischten Betriebssystemarchitekturen (32-Bit und 64-Bit) erstellen möchten, müssen Sie ESET Security for Microsoft SharePoint manuell installieren. Die verwendeten Betriebssysteme werden in den nächsten Schritten ermittelt, und die Informationen werden im Log-Fenster angezeigt.

Clusterassistent – Knotenprüfung

Nach dem Festlegen der Installationsdetails wird eine Knotenprüfung ausgeführt. Die folgenden Informationen werden im **Knotenprüfungs-Log** angezeigt:

- Alle vorhandenen Knoten sind online.
- Die neuen Knoten sind erreichbar.
- Der Knoten ist online.
- Der Zugriff auf die administrative Freigabe ist möglich.
- Die Remote-Ausführung ist möglich.
- Die richtigen Produktversionen sind installiert bzw. es ist kein Produkt installiert.
- Die neuen Zertifikate sind vorhanden.

Node check log

[2:07:55 PM] Node check started
[2:07:55 PM] PING test:
[2:07:55 PM] OK
[2:07:55 PM] Administration share access test:
[2:07:57 PM] OK
[2:07:57 PM] Service manager access test:
[2:08:04 PM] OK
[2:08:04 PM] Checking installed product version and features:
[2:08:04 PM] 0% (W2012R2-NODE1)...

Abort

< Previous

Next >

Cancel

Nach dem Abschließen der Knotenprüfung wird der Bericht angezeigt:

Node check log

[2:07:55 PM] Node check started
[2:07:55 PM] PING test:
[2:07:55 PM] OK
[2:07:55 PM] Administration share access test:
[2:07:57 PM] OK
[2:07:57 PM] Service manager access test:
[2:08:04 PM] OK
[2:08:04 PM] Checking installed product version and features:
[2:08:06 PM] W2012R2-NODE3: Remote machine has different set of ESET product features installed. Product will be reinstalled.
[2:08:07 PM] W2012R2-NODE2: Install will be performed.
[2:08:08 PM] OK

Check

< Previous

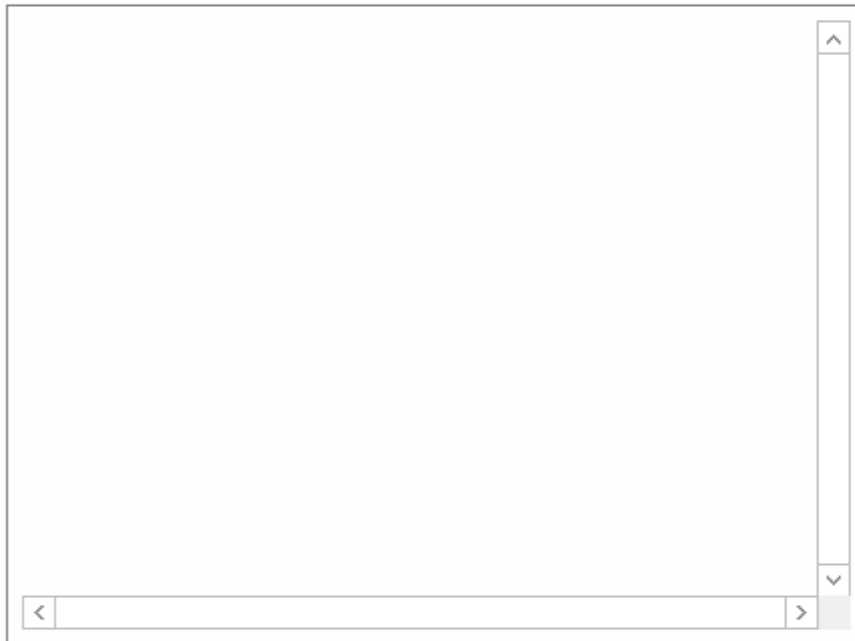
Next >

Cancel

Clusterassistent - Knoteninstallation

Wenn Sie das Produkt bei der Initialisierung des ESET-Clusters auf einem Remotecomputer installieren, sucht der Assistent das Installationspaket im Verzeichnis *%ProgramData%\ESET\ESET Security\Installer*. Wenn das Installationspaket dort nicht gefunden wird, werden Sie aufgefordert, den Speicherort der Datei anzugeben.

Product install log

[Install](#)

< Previous

Finish

Cancel

HINWEIS

Wenn Sie versuchen, eine automatische Remoteinstallation für einen Knoten einer anderen Plattform (32-Bit im Gegensatz zu 64-Bit) auszuführen, erkennt das Programm die Situation und fordert Sie auf, eine manuelle Installation auszuführen.

Product install log

```
[12:56:34 PM] Generating certificates for cluster nodes...  
[12:56:36 PM] All certificates created.  
[12:56:36 PM] Copying files to remote machines:  
[12:56:41 PM] All files have been copied to remote machines.  
[12:56:41 PM] Installing product:  
[12:56:42 PM] Number of installers started: 2  
[12:59:35 PM] ESET product is installed on all remote machines.  
[12:59:35 PM] Enrolling certificates:  
[12:59:38 PM] All certificates have been enrolled to remote  
machines.  
[12:59:38 PM] Activating cluster feature:  
[12:59:40 PM] ESET cluster feature has been activated on all  
machines.
```

[Install](#)

< Previous

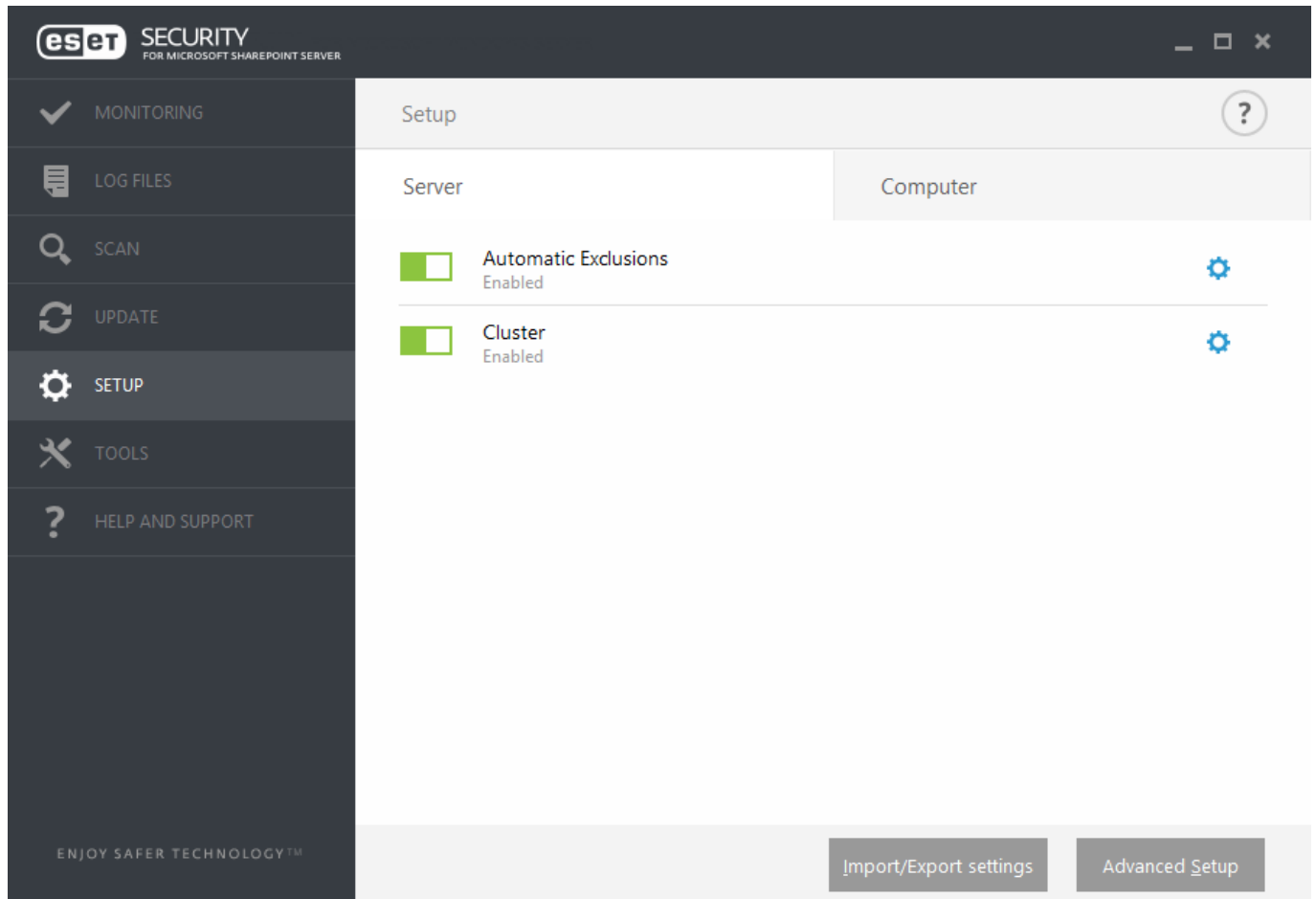
Finish

Cancel

Nachdem Sie den ESET-Cluster richtig konfiguriert haben, wird er auf der Seite **Einstellungen > Server** mit dem Status „aktiviert“ angezeigt.

HINWEIS

Wenn auf einigen Knoten bereits eine ältere Version von ESET Security for Microsoft SharePoint installiert ist, wird eine Benachrichtigung angezeigt, dass die aktuelle Version auf diesen Computern benötigt wird. Bei der Aktualisierung von ESET Security for Microsoft SharePoint wird unter Umständen ein Neustart durchgeführt.



Sie können den aktuellen Status auch auf der Clusterstatusseite (**Tools > Cluster**) überprüfen.

ESET-Shell

eShell (Abkürzung für ESET Shell) ist eine Kommandozeilen-Schnittstelle für ESET Security for Microsoft SharePoint. Es handelt sich dabei um eine Alternative zur grafischen Benutzeroberfläche (GUI). Über eShell haben Sie Zugriff auf alle Funktionen und Optionen, die Ihnen sonst über die Benutzeroberfläche zur Verfügung stehen. Mit eShell können Sie ohne die GUI das gesamte Programm konfigurieren und verwalten.

Neben der Bereitstellung aller Funktionen und Optionen, die über die Benutzeroberfläche steuerbar sind, bietet die Kommandozeile auch die Möglichkeit, Prozesse durch Skripte zu automatisieren. Mit ihnen können Sie das Programm konfigurieren, Änderungen vornehmen und Aktionen ausführen. Außerdem ist eShell nützlich für alle Benutzer, die eine Kommandozeile generell der Benutzeroberfläche vorziehen.

HINWEIS

Um den vollständigen Funktionsumfang zu nutzen, sollten Sie eShell mit der Option Als Administrator ausführen starten. Dies gilt auch, wenn Sie einzelne Befehle über die Windows-Eingabeaufforderung (cmd) eingeben. Öffnen Sie die Eingabeaufforderung mit Als Administrator ausführen. Wenn Sie die Eingabeaufforderung nicht als Administrator ausführen, können Sie manche Befehle mangels Berechtigungen nicht ausführen.

eShell kann in den folgenden beiden Modi ausgeführt werden:

1. **Interaktiver Modus** - Dieser Modus eignet sich, wenn Sie umfassend mit eShell arbeiten möchten (also nicht nur einzelne Befehle ausführen), z. B. zum Ändern der Konfiguration oder Anzeigen von Log-Dateien.

Der interaktive Modus bietet sich auch an, wenn Sie noch nicht mit allen Befehlen vertraut sind. Der interaktive Modus erleichtert die Navigation durch eShell. In diesem Modus werden auch die im jeweiligen Kontext verfügbaren Befehle angezeigt.

2. Einzelner Befehl/Batch-Modus - Verwenden Sie diesen Modus, wenn Sie nur einen Befehl ausführen müssen, ohne dabei den interaktiven Modus von eShell zu verwenden. Geben Sie dazu in der Windows-Eingabeaufforderung eshell mit den entsprechenden Parametern ein.

BEISPIEL

```
eshell get status oder eshell computer set real-time status disabled lh
```

Um bestimmte Befehle (wie das zweite Beispiel oben) ausführen zu können, müssen Sie zunächst einige Einstellungen [konfigurieren](#). Andernfalls erhalten Sie die Nachricht **Zugriff verweigert**. Dies ist aus Sicherheitsgründen erforderlich.

HINWEIS

Sie benötigen die Berechtigung zur Ausführung von eShell-Befehlen in einer Windows-Eingabeaufforderung, um Einstellungen ändern zu können. Weitere Informationen zum Ausführen von Batch-Dateien finden Sie [hier](#).

Sie können den interaktiven Modus in eShell auf zwei Arten aktivieren:

1. Über das **Windows-Startmenü**: Start > Alle Programme > ESET > ESET Security for Microsoft SharePoint > ESET-Shell
2. Über die **Windows-Eingabeaufforderung** Geben Sie `eshell` ein und drücken Sie die Eingabetaste

WICHTIG

Falls der Fehler 'eshell' is not recognized as an internal or external command angezeigt wird, wurden die neuen Umgebungsvariablen nach der Installation von ESET Security for Microsoft SharePoint nicht vom System geladen. Öffnen Sie eine neue Eingabeaufforderung und starten Sie eShell neu. Falls der Fehler weiterhin auftritt oder Sie eine [Core-Installation](#) von ESET Security for Microsoft SharePoint verwenden, starten Sie eShell mit dem absoluten Pfad, zum Beispiel "%PROGRAMFILES%\ESET\ESET Security\eshell.exe" (Die Anführungszeichen "" sind erforderlich für den Befehl).

Wenn Sie eShell zum ersten Mal im interaktiven Modus ausführen, wird ein Willkommens- (Anleitungsbildschirm) angezeigt.

HINWEIS

Wenn Sie diesen Bildschirm später erneut aufrufen möchten, geben Sie den Befehl `guide` ein. Hier sehen Sie einfache Beispiele für die Verwendung von eShell sowie Informationen zu Syntax, Präfixen, Befehlspfaden, Abkürzungen, Aliasnamen usw.

Bei der nächsten Ausführung von eShell wird dieser Bildschirm angezeigt:


```
ESET Shell
ESET Shell 2.0 (6.5.12009.1)
Copyright (c) 1992-2017 ESET, spol. s r.o. All rights reserved.

Maximum protection

License validity:      12/30/2021
Last successful update: N/A

Automatic exclusions:      Enabled
Anti-Stealth protection:   Enabled
Document protection:       Disabled
HIPS:                      Enabled
Real-time file system protection: Enabled
Device control:            Disabled
ESET Cluster:              Disabled
Diagnostic logging:         Disabled
Presentation mode:         Paused
Anti-Phishing protection:  Enabled
Email client protection:   Enabled
Web access protection:     Enabled

ABOUT      ANTI VIRUS    DEVICE      GUIDE      LICENSE
PASSWORD    RUN            SCHEDULER  SETTINGS  SIGN
STATUS      TOOLS           UI          UPDATE    VIRLOG
WARNLOG     WEB-AND-EMAIL

eShell>
```

HINWEIS

Groß- und Kleinschreibung ist für Befehle nicht relevant. Der Befehl wird unabhängig davon ausgeführt, ob Sie Groß- oder Kleinbuchstaben verwenden.

Anpassen eShell

Sie können eShell im `ui eshell`-Kontext anpassen. Sie können Aliase, Farben, Sprache, Ausführungsrichtlinie für [Skripts](#) konfigurieren, ausgeblendete Befehle anzeigen und andere Einstellungen vornehmen.

Nutzung

Syntax

Die Befehle funktionieren nur dann ordnungsgemäß, wenn sie mit der richtigen Syntax eingegeben werden. Sie können aus einem Präfix, einem Kontext, Argumenten, Optionen usw. bestehen. Allgemein verwendet eShell die folgende Syntax:

[<Präfix>] [<Befehlspfad>] <Befehl> [<Argumente>]

Beispiel (aktiviert den Dokumentenschutz):

```
SET COMPUTER SCANS DOCUMENT REGISTER ENABLED
```

SET - Ein Präfix

COMPUTER SCANS DOCUMENT - Pfad zu einem bestimmten Befehl, also der Kontext des Befehls

REGISTER - Der eigentliche Befehl

ENABLED - Ein Argument für den Befehl

Wenn Sie `?` als Argument für einen Befehl angeben, wird die Syntax des entsprechenden Befehls angezeigt. `STATUS ?` zeigt beispielsweise die Syntax für den Befehl `STATUS` an:

SYNTAX:

[get] status

VORGÄNGE:

get - Status aller Schutzmodule anzeigen

Beachten Sie, dass [get] in Klammern steht. Dies bedeutet, dass das Präfix `get` das Standardpräfix für den Befehl `status` ist. Wird also dem Befehl `status` kein bestimmtes Präfix zugewiesen, wird das Standardpräfix verwendet (in diesem Fall `get status`). Wenn Sie das Präfix weglassen, sparen Sie Zeit beim Eingeben von Befehlen. Üblicherweise ist `get` das Standardpräfix der meisten Befehle. Dennoch sollten Sie das Standardpräfix des jeweiligen Befehls kennen und sich sicher sein, dass Sie ihn so ausführen möchten.

HINWEIS

Bei der Befehlseingabe müssen Sie nicht auf Groß- und Kleinschreibung achten. Der Befehl wird unabhängig davon ausgeführt, ob Sie Groß- oder Kleinbuchstaben verwenden.

Präfix / Vorgang

Ein Präfix ist ein Vorgang. Das Präfix `GET` zeigt die Konfiguration einer bestimmten ESET Security for Microsoft SharePoint-Funktion oder den Status an (z. B. zeigt `GET COMPUTER REAL - TIME STATUS` den aktuellen Schutzstatus an). Das Präfix `SET` konfiguriert die Funktion bzw. ändert ihren Status (`SET COMPUTER REAL - TIME STATUS ENABLED` aktiviert den Schutz).

Die nachfolgend genannten Präfixe stehen in eShell zur Verfügung. Je nach Befehl werden bestimmte Präfixe unterstützt.

GET	gibt aktuelle Einstellung/aktuellen Status zurück
SET	legt Wert/Status fest
SELECT	element auswählen
ADD	element hinzufügen
REMOVE	element entfernen
CLEAR	entfernt alle Elemente/Dateien
START	aktion starten
STOP	aktion beenden
PAUSE	Aktion anhalten
RESUME	aktion fortsetzen
RESTORE	stellt Standardeinstellungen/-objekt/-datei wieder her
SEND	objekt/Datei senden
IMPORT	aus Datei importieren
EXPORT	in Datei exportieren

HINWEIS

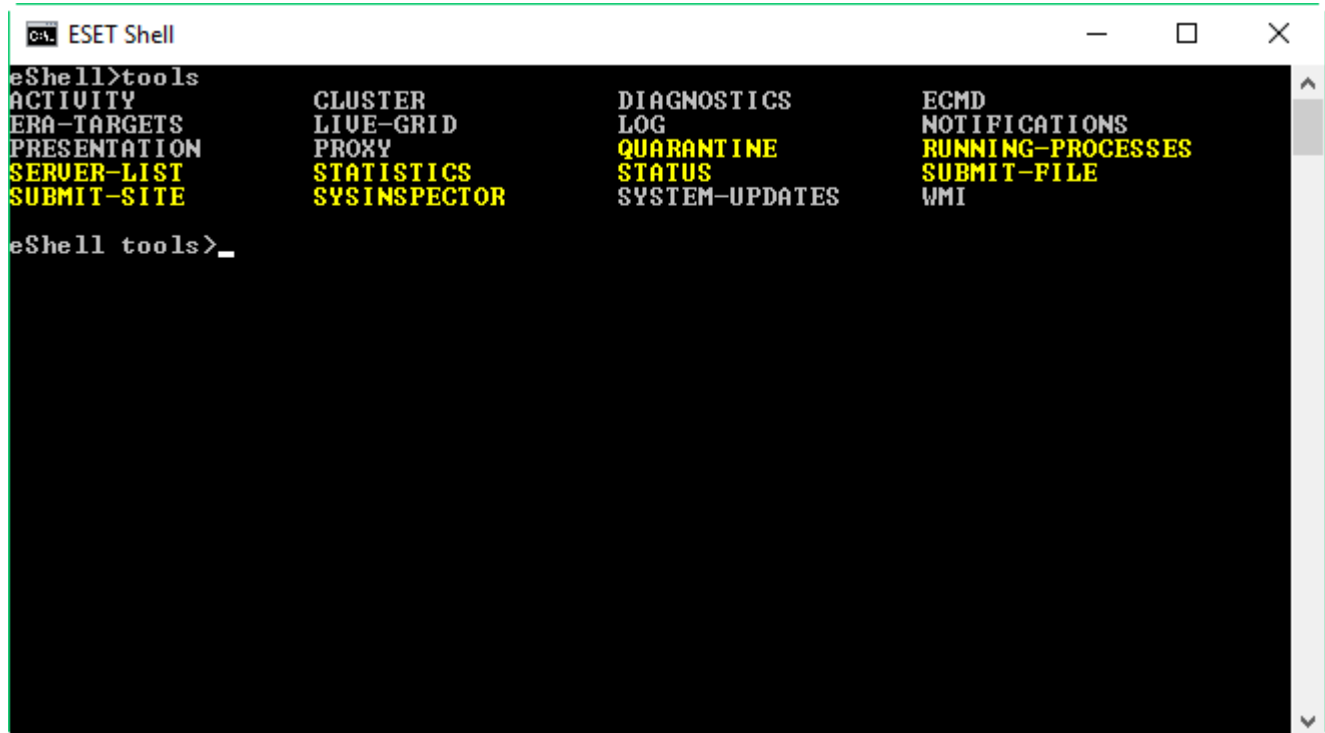
Präfixe wie `GET` und `SET` werden für viele, aber nicht alle Befehle verwendet. Der Befehl `EXIT` verwendet zum Beispiel kein Präfix.

Befehlspfad / Kontext

Befehle sind in einen Kontext in Form einer Baumstruktur eingebettet. Die höchste Ebene bildet der Kontext „root“. Beim Start von eShell befinden Sie sich also auf der Root-Ebene.

eShell>

Hier können Sie entweder einen Befehl ausführen oder den Kontextnamen eingeben, um auf die entsprechende Ebene zu gelangen. Wenn Sie zum Beispiel den Kontext **T00LS** eingeben, werden alle dort verfügbaren Befehle und untergeordneten Kontexte aufgelistet.



Gelbe Elemente stellen ausführbare Befehle und graue Elemente stellen auswählbare untergeordnete Kontexte dar. Ein untergeordneter Kontext enthält weitere Befehle.

Wenn Sie auf eine höhere Ebene zurückkehren möchten, geben Sie `..` ein (zwei Punkte).

BEISPIEL

Nehmen wir beispielsweise an, Sie befinden sich hier:

```
eShell computer real-time>
```

Geben Sie `..` ein, um zur nächsthöheren Ebene zu wechseln:

```
eShell computer>
```

Wenn Sie dagegen von `eShell computer real-time>` wieder die zwei Ebenen zur Root-Ebene hochgehen möchten, geben Sie `.. ..` ein (zwei Punkte, Leerzeichen, zwei Punkte). So gelangen Sie zwei Ebenen höher (in diesem Fall zur Root-Ebene). Verwenden Sie den umgekehrten Schrägstrich `\\`, um von jeder beliebigen Ebene in der Kontextstruktur direkt zur Stammebene zu gelangen. Um zu einem bestimmten Kontext in höheren Ebenen zu gelangen, verwenden Sie die entsprechende Anzahl von `...`-Befehlen. Verwenden Sie Leerzeichen als Trennzeichen. Um drei Ebenen nach oben zu gelangen, verwenden Sie `.. ..`.

Der Pfad ist relativ zum aktuellen Kontext. Geben Sie den Pfad nicht ein, wenn der Befehl im aktuellen Kontext enthalten ist. Um zum Beispiel `GET COMPUTER REAL-TIME STATUS` auszuführen, geben Sie Folgendes ein:

`GET COMPUTER STATUS` - wenn Sie sich im Root-Kontext befinden (Kommandozeile zeigt an `eShell>`)

`GET STATUS` - wenn Sie sich im Kontext befinden (Kommandozeile zeigt an `eShell computer>`)

`.. GET STATUS` - wenn Sie sich im Kontext befinden (Kommandozeile zeigt an `eShell computer real-`)


```
time>
```

Sie können einen einfachen Punkt (.) verwenden, weil ein einzelner Punkt eine Abkürzung für zwei Punkte (..) ist.

BEISPIEL

```
. GET STATUS - wenn Sie sich im Kontext befinden (Kommandozeile zeigt an eShell computer real-time>
```

Argument

Ein Argument ist eine Aktion, die für einen bestimmten Befehl ausgeführt wird. Der Befehl **CLEAN-LEVEL** (unter **COMPUTER REAL-TIME ENGINE**) kann mit den folgenden Argumenten verwendet werden:

rigorous - Ereignis immer beheben
safe - Ereignis beheben, falls sicher, andernfalls beibehalten
normal - Ereignis beheben, falls sicher, andernfalls nachfragen
none - Immer den Endbenutzer fragen

Weitere Beispiele sind die Argumente **ENABLED** oder **DISABLED**, mit denen Sie bestimmte Optionen oder Funktionen aktivieren oder deaktivieren können.

Kurzformen

In eShell können Sie Kontexte, Befehle und Argumente abkürzen (falls es sich bei dem Argument um einen Switch oder eine alternative Option handelt). Die Abkürzung eines Präfixes oder eines Arguments in Form eines konkreten Wertes (z. B. Nummer, Name oder Pfad) ist nicht möglich. Sie können die Ziffern **1** und **0** anstelle der Argumente „enabled“ und „disabled“ verwenden.

BEISPIEL

```
computer set real-time status enabled    =>  com set real stat 1  
computer set real-time status disabled    =>  com set real stat 0
```

Beispiele für die Kurzform:

BEISPIEL

```
computer set real-time status enabled    =>  com set real stat en  
computer exclusions add detection-excludes object C:\path\file.ext    =>  com  
excl add det obj C:\path\file.ext  
computer exclusions remove detection-excludes 1    =>  com excl rem det 1
```

Wenn zwei Befehle oder Kontexte gleich beginnen (z. B. **ADVANCED** and **AUTO-EXCLUSIONS**) und Sie **A** als verkürzte Befehlsform wählen, kann eShell nicht bestimmen, welchen der beiden Befehle Sie ausführen möchten. In diesem Fall wird eine Fehlermeldung und eine Liste der verfügbaren Befehle mit dem Anfangsbuchstaben **A** angezeigt:

```
eShell>a
```

```
The following command is not unique: a
```

Die folgenden Unterkontexte sind im Kontext **COMPUTER** verfügbar:

Wenn Sie mehrere Buchstaben eingeben (z. B. `AD` anstelle von `A`), wechselt eShell zum Unterkontext `ADVANCED`, da der Befehl jetzt eindeutig ist. Dasselbe gilt für abgekürzte Befehle.

HINWEIS

Um den Befehl korrekt auszuführen, sollten Sie Befehle, Argumente usw. nicht abkürzen, sondern vollständig angeben. Auf diese Weise führt eShell die Befehle genau wie angegeben aus, und unerwünschte Fehler werden vermieden. Dies gilt vor allem für Batch-Dateien und Skripte.

Automatische Vervollständigung

Diese mit Version eShell 2.0 eingeführte Funktion entspricht der automatischen Vervollständigung in der Windows-Befehlszeile. Während die Windows-Befehlszeile nur Dateipfade vervollständigt, verwendet eShell diese Funktion auch für Befehle, Kontext- und Vorgangsnamen. Die Vervollständigung von Argumenten wird nicht unterstützt. Drücken Sie bei der Eingabe eines Befehls die TAB-Taste, um den Befehl zu vervollständigen oder durch die möglichen Variationen zu blättern. Drücken Sie UMSCH + TAB, um rückwärts zu blättern. Mischungen zwischen abgekürzter Form und automatischer Vervollständigung werden nicht unterstützt. Sie können jeweils nur eine der beiden Formen verwenden. Wenn Sie zum Beispiel `computer real-time additional` eingeben, bewirkt TAB nichts. Geben Sie stattdessen `com` ein und drücken Sie TAB, um `computer` zu vervollständigen, geben Sie dann `real` + TAB und `add` + TAB ein und drücken Sie die Eingabetaste. Geben Sie `on` + TAB ein und drücken Sie mehrfach auf TAB, um alle möglichen Variationen zu durchlaufen: `on-execute-ah`, `on-execute-ah-removable`, `on-write-ah`, `on-write-archive-default` usw..

Aliasnamen

Ein Alias ist ein alternativer Name, um einen Befehl auszuführen (vorausgesetzt, dass diesem Befehl ein Alias zugewiesen wurde). Dies sind die Standard-Aliase:

```
(global) close - exit
(global) quit - exit
(global) bye - exit
warnlog - tools log events
virlog - tools log detections
```

„(global)“ bedeutet, dass der Befehl kontextunabhängig verwendet werden kann. Einem Befehl können mehrere Aliasnamen zugewiesen werden. So hat der Befehl `EXIT` die Aliasnamen `CLOSE`, `QUIT` und `BYE`. Wenn Sie eShell beenden möchten, können Sie den Befehl `EXIT` oder einen seiner Aliasnamen verwenden. Der Aliasname `VIRLOG` bezieht sich auf den Befehl `DETECTIONS` im Kontext `TOOLS LOG`. Mit diesem Alias ist der Befehl im Kontext `ROOT` verfügbar und so leichter erreichbar (Sie müssen nicht erst in die Kontexte `TOOLS` und dann `LOG` wechseln, sondern starten den Befehl direkt in `ROOT`).

Mit eShell können Sie eigene Aliasnamen festlegen. Der Befehl `ALIAS` befindet sich im Kontext `UI ESHELL`.

Einstellungen mit Passwort schützen

Die ESET Security for Microsoft SharePoint-Einstellungen können mit einem Passwort geschützt werden. Sie können das [Passwort in der Benutzeroberfläche](#) oder in eShell mit dem Befehl `set ui access lock-password` festlegen. Anschließend müssen Sie dieses Passwort interaktiv für bestimmte Befehle eingeben (z. B. beim Ändern von Einstellungen oder von Daten). Wenn Sie über längere Zeit mit eShell arbeiten und das Passwort nicht ständig eingeben möchten, können Sie es in eShell mit dem Befehl `set password` speichern (als `root`

ausgeführt). Das Passwort wird anschließend automatisch für alle Befehle ausgefüllt, für die ein Passwort erforderlich ist. Es bleibt gespeichert, bis Sie eShell verlassen. Sie müssen `set password` also erneut ausführen, wenn Sie Ihr Passwort in einer neuen eShell-Sitzung erneut speichern möchten.

Guide / Help

Wenn Sie den Befehl `GUIDE` oder `HELP` ausführen, wird ein Bildschirm mit Benutzungshinweisen für eShell angezeigt. Dieser Befehl ist nur im Kontext `ROOT` verfügbar (`eShell>`).

Befehlsverlauf

eShell speichert einen Verlauf der bereits ausgeführten Befehle. Gespeichert werden aber nur die Befehle der aktuellen interaktiven eShell-Sitzung. Wenn Sie eShell beenden, wird der Befehlsverlauf gelöscht. Mit den Pfeiltasten „Auf“ und „Ab“ können Sie durch den Verlauf blättern. Wenn Sie den gesuchten Befehl gefunden haben, können Sie ihn erneut ausführen oder ändern, ohne den gesamten Befehl erneut eingeben zu müssen.

CLS / Bildschirm löschen

Der Befehl `CLS` löscht den Bildschirm, genau wie in der Windows-Eingabeaufforderung oder ähnlichen Kommandozeilenprogrammen.

EXIT / CLOSE / QUIT / BYE

Zum Schließen oder Beenden von eShell stehen Ihnen diese vier Befehle zur Verfügung (`EXIT`, `CLOSE`, `QUIT` oder `BYE`).

Befehle

Dieser Abschnitt enthält einige grundlegende eShell-Befehle mit einer Beschreibung.

HINWEIS

Bei der Befehlseingabe müssen Sie nicht auf Groß- und Kleinschreibung achten. Der Befehl wird unabhängig davon ausgeführt, ob Sie Groß- oder Kleinbuchstaben verwenden.

Beispielbefehle (Befehle im Kontext `ROOT`):

ABOUT

Zeigt Programminformationen an. Hier finden Sie die folgenden Informationen:

- Name und Versionsnummer des installierten ESET-Sicherheitsprodukts.
- Betriebssystem und allgemeine Hardwareinformationen.
- Benutzername (inklusive Domäne), vollständiger Computername (FQDN, falls Ihr Server Mitglied einer Domäne ist) und Lizenzname.
- Installierte Komponenten Ihres ESET-Sicherheitsprodukts inklusive der Versionsnummern aller Komponenten.

KONTEXTPFAD:

`root`

PASSWORD

Wenn Sie passwortgeschützte Befehle ausführen möchten, werden Sie aus Sicherheitsgründen in der Regel aufgefordert, ein Passwort einzugeben. Dies betrifft Befehle, die zum Beispiel die Deaktivierung des Schutzes zur Folge haben oder die Konfiguration von ESET Security for Microsoft SharePoint beeinflussen könnten. Jedes Mal, wenn ein solcher Befehl ausgeführt werden soll, muss das Passwort eingegeben werden. Um das Passwort nicht jedes Mal selbst eingeben zu müssen, können Sie es festlegen. eShell ruft das Passwort automatisch ab, wenn ein passwortgeschützter Befehl ausgeführt werden soll.

HINWEIS

Das festgelegte Passwort gilt nur für die aktuelle eShell-Sitzung im interaktiven Modus. Wenn Sie eShell beenden, wird das festgelegte Passwort gelöscht. Für die nächste Ausführung von eShell müssen Sie das Passwort erneut festlegen.

Das festgelegte Passwort kann auch für die Ausführung unsignierter Batchdateien oder Skripts verwendet werden. Legen Sie die [ESET-Shell-Ausführungsrichtlinie](#) auf Vollzugriff fest, wenn Sie unsignierte Batchdateien ausführen möchten. Hier ein Beispiel für eine solche Batch-Datei:

```
eshell set password plain <yourpassword> "&" computer set real-time status disabled
```

Dieser verkettete Befehl legt das Passwort fest und deaktiviert den Schutz.

WICHTIG

Verwenden Sie nach Möglichkeit immer signierte Batchdateien. Auf diese Weise müssen Sie keine Klartextpasswörter in den Batchdateien verwenden (falls Sie die oben beschriebene Methode verwenden). Siehe [Batchdateien / Skripts](#) (Abschnitt Signierte Batchdateien) für weitere Details.

KONTEXTPFAD:

root

SYNTAX:

```
[get] | restore password
```

```
set password [plain <password>]
```

VORGÄNGE:

get - Passwort anzeigen

set - Passwort speichern oder löschen

restore - Passwort löschen

ARGUMENTE:

plain - Passwort als Parameter eingeben

password - Passwort

BEISPIELE:

```
set password plain <yourpassword> - Legt das Passwort für passwortgeschützte Befehle fest
```


`restore password` - Löscht das Passwort

BEISPIELE:

`get password` - Mit diesem Befehl können Sie überprüfen, ob ein Passwort konfiguriert wurde. Es werden nur Sternchen (*) angezeigt, nicht das eigentliche Passwort. Wenn keine Sternchen sichtbar sind, dann wurde auch kein Passwort festgelegt

`set password plain <IhrPasswort>` - Festgelegtes Passwort speichern

`restore password` - Festgelegtes Passwort löschen

STATUS

Zeigt den aktuellen Echtzeit-Schutzstatus von ESET Security for Microsoft SharePoint an, und Sie können den Schutz anhalten oder fortsetzen (ähnlich wie in der Benutzeroberfläche).

KONTEXTPFAD:

`computer real-time`

SYNTAX:

`[get] status`

`set status enabled | disabled [10m | 30m | 1h | 4h | temporary]`

`restore status`

VORGÄNGE:

`get` - Aktuelle Einstellung/Status zurückgeben

`set` - Wert/Status festlegen

`restore` - Standardeinstellungen/-objekt/-datei wiederherstellen

ARGUMENTE:

`enabled` - Schutz/Funktion aktivieren

`disabled` - Schutz/Funktion deaktivieren

`10m` - 10 Minuten lang deaktivieren

`30m` - 30 Minuten lang deaktivieren

`1h` - 1 Stunde lang deaktivieren

`4h` - 4 Stunden lang deaktivieren

`temporary` - Bis zum Neustart deaktivieren

HINWEIS

Es ist nicht möglich, alle Schutzfunktionen mit einem einzigen Befehl zu deaktivieren. Sie können die Schutzfunktionen und Module einzeln mit dem `status`-Befehl verwalten. Jede Schutzfunktion und jedes Modul verwendet einen eigenen `status`-Befehl.

Liste der Funktionen mit `status`-Befehl:

Funktion	Kontext und Befehl
Automatische Ausschlüsse	COMPUTER AUTO-EXCLUSIONS STATUS
Host Intrusion Prevention System (HIPS)	COMPUTER HIPS STATUS
Echtzeit-Dateischutz	COMPUTER REAL-TIME STATUS
Medienkontrolle	DEVICE STATUS
Botnetz-Schutz	NETWORK ADVANCED STATUS-BOTNET
Netzwerkangriffsschutz (IDS)	NETWORK ADVANCED STATUS-IDS
Netzwerkisolierung	NETWORK ADVANCED STATUS-ISOLATION
ESET-Cluster	TOOLS CLUSTER STATUS
Diagnose-Logging	TOOLS DIAGNOSTICS STATUS
Präsentationsmodus	TOOLS PRESENTATION STATUS
Phishing-Schutz	WEB-AND-EMAIL ANTIPHISHING STATUS
E-Mail-Client-Schutz	WEB-AND-EMAIL MAIL-CLIENT STATUS
Web-Schutz	WEB-AND-EMAIL WEB-ACCESS STATUS

VIRLOG

Dieser Alias für den Befehl `DETECTIONS` ist hilfreich, um Informationen zu erkannter eingedrungener Schadsoftware anzuzeigen.

WARNLOG

Dieser Alias für den Befehl `EVENTS` ist hilfreich, um Informationen zu verschiedenen Ereignissen anzuzeigen.

Batchdateien / Skripts

Sie können eShell als leistungsstarkes Skripting-Tool für die Automatisierung verwenden. Um eine Batch-Datei mit eShell zu verwenden, erstellen Sie eine Datei mit einem eShell-Befehl.

BEISPIEL

```
eshell get computer real-time status
```

Sie können Befehle auch verketten. Geben Sie z. B. Folgendes ein, um den Typ eines bestimmten geplanten Tasks abzurufen:

```
eshell select scheduler task 4 "&" get scheduler action
```

Die Auswahl eines Elements (Task Nummer 4 in diesem Fall) bezieht sich nur auf eine aktuell laufende Instanz von eShell. Wenn Sie diese beiden Befehle nacheinander ausführen, schlägt der zweite Befehl mit der Fehlermeldung "Kein Task ausgewählt oder ausgewählter Task ist nicht mehr vorhanden" fehl.

Aus Sicherheitsgründen ist die [Ausführungsrichtlinie](#) standardmäßig auf **Eingeschränktes Skripting** beschränkt.

Mit dieser Einstellung können Sie eShell als Überwachungstool verwenden, jedoch keine skriptgesteuerten Konfigurationsänderungen an ESET Security for Microsoft SharePoint vornehmen. Wenn Sie ein Skript mit sicherheitsrelevanten Befehlen ausführen, z. B. zum Deaktivieren des Schutzes, erhalten Sie die Nachricht **Zugriff verweigert**. Verwenden Sie nach Möglichkeit signierte Batchdateien, um Befehle mit Konfigurationsänderungen auszuführen.

Um die Konfiguration mit einzelnen Befehlen in der Windows-Eingabeaufforderung zu ändern, müssen Sie eShell Vollzugriff gewähren (nicht empfohlen). Um den Vollzugriff zu gewähren, verwenden Sie den Befehl `ui eshell shell-execution-policy` im interaktiven Modus von eShell oder in der Benutzeroberfläche unter **Erweiterte Einstellungen (F5) > Benutzeroberfläche > [ESET-Shell](#)**.

Mit signierten Batchdateien

Mit eShell können Sie gewöhnliche Batchdateien (*.bat) mit einer Signatur sichern. Skripts werden mit demselben Passwort signiert, das für den Schutz der Einstellungen verwendet wurde. Um ein Skript zu signieren, müssen Sie zunächst die Option [Einstellungen schützen](#) aktivieren, entweder in der Benutzeroberfläche oder in eShell mit dem Befehl `set ui access lock-password`. Sobald Sie das Passwort für den Schutz der Einstellungen eingerichtet haben, können Sie Batchdateien signieren.

HINWEIS

Wenn Sie das Passwort für den [Schutz der Einstellungen](#) ändern, müssen Sie alle Skripte erneut signieren, da diese andernfalls nicht mehr ausgeführt werden können. Das beim Signieren der Skripte eingegebene Passwort muss mit dem Passwort für den Schutz der Einstellungen auf dem Zielsystem übereinstimmen.

Um eine Batchdatei zu signieren, führen Sie `sign <script.bat>s` im Stammkontext von eShell aus, wobei *script.bat* der Pfad zum Skript ist, das Sie signieren möchten. Geben Sie das Signierungspasswort ein und bestätigen Sie es. Dieses Passwort muss mit Ihrem Passwort für den Schutz der Einstellungen übereinstimmen. Die Signatur wird in Form eines Kommentars an das Ende der Batchdatei angehängt. Falls das Skript bereits signiert war, wird die vorhandene Signatur durch die neue Signatur ersetzt.

HINWEIS

Wenn Sie eine zuvor signierte Batchdatei bearbeiten, müssen Sie diese anschließend erneut signieren.

Geben Sie den folgenden Befehl ein, um eine signierte Batchdatei in der Windows-Befehlszeile oder als geplanten Task auszuführen:


```
eshell run <script.bat>
```

Script.bat ist in diesem Fall der Pfad zur Batchdatei.

BEISPIEL

```
eshell run d:\myeshellscript.bat
```

ESET SysInspector

[ESET SysInspector](#)  ist eine Anwendung, die Ihren Computer gründlich durchsucht und eine genaue (Risikostufen-)Analyse Ihrer Systemkomponenten erstellt. Hierzu zählen u. a. installierte 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.

Klicken Sie auf **Erstellen** und geben Sie einen kurzen **Kommentar** ein, der das zu erstellende Log beschreibt. Warten Sie, bis das ESET SysInspector-Log erstellt wurde (Status ist 'Erstellt'). Je nach Hardwarekonfiguration und Systemdaten kann die Log-Erstellung eine gewisse Zeit in Anspruch nehmen.

Das ESET SysInspector-Fenster zeigt folgende Informationen zu erstellten Logs an:

- **Zeit** - Zeitpunkt der Log-Erstellung.
- **Kommentar** - Eine kurze Beschreibung.
- **Benutzer** - Der Name des Benutzers, der das Log erstellt hat.
- **Status** - Status bei der Log-Erstellung.


Folgende Aktionen stehen zur Verfügung:

- **Anzeigen** - Öffnet das erstellte Log. Sie können auch mit der rechten Maustaste auf eine Log-Datei klicken und im Kontextmenü die Option „Anzeigen“ auswählen.
- **Vergleichen** - Vergleicht zwei vorhandene Logs.
- **Erstellen** - Erstellt ein neues Log. Geben Sie einen kurzen Kommentar zum neuen Log ein und klicken Sie auf „Erstellen“. Warten Sie, bis das ESET SysInspector-Log erstellt wurde (Status wird als „Erstellt“ angezeigt).
- **Löschen** - Entfernt die ausgewählten Logs aus der Liste.

Mit einem Rechtsklick auf ein oder mehrere ausgewählte Logs stehen im Kontextmenü die folgenden Optionen zur Verfügung:

- **Anzeigen** - Anzeige des ausgewählten Logs in ESET SysInspector (entspricht einem Doppelklick auf einen beliebigen Eintrag).
- **Vergleichen** - Vergleicht zwei vorhandene Logs.
- **Erstellen** - Erstellt ein neues Log. Geben Sie einen kurzen Kommentar zum neuen Log ein und klicken Sie auf **Erstellen**. Warten Sie, bis das ESET SysInspector-Log erstellt wurde (**Status** wird als „Erstellt“ angezeigt).
- **Löschen** - Entfernt die ausgewählten Logs aus der Liste.
- **Alle löschen** - Löschen aller Logs.
- **Export** - Exportieren des Logs in eine .xml-Datei oder komprimierte .xml-Datei.

ESET SysRescue Live

[ESET SysRescue Live](#)  ist ein kostenloses Hilfsprogramm, mit dem Sie ein bootfähiges Rettungsmedium (CD/DVD oder USB-Laufwerk) erstellen können. Anschließend können Sie einen infizierten Computer mit diesem Medium starten, nach Malware scannen und infizierte Dateien säubern.

ESET SysRescue Live bietet den wichtigen Vorteil, dass die ESET Security-Lösungen unabhängig vom Host-Betriebssystem ausgeführt werden, aber direkten Zugriff auf die Festplatte und das Dateisystem haben. Auf diese Weise lassen sich auch Bedrohungen entfernen, bei denen dies normalerweise (z. B. bei laufendem Betriebssystem) nicht möglich wäre.

Taskplaner

Der Taskplaner verwaltet und startet geplante Tasks basierend auf definierten Parametern. Hier können Sie eine Liste aller geplanten Tasks als Tabelle mit Parametern wie Typ und Name des Tasks, Startzeit und Zeitpunkt der letzten Ausführung anzeigen. Sie können auch neue geplante Tasks erstellen, indem Sie auf [Task hinzufügen](#) klicken. Um die Konfiguration eines vorhandenen geplanten Tasks zu bearbeiten, klicken Sie auf die Schaltfläche **Bearbeiten**. Setzen Sie die Liste der geplanten Tasks auf die Standardeinstellungen zurück, indem Sie auf **Standard** und dann auf **Auf Standard zurücksetzen** klicken. Alle Änderungen gehen in diesem Fall verloren und dieser Vorgang kann nicht rückgängig gemacht werden.

Es gibt einen Satz vordefinierter Standard-Tasks:

- Log-Wartung
- Automatische Updates in festen Zeitabständen (dieser Task legt die [Updatehäufigkeit](#) fest)
- Automatische Updates beim Herstellen von DFÜ-Verbindungen
- Automatische Updates beim Anmelden des Benutzers
- Prüfung Systemstartdateien (nach Benutzeranmeldung)
- Prüfung Systemstartdateien (nach erfolgreichem Modul-Update)

HINWEIS

Wählen Sie die entsprechenden Kontrollkästchen aus, um Tasks zu aktivieren oder zu deaktivieren.

The screenshot shows the ESET Security for Microsoft SharePoint Server interface. On the left is a sidebar with navigation options: MONITORING, LOG FILES, SCAN, UPDATE, SETUP, TOOLS, and HELP AND SUPPORT. The main window is titled 'Scheduler' and contains a table of tasks. The table has columns: Task, Name, Launch time, and Last run. The tasks listed are: Log maintenance, Update (Regular automatic update), Update (Automatic update after dial...), Update (Automatic update after use...), System startup file check (Automatic startup file check), and System startup file check (Automatic startup file check). A context menu is open over the 'Update' task, showing options: Show task details, Run now, Add..., Edit..., and Delete. At the bottom of the Scheduler window are buttons: Add task, Edit, Delete, and Default.

Task	Name	Launch time	Last run
<input checked="" type="checkbox"/> Log maintenance	Log maintenance	Task will be run every day at...	8/13/2020 9:53:26 AM
<input checked="" type="checkbox"/> Update	Regular automatic update	Task will be run repeatedly...	8/13/2020 9:53:26 AM
<input checked="" type="checkbox"/> Update	Automatic update after dial...		
<input type="checkbox"/> Update	Automatic update after use...		
<input checked="" type="checkbox"/> System startup file check	Automatic startup file check		2020 9:51:26 AM
<input checked="" type="checkbox"/> System startup file check	Automatic startup file check		2020 9:54:49 AM

Klicken Sie mit der rechten Maustaste auf einen Task, um eine der folgenden Aktionen auszuführen:

Task-Eigenschaften anzeigen	Zeigt detaillierte Informationen zum geplanten Task an, wenn Sie auf einen Task doppelklicken oder mit der rechten Maustaste klicken.
Jetzt ausführen	Führt den ausgewählten geplanten Task sofort aus.
Hinzufügen...	Startet einen Assistenten, mit dem Sie einen neuen geplanten Task erstellen können.
Bearbeiten...	Bearbeiten Sie einen vorhandenen geplanten Task (Standardtasks und benutzerdefinierte Tasks).
Löschen	Löschen Sie einen vorhandenen Task.

Taskplaner - Task hinzufügen

So erstellen Sie einen neuen geplanten Task:

1. Klicken Sie auf **Task hinzufügen**.
2. Geben Sie einen **Tasknamen** ein und konfigurieren Sie Ihren benutzerdefinierten geplanten Task.
3. [Tasktyp](#) - Wählen Sie den passenden **Tasktyp** im Dropdownmenü aus.

Task details

?

Task name

Task type

Enabled

Name

Run external application

Run external application

Log maintenance

System startup file check

Create a computer status snapshot

On-demand computer scan

First-scan

Update

Hyper-V scan

Back

Next

Cancel

HINWEIS

Klicken Sie auf den Schalter neben **Aktiviert**, um den Task zu deaktivieren. Sie können den Task später über das Kontrollkästchen in der Ansicht [Taskplaner](#) erneut aktivieren.

4. [Taskausführung](#) - Wählen Sie eine der Optionen aus, um festzulegen, wann Ihr Task ausgeführt werden soll. Je nach Ihrer Auswahl müssen Sie eine Uhrzeit, einen Tag, ein Intervall oder ein Ereignis auswählen.

Task timing
?

Schedule task to run

☒ Once
☐ Repeatedly
☐ Daily
☐ Weekly
☐ Event triggered

Skip task when running on battery power
☐ ×

Back
Next
Cancel

5. [Übersprungener Task](#) - Wenn der Task nicht zur festgelegten Zeit ausgeführt werden konnte, können Sie einen [Zeitpunkt für die nächste Ausführung](#) angeben.

Skipped task
?

A task can be skipped if the computer is powered off or running on battery.

If task was skipped the next run should occur

☒ At the next scheduled time
☐ As soon as possible
☐ Immediately, if time since last run exceeds a specified value

Time since last run (hours)

Back
Finish
Cancel

6. [Anwendung starten](#) - Wählen Sie eine ausführbare Datei in der Verzeichnisstruktur aus, falls der Task eine externe Anwendung ausführen soll.

7. Falls Sie Änderungen vornehmen möchten, klicken Sie auf **Zurück**, um zu den vorherigen Schritten zurückzukehren und die Parameter zu ändern.

8. Klicken Sie auf **Fertig stellen**, um den Task zu erstellen oder die Änderungen zu übernehmen.

Der neu erstellte Task in der Ansicht [Taskplaner](#) angezeigt.

Tasktyp

Dieser Konfigurationsassistent hängt vom jeweiligen [Typ](#) eines geplanten Tasks ab. Geben Sie den **Tasknamen** ein und wählen Sie den gewünschten **Tasktyp** im Dropdownmenü aus:

- **Externe Anwendung ausführen** - 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 der Systemstartdateien** - Prüft Dateien, die beim Systemstart oder bei 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, um die Erkennungsroutine und die Programmmodule zu aktualisieren.
- **Regelmäßiger Datenbank-Scan** - Mit dieser Option können Sie eine Datenbankprüfung planen und die zu prüfenden Elemente auswählen. Diese Funktion entspricht einer [On-Demand-Datenbankprüfung](#).
- **Hyper-V-Scan** - Plant eine Prüfung der virtuellen Datenträger in [Hyper-V](#).

Klicken Sie auf den Schalter neben **Aktiviert**, um den Task nach der Erstellung zu deaktivieren. Sie können den Task später über das Kontrollkästchen in der Ansicht [Taskplaner](#) erneut aktivieren. Klicken Sie auf **Weiter**, um mit dem [nächsten Schritt](#) fortzufahren.

Task-Zeitplanung

Wählen Sie eine der folgenden Optionen für die Zeitplanung aus:

- **Einmalig** - Der Task wird nur einmalig zum angegebenen Zeitpunkt ausgeführt. Geben Sie Datum und Uhrzeit für die Ausführung unter **Taskausführung** ein.
- **Wiederholt** - Der Task wird in den (in Minuten) angegebenen Zeitabständen ausgeführt. Geben Sie unter **Taskausführung** an, zu welcher Uhrzeit der Task jeden Tag ausgeführt werden soll.
- **Täglich** - Der Task wird jeden Tag zur festgelegten Uhrzeit ausgeführt.
- **Wöchentlich** - Der Task wird ein- oder mehrmals pro Woche an den ausgewählten Tagen und Uhrzeiten ausgeführt. Geben Sie die Startzeit unter „Uhrzeit Taskausführung“ ein. Wählen Sie den oder die Wochentage aus, an denen der Task ausgeführt werden soll.
- [Durch Ereignis ausgelöst](#) - Der Task wird ausgeführt, wenn ein bestimmtes Ereignis eintritt.

Wenn Sie die Option **Task im Akkubetrieb überspringen** aktivieren, wird der Task nicht gestartet, wenn sich der Computer zum geplanten Startzeitpunkt im Akkubetrieb befindet. Zum Beispiel für Computer, die an eine USV

(unterbrechungsfreie Stromversorgung) angeschlossen sind.

Durch Ereignis ausgelöst

Beim Planen eines Vorgangs, der durch ein Ereignis ausgelöst wird, können Sie einen Mindestzeitraum zwischen Ausführungen des Tasks angeben.

Der Task wird durch eines der folgenden Ereignisse ausgelöst:

- **Bei jedem Computerstart**
- **Jeden Tag beim ersten Start des Computers**
- **Wählverbindung zum Internet/VPN**
- **Erfolgreiches Modulupdate**
- **Erfolgreiches Produktupdate**
- **Benutzeranmeldung** - Der Task wird bereitgestellt, wenn sich der Benutzer beim System anmeldet. Wenn Sie sich mehrmals täglich bei Ihrem Computer anmelden, können Sie „24 Stunden“ auswählen, um den Task nur bei der ersten Anmeldung des Tages und dann erst wieder am nächsten Tag auszuführen.
- **Erkennung von Bedrohungen**

Anwendung starten

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 **Durchsuchen (...)** oder geben Sie den Pfad manuell 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).

Übersprungener Task

Wenn der Vorgang nicht zur festgelegten Zeit ausgeführt werden konnte, können Sie einen Zeitpunkt für die Ausführung angeben:

- **Zur nächsten geplanten Ausführungszeit** - Der Task wird zum festgelegten Zeitpunkt (z. B. nach 24 Stunden) ausgeführt.
- **Baldmöglichst** - Der Task wird baldmöglichst ausgeführt, d. h. wenn die Aktionen, die seine Ausführung ursprünglich verhindert haben, nicht mehr wirksam sind.
- **Sofort ausführen, wenn Intervall seit letzter Ausführung überschritten - Zeit seit letzter Ausführung (Stunden)** - Wenn Sie diese Option aktivieren, wird der Task immer wieder nach Ablauf einer festgelegten

Zeitspanne (in Stunden) ausgeführt.

Übersicht über geplante Tasks

In diesem Dialogfenster werden detaillierte Informationen zum geplanten Task angezeigt, wenn Sie in der Ansicht **Taskplaner** auf einen Task doppelklicken oder mit der rechten Maustaste auf einen geplanten Task klicken und anschließend **Taskdetails anzeigen** auswählen.

Datei zur Analyse einreichen

Über das Dialogfenster zum Probenversand können Sie Dateien bei ESET zur Analyse einreichen. Wenn Ihnen eine Datei auf Ihrem Computer oder eine Webseite verdächtig erscheint, können Sie die Datei zur Analyse an ESET senden. Wenn sich herausstellt, dass die Datei bzw. Webseite Schadcode enthält, werden entsprechende Erkennungsfunktionen in zukünftigen Updates berücksichtigt.

Um eine Datei per E-Mail einzusenden, komprimieren Sie sie mit einem Programm wie WinRAR oder WinZip, schützen Sie das Archiv mit dem Passwort *infected* und senden Sie es an samples@eset.com. Formulieren Sie eine aussagekräftige Betreffzeile, und notieren Sie möglichst viele ergänzende Informationen zu den eingesandten Dateien (z. B. von welcher Website Sie die Dateien heruntergeladen haben).

Die an ESET übermittelten Proben sollten mindestens eines der folgenden Kriterien erfüllen:

- Die Datei oder Website wird nicht als Bedrohung erkannt
- Die Datei oder Website wird als Bedrohung erkannt, obwohl sie keinen Schadcode enthält

Falls mindestens eine dieser Anforderungen nicht erfüllt ist, erhalten Sie erst eine Antwort, wenn weitere Informationen angegeben wurden.

Wählen Sie im Dropdownmenü **Grund für Einreichen der Probe** die Beschreibung aus, die am besten auf Ihre Mitteilung zutrifft:

- [Verdächtige Datei](#)
- [Verdächtige Webseite](#) (eine Webseite, die mit Schadsoftware infiziert ist)
- [Fehlalarm Datei](#) (als Infektion erkannte Datei, die jedoch nicht infiziert ist)
- [Fehlalarm Webseite](#)
- [Sonstige](#)

Site:

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. ESET kann über diese Adresse Kontakt mit Ihnen aufnehmen, wenn zusätzliche Angaben für die Dateianalyse benötigt werden. Diese Angabe ist freiwillig. Sie erhalten nur eine Antwort von ESET, falls wir weitere Informationen benötigen, da täglich mehrere Zehntausend Dateien auf unseren Servern eingehen und wir nicht jede Meldung einzeln beantworten können.

Anonym übermitteln

Verwenden Sie das Kontrollkästchen **Anonym übermitteln**, um verdächtige Dateien oder Websites ohne Angabe Ihrer E-Mail-Adresse zu übermitteln.

Verdächtige Datei

Beobachtete Anzeichen und Symptome einer Infektion durch Schadsoftware

Beschreiben Sie, wie sich die verdächtige Datei auf Ihrem Computer verhält.

Herkunft der Datei (URL oder Hersteller)

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, um die Identifizierung und Auswertung der verdächtigen Datei zu erleichtern.

HINWEIS

Der erste Parameter **Beobachtete Anzeichen und Symptome einer Malware-Infektion** muss stets ausgefüllt werden, Zusatzangaben helfen dem Virenlabor jedoch erheblich bei der Identifizierung und Probenauswertung.


Verdächtige Webseite

Wählen Sie eine der folgenden Optionen im Dropdownmenü **Was stimmt mit der Site nicht** aus:

Infiziert

Eine Webseite, die Viren oder sonstige Schadsoftware enthält, die auf verschiedenen Wegen verbreitet werden.

Phishing

Wird oft eingesetzt, um Zugriff auf vertrauliche Daten wie Kontonummern oder PIN-Codes zu erlangen. Weitere Informationen zu dieser Angriffsart finden Sie im [Glossar](#) .

Betrug

Betrügerische Webseite.

Sonstige

Verwenden Sie diese Option, wenn keine der anderen Optionen auf die Website zutrifft.

Hinweise und Zusatzangaben

Hier können Sie zusätzliche Informationen oder eine Beschreibung eingeben, um die Analyse der verdächtigen Webseite zu erleichtern.

Fehlalarm Datei

Wenn eine Datei als Infektion erkannt wird, tatsächlich aber nicht infiziert ist, bitten wir Sie, diese Datei einzusenden, damit wir unseren Viren- und Spyware-Schutz für Sie und andere Benutzer verbessern können. Fehlerkennungen können auftreten, wenn eine Datei einem Muster entspricht, das in einer Erkennungsroutine gespeichert ist.

HINWEIS

Die ersten drei Angaben sind notwendig, um legitime Anwendungen zu identifizieren und von Schadcode zu unterscheiden. Zusatzangaben helfen dem Virenlabor erheblich bei der Identifizierung einer Bedrohung und der Auswertung von Proben.

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.

Fehlalarm Webseite

Wir bitten Sie, Webseiten, die fälschlicherweise als infiziert, Betrug oder Phishing erkannt werden, einzusenden. Fehlerkennungen können auftreten, wenn eine Datei einem Muster entspricht, das in einer Erkennungsroutine gespeichert ist. Wenn Sie solche Webseiten einsenden, helfen Sie uns dabei, unseren Viren- und Spyware-Schutz für Sie und andere Benutzer zu verbessern.

Hinweise und Zusatzangaben

Hier können Sie zusätzliche Informationen oder eine Beschreibung eingeben, die die Auswertung der verdächtigen Datei erleichtern.

Sonstige

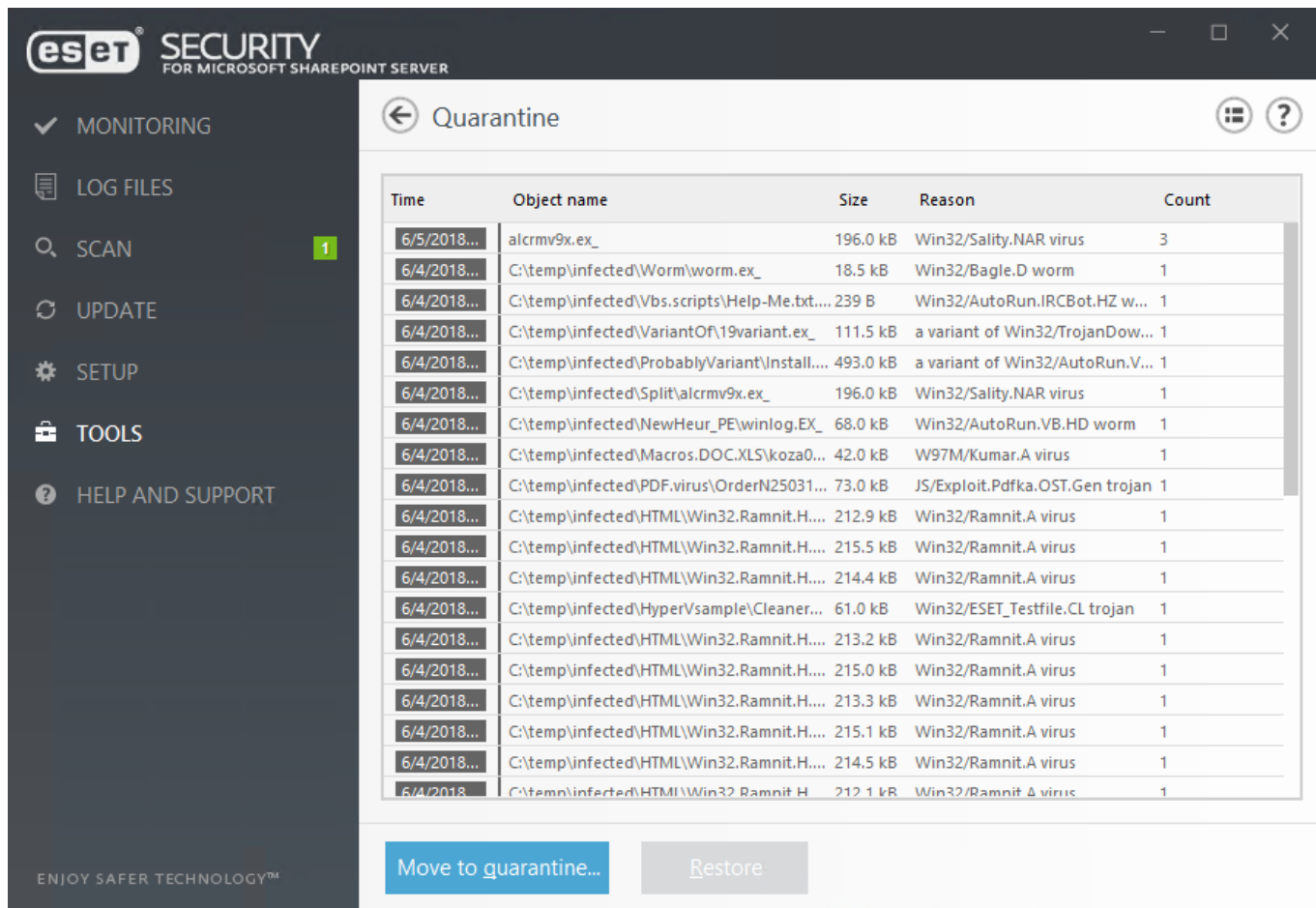
Verwenden Sie diese Auswahlmöglichkeit, wenn die Datei keine **Verdächtige Datei** und kein **Fehlalarm** ist.

Grund für Einreichen der Datei

Geben Sie eine genaue Beschreibung und den Grund für das Einreichen der Datei ein.

Quarantäne

Die Quarantäne dient hauptsächlich dazu, infizierte Dateien sicher aufzubewahren. Dateien sollten in die Quarantäne verschoben werden, wenn sie nicht gesäubert werden können, wenn es nicht sicher oder ratsam ist, sie zu löschen, oder wenn sie von ESET Security for Microsoft SharePoint fälschlicherweise erkannt wurden. Sie können beliebige Dateien gezielt in die Quarantäne verschieben. Dies macht Sinn für Dateien, die sich verdächtig verhalten, aber vom Malware-Scanner nicht erkannt werden. Dateien aus der Quarantäne können zur Analyse an ESET eingereicht werden.



Time	Object name	Size	Reason	Count
6/5/2018...	alcrmv9x.ex_	196.0 kB	Win32/Sality.NAR virus	3
6/4/2018...	C:\temp\infected\Worm\worm.ex_	18.5 kB	Win32/Bagle.D worm	1
6/4/2018...	C:\temp\infected\Vbs.scripts\Help-Me.txt....	239 B	Win32/AutoRun.IRCBot.HZ w...	1
6/4/2018...	C:\temp\infected\VariantOf\19variant.ex_	111.5 kB	a variant of Win32/TrojanDow...	1
6/4/2018...	C:\temp\infected\ProbablyVariant\Install....	493.0 kB	a variant of Win32/AutoRun.V...	1
6/4/2018...	C:\temp\infected\Split\alcrmv9x.ex_	196.0 kB	Win32/Sality.NAR virus	1
6/4/2018...	C:\temp\infected\NewHeur_PE\winlog.EX_	68.0 kB	Win32/AutoRun.VB.HD worm	1
6/4/2018...	C:\temp\infected\Macros.DOC.XLS\koza0...	42.0 kB	W97M/Kumar.A virus	1
6/4/2018...	C:\temp\infected\PDF.virus\OrderN25031...	73.0 kB	JS/Exploit.Pdfka.OST.Gen trojan	1
6/4/2018...	C:\temp\infected\HTML\Win32.Ramnit.H....	212.9 kB	Win32/Ramnit.A virus	1
6/4/2018...	C:\temp\infected\HTML\Win32.Ramnit.H....	215.5 kB	Win32/Ramnit.A virus	1
6/4/2018...	C:\temp\infected\HTML\Win32.Ramnit.H....	214.4 kB	Win32/Ramnit.A virus	1
6/4/2018...	C:\temp\infected\HyperVsample\Cleaner...	61.0 kB	Win32/ESET_Testfile.CL trojan	1
6/4/2018...	C:\temp\infected\HTML\Win32.Ramnit.H....	213.2 kB	Win32/Ramnit.A virus	1
6/4/2018...	C:\temp\infected\HTML\Win32.Ramnit.H....	215.0 kB	Win32/Ramnit.A virus	1
6/4/2018...	C:\temp\infected\HTML\Win32.Ramnit.H....	213.3 kB	Win32/Ramnit.A virus	1
6/4/2018...	C:\temp\infected\HTML\Win32.Ramnit.H....	215.1 kB	Win32/Ramnit.A virus	1
6/4/2018...	C:\temp\infected\HTML\Win32.Ramnit.H....	214.5 kB	Win32/Ramnit.A virus	1
6/4/2018...	C:\temp\infected\HTML\Win32.Ramnit.H....	212.1 kB	Win32/Ramnit.A virus	1


Die Dateien im Quarantäneordner können in einer Tabelle angezeigt werden, die Datum und Uhrzeit der Quarantäne, den Pfad zum ursprünglichen Speicherort der infizierten Datei, ihre Größe in Byte, einen Grund (z. B. Objekt hinzugefügt durch Benutzer) und die Anzahl der Bedrohungen (z. B. bei Archiven, in denen an mehreren Stellen Schadcode erkannt wurde) enthält.

Wenn E-Mail-Nachrichtenobjekte in die Dateiquarantäne verschoben werden, wird ein Pfad zum Postfach/Ordner/Dateinamen angezeigt.

Quarantäne für Dateien

ESET Security for Microsoft SharePoint verschiebt gelöschte Dateien automatisch in den Quarantäneordner (sofern diese Option nicht im Warnfenster deaktiviert wurde). Klicken Sie auf **Quarantäne**, um eine verdächtige Datei manuell in die Quarantäne zu verschieben. In die Quarantäne verschobene Dateien werden von ihrem ursprünglichen Speicherort entfernt. Alternativ können Sie das Kontextmenü verwenden: Klicken Sie mit der rechten Maustaste in das Fenster **Quarantäne**, und wählen Sie **Quarantäne** aus.

Wiederherstellen aus Quarantäne

Dateien aus der Quarantäne können auch an ihrem ursprünglichen Speicherort wiederhergestellt werden. Verwenden Sie dazu die Funktion **Wiederherstellen** aus dem Kontextmenü, das Sie per Rechtsklick auf die entsprechende Datei im Fenster „Quarantäne“ aufrufen können. Wenn eine Datei als [eventuell unerwünschte Anwendung](#)  gekennzeichnet ist, wird die Funktion **Wiederherstellen und von Prüfung ausschließen** verfügbar. Das Kontextmenü enthält außerdem die Option **Wiederherstellen nach**, mit der Dateien an einem anderen als ihrem ursprünglichen Speicherort wiederhergestellt werden können.

HINWEIS

Wenn versehentlich eine harmlose Datei in die Quarantäne versetzt wurde, [schließen Sie die Datei nach der Wiederherstellung vom Scan aus](#) und senden Sie sie an den ESET-Support.

Einreichen einer Datei aus der Quarantäne

Wenn Sie eine verdächtige, nicht vom Programm erkannte Datei in Quarantäne versetzt haben oder wenn eine Datei fälschlich als infiziert eingestuft wurde (etwa durch die heuristische Analyse des Codes) und infolgedessen in den Quarantäneordner verschoben wurde, senden Sie die Datei zur Analyse an ESET. Um eine Datei zu senden, die in der Quarantäne gespeichert ist, klicken Sie mit der rechten Maustaste auf die Datei und wählen im angezeigten Kontextmenü die Option [Datei zur Analyse einreichen](#).

Aus Quarantäne löschen

Klicken Sie mit der rechten Maustaste auf ein Element und wählen Sie **Zur Analyse einreichen** aus. Alternativ können Sie das zu löschende Element auswählen und die **Entf**-Taste auf der Tastatur drücken.


Server-Schutzeinstellungen

ESET Security for Microsoft SharePoint bietet mit den folgenden Funktionen Schutz für Ihren Microsoft SharePoint Server:

- [Echtzeitfilter](#)
- [On-Demand-Datenbankprüfung](#)
- [Regeln](#)

WICHTIG

Dieses Konto benötigt SharePoint Farm-Administratorberechtigungen, um beim Scannen auf Websitesammlungen zuzugreifen, sowie die "Als Dienst anmelden"-Berechtigung. Wenn sich SharePoint per Windows-Authentifizierung mit der Datenbank verbindet, muss dieses Konto außerdem Mitglied der SQL SysAdmin-Rolle auf dem Datenbankserver sein. Verwenden Sie nach Möglichkeit das Farm Administrator-Konto, das bei der SharePoint-Installation erstellt wurde. Wenn Sie keine gültigen Anmeldeinformationen eingeben, ist ESET Security for Microsoft SharePoint nach der Installation nicht funktionstüchtig. Wenn die Installation ohne die GUI durchgeführt wird, müssen Sie das SharePoint-Administratorkonto im Anschluss über die GUI oder per [eShell](#) eingeben. Andernfalls ist das Produkt nicht funktionstüchtig.

In mit ESET Security Management Center verwalteten Umgebungen können Sie den Client-Task [Befehl ausführen](#)  verwenden, um eShell-Befehle auszuführen. Dies ist besonders hilfreich in großen Umgebungen mit vielen SharePoint-Instanzen oder wenn Sie die Anmeldeinformationen remote angeben möchten. Geben Sie beim Erstellen eines neuen ESET Security Management Center-Client-Tasks die **auszuführende**

Befehlszeile an:

```
powershell eshell server set farm-username <domain\user> && eshell server set farm-password plain <password>
```

Der Befehl wird nur ausgeführt, wenn Sie unter [ESET-Shell-Ausführungsrichtlinie](#) die Option **Vollzugriff** festgelegt haben.

HINWEIS

Um Ihr System fortlaufend zu schützen, müssen Sie die Anmeldeinformationen für das SharePoint-Administratorkonto stets aktualisieren, wenn sich diese Informationen ändern. Wenn die hier eingegebenen Anmeldeinformationen nicht mit dem SharePoint-Administratorkonto übereinstimmen, funktioniert ESET Security for Microsoft SharePoint nicht korrekt und bietet nicht den maximalen Schutz.

Advanced setup

SERVER

- On-access filter
- On-demand database scan
- Rules

COMPUTER

UPDATE

NETWORK PROTECTION

WEB AND EMAIL

DEVICE CONTROL

TOOLS

USER INTERFACE

BASIC

SHAREPOINT FARM ADMINISTRATOR ACCOUNT

The account is used to access SharePoint configuration and files. This account must have SharePoint Farm Administrators privileges, access to web site collections to be scanned and 'Log on as service' privileges. If SharePoint is configured to connect to the database using Windows authentication, this account must also be a member of the SQL sysadmin role on the database server. It is recommended to use the Farm Administrator account created during the SharePoint install.

Username: Administrator

Password:

SHAREPOINT INTEGRATION

Direct SQL database access: ☒

PERFORMANCE COUNTERS

Default OK Cancel

Direktzugriff auf SQL-Datenbanken

Ermöglicht schreibgeschützten Zugriff auf SharePoint-Datenbanken. ESET Security for Microsoft SharePoint liest Daten direkt aus SQL Server (SharePoint-Inhaltsdatenbanken). Der direkte Datenbankzugriff bietet mehrere Vorteile gegenüber dem SharePoint-Objektmodell. Der Direktzugriff ist schneller, bietet eine bessere Gesamtleistung und verwendet weniger Systemressourcen. Dies ist hilfreich beim Scannen. Der direkte Datenbankzugriff wird für alle Lesevorgänge verwendet, während alle Schreibvorgänge (Säubern, Löschen usw.) über das SharePoint-Objektmodell ausgeführt werden. Wenn Sie den direkten SQL-Datenbankzugriff deaktivieren, wird das SharePoint-Objektmodell für Lese- und Schreibvorgänge verwendet. Beide Modi unterstützen parallele Downloads. Sie können diese Funktion konfigurieren, indem Sie die **Anzahl paralleler Downloads** unter [On-On-Demand-Datenbankprüfung](#) festlegen.

Leistungsindikatoren

Mit den ESET Security for Microsoft SharePoint-Leistungsindikatoren können Sie die Leistung von ESET Security for Microsoft SharePoint überwachen. Diese Funktion ist in Microsoft Windows Server 2008 R2 SP1 und neueren Versionen verfügbar.

Leistungsindikatoren


Mit den ESET Security for Microsoft SharePoint-Leistungsindikatoren können Sie die Leistung der Scanprozesse von ESET Security for Microsoft SharePoint überwachen. Die Indikatoren enthalten Informationen wie die Anzahl der verarbeiteten und gescannten Dateien, die Menge der von Microsoft SharePoint heruntergeladenen Daten, durchschnittliche Scandauer usw. In den folgenden Tabellen finden Sie eine Liste der verfügbaren Zähler. Die ESET Security for Microsoft SharePoint-Leistungsindikatoren sind nach ihrem Schutztyp (On-Demand oder Echtzeit) in zwei Gruppen unterteilt. Beide Gruppen enthalten dieselben Leistungsindikatoren.

Die ESET Security for Microsoft SharePoint-Leistungsindikatoren werden bei der Installation von ESET Security for Microsoft SharePoint automatisch im Betriebssystem registriert. Sobald Sie die Leistungsindikatoren aktivieren, beginnt Ihr ESET Security for Microsoft SharePoint damit, Leistungsdaten zu liefern. Wenn Sie die Leistungsindikatoren deaktivieren, bleiben die Leistungsindikatoren weiterhin im System registriert, aber ESET Security for Microsoft SharePoint liefert keine Leistungsdaten mehr. Wenn Sie ESET Security for Microsoft SharePoint deinstallieren, wird die Registrierung der Leistungsindikatoren automatisch aus dem System entfernt.

ESET Security for Microsoft SharePoint verwendet eine neue Architektur (Version 2.0) zum Bereitstellen der Leistungsindikatorendaten. Die ESET Security for Microsoft SharePoint-Leistungsindikatorendaten können direkt im Windows Server-Systemmonitor verarbeitet und angezeigt werden. Alternativ können die Daten auch in der Performance Data Helper (PDH)-Oberfläche verwendet werden.

HINWEIS

Die ESET Security for Microsoft SharePoint-Leistungsindikatoren sind für Microsoft Windows Server 2008 R2 SP1 und neuere Versionen verfügbar.

Wenn Sie die ESET Security for Microsoft SharePoint-Leistungsindikatoren aktivieren, können Sie den Systemmonitor öffnen und die gewünschten Indikatoren aus den folgenden beiden Gruppen hinzufügen: **ESET Security for Microsoft SharePoint - On-access Scan** und **ESET Security for Microsoft SharePoint - On-access Scan - On-demand Scan**. Weitere Informationen zum Systemmonitor finden Sie im Microsoft-Artikel [Übersicht zum Windows-Systemmonitor](#)  (in englischer Sprache).

Liste der verfügbaren Indikatoren:

Echtzeit-Leistungsindikatoren (Gruppenname: ESET Security for Microsoft SharePoint - On-access Scan)

Indikatorname	Beschreibung
OA - Processed Files	Gesamtzahl der verarbeiteten Dateien seit dem Start von ESET Security for Microsoft SharePoint.
OA - Processed Files/sec	Anzahl der verarbeiteten Dateien pro Sekunde.
OA - Processed Files/sec (Average)	Gleitender Durchschnitt der Anzahl der verarbeiteten Dateien.
OA - Scanned Files	Gesamtzahl der gescannten Dateien seit dem Start von ESET Security for Microsoft SharePoint.
OA - Scanned Files/sec	Anzahl der gescannten Dateien pro Sekunde.
OA - Scanned Files/sec (Average)	Gleitender Durchschnitt der Anzahl der gescannten Dateien.
OA - File Processing Time (ms) (Average)	Durchschnittliche Verarbeitungsdauer pro Datei in Millisekunden (die Summe aus Download, Regelauswertung und Scannen der Datei).
OA - File Downloading Time (ms) (Average)	Durchschnittliche Downloaddauer einer Datei aus Microsoft SharePoint in Millisekunden.

Indikatorname	Beschreibung
OA - File Scanning Time (ms) (Average)	Durchschnittliche Scandauer einer Datei auf Bedrohungen in Millisekunden.
OA - File Rule Checking Time (ms) (Average)	Durchschnittliche Dauer der Regelauswertung für eine Datei in Millisekunden.
OA - Downloaded MB	Gesamtmenge der aus Microsoft SharePoint heruntergeladenen Daten in MB seit dem Start von ESET Security for Microsoft SharePoint.
OA - Download Speed KB/sec (Average)	Durchschnittliche Downloadgeschwindigkeit von Microsoft SharePoint in KB pro Sekunde.

On-Demand-Leistungsindikatoren (Gruppenname: ESET Security for Microsoft SharePoint - On-demand Scan)

Indikatorname	Beschreibung
OD - Processed Files	Gesamtzahl der verarbeiteten Dateien seit dem Start von ESET Security for Microsoft SharePoint.
OD - Processed Files/sec	Anzahl der verarbeiteten Dateien pro Sekunde.
OD - Processed Files/sec (Average)	Gleitender Durchschnitt der Anzahl der verarbeiteten Dateien.
OD - Scanned Files	Gesamtzahl der gescannten Dateien seit dem Start von ESET Security for Microsoft SharePoint.
OD - Scanned Files/sec	Anzahl der gescannten Dateien pro Sekunde.
OD - Scanned Files/sec (Average)	Gleitender Durchschnitt der Anzahl der gescannten Dateien.
OD - File Processing Time (ms) (Average)	Durchschnittliche Verarbeitungsdauer pro Datei in Millisekunden (die Summe aus Download, Regelauswertung und Scannen der Datei).
OD - File Downloading Time (ms) (Average)	Durchschnittliche Downloaddauer einer Datei aus Microsoft SharePoint in Millisekunden.
OD - File Scanning Time (ms) (Average)	Durchschnittliche Scandauer einer Datei auf Bedrohungen in Millisekunden.
OD - File Rule Checking Time (ms) (Average)	Durchschnittliche Dauer der Regelauswertung für eine Datei in Millisekunden.
OD - Downloaded MB	Gesamtmenge der aus Microsoft SharePoint heruntergeladenen Daten in MB seit dem Start von ESET Security for Microsoft SharePoint.
OD - Download Speed KB/sec (Average)	Durchschnittliche Downloadgeschwindigkeit von Microsoft SharePoint in KB pro Sekunde.

Echtzeitfilter

In diesem Fenster können Sie die Parameter für den Echtzeitfilter anpassen. Hier können Sie den Echtzeitfilter aktivieren (Standard) oder deaktivieren. Wenn Sie den Echtzeitfilter deaktivieren, werden die folgenden Optionen deaktiviert.

Wenn Sie den Echtzeitfilter deaktivieren, prüft ESET Security for Microsoft SharePoint keine Dokumente beim Hoch- oder Herunterladen, es werden keine Echtzeitfilter-Regeln angewendet, und eine Warnmeldung wird unter [Überwachung](#) angezeigt.

HINWEIS

Der **Echtzeitfilter** sollte stets aktiviert sein, um maximalen Schutz zu gewährleisten.

SharePoint-Schutzeinstellungen (Diese Einstellungen können auch in der SharePoint-Zentraladministration

verwaltet werden):

Link zur SharePoint-Zentraladministration

Klicken Sie auf die URL, um die Virenschutzeinstellungen in der SharePoint-Zentraladministration zu öffnen. Wenn Sie die Einstellungen in der SharePoint-Zentraladministration ändern, kann es einige Zeit dauern, bis die Änderungen in ESET Security for Microsoft SharePoint übernommen werden.

Dokumente beim Hochladen scannen

Die in SharePoint hochgeladenen Dokumente werden über die Web-Schnittstelle geprüft, wenn sie in MS Office-Programmen gespeichert werden und bei der Synchronisierung mit dem SharePoint-Arbeitsbereich.

Dokumente beim Herunterladen scannen

Die über die Web-Schnittstelle aus SharePoint heruntergeladenen Dateien werden beim Download geprüft, inklusive Bilder und Dokumente, die bei der Synchronisierung mit dem SharePoint-Arbeitsbereich in MS Office-Programmen geöffnet werden.

Zulassen, dass Benutzer infizierte Dokumente herunterladen

Wenn diese Option aktiviert ist, zeigt SharePoint eine Warnung für infizierte Dateien an, aber die infizierten Dateien können weiterhin geöffnet werden und werden blockiert anstatt gelöscht. Wenn diese Option deaktiviert ist, wird eine Nachricht mit der Meldung angezeigt, dass das Dokument infiziert ist und der Download nicht möglich ist. Der SharePoint-Administrator kann infizierte Dateien jederzeit unabhängig von dieser Einstellung herunterladen.

Versuchen, infizierte Dokumente zu säubern

Wenn diese Option aktiviert ist, werden infizierte Dokumente gesäubert, falls möglich.

Dauer für Zeitüberschreitung (in Sekunden)

Die maximale Zeitdauer, die SharePoint auf eine Antwort von ESET Security for Microsoft SharePoint wartet. Wenn keine Antwort eingeht, wird ein AV-Scanfehler gemeldet. Das Standardintervall beträgt 300 Sekunden.

Anzahl der Scanthreads

Anzahl der Instanzen pro w3wp-Prozess. SharePoint verwendet normalerweise drei w3wp-Prozesse. Insgesamt stehen 15 (3x5) Prüfobjekte zur Verfügung. Diese Anzahl begrenzt die maximale Anzahl gleichzeitig herunter- bzw. hochgeladener Dateien. Diese Anzahl hängt nicht mit der Anzahl der ThreatSense-Scanmodule zusammen.

Viren- und Spyware-Schutz

Auszuführende Aktion, falls keine Säuberung möglich ist

Mit diesem Aktionsfeld können Sie eine auszuführende Aktion auswählen, falls eine infizierte Datei gefunden wird und nicht gesäubert werden kann:

- **Keine Aktion** – Es werden keine Änderungen vorgenommen. Hochgeladene und infizierte Dateien werden in SharePoint gespeichert, und die Benutzer haben Zugriff auf diese Dateien.

- **Blockieren** – Die infizierte Datei wird blockiert und kann nicht hoch- oder heruntergeladen werden. Ggf. wird außerdem eine Nachricht für den Benutzer mit einer Begründung angezeigt, warum der Upload/Download nicht ausgeführt wurde.
- **Zum Löschen vormerken** – Die Datei wird für die Löschung markiert, und SharePoint entscheidet selbst über die Löschung. Während eines Benutzerzugriffs (beim Download) kann die Datei normalerweise nicht gelöscht werden, da die Benutzer keine Schreib- bzw. Löschberechtigung haben. Diese Option ist nicht verfügbar, wenn die Säuberungsstufe im ThreatSense-Modul auf „Nicht säubern“ festgelegt ist. Wenn der herunterladende Benutzer jedoch über die entsprechende Berechtigung verfügt, wird die Datei gelöscht. Der für den Benutzer angezeigte Nachrichtentyp wird von SharePoint verwaltet. In SharePoint 2010, 2013 und 2016 wird eine korrekte Nachricht angezeigt. In SharePoint 2007 wird eine Löschung der Datei gemeldet, selbst wenn der Benutzer nicht über die entsprechende Berechtigung verfügt und die Datei nicht gelöscht wurde.

HINWEIS

Wenn ein Dokument gelöscht wird, werden dessen ältere Versionen ebenfalls gelöscht. Daher sollten Sie die Aktion Block verwenden. Verwenden Sie stattdessen die On-Demand-Datenbankprüfung, um infizierte Dokumente aus SharePoint zu löschen.

Infizierte Dateien in Quarantäne verschieben

Mit dieser Option werden die zur Löschung markierten Dateien in die Quarantäne verschoben. Deaktivieren Sie diese Option und damit die Quarantäne, um zu verhindern, dass sich Dateien in der Quarantäne ansammeln. Dies macht z. B. Sinn, wenn die Partition, auf der sich die Quarantäne befindet, zu klein oder fast voll ist. Die Quarantäne sollte nicht deaktiviert werden. Diese Option wirkt sich auf die Quarantäne-Richtlinie für säubere und nicht säubere Dateien aus. Die Nutzung der Quarantäne wirkt sich nicht auf die Regeln aus.

Vorlage einer Meldung, die bei erkannter Bedrohung angezeigt wird

Sie können die Nachricht anpassen, die im Browser der Benutzer angezeigt wird, wenn eine Bedrohung erkannt und gesäubert, blockiert oder gelöscht wurde. Geben Sie den gewünschten Text in das Feld „Vorlage einer Meldung, die bei erkannter Bedrohung angezeigt wird“ ein. Die Nachricht wird nur in der Web-Schnittstelle angezeigt. Die Standardnachricht unterscheidet sich zwischen SharePoint 2007 bzw. SharePoint 2010, 2013 und 2016. Sie können die folgenden Variablen in der Nachricht verwenden:

%VIRUSNAME% - Name der Infiltration aus dem Prüfmodul.

%FILENAME% - Dateiname.

%FILESIZE% - Dateigröße.

%PRODUCTNAME% - Produktname, in diesem Fall: ESET Security for Microsoft SharePoint.

ThreatSense-Parameter

In diesem Bereich können Sie die Scaneinstellungen für den Echtzeitfilter anpassen.

Zugriffsfilter- und Machine-Learning-Schutz

Die Berichterstellung wird von der Erkennungsroutine und der Machine-Learning-Komponente ausgeführt.

On-Demand-Datenbankprüfung

Pro ausgewählte Website wird deren gesamte Ordner- und Dateihierarchie geprüft. Alle Dateien, Benutzerdokumente und andere interne SharePoint-Dateien werden in temporären Dateien gespeichert, die anschließend zur Prüfung an den Kernel übermittelt werden. Wenn ältere Versionen einer Datei vorhanden sind und die Funktion **Dokumentversionen prüfen** aktiviert ist, werden die älteren Versionen des Dokuments zuerst überprüft.

Im schreibgeschützten Modus scannen

Infizierte Dokumente werden nicht gesäubert oder gelöscht. Die Aktion der Löschregel wird nicht angewendet.

Dokumentversionen scannen

Wenn andere Versionen desselben Dokuments in der SharePoint-Datenbank existieren, werden diese ebenfalls gescannt.

Beim Löschen des Dokuments die letzte saubere Version wiederherstellen

Wenn ein infiziertes Dokument gelöscht wird, werden ältere, nicht infizierte Versionen gescannt. Falls eine ältere, nicht infizierte Version existiert, wird die aktuellste nicht infizierte Version wiederhergestellt und als aktuelle Version deklariert. Wenn die Option „Im schreibgeschützten Modus scannen“ aktiviert ist, steht diese Option nicht zur Verfügung.

Scanziele

Ein Fenster wird geöffnet, in dem Sie entweder alle Ziele überprüfen oder bestimmte Ziele auswählen können. Weitere Informationen finden Sie unter [Scanziele für die On-Demand-Datenbankprüfung](#).

Anzahl paralleler Downloads

Dieser Parameter ermöglicht die parallele Überprüfung durch mehrere Threads. Wenn dieser Wert auf 0 festgelegt ist, wird die ältere sequenzielle Prüfmethode verwendet.

Prüfziele für die On-Demand-Datenbankprüfung

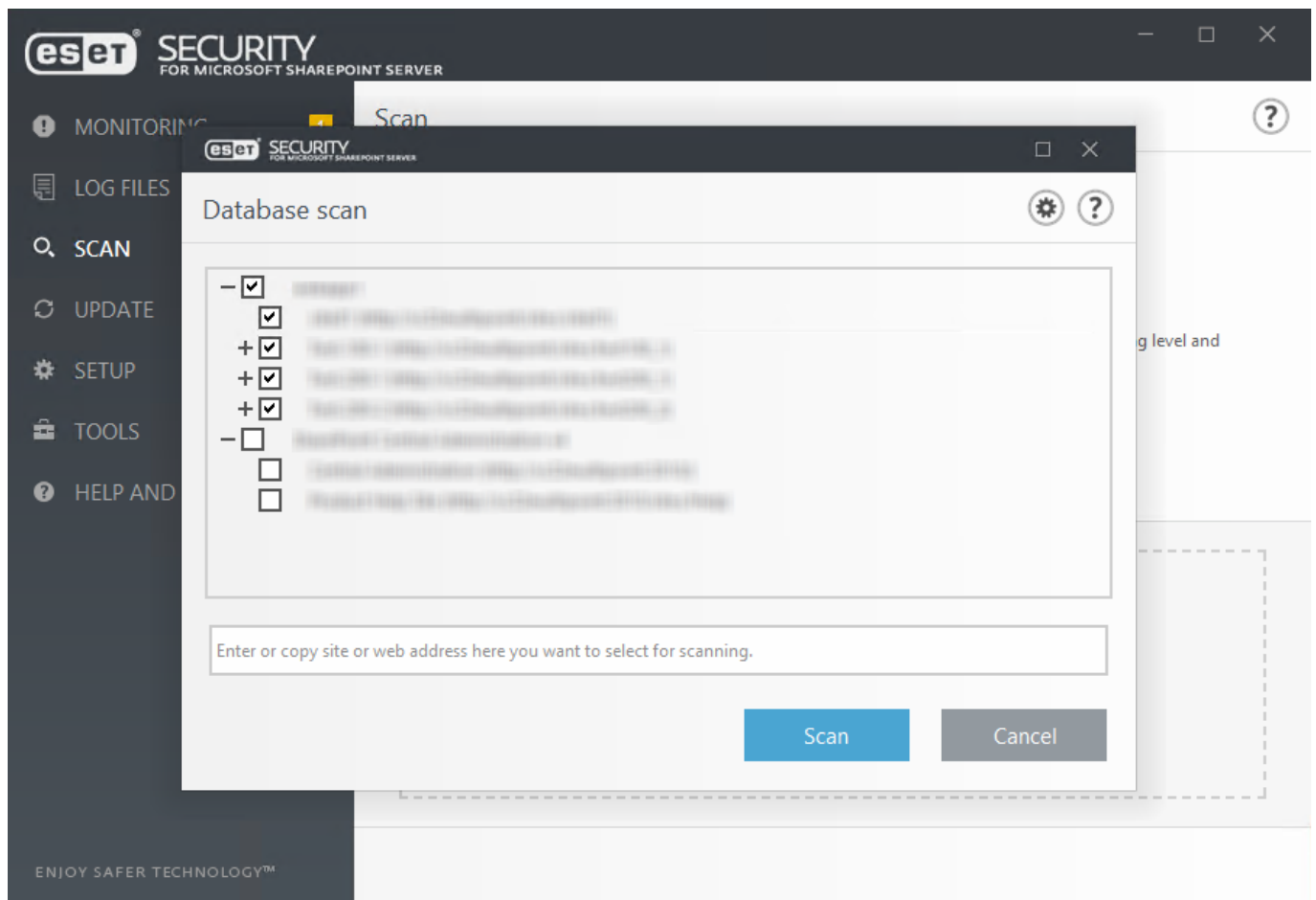
In diesem Dialogfenster können Sie auswählen, welche SharePoint-Websites gescannt werden sollen und können den Scanvorgang starten. Eine Liste der vorhandenen Websites wird angezeigt. Im Dropdownmenü **Scanziele** können Sie entweder **Alle Ziele** oder **Benutzerdefinierte Ziele** auswählen.

Bei der manuellen Zielauswahl markieren Sie das Kontrollkästchen neben einer Website, um diese zum Scan hinzuzufügen.

Um eine Website hinzuzufügen, kopieren Sie deren URL und fügen Sie die URL in das Dialogfenster ein. Je nach Anzahl und Komplexität der Sites in der Liste kann es einige Zeit dauern, bis die Liste ausgefüllt wird. Nach Änderungen an den Sites können Sie **F5** drücken, um die Liste zu aktualisieren. Wenn die Liste angezeigt wird, können Sie die zu prüfenden Websites über die entsprechenden Kontrollkästchen auswählen.

In der unten gezeigten Hierarchie befindet sich eine SharePoint-Webanwendung an der Spitze, die eine oder mehrere SharePoint-Websitesammlungen enthält, die wiederum selbst SharePoint-Websites enthalten. Die

Websites sind hierarchisch angeordnet, und an der Spitze befindet sich immer genau eine Website.



- **Im schreibgeschützten Modus prüfen** - Infizierte Dokumente werden nicht gesäubert oder gelöscht. Die Aktion der Löschregel wird nicht angewendet.
- **Dokumentversionen prüfen** - Wenn andere Versionen desselben Dokuments in der SharePoint-Datenbank existieren, werden diese ebenfalls geprüft.
- **Beim Löschen des Dokuments die letzte saubere Version wiederherstellen** - Wenn ein infiziertes Dokument gelöscht wird, werden ältere, nicht infizierte Versionen gescannt. Falls eine ältere, nicht infizierte Version existiert, wird die aktuellste nicht infizierte Version wiederhergestellt und als aktuelle Version deklariert. Wenn die Option „Im schreibgeschützten Modus scannen“ aktiviert ist, steht diese Option nicht zur Verfügung.

Legen Sie die gewünschten zu scannenden Objekte und Parameter fest und klicken Sie auf **Scannen**, um das Scannen zu starten.

Die Website-Hierarchie wird bei der ersten Anzeige von SharePoint abgerufen und für den schnelleren Zugriff im ESET SharePoint-Helferdienst zwischengespeichert. Die Website-Hierarchie wird nach einer gewissen Zeit automatisch aktualisiert. Sie können jedoch jederzeit **F5** drücken, um die Liste manuell zu aktualisieren.

Viren- und Spyware-Schutz

Auszuführende Aktion, falls keine Säuberung möglich ist

Wählen Sie eine auszuführende Aktion aus, falls eine infizierte Datei gefunden wird und nicht gesäubert werden kann (Löschen gilt nicht als Säuberung):

- **Keine Aktion** – Es werden keine Änderungen vorgenommen, die Dateien werden hoch- bzw. heruntergeladen.
- **Löschen** – Die Datei wird aus der Datenbank gelöscht. Wenn beim Löschen ein Fehler auftritt, wird der Fehler in das Datenbank-Prüf-Log geschrieben. Diese Option ist nicht verfügbar, wenn die Säuberungsstufe im ThreatSense-Modul auf „Nicht säubern“ festgelegt ist.

Infizierte Dateien in Quarantäne verschieben

Mit dieser Option werden die zur Löschung markierten Dateien in die Quarantäne verschoben. Mit dieser Option können Sie die Quarantäne deaktivieren, um zu verhindern, dass sich Dateien in der Quarantäne ansammeln. Dies macht z. B. Sinn, wenn die Partition, auf der sich die Quarantäne befindet, zu klein oder fast voll ist. Die Quarantäne sollte normalerweise nicht deaktiviert werden. Diese Option wirkt sich auf die Quarantäne-Richtlinie für säuberbare und nicht säuberbare Dateien aus. Die Nutzung der Quarantäne wirkt sich nicht auf die Regeln aus.

[ThreatSense-Parameter](#)

Hier können Sie die Scaneinstellungen für die On-Demand-Datenbankprüfung ändern.

[On-Demand-Datenbank-Scan & Machine-Learning-Schutz](#)

Die Berichterstellung wird von der Erkennungsroutine und der Machine-Learning-Komponente ausgeführt.

Regeln

Mit Regeln können Sie manuell Filterbedingungen für Dateien definieren und Aktionen mit gefilterten Dateien verknüpfen. Eine Regel besteht aus einer Kombination von Bedingungen. In den Regeln für den Echtzeitfilter und für die On-Demand-Datenbankprüfung können unterschiedliche Bedingungen und Aktionen festgelegt werden. Es gibt zwei grundsätzliche Arten von Regeln:

- [Echtzeitfilter](#)
- [On-Demand-Datenbankprüfung](#)

Klicken Sie auf **Bearbeiten**, um die Regelliste zu öffnen. Klicken Sie auf **Hinzufügen** und folgen Sie dem [Regelassistenten](#), um eine neue Regel zu erstellen.

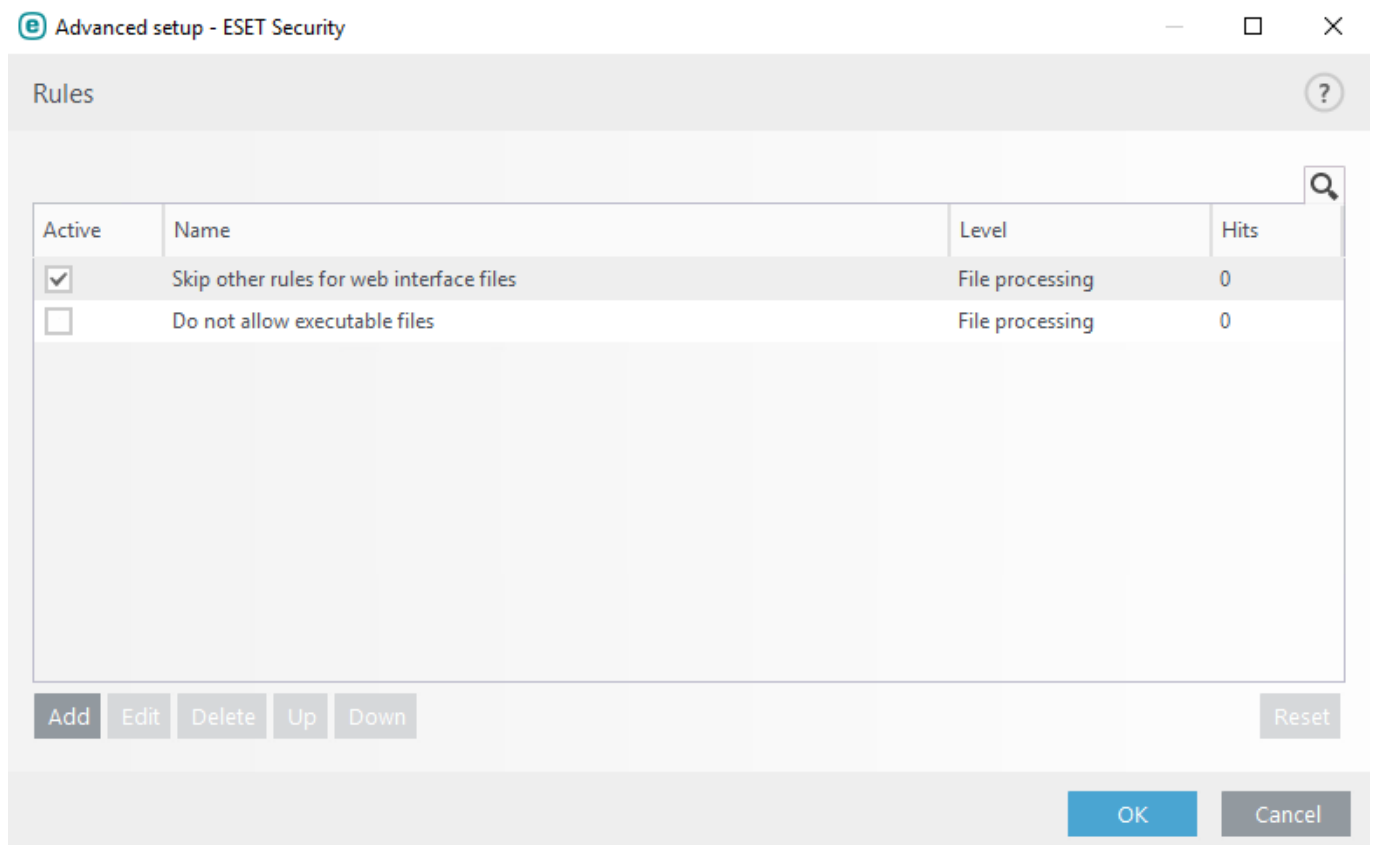
Regelliste

Regeln sind in drei Stufen unterteilt und werden in der folgenden Reihenfolge ausgewertet:

- **Filterregeln (1)** - Diese Regeln werden vor dem Virenschutz-Scan ausgewertet
- **Regeln für Anhänge (2)** – Diese Regeln werden beim Virenschutz-Scan ausgewertet
- **Regeln für Ergebnisse (3)** – Diese Regeln werden nach dem Virenschutz-Scan ausgewertet

Regeln derselben Ebene werden in der Reihenfolge ausgewertet, in der sie in der Regelliste angezeigt werden. Sie können die Reihenfolge nur für Regeln innerhalb derselben Ebene ändern. Wenn Sie mehrere Filterregeln haben, können Sie deren Reihenfolge festlegen. Sie können dagegen keine **Regeln für Dateien** vor die **Filterregeln** verschieben, da die Schaltflächen **Nach oben/Nach unten** nicht verfügbar sind. Sie können also keine Regeln aus unterschiedlichen **Ebenen** mischen.

Die Spalte **Treffer** zeigt an, wie oft die Regel erfolgreich ausgeführt wurde. Wenn Sie das Kontrollkästchen links neben dem Namen einer Regel deaktivieren, wird die entsprechende Regel deaktiviert, bis Sie das Kontrollkästchen erneut aktivieren.



Klicken Sie auf **Zurücksetzen**, um den Zähler für die ausgewählte Regel zurückzusetzen (Spalte **Treffer**). Unter **Ansicht** können Sie eine Konfiguration anzeigen, die über eine ESET Security Management Center-Policy angewendet wurde.

WICHTIG

Wenn die Bedingungen einer Regel erfüllt sind, endet normalerweise die Auswertung von Regeln mit niedrigerer Priorität. Bei Bedarf können Sie jedoch eine spezielle [Regelaktion](#) mit dem Namen **Andere Regeln bewerten** verwenden, um die Auswertung fortzusetzen.

- **Hinzufügen** – Neue Regel hinzufügen
- **Bearbeiten** – Bestehende Regel bearbeiten
- **Ansicht** – Konfiguration anzeigen, die über eine ESMC-Policy angewendet wurde
- **Entfernen** – Ausgewählte Regel entfernen
- **Nach oben** – Ausgewählte Regel in der Liste nach oben
- **Nach unten** – Ausgewählte Regel in der Liste nach unten
- **Zurücksetzen** – Zähler für die ausgewählte Regel zurücksetzen (Spalte "Treffer")

HINWEIS

Wenn eine neue Regel hinzugefügt oder eine bestehende Regel bearbeitet wird, beginnt automatisch eine erneute E-Mail-Prüfung nach den neuen/geänderten Regeln.

Regelassistent

Sie können Bedingungen und Aktionen im Regelassistenten definieren. Definieren Sie zunächst Bedingungen, und anschließend Aktionen. Manche Bedingungen und Aktionen haben unterschiedliche Funktionsweisen für den Echtzeitfilter und den On-Demand-Datenbanksan. Dies liegt daran, dass diese Schutztypen E-Mails auf unterschiedliche Arten verarbeiten.

1. Klicken Sie auf **Hinzufügen**, um ein Fenster für [Regelbedingungen](#) zu öffnen, in dem Sie Bedingungstyp, Vorgang und Wert festlegen können.

WICHTIG

Sie können mehrere Bedingungen festlegen. In diesem Fall müssen wird die Regel nur angewendet, wenn alle Bedingungen erfüllt sind. Alle Bedingungen werden mit dem logischen Operator **UND** verknüpft. Selbst wenn die meisten Bedingungen erfüllt sind und nur eine Bedingung nicht erfüllt ist, gilt das Auswertungsergebnis als *nicht erfüllt*, und die Aktion für die Regel wird nicht ausgeführt.

2. Klicken Sie auf **Hinzufügen** (am unteren Rand), um eine [Regelaktion](#) hinzuzufügen.

HINWEIS

Sie können mehrere Aktionen für eine Regel anlegen.

3. Definieren Sie Bedingungen und Regeln, und geben Sie anschließend einen **Namen** ein, mit dem Sie die Regel wiedererkennen. Dieser Name wird anschließend in der [Regelliste](#) angezeigt. Der **Name** ist ein Pflichtfeld. Falls dieses Feld rot hervorgehoben ist, geben Sie einen Regelnamen in das Textfeld ein und klicken Sie auf **OK**, um die Regel zu erstellen. Die rote Hervorhebung verschwindet nicht, nachdem Sie den Regelnamen eingegeben haben, sondern erst, wenn Sie auf **OK** klicken.

Rule

?

Active

☒

Name

⚠

Condition type	Operation	Parameters
File size	is greater than	4MB

Add

Edit

Delete

⬆

⬆

⬆

⬆

Action type	Parameters
Log to events	Rule "%RuleName%" applied.

Add

Edit

Delete

OK

Cancel

4. Wenn Sie eine Regel für die spätere Verwendung vorbereiten möchten, können Sie den Schieberegler neben **Aktiv** anklicken, um die Regel zu deaktivieren. Um eine Regel zu aktivieren, markieren Sie das Kontrollkästchen neben der entsprechenden Regeln in der [Regelliste](#).

HINWEIS

Wenn eine neue Regel hinzugefügt oder eine bestehende Regel bearbeitet wird, beginnt automatisch eine erneute E-Mail-Prüfung nach den neuen/geänderten Regeln.

Regelbedingung

Mit diesem Assistenten können Sie Bedingungen für eine Regel anlegen. Wählen Sie einen **Typ** für die Bedingung und eine **Operation** aus der Dropdownliste aus. Die Liste der Operationen hängt vom ausgewählte Regeltyp ab. Wählen Sie anschließend einen **Parameter** aus. Die Parameterfelder hängen vom ausgewählten Regeltyp und von der Operation ab. Wählen Sie zum Beispiel **Dateigröße > ist größer als** aus und geben Sie im Feld **Parameter** den Wert 10 MB ein. Mit dieser Einstellung werden alle Dateien größer als 10 MB mit den [Regelaktionen](#) verarbeitet, die Sie ausgewählt haben. Wählen Sie daher die gewünschte Aktion beim Auslösen dieser Regel aus, falls Sie dies beim Einstellen der Parameter für die Regel noch nicht getan haben.

Alternativ können Sie **reguläre Ausdrücke verwenden**, indem Sie **Operation: Treffer für regulären Ausdruck** oder **kein Treffer für regulären Ausdruck** auswählen. ESET Security for Microsoft SharePoint verwendet std::regex. Weitere Informationen zu regulären Ausdrücken finden Sie unter [ECMAScript Syntax](#).

WICHTIG

Sie können mehrere Bedingungen festlegen. In diesem Fall müssen wird die Regel nur angewendet, wenn alle Bedingungen erfüllt sind. Alle Bedingungen werden mit dem logischen Operator **UND** verknüpft. Selbst wenn die meisten Bedingungen erfüllt sind und nur eine Bedingung nicht erfüllt ist, gilt das Auswertungsergebnis als *nicht erfüllt*, und die Aktion für die Regel wird nicht ausgeführt.

Die folgenden Bedingungstypen sind für den Echtzeitfilter oder für den On-Demand-Datenbanksan verfügbar (je nach ausgewählten Bedingungen werden möglicherweise nicht alle Optionen angezeigt):

Bedingungsname	Echtzeitfilter	On-Demand-Datenbankprüfung	Beschreibung
Dateiname	<input type="checkbox"/>	<input type="checkbox"/>	Gilt für Dateien mit einem bestimmten Namen. Mit dieser Bedingung können Sie eine Maske für den gewünschten Dateinamen angeben, inklusive der Platzhalter *? usw. Diese Bedingung gilt nur für den Dateinamen, unabhängig vom Dateipfad.
Dateigröße	<input type="checkbox"/>	<input type="checkbox"/>	Gilt für Dateien, die die angegebene Größe überschreiten. Mit dieser Bedingung können Sie eine maximale Dateigröße angeben. Wenn eine Datei diese Größe überschreitet, wird die Regel angewendet.
Datei-URL	<input type="checkbox"/>	<input type="checkbox"/>	Gilt für Dateien, die sich unter einer bestimmten URL befinden. Mit dieser Bedingung können Sie eine URL und eine Maske für den gewünschten Dateinamen angeben, inklusive der Platzhalter *? usw.
Dateityp	<input type="checkbox"/>	<input type="checkbox"/>	Gilt für Dateien eines bestimmten Typs (der tatsächliche Dateityp wird unabhängig von Inhalt, Dateiname oder Dateierweiterung ermittelt). Mit dieser Bedingung können Sie einen oder mehrere Dateitypen für die Regel auswählen. Eine vollständige Liste der erkannten Dateitypen finden Sie in unserem Knowledgebase-Artikel .
Änderungsuhrzeit	<input type="checkbox"/>	<input type="checkbox"/>	Gilt für Dateien, die vor oder nach einem bestimmten Zeitpunkt zuletzt geändert wurden. Alternativ können Sie ein Zeitintervall angeben, um Dateien auszuwählen, die innerhalb dieses Intervalls zuletzt geändert wurden.
Scan-Ergebnis des Virenschutzes	<input type="checkbox"/>	<input type="checkbox"/>	Gilt für Dateien, die anhand einer Virenschutzprüfung als schädlich bzw. als unschädlich erkannt wurden.
Enthält passwortgeschütztes Archiv	<input type="checkbox"/>	<input type="checkbox"/>	Gilt für Archivdateien, die mit einem Passwort geschützt sind.
Enthält beschädigtes Archiv	<input type="checkbox"/>	<input type="checkbox"/>	Gilt für beschädigte Archivdateien, die vermutlich nicht geöffnet werden können.

Bedingungsname	Echtzeitfilter	On-Demand-Datenbankprüfung	Beschreibung
Geändert durch Benutzer	?	?	Gilt für Dateien, die zuletzt von einem bestimmten Benutzer geändert wurden.

HINWEIS

Die Anzahl der **Regeltreffer** im [Scan-Log](#) kann die **Anzahl der gescannten Objekte** überschreiten, wenn die Regel eine Bedingung für den **Dateityp** enthält. Dies kann beispielsweise der Fall sein, wenn die gescannten Objekte Archive oder Containerdateien sind, die andere Dateien (zum Beispiel *.docx*) enthalten. In diesem Fall wird jede enthaltene Datei in Bezug auf die Regel mit der Bedingung für den **Dateityp** geprüft, was dazu führen kann, dass die Anzahl der **Regeltreffer** die **Anzahl der gescannten Objekte** überschreitet.

Regelaktionen

In diesem Fenster können Sie Aktionen hinzufügen, die ausgeführt werden sollen, wenn eine Datei die in einer Regel definierten Bedingungen erfüllt.

HINWEIS

Sie können mehrere Aktionen für eine Regel anlegen.

Die folgenden Aktionen sind für den Echtzeitfilter oder für die On-Demand-Datenbankprüfung verfügbar (je nach ausgewählten Aktionen werden möglicherweise nicht alle Optionen angezeigt):

Aktionsname	Echtzeitfilter	On-Demand-Datenbankprüfung	Beschreibung
Datei in Quarantäne verschieben	?	?	Verschiebt die Datei in die Quarantäne, auch wenn die Virenschutz-Quarantäne deaktiviert ist.
Löschen	?	?	Datei wird aus der Datenbank gelöscht.
Zum Löschen vormerken	?	?	Datei wird bei einem Upload-Versuch nicht hochgeladen, wird bei der Indexierung gelöscht und bei einem Download-Versuch für die Löschung markiert.
Sperren	?	?	Uploads und Downloads der Datei werden blockiert.
Ereignisbenachrichtigung senden	?	?	Sendet eine Ereignisbenachrichtigung an den Administrator. Dazu müssen Sie die Option Ereignismeldungen per E-Mail versenden aktivieren und das Format der Ereignismeldungen definieren (In der QuickInfo werden Vorschläge angezeigt).

Aktionsname	Echtzeitfilter	On-Demand-Datenbankprüfung	Beschreibung
Andere Regeln bewerten			Lässt die Bewertung anderer Regeln zu und gibt dem Administrator die Möglichkeit, mehrere Bedingungssätze und mehrere bei Erfüllen bestimmter Bedingungen auszuführende Aktionen zu definieren. Wenn dies deaktiviert ist, werden keine Regeln bewertet, aber der Virenschutz-Scan wird dennoch ausgeführt.
Logging in Ereignissen			Angaben zur angewendeten Regel werden in das Ereignis-Log geschrieben. Sie können den Schweregrad und das Format der Ereignisnachrichten auswählen (In der QuickInfo werden Vorschläge angezeigt).
Scan des Virenschutzes überspringen			Die Datei wird nicht vom Antivirenprogramm geprüft.
Keine weiteren Regeln auswerten			Wenn diese Option als Aktion ausgewählt ist, werden alle weiteren Regeln übersprungen, die normalerweise folgen würden.

Allgemeine Einstellungen

In diesem Fenster können Sie persönliche Einstellungen vornehmen und Funktionen konfigurieren. Das Menü auf der linken Seite enthält die folgenden Kategorien:

[Computer](#)

Aktivieren bzw. deaktivieren Sie die Erkennung potenziell unerwünschter, unsicherer, und verdächtiger Anwendungen sowie die Anti-Stealth-Technologie. Legen Sie Ausschlüsse für Prozesse, Dateien oder Ordner fest. Konfigurieren Sie den Echtzeit-Dateischutz, ThreatSense-Parameter, den cloudbasierten Schutz (ESET LiveGrid®), Schadsoftwarescans (On-Demand-Computerscan und andere Scanoptionen), den Hyper-V-Scan und HIPS.

[Update](#)

Konfigurieren Sie Updateoptionen wie Profile, Alter der Erkennungsroutine, Momentaufnahmen für Modul-Rollbacks, Updatetyp, benutzerdefinierte Updateserver, Verbindungs- und Proxyserver, Updatemirror, Zugriff auf Update-Dateien, HTTP-Server, Details der Benutzerkonten für Netzwerkverbindungen usw.

[Web und E-Mail](#)

Konfigurieren Sie Protokollfilter und Ausschlüsse (ausgeschlossene Anwendungen und IP-Adressen), Optionen für die SSL/TLS-Protokollfilterung, E-Mail-Client-Schutz (Integration, E-Mail-Protokolle, Warnungen und Benachrichtigungen), Web-Schutz (HTTP/HTTPS-Webprotokolle und URL-Adressverwaltung) und den Phishing-Schutz für E-Mail-Clients.

[Medienkontrolle](#)

Aktivieren Sie die Integration und konfigurieren Sie Regeln und Gruppen für die Medienkontrolle.

[Tools](#)

Konfigurieren Sie Tools wie ESET CMD, ESET RMM, WMI-Anbieter, ESET Security Management Center-Scanziele, Windows Update-Benachrichtigungen, Logdateien, Proxyserver, E-Mail-Benachrichtigungen, Diagnose, Cluster usw.


[Benutzeroberfläche](#)

Konfigurieren Sie das Verhalten der grafischen Benutzeroberfläche des Programms, Statusmeldungen, Lizenzinformationen, Warnungen und Benachrichtigungen, Passwortschutz, eShell-Ausführungsrichtlinie usw.


Computer

Die Erkennungsroutine schützt Sie vor bösartigen Systemangriffen, indem Dateien, E-Mails und die Netzwerkkommunikation gescannt werden. Wenn ein als Malware eingestuftes Objekt erkannt wird, beginnt die Behebung. Die Erkennungsroutine kann das Ereignis zunächst blockieren und anschließend säubern, löschen oder in die Quarantäne verschieben.


Echtzeit- & Machine-Learning-Schutz

Advanced Machine Learning ist jetzt als zusätzliche Schutzebene in der Erkennungsroutine enthalten, um die Erkennung auf Basis von Machine Learning zu verbessern. Weitere Informationen zu diesem Schutztyp finden Sie in unserem [Glossar](#) . Sie können Berichterstellung 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 genauerer Begriff. Die Malware-Erkennung wird von der Erkennungsroutine zusammen mit der Machine-Learning-Komponente ausgeführt. Weitere Informationen zu diesen Anwendungstypen finden Sie im [Glossar](#) .

Eventuell unerwünschte Anwendungen

Eine eventuell unerwünschte Anwendung ist ein Programm, das nicht zwangsläufig nur böse Absichten verfolgt, jedoch zusätzliche unerwünschte Software installieren, das Verhalten des digitalen Geräts manipulieren, unerwünschte oder unerwartete Aktionen ausführen kann oder sonstige unklare Ziele verfolgt. Zu dieser Kategorie gehören: Software für Werbeeinblendungen, Download-Wrapper, verschiedene Browser-Werkzengleisten, Software mit irreführenden Verhaltensweisen, Bundleware, Trackware usw. Weitere Informationen zu diesem Anwendungstyp finden Sie im [Glossar](#) .

Verdächtige Anwendungen

Diese Kategorie umfasst Programme, die mit [Pack](#) - oder Schutzprogrammen komprimiert wurden. Diese Methoden werden häufig eingesetzt, um Reverse-Engineering zu verhindern oder um den Inhalt des Programms mit proprietären Kompressions- und/oder Verschlüsselungsmethoden zu verschleiern, z. B. um Malware zu verbergen.

In diese Kategorie gehören alle unbekannten Anwendungen, die mit Pack- oder Schutzprogrammen komprimiert wurden.

Potenziell unsichere Anwendungen

Diese Klassifizierung wird für gewerbliche und legitime Software vergeben, die jedoch für bösartige Zwecke missbraucht werden kann. Potenziell unsichere Anwendungen sind gewerbliche Programme, die zu bösartigen Zwecken missbraucht werden können.

Zu dieser Kategorie gehören: Cracker- und Hackerwerkzeuge, Programme zum Generieren von Lizenzschlüsseln, Suchprogramme für Produktschlüssel, Programme für Fernzugriff oder Fernsteuerung, Programme zum Entschlüsseln von Passwörtern, Keylogger usw. Diese Option ist in der Voreinstellung deaktiviert.

Weitere Informationen zu diesem Anwendungstyp finden Sie im [Glossar](#).

Lesen Sie die folgenden Informationen, bevor Sie einen Schwellenwert (oder eine Stufe) für die Berichterstellung oder den Schutz ändern:

▼ [Berichterstellung](#)

Die Berichterstellung wird von der Erkennungsroutine und der Machine-Learning-Komponente ausgeführt. Sie können den Schwellenwert für Berichte an Ihre Umgebung und Ihre Anforderungen anpassen. Es gibt keine allgemein gültige Konfiguration. Überwachen Sie das Verhalten in Ihrer Umgebung und passen Sie die Einstellung für die Berichterstellung entsprechend an.

Bei der Berichterstellung werden keine Aktionen an Objekten ausgeführt, sondern nur Informationen an die jeweilige Schutzebene weitergeleitet. Die Schutzebene ist für die entsprechenden Aktionen zuständig.

Aggressiv	Berichterstellung mit maximaler Empfindlichkeit. Weitere Ereignisse werden gemeldet. Die aggressive Einstellung ist zwar am sichersten, ist jedoch oft zu empfindlich, was sogar kontraproduktiv sein kann. <div>HINWEIS Bei der aggressiven Einstellung können Objekte fälschlicherweise als bösartig erkannt werden und Aktionen mit solchen Objekten ausgeführt werden (je nach Schutzeinstellungen).</div>
Ausgewogen	Diese Einstellung ist eine optimale Balance zwischen Leistung und Genauigkeit der Erkennungsraten und der Anzahl fälschlich gemeldeter Objekte.
Vorsichtig	Berichte zur Minimierung falsch erkannter Objekte unter Beibehaltung eines ausreichenden Schutzniveaus. Objekte werden nur gemeldet, wenn die Erkennung sehr wahrscheinlich ist und mit dem Verhalten von Malware übereinstimmt.
Aus	Die Berichterstellung ist nicht aktiv. Ereignisse werden nicht gefunden, gemeldet oder gesäubert. <div>HINWEIS Malware-Berichte können nicht deaktiviert werden. Daher ist die Einstellung Aus für Malware nicht verfügbar.</div>

Wenn Sie die Einstellungen in diesem Bereich auf die Standardwerte [zurücksetzen](#) möchten, klicken Sie auf den Umkehren-Pfeil neben der Abschnittsüberschrift. Die in diesem Abschnitt vorgenommenen Änderungen gehen dabei verloren.

▼ [Schutz](#)

Wenn ein Objekt gemäß der obigen Konfiguration und der Machine-Learning-Ergebnisse gemeldet wird, wird es gesperrt und eine Aktion wird ausgeführt (säubern, löschen oder in die Quarantäne verschieben).

Aggressiv	Gemeldete ausgewogene (oder niedrigere) Ereignisse werden blockiert und die automatische Behebung (z. B. Säuberung) wird gestartet.
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	Die Berichterstellung ist nicht aktiv, und es werden keine Ereignisse gefunden, gemeldet oder gesäubert.
	HINWEIS Malware-Berichte können nicht deaktiviert werden. Daher ist die Option Aus für Malware nicht verfügbar.

Wenn Sie die Einstellungen in diesem Bereich auf die Standardwerte [zurücksetzen](#) möchten, klicken Sie auf den Umkehren-Pfeil neben der Abschnittsüberschrift. Die in diesem Abschnitt vorgenommenen Änderungen gehen dabei verloren.

HINWEIS

Die oben genannten Machine-Learning-Schutzeinstellungen gelten standardmäßig auch für On-Demand-Scans. Bei Bedarf können Sie die Einstellungen für **On-Demand- und Machine-Learning-Schutz** separat konfigurieren. Klicken Sie auf das Schaltersymbol, um die Option **Einstellungen für den Echtzeit-Schutz verwenden** zu deaktivieren und die Konfiguration fortzusetzen.

Erkennung durch Machine Learning

Die Erkennungsroutine schützt Sie vor bösartigen Systemangriffen, indem Dateien, E-Mails und die Netzwerkkommunikation gescannt werden. Wenn ein als Malware eingestuftes Objekt erkannt wird, beginnt die Behebung. Die Erkennungsroutine kann das Ereignis zunächst blockieren und anschließend säubern, löschen oder in die Quarantäne verschieben.

Echtzeit- & Machine-Learning-Schutz

Advanced Machine Learning ist jetzt als zusätzliche Schutzebene in der Erkennungsroutine enthalten, um die Erkennung auf Basis von Machine Learning zu verbessern. Weitere Informationen zu diesem Schutztyp finden Sie in unserem [Glossar](#). Sie können Berichterstellung 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 genauerer Begriff. Die Malware-Erkennung wird von der Erkennungsroutine zusammen mit der Machine-Learning-Komponente ausgeführt. Weitere Informationen zu diesen Anwendungstypen finden Sie im [Glossar](#).

Eventuell unerwünschte Anwendungen

Eine eventuell unerwünschte Anwendung ist ein Programm, das nicht zwangsläufig nur böse Absichten verfolgt, jedoch zusätzliche unerwünschte Software installieren, das Verhalten des digitalen Geräts manipulieren, unerwünschte oder unerwartete Aktionen ausführen kann oder sonstige unklare Ziele verfolgt. Zu dieser Kategorie gehören: Software für Werbeeinblendungen, Download-Wrapper, verschiedene Browser-Werkzeugleisten, Software mit irreführenden Verhaltensweisen, Bundlware, Trackware usw.

Weitere Informationen zu diesem Anwendungstyp finden Sie im [Glossar](#).

Verdächtige Anwendungen

Diese Kategorie umfasst Programme, die mit [Pack](#)- oder Schutzprogrammen komprimiert wurden. Diese Methoden werden häufig eingesetzt, um Reverse-Engineering zu verhindern oder um den Inhalt des Programms mit proprietären Kompressions- und/oder Verschlüsselungsmethoden zu verschleiern, z. B. um Malware zu verbergen.

In diese Kategorie gehören alle unbekannten Anwendungen, die mit Pack- oder Schutzprogrammen komprimiert wurden.

Potenziell unsichere Anwendungen

Diese Klassifizierung wird für gewerbliche und legitime Software vergeben, die jedoch für bösartige Zwecke missbraucht werden kann. Potenziell unsichere Anwendungen sind gewerbliche Programme, die zu bösartigen Zwecken missbraucht werden können.

Zu dieser Kategorie gehören: Cracker- und Hackerwerkzeuge, Programme zum Generieren von Lizenzschlüsseln, Suchprogramme für Produktschlüssel, Programme für Fernzugriff oder Fernsteuerung, Programme zum Entschlüsseln von Passwörtern, Keylogger usw. Diese Option ist in der Voreinstellung deaktiviert.

Weitere Informationen zu diesem Anwendungstyp finden Sie im [Glossar](#).

Lesen Sie die folgenden Informationen, bevor Sie einen Schwellenwert (oder eine Stufe) für die Berichterstellung oder den Schutz ändern:

▼ [Berichterstellung](#)

Die Berichterstellung wird von der Erkennungsroutine und der Machine-Learning-Komponente ausgeführt. Sie können den Schwellenwert für Berichte an Ihre Umgebung und Ihre Anforderungen anpassen. Es gibt keine allgemein gültige Konfiguration. Überwachen Sie das Verhalten in Ihrer Umgebung und passen Sie die Einstellung für die Berichterstellung entsprechend an.

Bei der Berichterstellung werden keine Aktionen an Objekten ausgeführt, sondern nur Informationen an die jeweilige Schutzebene weitergeleitet. Die Schutzebene ist für die entsprechenden Aktionen zuständig.

Aggressiv	Berichterstellung mit maximaler Empfindlichkeit. Weitere Ereignisse werden gemeldet. Die aggressive Einstellung ist zwar am sichersten, ist jedoch oft zu empfindlich, was sogar kontraproduktiv sein kann.
	HINWEIS Bei der aggressiven Einstellung können Objekte fälschlicherweise als bösartig erkannt werden und Aktionen mit solchen Objekten ausgeführt werden (je nach Schutzeinstellungen).
Ausgewogen	Diese Einstellung ist eine optimale Balance zwischen Leistung und Genauigkeit der Erkennungsraten und der Anzahl fälschlich gemeldeter Objekte.
Vorsichtig	Berichte zur Minimierung falsch erkannter Objekte unter Beibehaltung eines ausreichenden Schutzniveaus. Objekte werden nur gemeldet, wenn die Erkennung sehr wahrscheinlich ist und mit dem Verhalten von Malware übereinstimmt.
Aus	Die Berichterstellung ist nicht aktiv. Ereignisse werden nicht gefunden, gemeldet oder gesäubert.
	HINWEIS Malware-Berichte können nicht deaktiviert werden. Daher ist die Einstellung Aus für Malware nicht verfügbar.

Wenn Sie die Einstellungen in diesem Bereich auf die Standardwerte [zurücksetzen](#) möchten, klicken Sie auf den Umkehren-Pfeil neben der Abschnittsüberschrift. Die in diesem Abschnitt vorgenommenen Änderungen gehen dabei verloren.

▼ [Zugriffsfilter- und Machine-Learning-Schutz](#)

Berichte

Wird von der Erkennungsroutine und der Machine-Learning-Komponente ausgeführt. Bei der Berichterstellung werden keine Aktionen an Objekten ausgeführt (dafür ist die jeweilige Schutzebene zuständig).

Schutz

Konfigurieren Sie die Parameter unter [Echtzeitfilter](#), um festzulegen, welche Aktionen an gemeldeten Objekten ausgeführt werden.

Wenn Sie die Einstellungen in diesem Bereich auf die Standardwerte [zurücksetzen](#) möchten, klicken Sie auf den Umkehren-Pfeil neben der Abschnittsüberschrift. Die in diesem Abschnitt vorgenommenen Änderungen gehen dabei verloren.

Konfigurieren Sie den Machine-Learning-Schutz mit eShell. Der Kontextname in eShell ist **MLP**. Öffnen Sie eShell im interaktiven Modus und navigieren Sie zu MLP:

```
server av transport mlp
```

Aktuelle Berichterstellungseinstellung für verdächtige Anwendungen anzeigen:

```
get suspicious-reporting
```

Ändern Sie die Einstellung zu „Vorsichtig“, um die Berichterstellungseinstellungen zu lockern:

```
set suspicious-reporting cautious
```

▼ [On-Demand-Datenbank-Scan und Machine-Learning-Schutz](#)

Berichte

Wird von der Erkennungsroutine und der Machine-Learning-Komponente ausgeführt. Bei der Berichterstellung werden keine Aktionen an Objekten ausgeführt (dafür ist die jeweilige Schutzebene zuständig).

Schutz

Konfigurieren Sie die Parameter unter [On-Demand-Datenbank-Scan](#), um festzulegen, welche Aktionen an gemeldeten Objekten ausgeführt werden.

Wenn Sie die Einstellungen in diesem Bereich auf die Standardwerte [zurücksetzen](#) möchten, klicken Sie auf den Umkehren-Pfeil neben der Abschnittsüberschrift. Die in diesem Abschnitt vorgenommenen Änderungen gehen dabei verloren.

Konfigurieren Sie den Machine-Learning-Schutz mit eShell. Der Kontextname in eShell ist **MLP**. Öffnen Sie eShell im interaktiven Modus und navigieren Sie zu MLP:

```
server av transport mlp
```

Aktuelle Berichterstellungseinstellung für verdächtige Anwendungen anzeigen:

```
get suspicious-reporting
```

Ändern Sie die Einstellung zu „Vorsichtig“, um die Berichterstellungseinstellungen zu lockern:

```
set suspicious-reporting cautious
```

Ausschlussfilter

Mit dem Ausschlussfilter können Sie festlegen, welche Dateien und Ordner von Scans ausgenommen werden sollen. Um zu gewährleisten, dass möglichst alle Objekte auf Bedrohungen gescannt werden, empfehlen wir, nur bei dringendem Bedarf Ausnahmen zu erstellen. Manche Objekte wie etwa sehr große Datenbankeinträge können vom Scannen ausgeschlossen werden, da andernfalls die Serverleistung zu stark beeinträchtigt würde. Dasselbe gilt für Software, die Konflikte mit dem Scan verursacht (z. B. Backup-Software).

WARNUNG

Nicht zu verwechseln mit [ausgeschlossenen Erweiterungen](#), [Prozessausschlüssen](#) oder dem [Ausschlussfilter](#).

HINWEIS

Eine Bedrohung, die sich in einer Datei befindet, die die Kriterien des Ausschlussfilters erfüllt, kann vom Echtzeit-Dateischutz und beim Scannen des Computers nicht erkannt werden.


Wählen Sie den Ausschlusstyp aus und klicken Sie auf **Bearbeiten**, um neue Elemente hinzuzufügen oder vorhandene zu ändern:

- [Leistungsausschlüsse](#) - Dateien und Ordner vom Scannen ausschließen.
- [Ereignisausschlüsse](#) - Objekte anhand von bestimmten Kriterien von der Prüfung ausschließen: Pfad, Dateihash oder Ereignisname.

Leistungsausschlüsse

Mit dieser Funktion können Sie Dateien und Ordner vom Scannen ausschließen. Leistungsausschlüsse sind hilfreich, um unternehmenskritische Anwendungen auf Dateiebene vom Scannen auszuschließen, oder wenn die Scans ein anomales Systemverhalten verursachen oder die Leistung beeinträchtigen.

Pfad

Schließt einen bestimmten Pfad (Datei oder Verzeichnis) für diesen Computer aus. Verwenden Sie keine Platzhalter (Sternchen *) in der Mitte von Pfaden. Weitere Informationen finden Sie im folgenden [Knowledgebase-Artikel](#) .

HINWEIS

Vergessen Sie beim Ausschließen von Ordnerinhalten nicht, das Sternchen (*) am Ende des Pfades hinzuzufügen (*C:\Tools**). *C:\Tools* wird nicht ausgeschlossen, da *Tools* aus der Perspektive des Scanners ebenfalls ein Dateiname sein könnte.

Kommentar

Fügen Sie einen optionalen **Kommentar** hinzu, um den Ausschluss in Zukunft leicht erkennen zu können.

BEISPIEL

Pfadausschlüsse mit Sternchen:

*C:\Tools** - Pfad muss mit umgekehrtem Schrägstrich (\) und Sternchen (*) enden, um anzugeben, dass es sich um einen Ordner handelt und dass sämtliche Ordnerinhalte (Dateien und Unterordner) ausgeschlossen werden.

C:\Tools. ** - Dasselbe Verhalten wie *C:\Tools**, also rekursive Funktionsweise

C:\Tools.dat* – Schließt *dat*-Dateien im Ordner „Tools“ aus.

C:\Tools\sg.dat – Schließt diese spezielle Datei im Ordner „Tools“ aus.

BEISPIEL

Um alle Dateien in einem bestimmten Ordner auszuschließen, geben Sie den Pfad zum Ordner mit der Maske **.** ein.

- Wenn Sie ein gesamtes Laufwerk einschließlich aller Dateien und Unterordner ausschließen möchten, geben Sie den Pfad mit der Maske *D:.** ein.
- Um nur DOC-Dateien auszuschließen, verwenden Sie die Maske **.doc*.
- Wenn der Name einer ausführbaren Datei aus einer bestimmten Anzahl von (variierenden) Zeichen besteht und Sie nur den ersten sicher wissen (zum Beispiel „D“), verwenden Sie folgendes Format:
D????.exe (Die Fragezeichen ersetzen die fehlenden oder unbekannten Zeichen)

BEISPIEL

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

- Um den Ordner „Programme“ mit dieser Systemvariable auszuschließen, verwenden Sie den Pfad *%PROGRAMFILES%* (achten Sie auf den umgekehrten Schrägstrich am Ende des Pfads, wenn Sie Ausschlüsse angeben).
- Um alle Dateien in einem Unterverzeichnis von *%HOMEDRIVE%* auszuschließen, verwenden Sie den Pfad *%HOMEDRIVE%\Excluded_Directory*.**.

Im Format für Pfad-Ausschlüsse können die folgenden Variablen verwendet werden:

%ALLUSERSPROFILE%

%COMMONPROGRAMFILES%

%COMMONPROGRAMFILES(X86)%

%COMSPEC%

%HOMEDRIVE%

%HOMEPATH%

%PROGRAMFILES%

%PROGRAMFILES(X86)%

%SystemDrive%

%SystemRoot%

%WINDIR%

%PUBLIC%

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


Ereignisausschlüsse

Dies ist eine andere Methode, um Objekte anhand von Ereignisname, Pfad oder Hash vom Scannen auszuschließen. 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.

Sie können einen erkenntnisbasierten Ausschluss mit einem vorhandenen Ereignis unter **Log-Dateien** > [Ereignisse](#) erstellen. Klicken Sie mit der rechten Maustaste auf einen Log-Eintrag (Ereignis) und klicken Sie auf **Ausschluss erstellen**. Daraufhin wird der [Ausschluss-Assistent](#) mit vordefinierten Kriterien geöffnet.

Um einen Erkennungsausschluss manuell zu erstellen, klicken Sie auf **Bearbeiten** > **Hinzufügen** (oder **Bearbeiten**, falls Sie ein vorhandenes Element bearbeiten) und geben Sie eines oder mehrere der folgenden Kriterien an (Kombinationen sind möglich):

Pfad

Schließt einen bestimmten Pfad (Datei oder Verzeichnis) aus. Sie können nach einem Speicherort oder einer Datei suchen oder die Zeichenfolge manuell eingeben. Verwenden Sie keine Platzhalter (Sternchen *) in der Mitte von Pfaden. Weitere Informationen finden Sie im folgenden [Knowledgebase-Artikel](#) .

HINWEIS

Vergessen Sie beim Ausschließen von Ordnerinhalten nicht, das Sternchen (*) am Ende des Pfades hinzuzufügen (*C:\Tools**). *C:\Tools* wird nicht ausgeschlossen, da *Tools* aus der Perspektive des Scanners ebenfalls ein Dateiname sein könnte.

Hash

Schließt eine Datei basierend auf dem angegebenen Hash (SHA1) und unabhängig von Dateityp, Speicherort, Name oder Erweiterung aus.

Ereignisname

Geben Sie einen gültigen Ereignisnamen (Bedrohungsname) ein. Ausschlüsse allein anhand des Ereignisnamens können ein Sicherheitsrisiko darstellen. Wir empfehlen, den Ereignisnamen mit dem Pfad zu kombinieren. Diese Ausschlusskriterien können nur für bestimmte Arten von Ereignissen verwendet werden.

Kommentar

Fügen Sie einen optionalen **Kommentar** hinzu, um den Ausschluss in Zukunft leicht erkennen zu können.

Mit ESET Security Management Center können Sie [Ereignisausschlüsse verwalten](#) , um Ereignisausschlüsse zu erstellen und sie auf mehreren Computern/Gruppen anzuwenden.

Mit Platzhaltern können Sie Gruppen von Dateien ausschließen. Dabei steht ein Fragezeichen (?) für genau ein beliebiges Zeichen, ein Sternchen (*) steht für beliebig viele Zeichen oder „kein Zeichen“.

BEISPIEL

Pfadausschlüsse mit Sternchen:

*C:\Tools** - Pfad muss mit umgekehrtem Schrägstrich (\) und Sternchen (*) enden, um anzugeben, dass es sich um einen Ordner handelt und dass sämtliche Ordnerinhalte (Dateien und Unterordner) ausgeschlossen werden.

C:\Tools. ** - Dasselbe Verhalten wie *C:\Tools**, also rekursive Funktionsweise

C:\Tools.dat* – Schließt *dat*-Dateien im Ordner „Tools“ aus.

C:\Tools\sg.dat – Schließt diese spezielle Datei im Ordner „Tools“ aus.

BEISPIEL

Um eine Bedrohung auszuschließen, geben Sie einen gültigen Ereignisnamen im folgenden Format an:

@NAME=Win32/Adware.Optmedia

@NAME=Win32/TrojanDownloader.Delf.QQI

@NAME=Win32/Bagle.D

BEISPIEL

Um alle Dateien in einem bestimmten Ordner auszuschließen, geben Sie den Pfad zum Ordner mit der Maske **.** ein.

- Wenn Sie ein gesamtes Laufwerk einschließlicb aller Dateien und Unterordner ausschließen möchten, geben Sie den Pfad mit der Maske *D:.** ein.

- Um nur DOC-Dateien auszuschließen, verwenden Sie die Maske **.doc*.

- Wenn der Name einer ausführbaren Datei aus einer bestimmten Anzahl von (variierenden) Zeichen besteht und Sie nur den ersten sicher wissen (zum Beispiel „D“), verwenden Sie folgendes Format:

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

BEISPIEL

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

- Um den Ordner „Programme“ mit dieser Systemvariable auszuschließen, verwenden Sie den Pfad *%PROGRAMFILES%* (achten Sie auf den umgekehrten Schrägstrich am Ende des Pfads, wenn Sie Ausschlüsse angeben).

- Um alle Dateien in einem Unterverzeichnis von *%HOMEDRIVE%* auszuschließen, verwenden Sie den Pfad *%HOMEDRIVE%\Excluded_Directory*.**.

Im Format für Pfad-Ausschlüsse können die folgenden Variablen verwendet werden:

%ALLUSERSPROFILE%

%COMMONPROGRAMFILES%

%COMMONPROGRAMFILES(X86)%

%COMSPEC%

%HOMEDRIVE%

%HOMEPATH%

%PROGRAMFILES%

%PROGRAMFILES(X86)%

%SystemDrive%

%SystemRoot%

%WINDIR%

%PUBLIC%

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

Assistent zum Erstellen von Ausschlüssen

Der empfohlene Ausschluss wird anhand des Ereignistyps vorab ausgewählt, Sie können jedoch weitere Ausschlusskriterien für Ereignisse festlegen. Klicken Sie auf **Kriterien ändern**:

- **Exakte Dateien** - Dateien nach ihrem SHA-1-Hash ausschließen.
- **Ereignis** - Geben Sie den Ereignisnamen an, um die Dateien auszuschließen, die dieses Ereignis enthalten.
- **Pfad + Ereignis** - Geben Sie den Ereignisnamen und -Pfad (inklusive Dateiname) an, um alle Dateien mit einem Ereignis am angegebenen Speicherort auszuschließen.

Fügen Sie einen optionalen **Kommentar** hinzu, um den Ausschluss in Zukunft leicht erkennen zu können.

Erweiterte Einstellungen

Anti-Stealth-Technologie

Ein fortschrittliches System zur Erkennung gefährlicher Programme wie [Rootkits](#), die sich vor dem Betriebssystem verstecken. Da sich die Rootkits verstecken, ist es nahezu unmöglich, sie mit herkömmlichen Prüfmethode zu erkennen.

AMSI

Mit der Microsoft Anti-Malware-Scan-Oberfläche (AMSI) können Sie PowerShell-Skripts scannen, die vom Windows Script Host ausgeführt werden.

Automatische Ausschlüsse

Die Entwickler von Server-Anwendungen und -Betriebssystemen empfehlen für die meisten ihrer Produkte, kritische Arbeitsdateien und -ordner vom Virenschutz auszuschließen. Malware-Scans können die Serverleistung beeinträchtigen, Konflikte verursachen und sogar die Ausführung mancher Anwendungen auf dem Server verhindern. Mit Ausschlussfiltern können Sie das Konfliktrisiko beim Ausführen Ihres Malware-Schutzes minimieren und die Gesamtleistung des Servers verbessern. Machen Sie sich mit der [Liste der vom Scannen ausgeschlossenen Dateien](#) für ESET-Serverprodukte vertraut.

ESET Security for Microsoft SharePoint identifiziert Anwendungen und Betriebssystem-Dateien, die für den Server kritisch sind, und fügt sie automatisch zur Liste der [Ausschlüsse](#) hinzu. Standardmäßig sind alle automatischen Ausschlüsse aktiviert. Sie können ausgeschlossene Serveranwendungen mit dem Schieberegler einzeln aktivieren oder deaktivieren. Dabei geschieht Folgendes:

- Wenn Sie eine Anwendung aktivieren, werden alle zugehörigen kritischen Dateien und Ordner zur Liste der vom Scannen ausgeschlossenen Elemente hinzugefügt. Bei jedem Neustart des Servers überprüft das System die Ausschlüsse automatisch und aktualisiert die Liste, falls Änderungen am System oder den Anwendungen vorgenommen wurden (z. B. wenn eine neue Serveranwendung installiert wurde). Diese Einstellung sorgt dafür, dass die empfohlenen automatischen Ausschlüsse immer angewendet werden.
- Beim Deaktivieren werden die ausgeschlossenen Dateien und Ordner aus der Liste entfernt. Vom Benutzer manuell definierte Ausschlüsse sind davon nicht betroffen.

ESET Security for Microsoft SharePoint verwendet die dedizierte Anwendung *eAutoExclusions.exe* im Installationsordner, um automatische Ausschlüsse zu identifizieren und zu generieren. Dazu ist kein Eingreifen Ihrerseits erforderlich, aber Sie können *eAutoExclusions.exe -servers* in der Befehlszeile ausführen, um die auf Ihrem System erkannten Serveranwendungen aufzulisten. Mit *eAutoExclusions.exe -?* können Sie die vollständige Syntax anzeigen.

Shared local cache

Der freigegebene lokale ESET-Cache verbessert die Leistung in virtualisierten Umgebungen, indem er doppelte Prüfungen im Netzwerk vermeidet. Somit wird jede Datei nur einmal gescannt und im gemeinsamen Cache gespeichert. Durch Aktivieren der **Caching-Option** werden Informationen zu Scans von Dateien und Ordnern im Netzwerk im lokalen Cache gespeichert. Beim nächsten Scan sucht ESET Security for Microsoft SharePoint nach gescannten Dateien im Cache. Übereinstimmende Dateien werden vom Scan ausgeschlossen.

Die Einstellungen für den Cache-Server umfassen Folgendes:

- **Hostname** - Name oder IP-Adresse des Computers, auf dem sich der Cache befindet.
- **Port** - Nummer des für die Kommunikation verwendeten Ports (mit der im gemeinsam genutzten lokalen Cache festgelegten identisch).
- **Passwort** - Bei Bedarf können Sie ein Passwort für den gemeinsamen lokalen Cache festlegen.

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, Disketten usw.).

Standardmäßiges Verhalten

ESET Security for Microsoft SharePoint kann Bedrohungen mit einem der folgenden Module erkennen:

- [Echtzeit-Dateischutz](#)
- [Web-Schutz](#)
- [E-Mail-Schutz](#)
- [On-Demand-Prüfung](#)

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

Schadcode entfernen 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 diesem Fall sollten Sie versuchen, den Schadcode aus der infizierten Datei zu entfernen und ihren Originalzustand wiederherzustellen. Wenn die Datei ausschließlich Schadcode enthält, wird sie gelöscht.

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

Mehrere Bedrohungen

Falls infizierte Dateien während der Prüfung des Computers nicht gesäubert wurden (oder die [Säuberungsstufe](#) auf **Nicht säubern** festgelegt wurde), so wird ein Warnfenster angezeigt. In diesem wird danach gefragt, wie mit den Dateien verfahren werden soll. Wählen Sie individuelle Aktionen für einzelne Bedrohungen in der Liste aus oder **wählen Sie eine Aktion für alle aufgelisteten Bedrohungen aus**, wählen Sie eine Aktion für alle Bedrohungen in der Liste aus und klicken Sie 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 überwacht alle Systemereignisse im Zusammenhang mit Malware. Alle Dateien werden beim Öffnen, Erstellen oder Ausführen auf Ihrem Computer auf Schadcode geprüft. Der Echtzeit-Dateischutz wird standardmäßig zusammen mit dem System gestartet und fortlaufend ausgeführt. In Ausnahmefällen (z. B. bei Konflikten mit einer anderen Echtzeitprüfung) kann der Echtzeit-Dateischutz deaktiviert werden. Deaktivieren Sie dazu die Option **Echtzeit-Schutz automatisch starten** in den **Erweiterten Einstellungen (F5)** unter **Echtzeit-Dateischutz > Einfach**.

Zu scannende Datenträger

In der Standardeinstellung werden alle Datenträger auf mögliche Bedrohungen geprüft:

- **Lokale Laufwerke** - Geprüft werden alle lokalen Laufwerke
- **Wechselmedien** - Geprüft werden CDs/DVDs, USB-Speichergeräte, Bluetooth-Geräte usw.
- **Netzlaufwerke** - Geprüft werden alle zugeordneten Netzlaufwerke

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

Prüfen beim

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 von Dateien beim Öffnen / Zugreifen.
- **Erstellen von Dateien** - Scannen von Dateien beim Erstellen / Bearbeiten.
- **Ausführen von Dateien** - Scannen von Dateien beim Ausführen.
- **Wechselmedienzugriff** - Scannen beim Zugriff auf Wechselmedien. Wenn Wechselmedien, die einen Bootsektor enthalten, in das Gerät eingefügt werden, wird der Bootsektor sofort gescannt. Mit dieser Option wird das Scannen von Dateien auf Wechselmedien nicht aktiviert. Die Option zum Scannen von Dateien auf Wechselmedien befindet sich unter **Zu scannende Datenträger > Wechselmedien**. Lassen Sie die Option **Bootsektoren/UEFI** in den ThreatSense-Parametern aktiviert, um Wechselmedien mit Bootsektoren korrekt scannen zu können.

[Ausgeschlossene Prozesse](#)

Mit dieser Funktion können Sie bestimmte Prozesse ausschließen. Wenn Sie z. B. die Prozesse Ihrer Sicherungssoftware ausschließen, werden alle Dateioperationen dieser Prozesse ignoriert und als sicher betrachtet. Auf diese Weise werden Wechselwirkungen mit dem Sicherungsprozess minimiert.

ThreatSense-Parameter

Der Echtzeit-Dateischutz überwacht alle Datenträger auf das Eintreten bestimmter Ereignisse wie den Zugriff auf eine Datei. Der Echtzeit-Dateischutz kann so konfiguriert werden, dass neu erstellte und vorhandene Dateien unterschiedlich behandelt werden. Sie können den Echtzeit-Dateischutz z. B. so konfigurieren, dass neu erstellte Dateien genauer überwacht werden.

Bereits geprüfte Dateien werden nicht erneut geprüft (sofern sie nicht geändert wurden), um die Systembelastung durch den Echtzeit-Schutz zu minimieren. Nach einem Update der Datenbank der Malware Scan Engine 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 bearbeiten, öffnen Sie das Fenster mit den **erweiterten Einstellungen** mit der Taste **F5** und erweitern Sie den Eintrag **Computer > Echtzeit-Dateischutz**. Klicken Sie auf **ThreatSense-Parameter > Sonstige**, und aktivieren oder deaktivieren Sie die Option **Smart-Optimierung aktivieren**.

Zusätzliche ThreatSense-Parameter

Sie können die Optionen für **Zusätzliche ThreatSense-Parameter für neu erstellte und geänderte Dateien** bzw. **Zusätzliche ThreatSense-Parameter für ausführbare Dateien** ausführlich bearbeiten.

ThreatSense-Parameter

ThreatSense ist eine Technologie, die verschiedene Methoden zur Erkennung von Bedrohungen verwendet. 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. Die Prüfengine kann verschiedene Datenströme gleichzeitig kontrollieren und so die Effizienz und Erkennungsrate steigern. Die ThreatSense-Technologie entfernt auch erfolgreich Rootkits.

HINWEIS

Weitere Hinweise zur Prüfung der Systemstartdateien finden Sie unter [Prüfung Systemstartdateien](#).

in den Einstellungen für ThreatSense können Sie verschiedene Prüfparameter festlegen:

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

Um das Einstellungsfenster zu öffnen, klicken Sie **im Fenster Erweiterte Einstellungen (F5)** auf **ThreatSense-Einstellungen**. Dies gilt für beliebige Module, 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:

- [Echtzeitfilter](#)
- [On-Demand-Datenbankprüfung](#)
- [Hyper-V-Scan](#)
- [Echtzeit-Dateischutz](#)

- [Malware-Prüfungen](#)
- [Prüfen im Leerlaufbetrieb](#)
- [Prüfung der Systemstartdateien](#)
- [Dokumentenschutz](#)
- [E-Mail-Schutz](#)
- [Web-Schutz](#)

Die ThreatSense-Parameter sind für jedes Modul optimal eingerichtet. Eine Veränderung der Einstellungen kann den Systembetrieb deutlich beeinflussen. So kann zum Beispiel eine Änderung der Einstellungen für das Prüfen laufzeitkomprimierter Dateien oder die Aktivierung der Advanced Heuristik im Modul „Echtzeit-Dateischutz“ dazu führen, dass das System langsamer arbeitet (normalerweise werden mit diesen Methoden nur neu erstellte Dateien geprüft). Es wird empfohlen, die Standard-Parameter für ThreatSense in allen Modulen unverändert beizubehalten. Änderungen sollten nur im Modul „Computer prüfen“ vorgenommen werden.

[Zu prüfende Objekte](#)

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

Arbeitsspeicher

Scannt nach Bedrohungen für den Arbeitsspeicher des Systems.

Bootsektoren/UEFI

Scannt die Bootsektoren auf Viren im Master Boot Record. Im Fall von virtuellen Hyper-V-Computern wird der Laufwerks-MBR im schreibgeschützten Modus geprüft.

E-Mail-Dateien

Das Programm unterstützt die folgenden Erweiterungen: DBX (Outlook Express) und EML.

Archive

Folgende Erweiterungen werden vom Programm unterstützt: 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 Archive, die ohne externe Programme dekomprimiert werden können.

Laufzeitkomprimierte Dateien

Im Unterschied zu Standardarchiven werden laufzeitkomprimierte Dateien nach dem Start 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. Die folgenden Optionen stehen zur Verfügung:

Heuristik

Heuristische Methoden sind Verfahren, die (böartige) Aktivitäten von Programmen analysieren. Auf diese Weise können auch böartige Programme erkannt werden, die noch nicht in der Malware Scan Engine verzeichnet sind.

Advanced Heuristik/DNA-Signaturen

Advanced Heuristik beschreibt besondere heuristische Verfahren, die von ESET entwickelt wurden, um eine verbesserte Erkennung von Würmern und Trojanern zu ermöglichen und um Schadprogramme zu finden, die in höheren Programmiersprachen geschrieben wurden. Mit Advanced Heuristik werden die Fähigkeiten von ESET-Produkten zur Erkennung von Bedrohungen beträchtlich gesteigert. Mit Signaturen können Viren zuverlässig erkannt werden. Mit automatischen Updates sind Signaturen für neue Bedrohungen innerhalb weniger Stunden verfügbar. Signaturen haben den Nachteil, dass nur bekannte Viren und gering modifizierte Varianten bekannter Viren erkannt werden können.

[Säubern](#)

Die Einstellungen zum Entfernen von Schadcode legen fest, wie beim Entfernen vorgegangen werden soll. Es gibt drei Arten der Schadcodeentfernung:

Kein Säubern

Der in infizierten Objekten erkannte Schadcode wird nicht automatisch entfernt. Eine Warnung wird angezeigt, und der Benutzer wird aufgefordert, eine Aktion auszuwählen. Diese Stufe eignet sich für fortgeschrittene Benutzer, die wissen, wie sie im Falle eingedrungener Schadsoftware vorgehen sollen.

Normale Säuberung

Das Programm versucht, infizierte Dateien automatisch zu säubern oder zu löschen. Es wendet hierzu vordefinierte Aktionen an (je nach Art der Infiltration). Ein Hinweis am unteren rechten Bildschirmrand informiert über die Erkennung und das Löschen infizierter Dateien. Wenn es nicht möglich ist, die angemessene Aktion automatisch zu bestimmen, schlägt das Programm verschiedene Aktionen vor. Dies gilt auch für Fälle, in denen eine vordefinierte Aktion nicht erfolgreich abgeschlossen werden kann.

Strenges Säubern

Das Programm entfernt den Schadcode aus infizierten Dateien oder löscht diese Dateien. Ausnahmen gelten nur für Systemdateien. Wenn eine Datei nicht gesäubert werden kann, wird der Benutzer zur Auswahl einer Aktion aufgefordert.

WARNUNG

Wenn infizierte Dateien in einem Archiv gefunden werden, sind zwei Vorgehensweisen möglich. Im Standardmodus (**normales Säubern**) wird die Archivdatei nur dann gelöscht, wenn alle Dateien im Archiv infiziert sind. Wenn die Option **Immer versuchen, automatisch zu entfernen** aktiviert ist, wird die Archivdatei gelöscht, sobald eine einzige Datei im Archiv infiziert ist.

WICHTIG

Auf Hyper-V-Hosts mit Windows Server 2008 R2 SP1 werden die Optionen **Normale Säuberung** und **Immer versuchen, automatisch zu entfernen** nicht unterstützt. Die Laufwerke der virtuellen Computer werden im schreibgeschützten Modus geprüft, es wird keine Säuberung durchgeführt. Die Prüfung erfolgt immer im schreibgeschützten Modus, unabhängig von der ausgewählten Säuberungsstufe.

[Ausschlussfilter](#)

Die Erweiterung ist der Teil des Dateinamens nach dem Punkt. Die Erweiterung definiert den Typ und den Inhalt einer Datei. In diesem Teil der ThreatSense-Einstellungen können Sie die Dateitypen festlegen, die [nicht gescannt werden](#) sollen.

Sonstige

Bei der Konfiguration der Einstellungen für 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

Jeder Scanvorgang nimmt eine bestimmte Menge von Systemressourcen in Anspruch. Wenn Sie mit ressourcenintensiven Anwendungen arbeiten, können Sie eine Hintergrundprüfung mit geringer Priorität aktivieren, um Ressourcen für die Anwendungen zu sparen.

Alle Objekte in Log aufnehmen

Wenn Sie diese Option auswählen, enthält die Logdatei alle gescannten Dateien, und nicht nur infizierte Dateien.

Smart-Optimierung aktivieren

Die Smart-Optimierung verwendet die optimalen Einstellungen, um möglichst effiziente Scanvorgänge bei höchster Geschwindigkeit zu gewährleisten. Die verschiedenen Schutzmodule scannen intelligent und verwenden unterschiedliche Scanmethoden für die jeweiligen Dateitypen. Wenn die Smart-Optimierung deaktiviert ist, werden nur die benutzerdefinierten Einstellungen im ThreatSense-Kern der entsprechenden Module für die Prüfung verwendet.

Datum für 'Geändert am' beibehalten

Aktivieren Sie diese Option, um den Zeitpunkt des ursprünglichen Zugriffs auf geprüfte Dateien beizubehalten (z. B. für die Verwendung mit Datensicherungssystemen), anstatt ihn zu aktualisieren.

[Grenzen](#)

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

Standard-Einstellungen Objektprüfung

Aktivieren Sie diese Option, um die Standardeinstellungen zu verwenden (keine Einschränkungen). ESET Security for Microsoft SharePoint ignoriert Ihre benutzerdefinierten Einstellungen.

Maximale Objektgröße

Definiert die Maximalgröße der zu scannenden Elemente. Das entsprechende Schutzmodul scannt nur Elemente, die kleiner als die angegebene Maximalgröße sind. Diese Option sollte nur von erfahrenen Benutzern geändert werden, die größere Elemente aus bestimmten Gründen vom Scannen ausschließen möchten. Der Standardwert ist unbegrenzt.

Maximale Scanzeit pro Objekt (Sek.)

Definiert die maximale Scan-Dauer für Elemente. Wenn hier ein benutzerdefinierter Wert eingegeben wurde, beendet das Schutzmodul das Scannen von Elementen, sobald diese Zeit abgelaufen ist, egal ob der Scanvorgang abgeschlossen wurde. Der Standardwert ist unbegrenzt.

Einstellungen für Archivprüfung

Deaktivieren Sie die Option **Standardeinstellungen Archivprüfung**, um die Scaneinstellungen für Archive zu ändern.

Archiv-Verschachtelungstiefe

Legt die maximale Tiefe der Virenprüfung von Archiven fest. Der Standardwert ist 10. Für Objekte mit Mail-Transportschutz gilt die Verschachtelungstiefe +1, da der Archivanhang in einer E-Mail bereits als erste Ebene gilt.

BEISPIEL

Wenn Sie die Verschachtelungstiefe auf 3 festgelegt haben, werden Archivdateien mit der Verschachtelungstiefe 3 auf der Transportebene nur bis zur Ebene 2 geprüft. Wenn der Mail-Transportschutz Archive bis zur Ebene 3 prüfen soll, müssen Sie den Wert für die **Archiv-Verschachtelungstiefe** auf 4 festlegen.

Maximalgröße von Dateien im Archiv

Mit dieser Option können Sie die maximale Dateigröße für Dateien in Archiven (nach der Extraktion) angeben, die geprüft werden sollen. Der Standardwert ist unbegrenzt.

HINWEIS

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

Zusätzliche ThreatSense-Parameter

Zusätzliche ThreatSense-Parameter für neu erstellte und geänderte Dateien

Das Infektionsrisiko für neu erstellte oder geänderte Dateien ist vergleichsweise größer als für vorhandene Dateien. Daher prüft das Programm solche Dateien mit zusätzlichen Scanparametern. Zusätzlich zu den üblichen Prüfmethoden auf Signaturbasis wird die Advanced Heuristik verwendet. Diese Methode erkennt

neue Bedrohungen, bevor ein Update des Moduls veröffentlicht wird. Neben neu erstellten Dateien werden auch selbstentpackende Archive (SFX) und Laufzeit-Packprogramme (intern komprimierte, ausführbare Dateien) gescannt. In den Standardeinstellungen werden Archive unabhängig von ihrer eigentlichen Größe bis zur 10. Verschachtelungstiefe geprüft. Deaktivieren Sie die Option **Standardeinstellungen Archivprüfung**, um die Archivprüfeinstellungen zu ändern.

Zusätzliche ThreatSense-Parameter für ausführbare Dateien

Standardmäßig wird bei der Dateiausführung keine [Advanced Heuristik](#) verwendet. Wenn diese Option aktiviert ist, sollten [Smart-Optimierung](#) und ESET LiveGrid® unbedingt aktiviert bleiben, um die Auswirkungen auf die Systemleistung gering zu halten.

Von der Prüfung ausgeschlossene Dateierweiterungen

Die Erweiterung ist der Teil des Dateinamens nach dem Punkt. Die Erweiterung definiert den Typ und den Inhalt einer Datei. Normalerweise werden alle Dateien gescannt. Falls Sie jedoch Dateien mit einer bestimmten Erweiterung ausschließen möchten, können Sie mit dem ThreatSense-Parameter Dateien anhand ihrer Erweiterung von der Prüfung ausschließen. Dies ist hilfreich, wenn die Prüfung bestimmter Dateitypen dazu führt, dass eine Anwendung nicht korrekt ausgeführt wird.

BEISPIEL

Klicken Sie auf **Hinzufügen**, um eine neue Erweiterung zur Liste hinzuzufügen. Geben Sie die Erweiterung in das Textfeld ein (z. B. `.tmp`), und klicken Sie auf **OK**. Mit der Option **Mehrere Werte eingeben** können Sie mehrere durch Zeilenumbrüche, Kommas oder Semikolon getrennte Erweiterungen eingeben (wählen Sie z. B. **Semikolon** als Trennzeichen im Dropdownmenü aus, und geben Sie `edb;eml;.tmp` ein). Sie können das Fragezeichen (?) als Sonderzeichen verwenden. Das Fragezeichen steht für ein beliebiges Symbol (z. B. `?db`).

HINWEIS

Um die Erweiterung (den Dateityp) für alle Dateien unter Windows anzuzeigen, müssen Sie die Markierung der Option **Erweiterungen bei bekannten Dateitypen ausblenden** unter **Systemsteuerung > Ordneroptionen > Ansicht** aufheben.

Ausgeschlossene Prozesse

Mit der Funktion zum Definieren ausgeschlossener Prozesse können Anwendungsprozesse nur von der Anti-Malware-Echtzeitprüfung ausgeschlossen werden. Aufgrund der entscheidenden Rolle wichtiger Server (Anwendungsserver, Speicherserver usw.) müssen unbedingt regelmäßig Sicherungen angelegt werden, um die Server bei einer Störung wiederherstellen zu können. Zur Verbesserung von Sicherungsgeschwindigkeit, Prozessintegrität und Dienstverfügbarkeit werden bei Sicherungen bestimmte Techniken verwendet, die zu Konflikten mit Malware-Schutzlösungen auf der Dateiebene führen können. Bei Live-Migrationen virtueller Maschinen können ähnliche Probleme auftreten. Die einzig effektive Lösung zur Vermeidung dieser beiden Situationen ist eine Deaktivierung der Anti-Malware-Software. Wenn Sie Prozesse ausschließen (z. B. die Prozesse der Sicherungssoftware), werden alle Dateioperationen dieser Prozesse ignoriert und als sicher betrachtet, um Wechselwirkungen mit dem Sicherungsprozess zu minimieren. Gehen Sie beim Ausschließen von Prozessen mit Bedacht vor, da ausgeschlossene Sicherungssoftware zum Beispiel auf infizierte Dateien zugreifen kann, ohne einen Alarm auszulösen. Aus diesem Grund sind erweiterte Berechtigungen nur für den Echtzeit-Schutz erlaubt.

Durch Ausschließen von Prozessen können Sie die Gefahr von Konflikten minimieren und die Leistung der

ausgeschlossenen Anwendungen verbessern, was sich wiederum positiv auf die Gesamtleistung des Betriebssystems auswirkt. Prozesse und Anwendungen werden anhand ihrer ausführbaren Dateien (.exe) ausgeschlossen.

Sie können ausführbare Dateien unter **Erweiterte Einstellungen (F5) > Computer > Echtzeit-Dateischutz > Allgemein > Ausgeschlossene Prozesse** zur Liste der ausgeschlossenen Prozesse hinzufügen oder die Liste der ausgeführten Prozesse im Hauptmenü unter **Tools > Ausgeführte Prozesse** verwenden.

Diese Funktion wurde entwickelt, um Sicherungstools auszuschließen. Durch das Ausschließen des Sicherungsprozesses wird die Systemstabilität gewährleistet und die Leistung der Sicherung verbessert, da die Sicherung bei der Ausführung nicht verlangsamt wird.

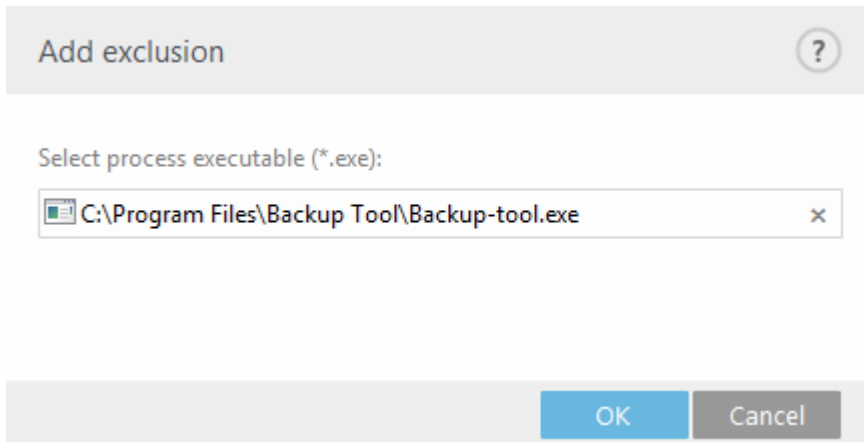
BEISPIEL

Klicken Sie auf **Bearbeiten**, um das Fenster **Ausgeschlossene Prozesse** zu öffnen, in dem Sie Ausschlüsse **hinzufügen** und nach ausführbaren Dateien (z. B. *Backup-tool.exe*) suchen können, die Sie vom Scannen ausschließen möchten.

Sobald Sie die .exe-Datei zu den Ausschlüssen hinzugefügt haben, wird die Aktivität des Prozesses nicht mehr von ESET Security for Microsoft SharePoint überwacht, und die Dateiaktivitäten dieses Prozesses werden nicht mehr gescannt.

WICHTIG

Falls Sie die ausführbare Datei nicht über die Durchsuchen-Funktion auswählen, müssen Sie deren vollständigen Pfad manuell angeben. Andernfalls funktioniert der Ausschluss nicht korrekt, und [HIPS](#) meldet möglicherweise Fehler.



Sie können vorhandene Prozesse **bearbeiten** oder aus den Ausschlüssen **löschen**.

HINWEIS

Der Web-Schutz berücksichtigt diese Liste dagegen nicht. Wenn Sie also die ausführbare Datei Ihres Webbrowsers ausschließen, werden heruntergeladene Dateien dennoch gescannt. Auf diese Weise können Angriffe weiterhin erkannt werden. Dieses Szenario ist lediglich ein Beispiel und keine Empfehlung, Webbrowser auszuschließen.

Cloudbasierter Schutz

ESET LiveGrid® ist ein modernes Frühwarnsystem, das mehrere Cloud-basierte Technologien umfasst. Es unterstützt die Erkennung neuer Bedrohungen auf Grundlage einer Reputationstechnologie und verbessert durch die Verwendung von Positivlisten die Scan-Leistung. Neue Bedrohungsinformationen werden in Echtzeit zur Cloud

gesendet, sodass das ESET-Virenlabor jederzeit einen schnellen und konsistenten Schutz vor Bedrohungen bieten kann. Benutzer können sich direkt im Programmfenster oder im jeweiligen Kontextmenü anzeigen lassen, wie ausgeführte Prozesse oder Dateien eingeschätzt werden. Zudem sind über ESET LiveGrid® weitere Informationen verfügbar.

Wählen Sie bei der Installation von ESET Security for Microsoft SharePoint eine der folgenden Optionen aus:

- Sie haben die Möglichkeit, ESET LiveGrid® nicht zu aktivieren. Die Funktionalität in der Software geht nicht verloren, in einigen Fällen reagiert ESET Security for Microsoft SharePoint jedoch möglicherweise langsamer auf neue Bedrohungen als ein Update der Datenbank der Malware Scan Engine.
- Sie können ESET LiveGrid® so konfigurieren, dass Informationen über neue Bedrohungen und Fundstellen von gefährlichem Code übermittelt werden. Diese Datei kann zur detaillierten Analyse an ESET gesendet werden. Durch die Untersuchung dieser Bedrohungen kann ESET die Fähigkeit seiner Software zur Erkennung von Schadsoftware aktualisieren und verbessern.

ESET LiveGrid® sammelt Daten über neue Bedrohungen, die auf Ihrem Computer erkannt wurden. Dazu können auch Proben oder Kopien der Datei gehören, in der eine Bedrohung aufgetreten ist, der Pfad zu dieser Datei, der Dateiname, Datum und Uhrzeit, der Prozess, über den die Bedrohung auf Ihrem Computer in Erscheinung getreten ist, und Informationen zum Betriebssystem des Computers.

ESET Security for Microsoft SharePoint ist standardmäßig so konfiguriert, dass verdächtige Dateien zur Analyse an ESET eingereicht werden. Dateien mit bestimmten Erweiterungen (z. B. *.docx* oder *.xlsx*) sind immer von der Übermittlung ausgeschlossen. Sie können andere Dateierweiterungen hinzufügen, wenn es bestimmte Dateitypen gibt, die Sie oder Ihr Unternehmen nicht übermitteln möchten.

ESET LiveGrid®-Reputationssystem aktivieren (empfohlen)

Das ESET LiveGrid®-Reputationssystem verbessert die Wirksamkeit der ESET-Sicherheitslösungen, indem es gescannte Dateien mit Positiv- und Negativlisten in einer Datenbank in der Cloud vergleicht.

ESET LiveGrid®-Feedbacksystem aktivieren (empfohlen)

Die Daten werden zur weiteren Analyse an das ESET-Virenlabor übermittelt.

Absturzberichte und Diagnosedaten senden

Reichen Sie Daten wie Absturzberichte, Module und Arbeitsspeicherdumps ein.

Anonyme Statistiken senden

Ermöglicht ESET die Erfassung von Informationen über neu erkannte Bedrohungen wie Name, Datum und Uhrzeit der Erkennung, Erkennungsmethode und verknüpfte Metadaten, gescannte Dateien (Hash, Dateiname, Ursprung der Datei, Telemetrie), gesperrte oder verdächtige URLs und 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](#)

Infizierte Sample automatisch einreichen

Diese Option sendet alle infizierten Proben zur Analyse und Verbesserung der zukünftigen Erkennung an ESET.

- Alle infizierten Proben
- Alle Proben mit Ausnahme von Dokumenten
- Nicht übermitteln

Verdächtige Sample automatisch einreichen

Verdächtige Dateien mit möglichen Bedrohungen und/oder Dateien mit ungewöhnlichen Eigenschaften oder Verhaltensweisen werden zur Analyse an ESET gesendet.

- **Ausführbar** - Ausführbare Dateien: *.exe, .dll, .sys*
- **Archive** - Archivdateien: *.zip, .rar, .7z, .arch, .arj, .bzip2, .gzip, .ace, .arc, .cab*
- **Skripts** - Skriptdateien: *.bat, .cmd, .hta, .js, .vbs, .js, .ps1*
- **Andere** - Andere Dateitypen: *.jar, .reg, .msi, .swf, .lnk*
- **Mögliche Spam-E-Mails** – Verbessert die globale Spam-Erkennung.
- **Dokumente** - Microsoft Office-Dokumente und PDFs mit aktiven Inhalten.

Ausschlussfilter

Klicken Sie auf [Bearbeiten](#) neben „Ausschlussfilter“ in ESET LiveGrid®, um festzulegen, wie Bedrohungen zur Analyse an ESET gesendet werden.

Maximalgröße für Proben (MB)

Definiert die maximale Größe der zu scannenden Proben.

ESET Dynamic Threat Defense

So aktivieren Sie [ESET Dynamic Threat Defense](#) in der ESMC-Web-Konsole auf einem Clientcomputer: Erstellen Sie in der ESET Security Management Center-Web-Konsole [eine neue Policy](#) oder bearbeiten Sie eine vorhandene Policy und weisen Sie sie zu den Computern zu, auf denen Sie ESET Dynamic Threat Defense verwenden möchten.

Ausschlussfilter

Mit dem Ausschlussfilter können Sie bestimmte Dateien/Ordner von der Übermittlung ausschließen. So kann es beispielsweise nützlich sein, Dateien mit vertraulichen Informationen wie Dokumente oder Tabellenkalkulationen auszuschließen. Hier eingetragene Dateien werden nicht an ESET übermittelt, auch wenn sie verdächtigen Code enthalten. Einige typische Dateitypen sind bereits in der Standardeinstellung in die Liste eingetragen (z. B. *.doc*). Sie können weitere Dateien zur Ausschlussliste hinzufügen.

Exclusion filter?

*.dbf
*.doc
*.doc?
*.dot?
*.mdb
*.pot?
*.pps?
*.ppt?
*.rtf
*.sxc
*.sxw
*.xl?
*.xls?
*.xlt?

AddEditRemove

OKCancel

Wenn Sie ESET LiveGrid® einige Zeit verwendet haben, kann es sein, dass auch nach dem Deaktivieren des Systems noch einige Datenpakete zum Senden vorliegen. Derartige Datenpakete werden auch nach der Deaktivierung noch an ESET gesendet. Nachdem alle aktuellen Informationen versendet wurden, werden keine weiteren Pakete mehr erstellt.

Add exclusion?

Enter a path name and mask that defines the files you want to exclude.
An asterisk '*' denotes any number of any characters whereas '?' denotes a single character. e.g., *.TXT means you are selecting all text files of any name.

Folder...File...

Enter multiple valuesOKCancel

Wenn Sie eine verdächtige Datei finden, können Sie sie zur Analyse an unser Virenlabor einreichen. Sollte dabei schädlicher Code zu Tage treten, wird dieser beim nächsten Update des Erkennungsmoduls berücksichtigt.

Malware-Prüfungen

Dieser Abschnitt enthält Optionen für die Auswahl von Scanparametern.

HINWEIS

Diese Scanprofil-Auswahl gilt für **On-Demand**- und für [Hyper-V-Scans](#).

[Ausgewähltes Profil](#)

Diese Parameter werden vom On-Demand-Scanner verwendet. Sie können eines der vordefinierten Scanprofile verwenden oder ein neues Profil erstellen. Die Scanprofile verwenden jeweils unterschiedliche [Parameter für das ThreatSense-Modul](#).

[Profilliste](#)

Klicken Sie auf **Bearbeiten**, um ein neues Profil zu erstellen. Geben Sie einen Namen für das Profil ein und klicken Sie auf **Hinzufügen**. Das neue Profil wird im Dropdownmenü **Ausgewähltes Profil** neben den vorhandenen Scanprofilen angezeigt.

[Scanziele](#)

Wenn nur ein bestimmtes Objekt gescannt werden soll, können Sie auf **Bearbeiten** klicken und eine Option im Dropdownmenü oder bestimmte Objekte aus der Ordnerstruktur auswählen.

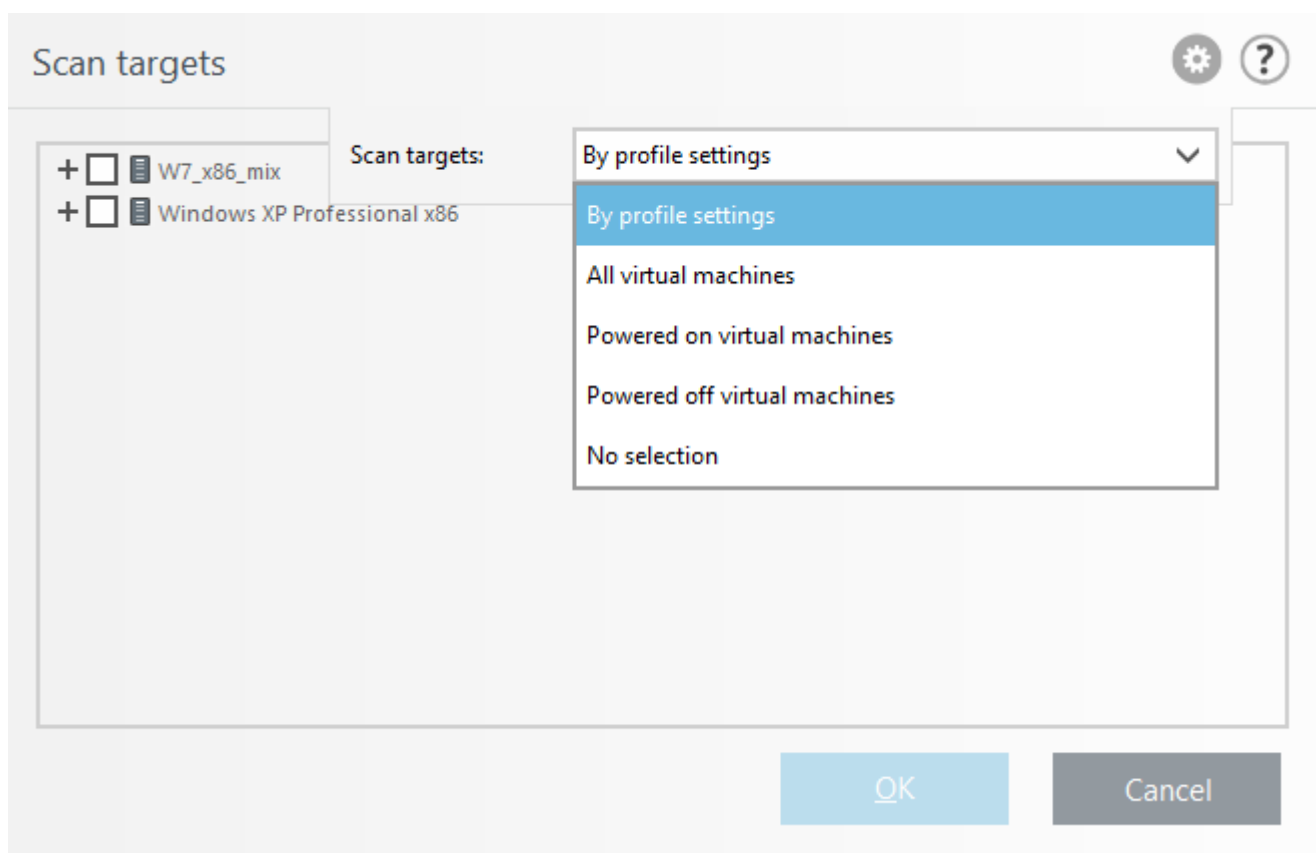
[ThreatSense-Parameter](#)

Hier können Sie die Einstellungen für den On-Demand-Scanner ändern.

[On-Demand- & Machine-Learning-Schutz](#)

Die Berichterstellung wird von der Erkennungsroutine und der Machine-Learning-Komponente ausgeführt.

Popupfenster **Hyper-V-Scan**:



Im Dropdownmenü **Scanziele** für **Hyper-V** können Sie vordefinierte Scanziele auswählen:

Nach Profileinstellungen	Die im Scanprofil ausgewählten Ziele werden verwendet.
Alle virtuellen Computer	Wählt alle virtuellen Computer aus.
Eingeschaltete virtuelle Computer	Wählt alle Online-VMs aus.
Ausgeschaltete virtuelle Computer	Wählt alle Offline-VMs aus.
Keine Auswahl	Löscht die bisherige Auswahl.

Klicken Sie auf **Scannen**, um den Scanvorgang mit den von Ihnen festgelegten Parametern auszuführen. Sehen Sie nach Abschluss der Scans unter **Log-Dateien** > [Hyper-V-Scan](#) nach.

Profilmanager

Im Dropdownmenü **Scanprofil** können Sie vordefinierte Scanprofile auswählen:

- **Smart-Prüfung**
- **Prüfung in Kontextmenüs**
- **Tiefenprüfung**
- **Mein Profil** (gilt für [Hyper-V-Scan](#), [Updateprofile](#))

Eine Beschreibung der einzelnen Scan-Profile finden Sie im Abschnitt [Einstellungen für ThreatSense](#). So können Sie ein Scan-Profil erstellen, das auf Ihre Anforderungen zugeschnitten ist.

Der Profilmanager wird an drei Stellen in ESET Security for Microsoft SharePoint verwendet.

On-Demand-Prüfung

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

[Update](#)

Mit dem Profil-Editor können Benutzer neue Update-Profile erstellen. Es macht nur dann Sinn, benutzerdefinierte Updateprofile zu erstellen, wenn Ihr Computer sich auf mehrere Arten mit den Updateservern verbindet.

[Hyper-V-Scan](#)

Erstellen Sie ein neues Profil, indem Sie neben **Profilliste** auf **Bearbeiten** klicken. Das neue Profil wird im Dropdownmenü **Ausgewähltes Profil** neben den vorhandenen Scanprofilen angezeigt.

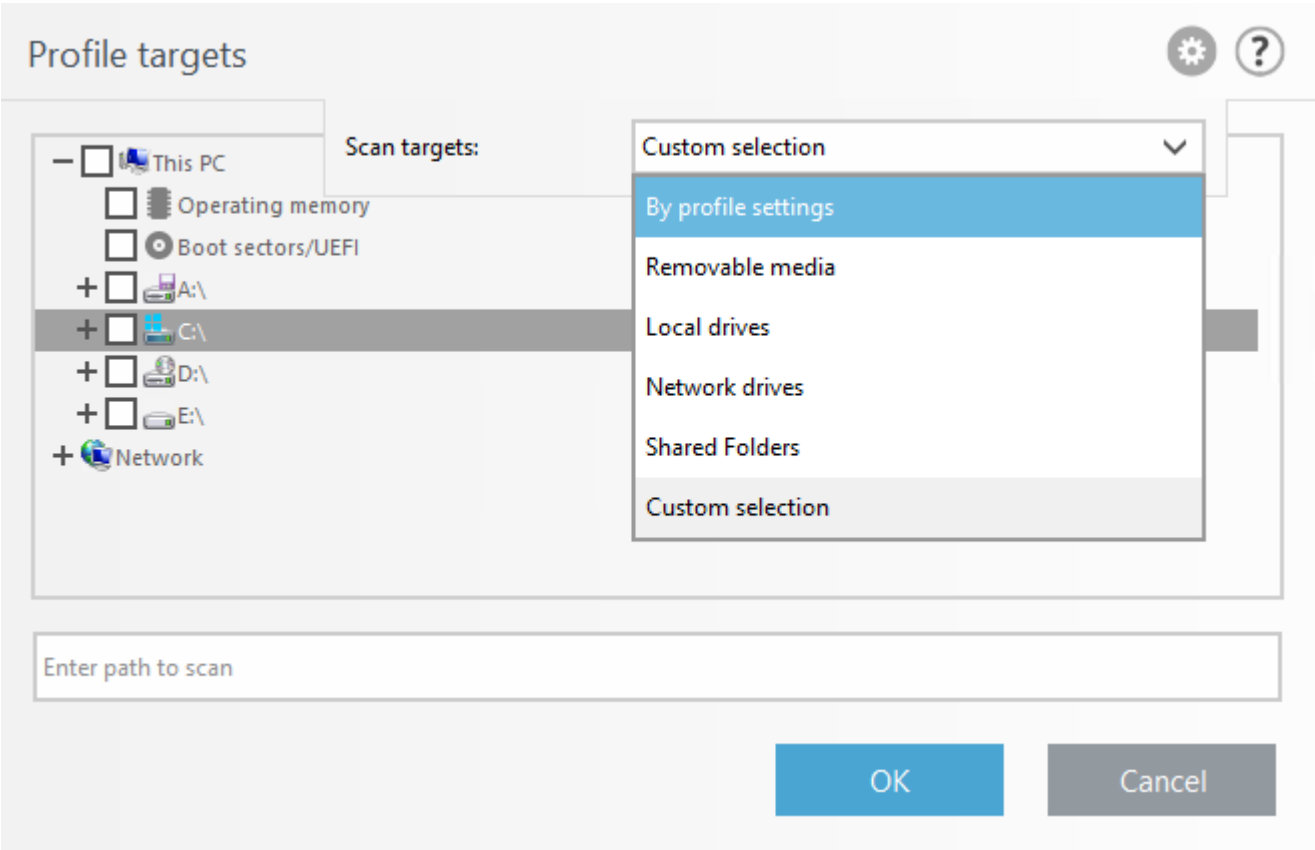
Profil-Ziele

Sie können die Ziele festlegen, die auf Schadcode gescannt werden. Wählen Sie Objekte (Arbeitsspeicher, Bootsektoren und UEFI, Laufwerke, Dateien und Ordner oder Netzwerk) in der Baumstruktur aus, die alle verfügbaren Ziele auf Ihrem System enthält.

HINWEIS

Diese Scanprofil-Auswahl gilt für **On-Demand**- und für [Hyper-V-Scans](#).

Klicken Sie auf das Zahnradsymbol in der oberen linken Ecke, um die Dropdownmenüs **Scanziele** und **Scanprofil** zu öffnen.



Im Dropdownmenü **Scanziele** können Sie ein vordefiniertes Scanziele auswählen:

Nach Profileinstellungen	Die im Scanprofil ausgewählten Ziele werden verwendet.
Wechselmedien	Disketten, USB-Speichergeräte, CDs/DVDs.
Lokale Laufwerke	Alle lokalen Systemlaufwerke.
Netzlaufwerke	Alle zugeordneten Netzlaufwerke.
Freigegebene Ordner	Alle freigegebenen Ordner auf dem lokalen Server.
Benutzerdefinierte Auswahl	Hebt die gesamte Auswahl auf. Anschließend können Sie Ihre eigene Auswahl treffen.

Geben Sie den Pfad eines Scanziels (Datei oder Ordner) in das Textfeld unter der Baumstruktur ein, um schnell zum entsprechenden Ziel zu navigieren und es zum Scan hinzuzufügen. Die Pfadangabe unterscheidet zwischen Groß- und Kleinschreibung.

Im Dropdownmenü **Scanprofil** können Sie vordefinierte Scanprofile auswählen:

- **Smart-Prüfung**
- **Prüfung in Kontextmenüs**
- **Tiefenprüfung**

Diese Scanprofile verwenden jeweils unterschiedliche [ThreatSense-Einstellungen](#).

Prüfungsfortschritt anzeigen

Wenn Sie nur das System ohne zusätzliche Säuberung prüfen möchten, wählen Sie die Option **Nur prüfen**,

keine Aktion. Auf diese Weise können Sie feststellen, ob Infektionen vorliegen und ggf. Details zu den Infektionen herausfinden. Außerdem können Sie zwischen drei Säuberungsstufen wählen. Klicken Sie dazu auf **Einstellungen > ThreatSense -Parameter > Säubern**. Die Informationen zur Prüfung werden in einem Log gespeichert.

Prüfen, ohne zu säubern

Wenn Sie **Ausschlüsse ignorieren** auswählen, können Sie einen Scan ohne die [Ausschlüsse](#) durchführen, die normalerweise gelten würden.

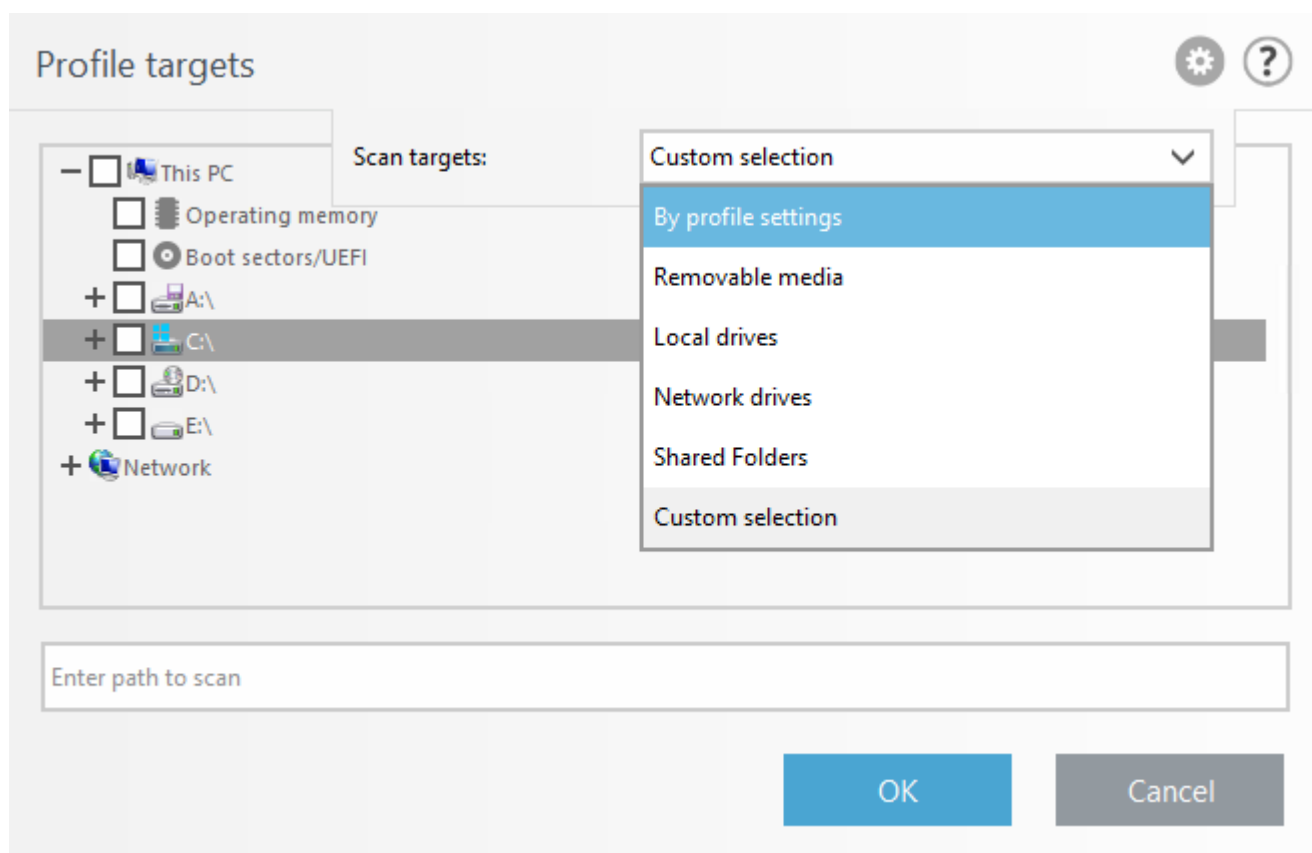
Scanziele

Wenn Sie nur bestimmte Objekte prüfen möchten, verwenden Sie die **benutzerdefinierte Prüfung** und wählen Sie die zu prüfenden Objekte im Dropdownmenü **Scan-Ziele** oder in der Ordnerstruktur (Baumstruktur) aus.

Die Auswahl der Scan-Ziele gilt für:

- [On-Demand-Scan](#)
- [Hyper-V-Scan](#)

Um schnell zu einem zu prüfenden Objekt zu navigieren oder um ein neues Ziel (Ordner oder Dateien) hinzuzufügen, geben Sie den Pfad in das leere Textfeld unter der Ordnerliste ein. Dies ist nur möglich, wenn keine Objekte aus der Baumstruktur zur Prüfung ausgewählt wurden und im Menü **Prüfziele** die Option **Keine Auswahl** festgelegt ist.



Im Dropdownmenü **Scan-Ziele** können Sie vordefinierte Scanziele auswählen.

Nach Profileinstellungen	Die im Scanprofil ausgewählten Ziele werden verwendet.
Wechselmedien	Disketten, USB-Speichergeräte, CDs/DVDs.
Lokale Laufwerke	Alle lokalen Systemlaufwerke.
Netzlaufwerke	Alle zugeordneten Netzlaufwerke.
Freigegebene Ordner	Alle freigegebenen Ordner auf dem lokalen Server.
Benutzerdefinierte Auswahl	Hebt die gesamte Auswahl auf. Anschließend können Sie Ihre eigene Auswahl treffen.

Im Dropdownmenü [Scan-Profil](#) können Sie ein Profil auswählen, um ausgewählte Objekte zu prüfen. Das Standardprofil ist **Smart-Scan**. Es stehen außerdem zwei weitere vordefinierte Prüfprofile zur Verfügung: **Tiefenprüfung** und **Kontextmenü-Prüfung**. Diese Prüfprofile verwenden unterschiedliche [Parameter für das ThreatSense-Modul](#).

Popupfenster **Benutzerdefinierter Scan**:

The screenshot shows a 'Computer scan' dialog box. On the left, there is a tree view of scan targets. The top level is 'This PC' (unchecked). Below it are 'Operating system' (unchecked), 'Boot sectors/L' (unchecked), and a list of drives: 'A:\', 'C:\', 'D:\', 'E:\' (all unchecked), and 'Network' (checked). On the right side, there are two dropdown menus: 'Scan targets' set to 'By profile settings' and 'Scan profile' set to 'Smart scan'. Below these are two checkboxes: 'Scan without cleaning' (unchecked) and 'Ignore exclusions' (unchecked). At the bottom, there is a text input field labeled 'Enter path to scan' and two buttons: 'Scan' (light blue) and 'Cancel' (grey).

Prüfungsfortschritt anzeigen

Wenn Sie nur das System ohne zusätzliche Säuberung prüfen möchten, wählen Sie die Option **Nur prüfen, keine Aktion**. Auf diese Weise können Sie feststellen, ob Infektionen vorliegen und ggf. Details zu den Infektionen herausfinden. Außerdem können Sie zwischen drei Säuberungsstufen wählen. Klicken Sie dazu auf **Einstellungen > ThreatSense -Parameter > Säubern**. Die Informationen zur Prüfung werden in einem Log gespeichert.

Prüfen, ohne zu säubern

Führt einen Scan ohne die [Ausschlüsse](#) durch, die normalerweise gelten würden.

Prüfen

Führt die Prüfung mit den von Ihnen festgelegten Parametern aus.

Als Administrator prüfen

Führt die Prüfung mit dem Administratorkonto aus. Wählen Sie diese Option, wenn der aktuell angemeldete Benutzer keine ausreichenden Zugriffsrechte für die zu scannenden Dateien hat. Diese Schaltfläche ist nur verfügbar, wenn der aktuell angemeldete Benutzer UAC-Vorgänge als Administrator aufrufen kann.

Scan im Leerlaufbetrieb

Wenn der Computer im Leerlauf ist, wird auf allen lokalen Festplatten eine Prüfung ausgeführt. Die **Prüfung im Leerlaufbetrieb** wird in den folgenden Computerzuständen ausgeführt:

- **Bildschirm ausgeschaltet oder Bildschirmschoner**
- **Computersperre**
- **Benutzerabmeldung**

Auch ausführen, wenn der Computer im Akkubetrieb läuft

Diese Prüfung wird nicht ausgeführt, wenn sich der Computer (Notebook) im Batteriebetrieb befindet.

Logging aktivieren

Legt das Ergebnis eines Computer-Scans in den [Log-Dateien](#) ab (Klicken Sie im Hauptprogrammfenster auf „Log-Dateien“ und wählen Sie „Computer-Scan“ im Dropdownmenü „Log“ aus).

[ThreatSense-Parameter](#)

Ändern Sie die Einstellungen für das Scannen im Leerlaufbetrieb.

Prüfung der Systemstartdateien

Die automatische Prüfung der Systemstartdateien wird standardmäßig beim Systemstart (Benutzeranmeldung) und nach einem erfolgreichen Modulupdate ausgeführt. Die Ausführung des Scans ist abhängig davon, wie der [Taskplaner](#) konfiguriert ist und welche Tasks eingerichtet wurden.

Die Optionen für die Prüfung der Systemstartdateien sind Bestandteil des Tasks **Prüfung der Systemstartdateien**.

Navigieren Sie zu **Tools > [Taskplaner](#)**, wählen Sie einen der Tasks mit dem Namen **Prüfung Systemstartdateien** (Benutzeranmeldung oder Modulupdate) aus und klicken Sie auf **Bearbeiten**. Wenn Sie sich durch den Assistenten klicken, können Sie im letzten Schritt ausführliche Optionen für die [Prüfung der Systemstartdateien](#) konfigurieren.

Prüfung Systemstartdateien

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

Im Dropdown-Menü Prüfziel können Sie die Prüftiefe für Dateien festlegen, die beim Systemstart ausgeführt

werden. Die Dateien werden auf Grundlage der folgenden Kriterien in aufsteigender Reihenfolge sortiert:

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

Außerdem stehen zwei besondere Gruppen als Prüfziel zur Verfügung:

Vor der Benutzeranmeldung ausgeführte Dateien

Enthält Dateien von Standorten, auf die ohne Benutzeranmeldung zugegriffen werden kann (nahezu alle Systemstartstandorte wie Dienste, Browserhilfsobjekte, Windows-Anmeldungshinweise, Einträge im Windows-Taskplaner, bekannte DLL-Dateien usw.).

Nach der Benutzeranmeldung ausgeführte Dateien

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 scannenden Dateien ist für jede der zuvor genannten Gruppen unveränderbar.

Scan-Priorität

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

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

Wechselmedien

ESET Security for Microsoft SharePoint bietet automatische Prüfmethode für Wechselmedien (CD/DVD/USB). Dieses Modul ermöglicht das Einrichten eines Scans für eingelegte Medien. Dies ist sinnvoll, wenn der Administrator verhindern möchte, dass Benutzer Wechselmedien mit unerwünschten Inhalten verwenden.

Aktion nach Einlegen von Wechselmedien

Wählen Sie die Aktion aus, die beim Einsetzen von Wechseldatenträgern (CD/DVD/USB) in den Computer ausgeführt werden soll.

- **Nicht scannen** - Es wird keine Aktion ausgeführt und das Fenster **Neues Gerät erkannt** wird geschlossen.
- **Automatischer Gerätescan** - Eine On-Demand-Prüfung des eingelegten Wechselmediums wird durchgeführt.
- **Scanoptionen anzeigen** - Öffnet die Einstellungen für Wechselmedien.

Beim Einlegen eines Wechselmediums wird folgender Dialog angezeigt:

- **Jetzt scannen** - Dies löst den Wechselmedienscan aus.

- **Später scannen** - Der Wechselmedienscan wird auf einen späteren Zeitpunkt verschoben.
- **Einstellungen** - Öffnet die erweiterten Einstellungen.
- **Immer die ausgewählte Option verwenden** - Wenn diese Option aktiviert ist, wird bei jedem Einlegen eines Wechselmediums die gleiche Aktion ausgeführt.

Außerdem enthält ESET Security for Microsoft SharePoint die Gerätesteuerung, mit der Sie Regeln für die Nutzung externer Geräte mit einem bestimmten Computer festlegen können. Weitere Informationen zur Medienkontrolle finden Sie im Abschnitt [Medienkontrolle](#).

Dokumentenschutz

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

Systemintegration

Diese Option verbessert den Schutz von Microsoft Office-Dokumenten (unter normalen Umständen nicht benötigt).

ThreatSense-Parameter

Ändern Sie die Parameter für den Dokumentenschutz.

HINWEIS

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

Hyper-V-Scan

Die aktuelle Version des Hyper-V-Scans unterstützt Scanvorgänge von virtuellen Systemen in Hyper-V im Online- oder Offlinezustand. Die unterstützten Scantypen hängen vom gehosteten Hyper-V-System und vom Zustand des virtuellen Systems ab:

Virtuelle Systeme mit Hyper-V-Funktion	Windows Server 2008 R2 SP1 Hyper-V	Windows Server 2012 Hyper-V	Windows Server 2012 R2 Hyper-V	Windows Server 2016 Hyper-V	Windows Server 2019 Hyper-V
Online-VM	Keine Prüfung	Schreibgeschützt	Schreibgeschützt	Schreibgeschützt	Schreibgeschützt
Offline-VM	Schreibgeschützt/säubern	Schreibgeschützt/säubern	Schreibgeschützt/säubern	Schreibgeschützt/säubern	Schreibgeschützt/säubern

Hardwareanforderungen

Der Server darf keine Performanceprobleme bei der Ausführung virtueller Computer haben. Der Scan verwendet hauptsächlich CPU-Ressourcen. Zum Scannen von Online-VMs wird freier Festplattenplatz benötigt. Es wird mindestens der doppelte freie Speicherplatz benötigt, der von Checkpoints/Snapshots und virtuellen Laufwerken belegt wird.

Spezielle Einschränkungen

- Prüfungen in RAID-Speichern, übergreifenden Volumes und [dynamischen Datenträgern](#)  werden

aufgrund der Funktionsweise dynamischer Datenträger nicht unterstützt. Daher sollten Sie den Einsatz dynamischer Datenträger in Ihren VMs nach Möglichkeit vermeiden.

- Der Scan wird immer für die aktuelle VM ausgeführt. Checkpoints und Snapshots sind nicht betroffen.
- Hyper-V auf Hosts in einem Cluster wird momentan von ESET Security for Microsoft SharePoint nicht unterstützt.
- Virtuelle Computer auf Hyper-V-Hosts unter Windows Server 2008 R2 SP1 können nur im schreibgeschützten Modus geprüft werden (keine Säuberung), unabhängig von der in den [ThreatSense-Parametern](#) ausgewählten Säuberungsstufe.

HINWEIS

Die ESET-Sicherheitsprodukte unterstützen zwar Prüfungen des MBR für virtuelle Datenträger, allerdings können diese Prüfungen für diese Ziele nur im schreibgeschützten Modus durchgeführt werden. Sie finden diese Einstellung unter **Erweiterte Einstellungen (F5) > Computer > Hyper-V-Scan > [ThreatSense-Parameter](#) > Bootsektoren**.

Zu prüfender virtueller Computer ist offline - (ausgeschaltet)

ESET Security for Microsoft SharePoint verwendet den Hyper-V-Manager, um virtuelle Datenträger zu erkennen und zu verbinden. Auf diese Weise hat ESET Security for Microsoft SharePoint denselben Zugriff auf den Inhalt der virtuellen Laufwerke wie beim Zugriff auf Daten und Dateien auf herkömmlichen Laufwerken.

Zu prüfender virtueller Computer ist online - (in Betrieb, angehalten, gespeichert)

ESET Security for Microsoft SharePoint verwendet den Hyper-V-Manager, um virtuelle Datenträger zu erkennen. Eine Verbindung zu diesen Datenträgern ist nicht möglich. Daher erstellt ESET Security for Microsoft SharePoint einen Checkpoint/Snapshot der virtuellen Maschine und verbindet sich anschließend mit diesem Checkpoint/Snapshot. Nach Abschluss der Prüfung wird der Checkpoint/Snapshot gelöscht. In diesem Fall wird also eine schreibgeschützte Prüfung durchgeführt, da die laufenden virtuellen Maschinen nicht von der Prüfung betroffen sind.

Warten Sie ca. eine Minute, bis ESET Security for Microsoft SharePoint beim Scannen einen Snapshot bzw. Checkpoint erstellt hat. Berücksichtigen Sie dies, wenn Sie Hyper-V-Scans für eine große Anzahl virtueller Computer planen.

Namenskonvention

Das Modul für die Hyper-V-Scan verwendet die folgende Namenskonvention:

`VirtualMachineName\DiskX\VolumeY`

Wobei X die Nummer des Laufwerks und Y die Nummer des Volumes ist. Beispiel:

`Computer\Disk0\Volume1`

Die Zahlen werden in der Reihenfolge der Erkennung angefügt. Diese Reihenfolge stimmt mit der Reihenfolge im Manager für virtuelle Datenträger überein. Die Namenskonvention wird in der Baumstruktur der Prüfziele, in der Fortschrittsleiste und in den Log-Dateien verwendet.

Ausführung einer Prüfung

- [On-Demand](#) - Klicken Sie auf **Hyper-V-Prüfung**, um eine Liste der für die Prüfung verfügbaren virtuellen

Computer und Laufwerke anzuzeigen. Wählen Sie die gewünschten VMs, Laufwerke oder Volumes für den Scanvorgang aus und klicken Sie auf **Scannen**.

- So erstellen Sie einen [Taskplaner-Task](#).
- Über ESET Security Management Center in Form eines Clienttasks mit dem Namen [Serverprüfung](#) [↗](#).
- Sie können Hyper-V-Scans in [eShell](#) verwalten und starten.

Sie können mehrere Hyper-V-Scans parallel ausführen. Nach Abschluss der Scans wird eine Benachrichtigung mit einem Link zu den Log-Dateien angezeigt.

Mögliche Probleme

- Beim Scannen eines aktiven virtuellen Computers wird ein Checkpoint/Snapshot des jeweiligen virtuellen Computers erstellt. Während der Erstellung von Checkpoint/Snapshot sind möglicherweise einige allgemeine Aktionen des virtuellen Computers eingeschränkt oder deaktiviert.
- Inaktive virtuelle Computer können nicht eingeschaltet werden, solange eine Prüfung ausgeführt wird.
- Im Hyper-V Manager können Sie zwei virtuelle Computer mit identischem Namen anlegen. Dies kann zu Problemen bei der Unterscheidung der Computer in den Prüf-Logs führen.

HIPS

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 ausgeführten 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.

WARNUNG

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


Selbstschutz aktivieren

ESET Security for Microsoft SharePoint enthält eine integrierte Selbstschutz-Technologie, um zu verhindern, dass Ihr Viren- und Spyware-Schutz durch Malware beschädigt oder deaktiviert werden kann und um Ihr System ununterbrochen zu schützen. Änderungen an den Optionen „HIPS aktivieren“ und „Selbstschutz aktivieren“ treten nach einem Neustart des Windows-Betriebssystems in Kraft. Zum Deaktivieren von HIPS ist ebenfalls ein Computer-Neustart erforderlich.


Protected Service aktivieren

Microsoft hat mit Microsoft Windows Server 2012 R2 das neue Konzept der geschützten Dienste eingeführt, um Dienste vor Angriffen durch Schadsoftware zu schützen. Der Kernel von ESET Security for Microsoft SharePoint wird standardmäßig als geschützter Dienst ausgeführt. Diese Funktion ist unter Microsoft Windows Server 2012 R2 und neueren Betriebssystemen verfügbar.


Advanced Memory Scanner aktivieren

Diese Funktion bietet zusammen mit dem Exploit-Blocker einen noch besseren Schutz vor Malware, die darauf ausgelegt ist, der Erkennung durch Anti-Malware-Produkte mittels Verschleierung oder Verschlüsselung zu entgehen. Das Advanced Memory Scanner ist standardmäßig aktiviert. Weitere Informationen zu diesem Schutztyp finden Sie in unserem [Glossar](#) .

Exploit-Blocker aktivieren

Sichert besonders anfällige Anwendungstypen wie Webbrowser, PDF-Leseprogramme, E-Mail-Programme und MS Office-Komponenten. Der Exploit-Blocker ist standardmäßig aktiviert. Weitere Informationen zu diesem Schutztyp finden Sie in unserem [Glossar](#) .

Ransomware-Schutz aktivieren

Aktivieren Sie HIPS und ESET Live Grid, um diese Funktion zu verwenden. Weitere Informationen zu Ransomware finden Sie im [Glossar](#) .

Filtermodus

Wählen Sie einen der folgenden Filtermodi aus:

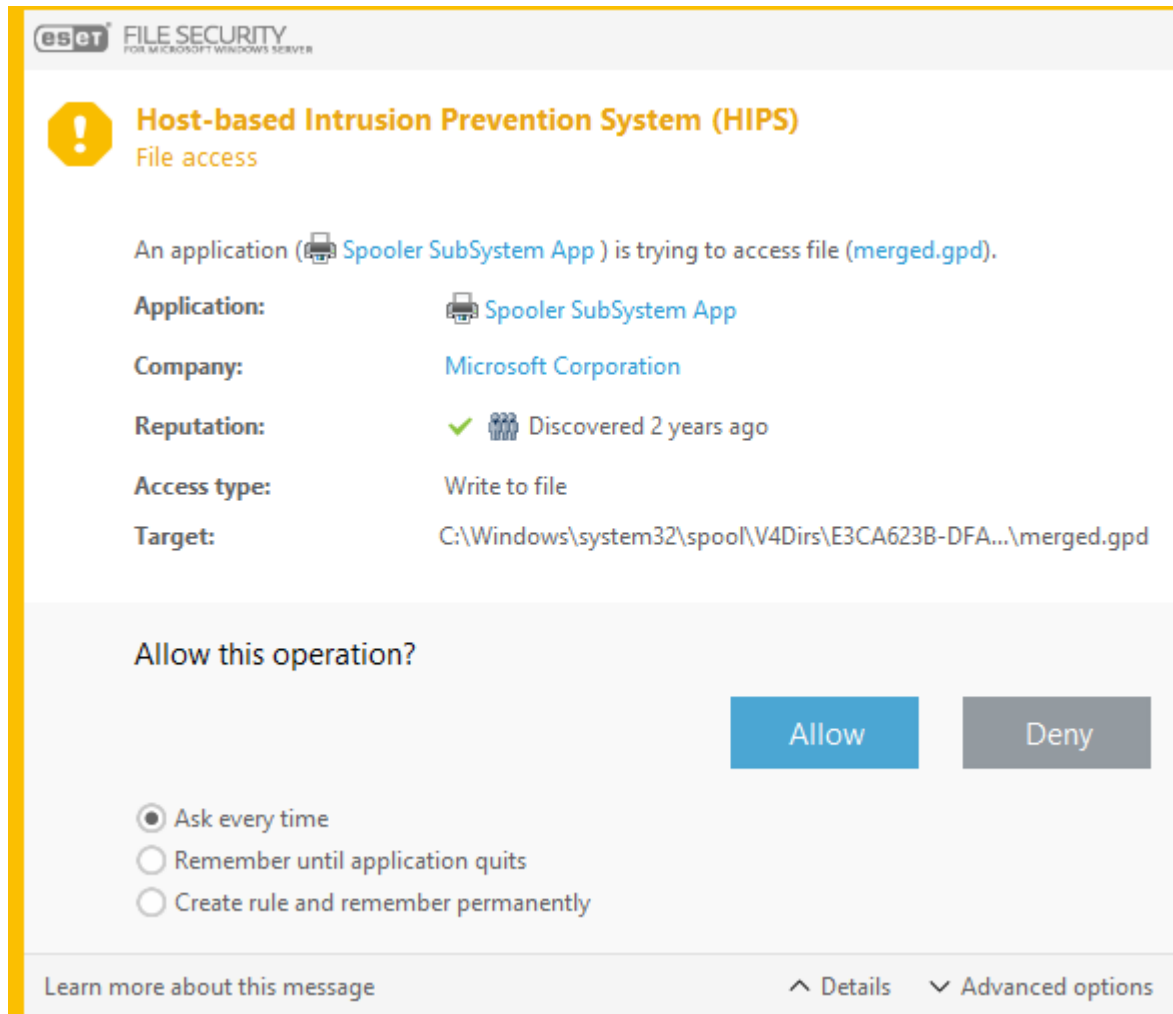
- **Automatischer Modus** - Vorgänge werden ausgeführt, mit Ausnahme der Vorgänge, die durch vordefinierte Regeln zum Schutz Ihres Systems blockiert wurden. Alle Vorgänge sind erlaubt, mit Ausnahme von Aktionen, die durch eine Regel blockiert werden.
- **Smart-Modus** - Der Benutzer wird nur über sehr verdächtige Ereignisse benachrichtigt.
- **Interaktiver Modus** - Der Benutzer wird zur Bestätigung von Vorgängen aufgefordert. Zugriff erlauben / verweigern, Regel erstellen, Diese Aktion vorübergehend anwenden.
- **Policy-basierter Modus** - Vorgänge werden blockiert. Akzeptiert nur Benutzer- oder vordefinierte Regeln.
- **Trainingsmodus** - Vorgänge werden ausgeführt und nach jedem Vorgang wird eine Regel erstellt. Die in diesem Modus erstellten Regeln können im Regel-Editor angezeigt werden, doch sie haben geringere Priorität als manuell erstellte Regeln oder Regeln, die im automatischen Modus erstellt wurden. Wenn Sie im Dropdownmenü für den HIPS-Filtermodus den **Trainingsmodus** auswählen, wird die Einstellung **Ende des Trainingsmodus** verfügbar. Wählen Sie eine Dauer für den Trainingsmodus aus. Die maximale Dauer ist 14 Tage. Wenn die festgelegte Dauer verstrichen ist, werden Sie aufgefordert, die von HIPS im Trainingsmodus erstellten Regeln zu bearbeiten. Sie können auch einen anderen Filtermodus auswählen oder die Entscheidung verschieben und den Trainingsmodus weiterverwenden.

Regeln

Regeln legen fest, welche Anwendungen auf welche Dateien, Registrierungsbereiche oder andere Anwendungen zugreifen dürfen. HIPS überwacht Ereignisse im Betriebssystem und führt Aktionen gemäß Regeln aus, die den Regeln für die Personal Firewall ähneln. Klicken Sie auf [Bearbeiten](#), um das Fenster für die HIPS-Regelverwaltung zu öffnen. Wenn die Standardaktion zu einer Regel **Nachfragen** lautet, 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 festlegen, wird gemäß den Regeln eine neue Aktion ausgewählt.

Im Dialogfenster können Sie eine Regel erstellen, die auf einer beliebigen neuen Aktion basiert, die HIPS erkennt. Definieren Sie dann die Bedingungen, unter denen die Aktion **zugelassen** oder **blockiert** werden soll. Unter **Details** finden Sie weitere Informationen. Auf diese Weise erstellte Regeln und manuell erstellte Regeln sind

gleichrangig. Daher können erstere allgemeiner sein als die Regel, die das Dialogfenster ausgelöst hat. Nach dem Erstellen einer solchen Regel kann derselbe Vorgang also dasselbe Fenster auslösen.



Jedes Mal fragen

Bei jedem Auslösen der Regel wird ein Dialogfeld angezeigt. Dort können Sie den Vorgang entweder **Blockieren** oder **Zulassen**.

Bis zum Beenden der Anwendung merken

Wenn Sie eine der Aktionen **Blockieren** oder **Zulassen** auswählen, wird eine temporäre HIPS-Regel erstellt und verwendet, bis die entsprechende Anwendung geschlossen wird. Wenn Sie den Filtermodus ändern, Regeln bearbeiten oder das HIPS-Modul aktualisieren und Ihr System neu starten, werden die temporären Regeln ebenfalls gelöscht.

Regel erstellen und dauerhaft merken

Erstellt eine neue HIPS-Regel. Sie können diese Regel später in der HIPS-Regelverwaltung bearbeiten.

HIPS-Regeleinstellungen

Dieses Fenster enthält eine Übersicht vorhandener HIPS-Regeln.

Regel	Benutzerdefinierter oder automatisch ausgewählter Regelname.
Aktiviert	Deaktivieren Sie diesen Schalter, wenn Sie die Regel nicht verwenden, jedoch nicht aus der Liste löschen möchten.
Aktion	Die Regel legt eine Aktion fest (Zulassen , Blockieren oder Fragen), die bei Eintreten der Bedingungen ausgeführt wird.
Quellen	Die Regel wird nur angewendet, wenn das Ereignis von einer Anwendung ausgelöst wird.
Ziele	Die Regel wird nur angewendet, wenn sich die Operation auf eine bestimmte Datei, eine Anwendung oder einen Registrierungseintrag bezieht.
Log-Schweregrad	Wenn Sie diese Option aktivieren, werden Informationen zu dieser Regel im HIPS-Log gespeichert.
Hinweis anzeigen	In der rechten unteren Ecke wird ein kleines Fenster angezeigt, wenn ein Ereignis ausgelöst wird.

Erstellen Sie eine neue Regeln, indem Sie auf **Hinzufügen** klicken und neue HIPS-Regeln erstellen, oder **Bearbeiten** Sie ausgewählte Einträge.

Regelname

Benutzerdefinierter oder automatisch ausgewählter Regelname.

Aktion

Die Regel legt eine Aktion fest (**Zulassen**, **Blockieren** 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. Die Regel besteht aus mehreren Teilen, mit denen die Auslösebedingungen der Regel beschrieben werden.

Quellanwendungen

Die Regel wird nur angewendet, wenn das Ereignis von der jeweiligen Anwendung ausgelöst wird. Wählen Sie **Bestimmte Anwendungen** im Dropdownmenü aus und klicken Sie auf **Hinzufügen**, um neue Dateien oder Ordner hinzuzufügen, oder wählen Sie den Eintrag **Alle Anwendungen** aus, um alle Anwendungen hinzuzufügen.

HINWEIS

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

Beschreibungen der wichtigsten Vorgänge:

Dateibezogene Vorgänge:

Datei löschen	Anwendung versucht, die Zieldatei zu löschen.
In Datei schreiben	Anwendung versucht, in die Zieldatei zu schreiben.

Datei löschen	Anwendung versucht, die Zieldatei zu löschen.
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, Festplattenvolumen zu reorganisieren.
Globalen Hook installieren	Bezieht sich auf das Aufrufen der Funktion SetWindowsHookEx aus der MSDN-Bibliothek.
Treiber laden	Lädt und installiert Treiber im System.

Die Regel wird nur angewendet, wenn sich der Vorgang auf dieses Ziel bezieht. Wählen Sie die Option **Bestimmte Dateien** im Dropdownmenü aus und klicken Sie auf **Hinzufügen**, um neue Dateien oder Ordner hinzuzufügen, oder wählen Sie **Alle Dateien** aus, um alle Anwendungen hinzuzufügen.

Anwendungsbezogene Vorgänge:

Andere Anwendung debuggen	Verknüpfen eines Debuggers mit dem Prozess. Beim Debuggen einer Anwendung können Informationen zu deren Verhalten angezeigt und verändert werden, und die Daten der Anwendung sind verfügbar.
Ereignisse von anderer Anwendung abfangen	Die Quellanwendung versucht, für die Zieldanwendung bestimmte Ereignisse abzufangen (Beispiel: ein Keylogger versucht, Ereignisse im Browser aufzuzeichnen).
Andere Anwendung beenden/unterbrechen	Die Anwendung unterbricht einen Prozess, setzt ihn fort oder beendet ihn (direkter Zugriff aus dem Prozess-Explorer oder im Fenster „Prozesse“ möglich).
Neue Anwendung starten	Starten neuer Anwendungen oder neuer Prozesse.
Zustand einer anderen Anwendung ändern	Die Quellanwendung versucht, in den Speicher der Zieldanwendung zu schreiben oder in ihrem Namen bestimmten Code auszuführen. Diese Funktion kann wichtige Anwendungen schützen, indem diese in einer Regel zum Blockieren des Vorgangs als Zieldanwendungen konfiguriert werden.

Die Regel wird nur angewendet, wenn sich der Vorgang auf dieses Ziel bezieht. Wählen Sie die Option **Bestimmte Anwendungen** im Dropdownmenü aus und klicken Sie auf **Hinzufügen**, um neue Dateien oder Ordner hinzuzufügen, oder wählen Sie **Alle Anwendungen** aus, um alle Anwendungen hinzuzufügen.

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.
Aus Registrierung löschen	Registrierungsschlüssel oder -wert löschen.
Registrierungsschlüssel umbenennen	Umbenennen von Registrierungsschlüsseln.
Registrierung ändern	Neue Werte für Registrierungsschlüssel erstellen, vorhandene Werte ändern, Daten im Verzeichnisbaum der Datenbank verschieben oder Benutzer- bzw. Gruppenrechte für Registrierungsschlüssel einrichten.

Die Regel wird nur angewendet, wenn sich der Vorgang auf dieses Ziel bezieht. Wählen Sie **bestimmte Einträge** im Dropdownmenü aus und klicken Sie auf **Hinzufügen**, um neue Dateien oder Ordner hinzuzufügen, oder wählen Sie **Alle Einträge** aus, um alle Anwendungen hinzuzufügen.

HINWEIS

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 zwar „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. | * in einem Registrierungspfad bedeutet „dieser Pfad oder jeder untergeordnete Pfad nach diesem Symbol“. Platzhalter können nur auf diese Weise für Zieldateien verwendet werden. Zuerst wird der spezifische Teil des Pfades überprüft, dann der Pfad nach dem Platzhalter (*).

WARNUNG

Sie erhalten eine Benachrichtigung, wenn Sie eine zu allgemeine Regel erstellen.

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. In dieser Liste angezeigte Treiber werden unabhängig vom HIPS-Filtermodus immer zugelassen, sofern sie nicht ausdrücklich durch eine Benutzerregel blockiert werden. Sie können neue Treiber **hinzufügen** oder ausgewählte Treiber in dieser Liste **bearbeiten** oder **löschen**.

HINWEIS

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

Alle blockierten Vorgänge in Log aufnehmen

Alle blockierten Vorgänge werden in das HIPS-Log geschrieben.

Änderungen an Autostart-Einträgen melden

Zeigt einen Desktophinweis an, wenn eine Anwendung vom Systemstart entfernt bzw. zum Systemstart hinzugefügt wird.

Update-Konfiguration

Dieser Abschnitt beschreibt Quellinformationen für Updates wie die verwendeten Updateserver und die Authentifizierungsdaten für diese Server.

HINWEIS

Um Updates fehlerfrei herunterladen zu können, müssen Sie alle Update-Einstellungen ordnungsgemäß eingeben. Falls Sie eine Firewall verwenden, stellen Sie sicher, dass sich das ESET-Programm mit dem Internet verbinden darf (zum Beispiel per HTTP).

[Einfach](#)

Standardupdateprofil auswählen

Wählen Sie ein Standardprofil für Updates aus, oder erstellen Sie ein neues Profil.

Update-Cache löschen

Wenn Probleme mit einem Update auftreten, klicken Sie auf **Löschen**, um den temporären Update-Cache zu leeren.

Maximales Alter der Erkennungsroutine automatisch festlegen / Maximales Alter der Erkennungsroutine (Tage)

Hier können Sie eine Zeitdauer in Tagen festlegen, nach der die Erkennungsroutine als veraltet gemeldet wird. Der Standardwert ist 7.

Modul-Rollback

Wenn Sie befürchten, dass ein neues Update der Erkennungsroutine oder der Programmmodule beschädigt oder nicht stabil ist, können Sie einen Rollback zur vorigen Version ausführen und Updates für einen bestimmten Zeitraum deaktivieren. Hier können Sie auch zuvor für einen unbegrenzten Zeitraum deaktivierte Updates wieder aktivieren. ESET Security for Microsoft SharePoint zeichnet Snapshots der Erkennungsroutine und der Programmmodule zur späteren Verwendung mit der [Rollback](#)-Funktion auf. Um Snapshots der Erkennungsroutine zu erstellen, lassen Sie die Option **Snapshots der Module erstellen** aktiviert.

Anzahl der lokal gespeicherten Snapshots

Definiert die Anzahl der gespeicherten älteren Modul-Snapshots.

[Profile](#)

Um ein benutzerdefiniertes Updateprofil zu erstellen, wählen Sie **Bearbeiten** neben **Profilliste** aus, geben Sie einen **Profilnamen** ein, und klicken Sie auf **Hinzufügen**. Wählen Sie das zu bearbeitende Profil aus und bearbeiten Sie die Parameter für Arten von **Modulupdates**, oder erstellen Sie einen **Update-Mirror**.

[Updates](#)

Wählen Sie den Updatetyp im Dropdownmenü aus:

- **Reguläres Update** - Standardmäßig ist der Update-Typ auf Reguläres Update eingestellt. Mit dieser Option werden Updates automatisch von dem ESET-Server heruntergeladen, der am wenigsten belastet ist.
- **Testmodus** - Test-Updates wurden intern umfassend geprüft und werden demnächst veröffentlicht. 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.

- **Verzögerte Updates** - Diese Option führt Updates über besondere Update-Server aus, die neue Versionen der Signaturdatenbank mit einer Verzögerung von mindestens X Stunden zur Verfügung stellen. Die Datenbanken wurden also bereits in einer Produktionsumgebung getestet und sind daher stabil.

Vor dem Download von Updates fragen

Wenn ein neues Update verfügbar ist, erhalten Sie vor dessen Download eine Aufforderung.

Nachfragen, falls Update größer ist als (KB)

Wenn die Größe der Updatedatei den in diesem Feld angegebenen Wert überschreitet, wird eine Benachrichtigung angezeigt.

Benachrichtigungen über erfolgreiche Updates deaktivieren

Deaktiviert die Benachrichtigungen im Infobereich der Taskleiste rechts unten auf dem Bildschirm. Diese Option macht Sinn für Vollbildanwendungen. Im Präsentationsmodus werden keine Benachrichtigungen angezeigt.

Modulupdates

Modulupdates sind standardmäßig auf **Automatische Auswahl** eingestellt. Der Update-Server dient als Speicher für die Updates. Falls Sie einen ESET-Server verwenden, sollten Sie die Standardoption beibehalten.

Wenn Sie einen lokalen HTTP-Server (auch als „Update-Mirror“ bezeichnet) verwenden, konfigurieren Sie den Server wie folgt:

http://computername_oder_IP_adresse:2221

Wenn Sie einen lokalen HTTP-Server mit SSL verwenden, konfigurieren Sie den Server wie folgt:

https://computername_oder_IP_adresse:2221

Wenn Sie einen lokalen freigegebenen Ordner verwenden, konfigurieren Sie den Server wie folgt:

\\computername_oder_IP_adresse\freigegebener_ordner

Aktiviert häufigere Updates für Erkennungssignaturen

Die Erkennungsroutine wird in kürzeren Abständen aktualisiert. Wenn Sie diese Option deaktivieren, kann sich dies negativ auf die Erkennungsrate auswirken.

Modulupdates von Wechselmedien zulassen

Updates werden von Wechselmedien ausgeführt, die einen Mirror enthalten. Mit der Option **Automatisch** werden die Updates im Hintergrund ausgeführt. Wählen Sie **Immer nachfragen** aus, um Update-Dialogfelder anzuzeigen.

Update für Programmkomponente

Im Dropdownmenü **Updatemodus** können Sie auswählen, wie die ESET Security for Microsoft SharePoint-Komponentenupdates installiert werden, wenn ein neues Update verfügbar ist. Komponentenupdates enthalten meistens Änderungen an vorhandenen Funktionen, manchmal jedoch auch neue Funktionen. Je nach ausgewähltem Updatemodus können Komponentenupdates ohne Eingriff oder Bestätigung automatisch installiert werden. Alternativ können Sie sich vor der Installation der Updates benachrichtigen lassen. Nach dem Komponentenupdate muss der Server unter Umständen neu gestartet werden. Sie haben die Wahl

zwischen den folgenden Updatemodi:

- **Vor Updates nachfragen** - Sie werden aufgefordert, verfügbare Produktupdates zu bestätigen oder abzulehnen. Dies ist die Standardoption. Nach dem Komponentenupdate muss der Server unter Umständen neu gestartet werden.
- **Automatisch aktualisieren** - Komponentenupdates werden automatisch heruntergeladen und installiert.
- **Nie aktualisieren** - Es werden keine Komponentenupdates durchgeführt. Wir empfehlen diese Option, da Sie die Komponentenupdates auf diese Weise manuell durchführen und Ihren Server während eines Wartungsfensters neu starten können.

WICHTIG

Im automatischen Aktualisierungsmodus wird Ihr Server nach Abschluss des Komponentenupdates neu gestartet.

[Verbindungsoptionen](#)

Proxyserver

Um auf die Optionen der Proxyserver-Einstellungen für ein bestimmtes Updateprofil zuzugreifen, klicken Sie auf die Registerkarte **Proxy-Modus** und wählen Sie eine dieser drei Optionen aus:

- **Keinen Proxyserver verwenden** - ESET Security for Microsoft SharePoint verwendet keinen Proxyserver für Updates.
- **Globale Proxyeinstellungen verwenden** - Die unter **Erweiterte Einstellungen (F5) > Tools > [Proxyserver](#)** festgelegte Proxyserver-Konfiguration wird übernommen.
- **Verbindung über Proxyserver** - Verwenden Sie diese Option in den folgenden Fällen:

Verwenden Sie für Updates von ESET Security for Microsoft SharePoint einen anderen Proxyserver als den in den allgemeinen Einstellungen festgelegten Proxyserver (Tools > [Proxyserver](#)). In diesem Fall sind an dieser Stelle Einstellungen erforderlich: Proxyserver-Adresse, Kommunikations-Port (standardmäßig 3128) sowie Benutzername und Passwort für den Proxyserver, falls erforderlich.

Die Proxyserver-Einstellungen nicht für das gesamte Programm festgelegt wurden, ESET Security for Microsoft SharePoint jedoch Updates über einen Proxyserver herunterladen soll.

Ihr Computer ist über einen Proxyserver mit dem Internet verbunden. Während der Installation werden die Einstellungen aus Internet Explorer übernommen. Falls Sie später Änderungen vornehmen (zum Beispiel wenn Sie den Internetanbieter wechseln), müssen Sie hier die HTTP-Proxy-Einstellungen prüfen und gegebenenfalls ändern. Sonst kann keine Verbindung zu den Update-Servern hergestellt werden.

HINWEIS

Die Felder mit den Anmeldedaten (**Benutzername** und **Passwort**) sind nur für den Zugriff auf den Proxyserver vorgesehen. Geben Sie in diesen Feldern nur Daten ein, wenn diese für den Zugriff auf den Proxyserver erforderlich sind. Beachten Sie, dass in diese Felder nicht das Passwort und der Benutzername für ESET Security for Microsoft SharePoint eingetragen werden. Eine Eingabe ist nur dann erforderlich, wenn Sie für die Internetverbindung über den Proxyserver ein Passwort benötigen.

Direktverbindung verwenden, wenn der Proxy nicht verfügbar ist

Wenn in der Produktkonfiguration die Nutzung eines HTTP-Proxys vorgesehen ist und der Proxy nicht erreichbar ist, umgeht das Produkt den Proxy und kommuniziert direkt mit ESET-Servern.

Windows-Freigaben

Beim Aktualisieren von einem lokalen Windows-Server ist standardmäßig eine Authentifizierung für jede Netzwerkverbindung erforderlich.

Verbindung mit LAN herstellen als

Wählen Sie eine der folgenden Optionen aus, um Ihr Konto zu konfigurieren:

- **Systemkonto (Standard)** - Verwendet das Systemkonto für die Authentifizierung. Normalerweise findet keine Authentifizierung statt, wenn in den Haupteinstellungen für Updates keine Anmeldedaten angegeben sind.
- **Aktueller Benutzer** - Das Programm meldet sich mit dem Konto des aktuell angemeldeten Benutzers an. Diese Lösung hat den Nachteil, dass sich das Programm nicht mit dem Update-Server verbinden kann, wenn kein Benutzer angemeldet ist.
- **Folgender Benutzer** - Mit dieser Option können Sie ein bestimmtes Benutzerkonto für die Authentifizierung angeben. Verwenden Sie diese Option, wenn eine Anmeldung mit dem standardmäßigen Systemkonto nicht möglich ist. Das ausgewählte Benutzerkonto benötigt Zugriffsrechte für den Ordner mit den Update-Dateien. Wenn der Benutzer keinen Zugriff hat, kann sich das Programm nicht verbinden und kann keine Updates herunterladen.

WARNUNG

Wenn entweder **Aktueller Benutzer** oder **Folgender Benutzer** aktiviert ist, kann ein Fehler beim Wechsel der Identität zum gewünschten Benutzer auftreten. Aus diesem Grund sollten Sie die LAN-Anmeldedaten in den Haupteinstellungen für Updates eingeben. Geben Sie die Anmeldedaten dort wie folgt ein: *domain_name\user (workgroup_name\name für eine Arbeitsgruppe)* und das Passwort. Für Aktualisierungen von der HTTP-Version des lokalen Servers ist keine Authentifizierung erforderlich.

Serververbindung nach Update trennen

Die Verbindung zum Server wird getrennt, wenn sie nach dem Abrufen von Update-Dateien weiterhin aktiv ist.

[Update-Mirror](#)

Sie finden die Konfigurationsoptionen für den lokalen Mirror-Server in den **Erweiterten Einstellungen (F5)** unter **Update > Profile > [Update-Mirror](#)**.

Update-Rollback

Wenn Sie auf **Rollback** klicken, müssen Sie im Dropdownmenü einen Zeitraum auswählen. Dieser Wert legt fest, wie lange die Updates der Datenbank der Malware Scan Engine und der Programmkomponenten angehalten werden.

Wählen Sie **Bis zur Aufhebung**, um keine regelmäßigen Updates auszuführen, bis die Update-Funktion manuell wieder aktiviert wird. Das Aktivieren dieser Option ist mit einem Sicherheitsrisiko verbunden und daher nicht empfehlenswert.

Die Version der Datenbank der Malware Scan Engine wird auf die älteste verfügbare Version herabgestuft und als Snapshot im lokalen Dateisystem des Computers gespeichert.

Geplanter Task - Update

Um das Programm mit zwei Update-Servern 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.

BEISPIEL

Mit den folgenden Schritten können Sie einen Task erstellen, um den vorhandenen Task **Automatische Updates in festen Zeitabständen** zu bearbeiten.

1. Wählen Sie im Hauptbildschirm des **Taskplaners** den Task **Update** mit dem Namen **Automatische Updates in festen Zeitabständen** aus, und klicken Sie auf **Bearbeiten**, um den Konfigurationsassistenten zu öffnen.
2. Wählen Sie eine der folgenden [Zeitangaben](#) für die Ausführung des geplanten Tasks aus.
3. Wenn Sie verhindern möchten, dass der Task ausgeführt wird, wenn das System im Akkubetrieb läuft (z. B. mit USV), klicken Sie auf den Schalter neben **Task im Akkubetrieb überspringen**.
4. Wählen Sie das gewünschte [Update-Profil](#) für das Update aus. Wählen Sie aus, welche Aktion ausgeführt werden soll, falls bei der Taskausführung ein Fehler auftritt.
5. Klicken Sie auf **Fertig stellen**, um den Task zu übernehmen.

Update-Mirror

ESET Security for Microsoft SharePoint Öffnen
Drücken Sie **F5 > Update > Profile > Update-Mirror**



ESET Security for Microsoft SharePoint bietet Ihnen die Möglichkeit, Kopien der Update-Dateien zu erstellen. Diese können Sie dann zur Aktualisierung anderer Workstations im Netzwerk verwenden. Das Verwenden eines „Update-Mirrors“ - das Vorhalten von Kopien der Update-Dateien im lokalen Netzwerk - kann vorteilhaft sein, da die Dateien dann nicht von allen Arbeitsplatzcomputern einzeln über das Internet heruntergeladen werden müssen. Updates werden auf den lokalen Mirror-Server heruntergeladen und von dort an die Arbeitsstationen verteilt. Die Internetverbindung wird erheblich entlastet. Das Aktualisieren der Clientcomputer von einem Update-Mirror optimiert die Lastenverteilung im Netzwerk und entlastet Internetverbindungen.

[Update-Mirror](#)

Update-Mirror erstellen

Aktiviert die Mirror-Konfigurationsoptionen.

Speicherordner

Klicken Sie auf **Löschen**, falls Sie den Standardordner für die Speicherung der Update-Dateien (*C:\ProgramData\ESET\ESET Security\mirror*) ändern möchten. Klicken Sie auf **Bearbeiten**, um einen lokalen oder Netzwerkordner anzugeben. Wenn für den angegebenen Ordner eine Authentifizierung erforderlich ist, müssen die Anmeldedaten in die Felder „Benutzername“ und „Passwort“ eingegeben werden. Wenn sich der Speicherordner auf einem Windows NT/2000/XP-Netzlaufwerk befindet, ist ein Benutzerkonto mit Schreibzugriff auf den Ordner erforderlich.

Der Benutzername muss im Format *Domain/User* oder *Workgroup/User* eingegeben werden. Denken Sie

daran, auch die entsprechenden Passwörter einzugeben.

Update für Programmkomponente

Dateien

Bei der Konfiguration des Mirrors können Sie die Sprachversionen der herunterzuladenden Updates festlegen. Die ausgewählte Sprache muss vom konfigurierten Mirror-Server unterstützt werden.

Komponenten automatisch aktualisieren

Ermöglicht das Installieren von neuen Funktionen und Updates für vorhandene Funktionen. Updates können automatisch oder nach Bestätigung durch den Benutzer gestartet werden. Nach der Installation von Produktupdates muss der Computer möglicherweise neu gestartet werden.

Jetzt ein Update der Komponenten ausführen

Aktualisiert die Programmkomponenten auf die neueste Version.

[HTTP-Server](#)

Server-Port

Der Standardport ist auf 2221 festgelegt. Ändern Sie diesen Wert, falls Sie einen anderen Port verwenden.

Authentifizierung

Definiert die Authentifizierungsmethode für den Zugriff auf die Update-Dateien. Die folgenden Optionen stehen zur Verfügung: **Keine**, **Einfach** und **NTLM**.

- Wählen Sie **Einfach** aus, um die Base64-Verschlüsselung und die einfache Authentifizierung mit Benutzername und Passwort zu verwenden.
- Bei Auswahl von **NTLM** wird eine sichere Verschlüsselungsmethode verwendet. Zur Authentifizierung wird der auf dem Computer erstellte Benutzer verwendet, der die Update-Dateien freigegeben hat.
- Die Standardeinstellung ist **Keine**, sodass für den Zugriff auf die Update-Dateien keine Authentifizierung erforderlich ist.

WARNUNG

Wenn Sie den Zugriff auf die Update-Dateien über einen HTTP-Server zulassen möchten, muss sich der Ordner mit den Kopien der Update-Dateien auf demselben Computer befinden wie die Instanz von ESET Security for Microsoft SharePoint, mit der dieser Ordner erstellt wird.

SSL für HTTP-Server

Hängen Sie die **Zertifikatskettendatei** an oder generieren Sie ein selbstsigniertes Zertifikat, wenn Sie den HTTP-Server mit HTTPS (SSL)-Unterstützung ausführen möchten. Folgende Zertifikattypen stehen zur Verfügung: PEM, PFX und ASN. Für zusätzliche Sicherheit können Update-Dateien mit dem HTTPS-Protokoll heruntergeladen werden. Das Nachverfolgen der übertragenen Daten und Anmeldeberechtigungen ist bei der Verwendung dieses Protokolls nahezu unmöglich.

Die Option **Typ des privaten Schlüssels** wird standardmäßig auf **Integriert** eingestellt, und die Option Datei mit privatem Schlüssel ist standardmäßig deaktiviert. Dies bedeutet, dass der private Schlüssel Bestandteil der ausgewählten Zertifikatskettendatei ist.

Windows-Freigaben

Beim Aktualisieren von einem lokalen Windows-Server ist standardmäßig eine Authentifizierung für jede Netzwerkverbindung erforderlich.

Verbindung mit LAN herstellen als

Wählen Sie eine der folgenden Optionen aus, um Ihr Konto zu konfigurieren:

- **Systemkonto (Standard)** - Verwendet das Systemkonto für die Authentifizierung. Normalerweise findet keine Authentifizierung statt, wenn in den Haupteinstellungen für Updates keine Anmeldedaten angegeben sind.
- **Aktueller Benutzer** - Das Programm meldet sich mit dem Konto des aktuell angemeldeten Benutzers an. Nachteil dieser Lösung ist, dass das Programm keine Verbindung zum Update-Server herstellen kann, wenn kein Benutzer angemeldet ist.
- **Folgender Benutzer** - Mit dieser Option können Sie ein bestimmtes Benutzerkonto für die Authentifizierung angeben. Verwenden Sie diese Option, wenn eine Anmeldung mit dem standardmäßigen Systemkonto nicht möglich ist. Das ausgewählte Benutzerkonto benötigt Zugriffsrechte für den Ordner mit den Update-Dateien. Wenn der Benutzer keinen Zugriff hat, kann sich das Programm nicht verbinden und kann keine Updates herunterladen.

WARNUNG

Wenn entweder **Aktueller Benutzer** oder **Folgender Benutzer** aktiviert ist, kann ein Fehler beim Wechsel der Identität zum gewünschten Benutzer auftreten. Aus diesem Grund sollten Sie die LAN-Anmeldedaten in den Haupteinstellungen für Updates eingeben. Geben Sie die Anmeldedaten dort wie folgt ein: *domain_name\user* (*workgroup_name\name* für eine Arbeitsgruppe) und das Passwort. Für Aktualisierungen von der HTTP-Version des lokalen Servers ist keine Authentifizierung erforderlich.

Serververbindung nach Update trennen

Die Verbindung zum Server wird getrennt, wenn sie nach dem Abrufen von Update-Dateien weiterhin aktiv ist.

Netzwerk-Schutz

Netzwerkangriffsschutz (IDS) aktivieren

Mit dieser Option können Sie den Zugriff auf bestimmte Dienste konfigurieren, die auf Ihrem Computer in der vertrauenswürdigen Zone ausgeführt werden, und können die Erkennung bestimmter Angriffsarten und Exploits aktivieren oder deaktivieren, die Ihrem Computer schaden könnten.

Botnetz-Schutz aktivieren

Erkennt und blockiert die Kommunikation mit bösartigen Steuerungszentralen anhand typischer Muster, wenn ein Computer infiziert wird und ein Bot versucht, zu kommunizieren.

IDS-Ausnahmen

Sie können sich Intrusion Detection System (IDS)-Ausnahmen als eine Art Netzwerkschutzregeln vorstellen. Klicken Sie auf [Bearbeiten](#), um IDS-Ausnahmen zu definieren.

Angriffsversuche (Intrusion) erkennen:

SMB-Protokoll - Erkennt und blockiert verschiedene Sicherheitsprobleme im SMB-Protokoll.

RPC-Protokoll - Erkennt und blockiert verschiedene CVEs im System für Remoteprozeduraufrufe, das für die Distributed Computing Environment (DCE) entwickelt wurde.

RDP-Protokoll - Erkennt und blockiert verschiedene CVEs im RDP-Protokoll (siehe oben).

Unsichere Adresse nach erkanntem Angriff blockieren - IP-Adressen, die als Angriffsquellen identifiziert wurden, werden zur Negativliste hinzugefügt, um die Verbindung für einen bestimmten Zeitraum zu unterbinden.

Hinweis bei erkanntem Angriff anzeigen - Aktiviert die Benachrichtigungen im Infobereich unten rechts auf dem Bildschirm.

Benachrichtigung auch bei eingehenden Angriffen auf Sicherheitslücken anzeigen - Warnt Sie, wenn Angriffe auf Sicherheitslücken erkannt werden oder wenn eine Bedrohung versucht, sich auf diese Weise Zugang zum System zu verschaffen.

Paketprüfung:

Eingehende Verbindungen zu administrativen Freigaben per SMB-Protokoll zulassen - Die administrativen Freigaben (Admin-Freigaben) sind Standardnetzwerkfreigaben für Festplattenpartitionen (C\$, D\$, ...) im System sowie für den Systemordner (ADMIN\$). Deaktivieren Sie Verbindungen zu Admin-Freigaben, um sich vor zahlreichen Sicherheitsrisiken zu schützen. Der Conficker-Wurm verwendet beispielsweise Wörterbuchangriffe, um sich mit Admin-Freigaben zu verbinden.

Alte (nicht unterstützte) SMB-Dialekte blockieren - SMB-Sitzungen, die einen alten und nicht von IDS unterstützten SMB-Dialekt verwenden, werden blockiert. Moderne Windows-Betriebssysteme unterstützen alte SMB-Dialekte für die Abwärtskompatibilität mit älteren Betriebssystemen wie Windows 95. Angreifer können einen alten Dialekt in einer SMB-Sitzung verwenden, um die Datenverkehrsanalyse zu umgehen. Blockieren Sie alte SMB-Dialekte, falls Ihr Computer keine Dateien mit älteren Windows-Versionen teilen oder allgemein per SMB mit diesen Versionen kommunizieren muss.

SMB-Sitzungen ohne Sicherheitserweiterungen blockieren - Mit der erweiterten Sicherheit kann bei der SMB-Sitzungsaushandlung ein besserer Authentifizierungsmechanismus als die LAN Manager Challenge/Response (LM)-Authentifizierung bereitgestellt werden. Das LM-Schema gilt als unsicher und sollte nach Möglichkeit nicht verwendet werden.

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

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

Verbindungen zu Remoteregistrierung zulassen - Weitere Informationen zu diesem Dienst finden Sie unter [\[MS-RRP\]](#).

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

Verbindungen zu Serverdienst zulassen - Weitere Informationen zu diesem Dienst finden Sie unter [\[MS-SRVS\]](#).

Verbindungen zu anderen Diensten zulassen - Andere MSRPC-Dienste.

IDS-Ausnahmen

Ausnahmen für das Intrusion Detection System (IDS) sind eine Art von Schutzregeln für das Netzwerk. Die Ausnahmen werden von oben nach unten ausgewertet. Im Editor für IDS-Ausnahmen können Sie das Verhalten des Netzwerkschutzes für verschiedene IDS-Ausnahmen festlegen. Die erste übereinstimmende Ausnahme wird für jeden Aktionstyp (Sperren, Benachrichtigen, Log) separat angewendet. Mit den Optionen **Anfang/Nach oben/Nach unten/Ende** können Sie die Prioritäten der Ausnahmen festlegen. Um eine neue IDS-Ausnahme zu erstellen, klicken Sie auf **Hinzufügen**. Klicken Sie auf **Bearbeiten**, um eine vorhandene IDS-Ausnahme zu bearbeiten, oder auf **Löschen**, um sie zu löschen.

Wählen Sie einen **Warnungstyp** in der Dropdownliste aus. Geben Sie den **Bedrohungsnamen** und die **Richtung** aus. Suchen Sie nach einer **Anwendung**, für die Sie die Ausnahme erstellen möchten. Geben Sie eine Liste von IP-Adressen (IPv4 oder IPv6) oder Subnetzen an. Mehrere Einträge können durch Komma voneinander getrennt werden.

Konfigurieren Sie die **Aktion** für die IDS-Ausnahme, indem Sie eine der Optionen im Dropdownmenü auswählen (**Standard, Ja, Nein**). Wiederholen Sie diesen Vorgang für alle Aktionstypen (**Sperren, Benachrichtigen, Log**).

BEISPIEL

Falls Sie bei einer IDS-Ausnahmenwarnung eine Benachrichtigung anzeigen und den Zeitpunkt des Ereignisses loggen möchten, lassen Sie für den Aktionstyp **Sperren** den Wert **Standard** eingestellt und wählen Sie für die anderen zwei Aktionstypen (**Benachrichtigen** und **Log**) jeweils die Option **Ja** im Dropdownmenü aus.

Vorübergehende Negativliste der IP-Adressen

Zeigt eine Liste von IP-Adressen an, die als Angriffsquellen identifiziert und zur Negativliste hinzugefügt wurden, um die Verbindung für einen bestimmten Zeitraum zu unterbinden. Zeigt die blockierten **IP-Adressen** an.

Blockierungsgrund

Zeigt den Angriffstyp an, der von dieser Adresse verhindert wurde (z. B. TCP-Portscan-Angriff).

Zeitüberschreitung

Zeigt das Datum und die Uhrzeit an, zu der die Adresse aus der Negativliste entfernt wird.

Entfernen / Alle entfernen

Entfernt die ausgewählte IP-Adresse aus der vorübergehenden Negativliste, bevor sie automatisch entfernt wird, oder entfernt alle Adressen sofort aus der Negativliste.

Ausnahme hinzufügen

Fügt eine Firewallausnahme für die ausgewählte IP-Adresse zum IDS-Filter hinzu.

Web und E-Mail

Sie können die Protokollprüfung, den E-Mail-Client-Schutz, den Web-Schutz und den Phishing-Schutz so konfigurieren, dass Ihr Server bei der Kommunikation mit dem Internet geschützt wird.

E-Mail-Schutz

Überwacht den gesamten E-Mail-Verkehr, schützt Sie vor Schadcode und bietet Ihnen eine Auswahl an Handlungsmöglichkeiten, wenn eine Infektion erkannt wurde.

Web-Schutz

Überwacht den Datenverkehr zwischen Webbrowsern und Remoteservern gemäß den für HTTP und HTTPS festgelegten Standards. Mit dieser Funktion können Sie außerdem bestimmte [URLs](#) blockieren, zulassen oder ausschließen.

Protokollprüfung

Bietet erweiterten Schutz für die verwendeten Anwendungsprotokolle durch das ThreatSense-Prüfmodul. Die Prüfung findet automatisch statt, egal ob ein Webbrowser oder ein E-Mail-Programm verwendet wird. Auch verschlüsselte Verbindungen ([SSL/TLS](#)) werden geprüft.

Phishing-Schutz

Hier können Sie Webseiten sperren, die Phishing-Inhalte verteilen.

Protokollprüfung

Die Scan Engine von ThreatSense bietet Malware-Schutz für Anwendungsprotokolle und enthält mehrere erweiterte Scan-Methoden. Die Protokollprüfung funktioniert unabhängig vom eingesetzten E-Mail-Programm oder Webbrowser. Wenn die Protokollprüfung aktiviert ist, überprüft ESET Security for Microsoft SharePoint sämtliche Kommunikation, die das SSL/TLS-Protokoll verwendet. Navigieren Sie zu **Web und E-Mail** > [SSL/TLS](#).

Prüfen von anwendungsspezifischen Protokollen aktivieren

Mit dieser Option können Sie die Protokollprüfung deaktivieren. Zahlreiche Komponenten von ESET Security for Microsoft SharePoint wie **Web-Schutz**, **E-Mail-Schutz** und **Phishing-Schutz** hängen jedoch von dieser Option ab und funktionieren ohne sie nicht ordnungsgemäß.

Ausgeschlossene Anwendungen

Wählen Sie aus der Liste die Netzwerk-Anwendungen, für deren Datenkommunikation keine Inhaltsprüfung erfolgen soll. Dies schließt die HTTP/POP3-Datenkommunikation ausgewählter Anwendungen von der Prüfung auf Bedrohungen aus, um bestimmte Anwendungen von der Protokollprüfung auszuschließen. Klicken Sie auf **Bearbeiten** bzw. auf **Hinzufügen**, um eine ausführbare Datei in der Liste der Anwendungen auszuwählen und von der Protokollprüfung auszuschließen.

WICHTIG

Aktivieren Sie diese Option nach Möglichkeit nur für Anwendungen, deren Datenkommunikation mit aktivierter Prüfung nicht ordnungsgemäß funktioniert.

Ausgeschlossene IP-Adressen

Ermöglicht das Ausschließen bestimmter Remoteadressen von der Protokollprüfung. Die IP-Adressen in dieser Liste werden von der Prüfung von Protokollen ausgenommen. Die HTTP/POP3/IMAP-Datenkommunikation von/zu den ausgewählten Adressen wird nicht auf Bedrohungen geprüft.

WICHTIG

Wir empfehlen, diese Option nur für Adressen zu aktivieren, die als vertrauenswürdig bekannt sind.

Klicken Sie auf **Bearbeiten** bzw. **Hinzufügen**, um eine IP-Adresse, einen Adressbereich oder ein Subnetz auszuschließen. Mit der Option **Mehrere Werte eingeben** können Sie mehrere durch Zeilenumbrüche, Kommas oder Semikolon getrennte IP-Adressen eingeben. Wenn die Mehrfachauswahl aktiviert ist, werden die Adressen in der Liste der ausgeschlossenen IP-Adressen angezeigt.

HINWEIS

Ausschlüsse sind nützlich, wenn die Protokollprüfung Kompatibilitätsprobleme verursacht.

Webbrowser und E-Mail-Programme

Da im Internet Sicherheitsbedrohungen allgegenwärtig sind, ist sicheres Internetsurfen besonders wichtig. Durch Sicherheitslücken in Webbrowsern und gefälschte Hyperlinks kann Schadcode unbemerkt in Ihr System eindringen. Deshalb bietet ESET Security for Microsoft SharePoint besondere Funktionen zur Verbesserung der Sicherheit von Webbrowsern an. Sie können beliebige Anwendungen, die auf das Internet zugreifen, als Webbrowser einstufen. Anwendungen, die bereits kommunikations- oder anwendungsspezifische Protokolle aus dem ausgewählten Pfad verwenden, können zur Liste der Webbrowser und E-Mail-Programme hinzugefügt werden.

SSL/TLS

ESET Security for Microsoft SharePoint kann Verbindungen die das Secure Sockets Layer (SSL)- / Transport Layer Security (TLS)-Protokoll verwenden, auf Bedrohungen überprüfen.

Für die Untersuchung von SSL-geschützten Verbindungen gibt es verschiedene Scan-Modi mit vertrauenswürdigen und unbekannten Zertifikaten sowie Zertifikaten, die von der Prüfung SSL-geschützter Verbindungen ausgeschlossen sind.

SSL/TLS-Protokollfilterung aktivieren

Wenn die Protokollfilterung deaktiviert ist, werden SSL/TLS-Verbindungen nicht geprüft. Für den Secure Sockets Layer (SSL)- / Transport Layer Security (TLS)-Protokollfiltermodus sind die folgenden Optionen verfügbar:

- **Automatischer Filtermodus** - Aktivieren Sie diese Option, um jegliche SSL/TLS-geschützte Kommunikation zu scannen (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.

- **Interaktiver Filtermodus** - Bei Eingabe einer neuen, mit SSL/TLS geschützten Seite (mit unbekanntem Zertifikat) wird ein Dialogfeld mit möglichen Aktionen angezeigt. In diesem Modus können Sie eine Liste von SSL/TLS-Zertifikaten erstellen, die von der Prüfung ausgeschlossen sind.
- **Policy-Modus** - Alle SSL/TLS-Verbindungen mit Ausnahme der konfigurierten Ausschlüsse werden gefiltert.

Liste der vom SSL/TLS-Filter betroffenen Anwendungen

Fügen Sie eine gefilterte Anwendung hinzu und legen Sie eine Scanaktion fest. Mit der Liste der vom SSL/TLS-Filter betroffenen Anwendungen können Sie das Verhalten von ESET Security for Microsoft SharePoint für bestimmte Anwendungen anpassen und ausgewählte Aktionen speichern, wenn der **Interaktive Modus** unter **Filtermodus für SSL/TLS-Protokoll** ausgewählt ist.

Liste bekannter Zertifikate

Mit der Liste bekannter Zertifikate können Sie das Verhalten von ESET Security for Microsoft SharePoint für bestimmte SSL-Zertifikate anpassen. Klicken Sie auf [Bearbeiten](#) neben der **Liste bekannter Zertifikate**, um die Liste anzuzeigen und zu verwalten.

Kommunikation mit vertrauenswürdigen Domains ausschließen

Schließt die Kommunikation mit erweiterten Validierungszertifikaten von der Protokollprüfung aus (Internetbanking).

Verschlüsselte Kommunikation sperren, die das veraltete SSL v2-Protokoll verwendet

Verbindungen, die die frühere Version des SSL-Protokolls verwenden, werden automatisch blockiert.

Stammzertifikat

Damit die SSL/TLS-Kommunikation in Ihren Browsern/E-Mail-Programmen ordnungsgemäß funktioniert, muss das Stammzertifikat für ESET der Liste der bekannten Stammzertifikate (Herausgeber) hinzugefügt werden. Bekanntem Browsern das Stammzertifikat hinzufügen sollte aktiviert sein. Wählen Sie diese Option aus, um das ESET-Stammzertifikat automatisch zu den bekannten Browsern (z. B. Opera oder Firefox) hinzuzufügen. Wenn ein Browser den Systemzertifizierungsspeicher verwendet, wird das Zertifikat automatisch hinzugefügt (z. B. Internet Explorer).

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

Gültigkeit des Zertifikats

Falls das Zertifikat nicht über die VSZS-Zertifikatablage geprüft werden kann

In manchen Fällen kann das Zertifikat nicht über den **Speicher vertrauenswürdiger Stammzertifizierungsstellen** geprüft werden. Das bedeutet, dass jemand das Zertifikat signiert hat (z. B. der Administrator eines Webserver oder ein Kleinunternehmen). Das Zertifikat als vertrauenswürdige einzustufen, stellt nicht immer ein Risiko dar. Die meisten großen Unternehmen (z. B. Banken) verwenden Zertifikate, die von einer vertrauenswürdigen Stammzertifizierungsstelle signiert sind. Wenn die Option **Gültigkeit des Zertifikats erfragen** ausgewählt ist (Standardeinstellung), muss der Benutzer eine Aktion

festlegen, die ausgeführt werden soll, wenn verschlüsselte Verbindungen aufgebaut werden. Aktivieren Sie die Option **Kommunikation blockieren, die das Zertifikat verwendet**, um verschlüsselte Verbindungen zu Sites, die nicht verifizierte Zertifikate verwenden, immer zu beenden.

Wenn das Zertifikat ungültig oder beschädigt ist

Ungültige Zertifikate sind entweder abgelaufen oder wurden fehlerhaft signiert. In diesem Fall sollten Sie die Option **Kommunikation blockieren, die das Zertifikat verwendet** aktiviert lassen.

Liste bekannter Zertifikate

Sie können das Verhalten von ESET Security for Microsoft SharePoint für Secure Sockets Layer (SSL) / Transport Layer Security (TLS)-Zertifikate festlegen und ausgewählte Aktionen speichern, wenn der **Interaktive Modus** unter [SSL/TLS](#)-Protokollprüfungsmodus ausgewählt ist. Sie können das ausgewählte Zertifikat konfigurieren oder ein neues Zertifikat aus einer URL oder einer Datei **hinzufügen**. Klicken Sie im Fenster „Zertifikat hinzufügen“ auf „URL“ oder auf „Datei“ und geben Sie eine Zertifikat-URL an bzw. navigieren Sie zu einer Zertifikatdatei. Die folgenden Felder werden automatisch mit Daten aus dem Zertifikat ausgefüllt:

- **Zertifikatname** - 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.

Zugriffsaktion

- **Auto** - vertrauenswürdige Zertifikate zulassen, bei nicht vertrauenswürdigen Zertifikaten nachfragen.
- **Zulassen oder Blockieren** - um die von diesem Zertifikat gesicherte Verbindung unabhängig von ihrer Vertrauenswürdigkeit zuzulassen oder zu blockieren.
- **Nachfragen** - um eine Nachfrage zu erhalten, wenn ein bestimmtes Zertifikat vorgefunden wird.

Scan-Aktion

- **Auto** - um im automatischen Modus zu scannen und im interaktiven Modus nachzufragen.
- **Scannen oder ignorieren** - um die mit diesem Zertifikat gesicherte Kommunikation zu scannen oder zu ignorieren.
- **Nachfragen** - um eine Nachfrage zu erhalten, wenn ein bestimmtes Zertifikat vorgefunden wird.

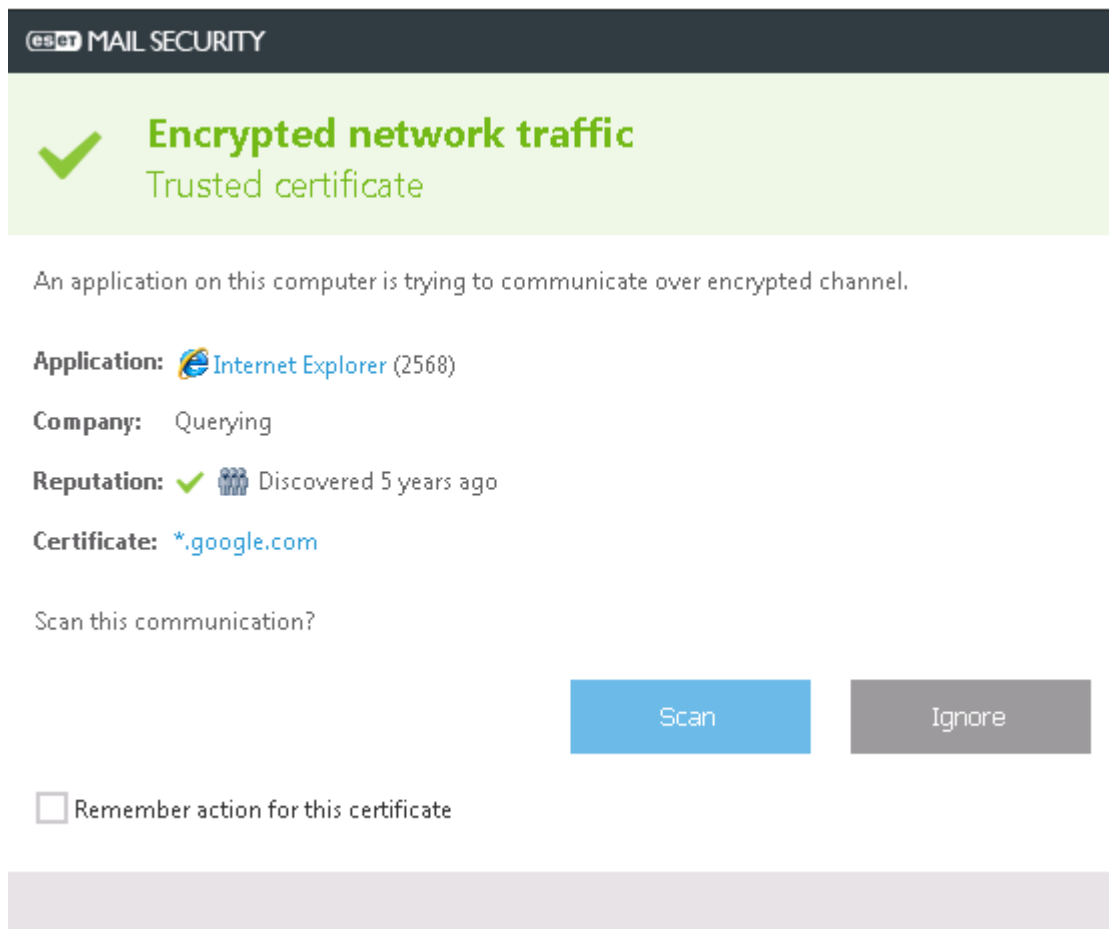
Verschlüsselte SSL-Kommunikation

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 Security for Microsoft SharePoint 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 gefragt, ob die Verbindung **zugelassen** oder **blockiert** werden soll.

Wenn die **SSL-Protokollprüfung** 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 Security for Microsoft SharePoint den Datenverkehr **ignorieren**, damit die Anwendung ordnungsgemäß funktioniert.



In beiden Fällen kann der Benutzer die ausgewählte Aktion speichern. Gespeicherte Aktionen werden in der [Liste bekannter Zertifikate](#) gespeichert.

E-Mail-Client-Schutz

Die Integration von ESET Security for Microsoft SharePoint mit E-Mail-Programmen verbessert den aktiven Schutz gegen Schadcode in E-Mail-Nachrichten. Wenn Ihr E-Mail-Programm dies unterstützt, kann die Integration in ESET Security for Microsoft SharePoint aktiviert werden. Wenn die Integration aktiviert ist, wird die ESET Security for Microsoft SharePoint-Symbolleiste direkt in das E-Mail-Programm integriert und ermöglicht einen effizienteren E-Mail-Schutz (bei neueren Versionen von Windows Live Mail wird die Symbolleiste nicht integriert).

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. Auch bei nicht aktivierter Integration ist die E-Mail-Kommunikation durch den E-Mail-Client-Schutz (POP3, IMAP) weiterhin geschützt. Eine vollständige Liste der unterstützten E-Mail-Programme und Versionen finden Sie im entsprechenden [Knowledgebase-Artikel](#).

Prüfen neuer Elemente im Posteingang deaktivieren

Falls das System bei der Arbeit mit Ihrem E-Mail-Programm verlangsamt wird (nur MS Outlook). Dies kann beispielsweise vorkommen, wenn Sie E-Mails vom Kerio Outlook Connector Store abrufen.

E-Mail-Schutz durch Client-Plugins aktivieren

Deaktiviert den E-Mail-Client-Schutz, ohne die Integration in Ihrem E-Mail-Programm zu entfernen. Sie können entweder alle Plugins deaktivieren, oder die folgenden Plugins einzeln auswählen:

- **Eingehende E-Mails** - Aktiviert/deaktiviert die Überprüfung empfangener Nachrichten.
- **Ausgehende E-Mails** - Aktiviert/deaktiviert die Überprüfung ausgehender Nachrichten.
- **E-Mails, die zum Lesen geöffnet werden** - Aktiviert/deaktiviert die Überprüfung gelesener Nachrichten.

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 folgenden Ordner verschieben** - Infizierte E-Mails werden automatisch in den angegebenen Ordner verschoben.
- **Ordner** - Geben Sie den Ordner an, in den erkannte infizierte E-Mails verschoben werden sollen.

Scan nach Signaturdatenbank-Update wiederholen

Aktiviert/deaktiviert das erneute Scannen nach einem Signaturdatenbank-Update.

Scanergebnisse von anderen Modulen akzeptieren

Wenn diese Option aktiviert ist, nimmt das E-Mail-Schutz-Modul Scanergebnisse von anderen Modulen entgegen (POP3-, IMAP-Protokollprüfung).

E-Mail-Protokolle

E-Mail-Schutz durch Protokollfilterung aktivieren

IMAP und POP3 sind die gängigsten Protokolle für den Empfang von E-Mails in E-Mail-Cliantwendungen. ESET Security for Microsoft SharePoint schützt diese Protokolle unabhängig vom eingesetzten E-Mail-Programm.

ESET Security for Microsoft SharePoint unterstützt außerdem die Prüfung von IMAPS- und POP3S-Protokollen, die Daten zwischen Server und Client über einen verschlüsselten Kanal übertragen. ESET Security for Microsoft SharePoint überwacht die über die Protokolle SSL (Secure Socket Layer) und TLS (Transport Layer Security) abgewinkelte Kommunikation. Unabhängig von der Version des Betriebssystems wird nur Datenverkehr an Ports gescannt, die in „Vom **IMAPS-/POP3S-Protokoll** verwendete Ports“ definiert wurden.

Einstellungen für IMAPS / POP3-Scanner

Verschlüsselter Datenverkehr wird mit den Standardeinstellungen nicht geprüft. Sie können die Prüfung von verschlüsseltem Datenverkehr in den erweiterten Einstellungen unter [SSL/TLS-Protokollprüfung](#) aktivieren.

Die Portnummer gibt an, um welchen Typ von Port es sich handelt. Eine Liste der Standardports für E-Mails:

Portname	Portnummern	Beschreibung
POP3	110	Standardport für unverschlüsseltes POP3.
IMAP	143	Standardport für unverschlüsseltes IMAP.
Sicheres IMAP (IMAP4-SSL)	585	SSL/TLS-Protokollfilterung aktivieren. Mehrere Portnummern müssen durch ein Komma voneinander getrennt sein.
IMAP4 über SSL (IMAPS)	993	SSL/TLS-Protokollfilterung aktivieren. Mehrere Portnummern müssen durch ein Komma voneinander getrennt sein.
Sicheres POP3 (SSL-POP)	995	SSL/TLS-Protokollfilterung aktivieren. Mehrere Portnummern müssen durch ein Komma voneinander getrennt sein.

Warnungen und Hinweise

Der E-Mail-Schutz dient der Überwachung eingehender E-Mails, die mit dem POP3-Protokoll übertragen werden. Mithilfe der Plug-In-Software für Microsoft Outlook und andere E-Mail-Programme stellt ESET Security for Microsoft SharePoint Kontrollfunktionen für die gesamte E-Mail-Kommunikation (POP3, MAPI, IMAP, HTTP) bereit. Für die Prüfung eingehender Nachrichten verwendet das Programm alle erweiterten ThreatSense-Scan-Methoden. Die Erkennung von Schadcode findet also noch vor dem Abgleich mit der Virenerkennungsdatenbank statt. Das Scannen der POP3-Kommunikation erfolgt unabhängig vom verwendeten E-Mail-Programm.

Nach erfolgter Prüfung kann ein Prüfhinweis mit dem Scan-Ergebnis zu der E-Mail-Nachricht hinzugefügt werden. Sie haben folgende Optionen: **Prüfhinweis zu eingehenden/gelesenen E-Mails hinzufügen**, **Prüfhinweis an den Betreff empfangener und gelesener infizierter E-Mails anhängen** oder **Prüfhinweis zu ausgehenden E-Mails hinzufügen**. 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. Die folgenden Optionen stehen zur Verfügung:

- **Nie** - Es werden keine Prüfhinweise zu E-Mails hinzugefügt.
- **Nur an infizierte E-Mails** - Prüfhinweise werden nur E-Mails hinzugefügt, in denen Schadcode erkannt wurde (Standardeinstellung).
- **Bei allen geprüften E-Mails** - Alle geprüften E-Mails werden mit Prüfhinweisen versehen.

Prüfhinweis an den Betreff ausgehender, infizierter E-Mails anhängen

Deaktivieren Sie dieses Kontrollkästchen, wenn Prüfhinweise zu den Betreffzeilen infizierter E-Mails hinzugefügt werden sollen. Ohne großen Aufwand können Sie in Ihrem E-Mail-Programm eine Filterregel erstellen, die diesen Prüfhinweis erkennt (falls Ihr E-Mail-Programm Filterregeln unterstützt). Diese Funktion erhöht beim Empfänger auch die Glaubwürdigkeit von Nachrichten. Bei der Erkennung von eingedrungener Schadsoftware stehen wertvolle Informationen zur Verfügung, um den Bedrohungsgrad durch die Nachricht oder den Absender einzuschätzen.

Text, der zur Betreffzeile infizierter E-Mails hinzugefügt wird

Bearbeiten Sie diese Vorlage, falls Sie das Format des Betreff-Präfix in infizierten E-Mails bearbeiten möchten. Diese Funktion ersetzt den Nachrichtenbetreff `Hello` durch einen angegebenen Präfixwert `[virus]` im folgenden Format: `[virus] Hello`. Die Variable `%VIRUSNAME%` wird durch die erkannte Bedrohung ersetzt.

Symbolleiste für MS Outlook

Für den Schutz von Microsoft Outlook wird ein Plug-In verwendet. Nach der Installation von ESET Security for Microsoft SharePoint wird diese Symbolleiste mit Malware-Schutzoptionen zu Microsoft Outlook hinzugefügt:

ESET Security for Microsoft SharePoint

Klicken Sie auf das **Symbol**, um das Hauptprogrammfenster von ESET Security for Microsoft SharePoint zu öffnen.

E-Mails erneut prüfen

E-Mail-Prüfung manuell 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-Schutz](#).

Einstellungen für Prüfung

Anzeige der Optionen für den [E-Mail-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 Security for Microsoft SharePoint wird diese Symbolleiste mit Malware-Schutzoptionen zu Outlook Express bzw. Windows Mail hinzugefügt:

ESET Security for Microsoft SharePoint

Klicken Sie auf das **Symbol**, um das Hauptprogrammfenster von ESET Security for Microsoft SharePoint zu öffnen.

E-Mails erneut prüfen

Mit dieser Funktion können Sie die E-Mail-Prüfung manuell starten. Sie können E-Mails festlegen, die gescannt werden sollen, und das erneute Prüfen empfangener E-Mails aktivieren. Weitere Informationen finden Sie unter [E-Mail-Schutz](#).

Einstellungen für Prüfung

Anzeige der Optionen für den [E-Mail-Schutz](#).

Anzeige anpassen

Sie können die Anzeige der Symbolleiste für Ihr E-Mail-Programm ändern. Deaktivieren Sie die Option für die Anpassung der Anzeige unabhängig von den Parametern des E-Mail-Programms.

- **Symboltitel anzeigen** - Beschreibung für Symbole anzeigen.
- **Symboltitel rechts** - Die Beschreibungen werden vom unteren zum seitlichen Bereich der Symbole verschoben.
- **Große Symbole** - Große Symbole für Menüeinstellungen.

Bestätigungsfenster

Mit diesem Hinweis wird geprüft, ob die ausgewählte Aktion wirklich durchgeführt werden soll. Dadurch sollen mögliche Fehler vermieden werden. In diesem Dialogfeld können Sie außerdem die Bestätigungen deaktivieren.

E-Mails erneut prüfen

Die in E-Mail-Programmen integrierte ESET Security for Microsoft SharePoint-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.
- **Bereits geprüfte E-Mails erneut prüfen** - Option einer erneuten Prüfung bereits geprüfter E-Mails.

Web-Schutz

Der Web-Schutz besteht in der Überwachung der Kommunikation zwischen Webbrowsern und Remoteservern, schützt Sie vor Onlinebedrohungen und entspricht den Regeln für HTTP (Hypertext Transfer Protocol) und HTTPS (verschlüsselte Kommunikation).

Der Zugriff auf Webseiten, die bekannterweise Schadcode enthalten, wird vor dem Herunterladen von Inhalten blockiert. Alle anderen Webseiten werden beim Laden vom ThreatSense-Modul gescannt und blockiert, wenn Schadcode gefunden wird. Der Web-Schutz bietet zwei Schutzebenen: Blockieren nach Negativliste und Blockieren nach Inhalt.

 [Einfach](#)

Der **Web-Schutz** sollte unbedingt immer aktiviert sein. Sie finden diese Option auch im Hauptfenster von ESET Security for Microsoft SharePoint unter **Einstellungen > Web und E-Mail > Web-Schutz**.

Erweiterte Überprüfung von Browser-Skripts aktivieren

Die Erkennungsroutine scannt standardmäßig alle in Webbrowsern ausgeführten JavaScript-Programme.

 [Webprotokolle](#)

Hier können Sie die Überwachung dieser von den meisten Internetbrowsern verwendeten Standardprotokolle konfigurieren. ESET Security for Microsoft SharePoint ist standardmäßig so konfiguriert, dass das von den meisten Internetbrowsern verwendete HTTP-Protokoll überwacht wird.

ESET Security for Microsoft SharePoint unterstützt auch die HTTPS-Protokollprüfung. Bei der HTTPS-Kommunikation wird zur Datenübertragung zwischen Server und Client ein verschlüsselter Kanal verwendet. ESET Security for Microsoft SharePoint 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 gescannt, die unter **Vom HTTPS-Protokoll verwendete Ports** definiert wurden.

Verschlüsselter Datenverkehr wird mit den Standardeinstellungen nicht gescannt. Sie können das Scannen des

verschlüsseltem Datenverkehrs in den **erweiterten Einstellungen (F5)** unter **Web und E-Mail** > [SSL/TLS](#) aktivieren.

[ThreatSense-Parameter](#)

Legen Sie Einstellungen für Scan-Typen (E-Mails, Archive usw.) und Erkennungsmethoden für den Web-Schutz fest.

URL-Adressverwaltung

Mit der URL-Adressverwaltung können Sie festlegen, welche HTTP-Adressen blockiert, zugelassen oder von der Prüfung ausgeschlossen werden sollen. Der Zugriff auf Websites in der Liste der blockierten Adressen ist nur dann möglich, wenn diese sich auch in der Liste der zulässigen Adressen befinden. Websites, die in der Liste der von der Prüfung ausgenommenen Adressen aufgeführt sind, werden vor dem Zugriff nicht auf Schadcode gescannt. Wenn neben HTTP-Webseiten auch HTTPS-Adressen gefiltert werden sollen, müssen Sie die Option [SSL/TLS-Protokollfilterung](#) aktivieren. Andernfalls werden nur die Domänen besuchter HTTPS-Sites hinzugefügt, jedoch nicht die kompletten URLs.

Eine Liste blockierter Adressen kann Adressen aus einer externen öffentlichen Negativliste und eine zweite Ihre eigene Negativliste enthalten. Auf diese Weise können Sie die externe Liste einfacher aktualisieren, während Ihre Liste intakt bleibt.

Klicken Sie auf **Bearbeiten**, um eine [neue Adressliste](#) zu den vordefinierten Listen **hinzuzufügen**. Dies ist hilfreich, wenn Sie verschiedene Gruppen und Adressen auf logische Art und Weise aufteilen möchten. Standardmäßig stehen die drei folgenden Listen zur Verfügung:

- **Liste von der Prüfung ausgeschlossener Adressen** - Für die Adressen in dieser Liste wird keine Prüfung auf Schadcode ausgeführt.
- **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.

Address list
?

List name	Address types	List description
List of allowed addresses	Allowed	
List of blocked addresses	Blocked	
List of addresses excluded from checking	Excluded from checking	

Add
Edit
Delete

Add a wildcard (*) to the list of blocked addresses to block all URLs except those included in a list of allowed addresses.

OK
Cancel

Sie können eine neue URL-Adresse zur Liste **hinzufügen**. Geben Sie mehrere Werte mit einem Trennzeichen ein. Klicken Sie auf **Bearbeiten**, um eine vorhandene Adresse in der Liste zu bearbeiten, oder auf **Löschen**, um sie zu löschen. Die Löschfunktion ist nur für die mit der Funktion **Hinzufügen** erstellten Adressen möglich, nicht für importierte Adressen.

In allen Listen können Sie die Platzhalterzeichen * (Sternchen) und ? (Fragezeichen) verwenden. Das Sternchen ersetzt eine beliebige Zahl oder ein beliebiges Zeichen, das Fragezeichen ein beliebiges Zeichen. 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.

HINWEIS

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.

Neue Liste erstellen

Die Liste legt fest, welche URL-Adressen/Masken blockiert, zugelassen oder vom Scannen ausgeschlossen werden sollen. Geben Sie bei der Erstellung einer neuen Liste Folgendes an:

- **Typ der Adressliste** - Wählen Sie den Typ (Von der Prüfung ausgeschlossen, Blockiert oder Erlaubt) aus der Dropdownliste aus.
- **Listenname** - Geben Sie den Namen der Liste ein. Bei der Bearbeitung einer der drei vordefinierten Listen ist dieses Feld ausgegraut.
- **Listenbeschreibung** - Geben Sie eine kurze Beschreibung für die Liste ein (optional). Wird bei der Bearbeitung einer der drei vordefinierten Listen ausgegraut.

- **Liste aktiv** - Mit diesem Schalter können Sie die Liste deaktivieren. Sie können die Liste später bei Bedarf aktivieren.
- **Bei Anwendung benachrichtigen** - Wenn Sie benachrichtigt werden möchten, wenn eine bestimmte Liste bei der Prüfung einer von Ihnen besuchten HTTP-Site verwendet wird. Mit dieser Option wird eine Benachrichtigung ausgegeben, wenn eine Website blockiert oder zugelassen wird, weil sie in der Liste der blockierten oder zugelassenen Adressen enthalten ist. Die Benachrichtigung enthält den Namen der Liste mit der angegebenen Website.
- Wählen Sie den **Logging-Schweregrad** (Kein, Diagnose, Information oder Warnung) in der Dropdownliste aus. Einträge mit dem Schweregrad **Warnung** können von ESET Security Management Center gesammelt werden.

ESET Security for Microsoft SharePoint kann den Zugriff auf bestimmte Webseiten sperren, sodass der Browser deren Inhalte nicht anzeigt. Darüber hinaus können Adressen angegeben werden, die nicht geprüft werden sollen. Wenn der vollständige Name des Remoteservers nicht bekannt ist oder eine ganze Gruppe von Remoteservern angegeben werden soll, können Sie sogenannte Masken verwenden.


Diese Masken verwenden die Symbole ? und *:

- Mit „??“ können Sie ein einzelnes Zeichen ersetzen.
- Mit * können Sie eine Zeichenfolge ersetzen.


BEISPIEL

*.c?m deckt alle Adressen ab, deren erster Buchstabe c ist, die mit dem Buchstaben „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 <https://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 können Sie eine gesamte Domäne inklusive aller Unterdomänen mit einer einzigen Maske erfassen. Die Maske *.domain.com erfasst z. B. auch <https://domain.com>. *domain.com wäre dagegen nicht korrekt, da diese Maske auch <https://anotherdomain.com> erfasst.

Add mask


Enter a mask that specifies a URL address



Enter multiple values
OK
Cancel

Mehrere Werte eingeben

Geben Sie mehrere durch Zeilenumbrüche, Kommas oder Semikolon getrennte URL-Adressen ein. Wenn die

Mehrfachauswahl aktiviert ist, werden die Adressen in der Liste angezeigt.

Importieren

Importiert eine Datei mit URL-Adressen (trennen Sie die Werte mit Zeilenumbrüchen, z. B. *.txt mit UTF-8).

Import

...

File(s) to import (separate values with a line break)

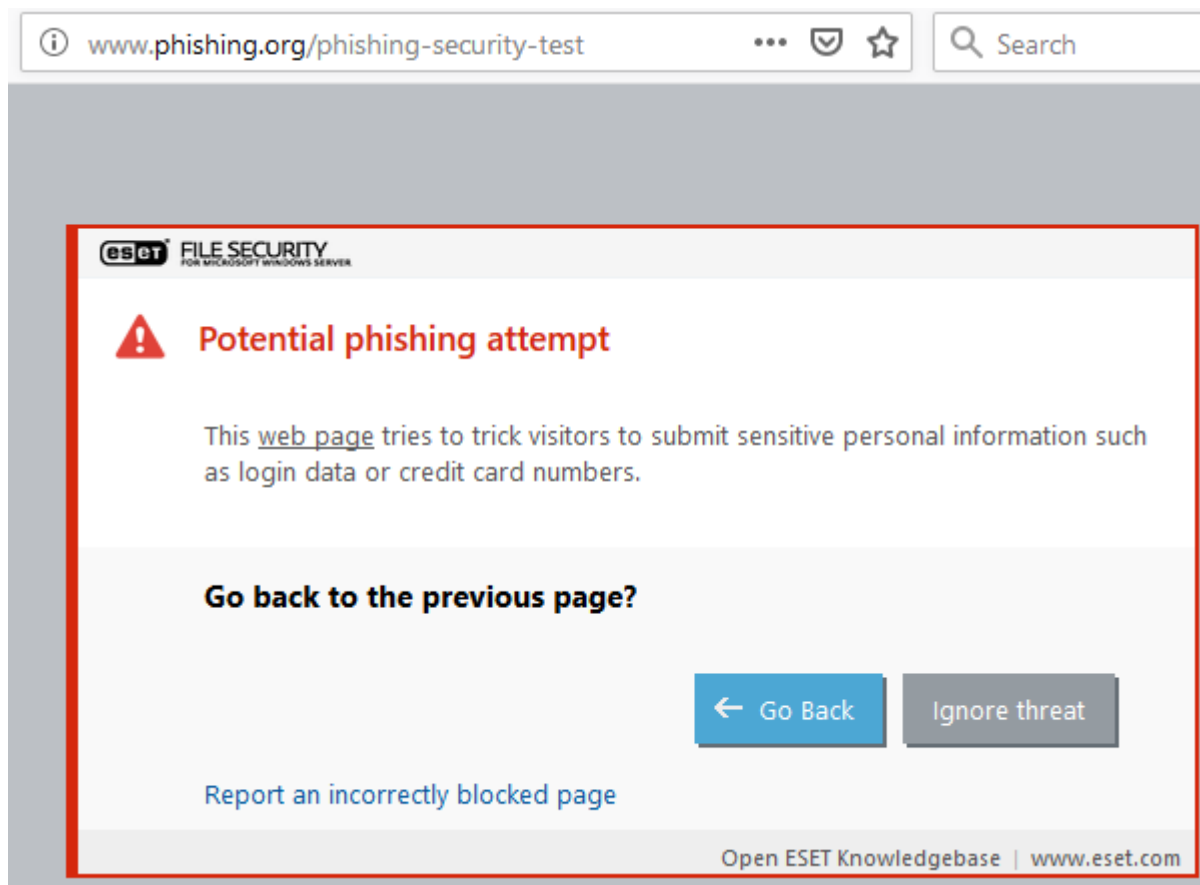
Import

Web-Phishing-Schutz

Der Begriff „Phishing“ bezeichnet eine kriminelle Vorgehensweise, die sich Techniken des Social Engineering (Manipulation von Benutzern zur Erlangung vertraulicher Informationen) zunutze macht. Phishing wird oft eingesetzt, um Zugriff auf vertrauliche Daten wie Kontonummern oder PIN-Codes zu erlangen.

ESET Security for Microsoft SharePoint umfasst den Phishing-Schutz, der Webseiten sperrt, die für diese Arten von Inhalten bekannt sind. Der Phishing-Schutz in ESET Security for Microsoft SharePoint sollte unbedingt aktiviert werden. Unser [Knowledgebase-Artikel](#) enthält weitere Informationen zum Phishing-Schutz in ESET Security for Microsoft SharePoint.

Wenn Sie auf eine erkannte Phishing-Website zugreifen, wird das folgende Dialogfenster im Webbrowser angezeigt. Wenn Sie die Website trotzdem öffnen möchten, klicken Sie auf **Bedrohung ignorieren** (nicht empfohlen).



HINWEIS

Potenzielle Phishing-Websites, die zur Positivliste hinzugefügt wurden, werden standardmäßig nach einigen Stunden wieder von der Liste gelöscht. Verwenden Sie die [URL-Adressverwaltung](#), um eine Website dauerhaft zuzulassen.

[Phishing-Seite melden](#)

Falls Sie eine verdächtige Website bemerken, auf der Sie Phishing oder andere bösartige Aktivitäten vermuten, können Sie diese zur Analyse an ESET übermitteln. Auf Websites, die Sie bei ESET melden, sollte mindestens eines der folgenden Kriterien zutreffen:

- Die Website wird nicht als Bedrohung erkannt.
- Die Website wird als Bedrohung erkannt, obwohl sie keinen Schadcode enthält. In diesem Fall können Sie einen [Phishing-Fehlalarm melden](#).

Sie können Websites auch per E-Mail melden. Senden Sie die E-Mail an samples@eset.com. Verwenden Sie einen treffenden Text in der Betreffzeile und liefern Sie möglichst viele Informationen zur Website (wie Sie auf die Website gelangt sind, wo Sie von der Website erfahren haben usw.).

Gerätesteuerung

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

HINWEIS

Mit dem Schalter **Systemintegration** können Sie die Gerätesteuerung von ESET Security for Microsoft SharePoint aktivieren. Die Änderung tritt jedoch erst nach einem Neustart des Systems in Kraft.

Die Gerätesteuerung wird aktiviert, und Sie können die Einstellungen bearbeiten. Wenn das System ein von einer bestehenden Regel blockiertes Gerät erkennt, wird ein Hinweisfenster angezeigt und es wird kein Zugriff auf das Gerät gewährt.

Regeln

Eine [Regel](#) für die Gerätesteuerung definiert die Aktion, die ausgeführt wird, wenn ein Gerät, das die Regelkriterien erfüllt, an den Computer angeschlossen wird.

Gruppen

Klicken Sie auf [Bearbeiten](#), um Gerätegruppen zu verwalten. Erstellen Sie eine neue Gerätegruppe oder wählen Sie eine vorhandene Gerätegruppe aus, um Geräte zur Liste hinzuzufügen oder daraus zu entfernen.

HINWEIS

Sie finden die Log-Einträge der Gerätesteuerung in den [Log-Dateien](#).

Geräteregeln

Bestimmte Gerätetypen können für Benutzer oder Benutzergruppen oder auf Grundlage weiterer, in der Regelkonfiguration festgelegter Parameter zugelassen oder gesperrt werden. Die Regelliste beschreibt die Regeln mit Namen, Gerätetyp, Aktion nach der Erkennung eines Geräts und Log-Schweregrad.

Sie können eine neuen Regel **hinzufügen** oder die Einstellungen einer vorhandenen Regeln bearbeiten. Geben Sie zur leichten Identifizierung der Regel im Feld **Name** eine Beschreibung ein. Über den Schalter neben **Regel aktiviert** wird die Regel deaktiviert bzw. aktiviert. Dies ist nützlich, wenn Sie eine Regel deaktivieren, jedoch nicht dauerhaft löschen möchten.

Anwendungszeitraum

Sie können Regeln mit [Zeitfenstern](#) einschränken. Ihre erstellten Zeitfenster werden im Dropdownmenü angezeigt.

Gerätetyp

Wählen Sie im Dropdown-Menü den Typ des externen Geräts aus (Datenträgerspeicher/tragbares Gerät/Bluetooth/FireWire/...). Die Gerätetypen werden vom Betriebssystem übernommen 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 liefern keine Informationen über Benutzer, sondern nur über deren Aktionen. Dies bedeutet, dass Bildverarbeitungsgeräte nur global gesperrt werden können.

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.

HINWEIS

Bestimmte Rechte (Aktionen) sind nur für bestimmte Gerätetypen verfügbar. Wenn das Gerät Speicherplatz enthält, sind alle vier Aktionen verfügbar. Bei anderen Geräten als Speichergeräten sind nur zwei Aktionen verfügbar. (Die Aktion **Nur Lesezugriff** ist für Bluetooth-Geräte nicht verfügbar. Diese Geräte können daher nur entweder gesperrt oder zugelassen werden).

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

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

HINWEIS

Wenn diese drei Bezeichner leer sind, ignoriert die Regel diese Felder bei der Zuordnung. Filterparameter in Textfeldern unterscheiden nicht zwischen Groß- und Kleinschreibung, und Platzhalter (*, ?) werden nicht unterstützt.

Um die Parameter eines Geräts zu ermitteln, erstellen Sie eine Regel für den entsprechenden Gerätetyp, schließen Sie das Gerät an den Computer an und überprüfen Sie dann die Gerätedetails im [Gerätesteuerung-Log](#).

Wählen Sie den **Logging-Schweregrad** in der Dropdownliste 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.

Die Regeln können auf bestimmte Benutzer oder Benutzergruppen beschränkt werden, indem Sie diese zur **Benutzerliste** hinzufügen. Klicken Sie auf **Bearbeiten**, um die Benutzerliste zu bearbeiten.

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

HINWEIS

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

Folgende Funktionen stehen zur Verfügung:

Bearbeiten

Mit dieser Option können Sie den Namen der ausgewählten Regel oder die Parameter der enthaltenen Geräte (Hersteller, Modell, Seriennummer) ändern.

Kopieren

Erstellt eine neue Regel mit den Parametern der ausgewählten Regel.

Löschen

Löscht die ausgewählte Regel. Alternativ können Sie eine Regel mit dem benachbarten Kontrollkästchen deaktivieren, falls Sie sie nicht dauerhaft löschen möchten, um sie später wieder verwenden zu können.

Auslesen

Bietet einen Überblick über alle aktuell angeschlossenen Geräte nebst Informationen zu Gerätetyp, Gerätehersteller, Modell und Seriennummer (sofern verfügbar). Wenn Sie ein Gerät (in der Liste der erkannten Geräte) auswählen und auf **OK** klicken, wird ein Regel-Editorfenster mit vordefinierten Informationen angezeigt (Sie können alle Einstellungen anpassen).

Die Regeln sind nach absteigender Priorität geordnet (Regeln mit höchster Priorität werden an oberster Stelle angezeigt). Sie können mehrere Regeln auswählen und Aktionen wie z. B. Löschen anwenden. Mit der Option **Oben/Nach oben/Nach unten/Unten** (Pfeilschaltflächen) können Sie außerdem alle Regeln in der Liste nach oben oder nach unten verschieben.

Gerätegruppen

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 vorhandenen Gruppen angezeigt. Wählen Sie rechts die Gruppe aus, in der die Geräte enthalten sind, die Sie anzeigen möchten.

Sie können unterschiedliche Gerätegruppen für Geräte erstellen, auf die jeweils unterschiedliche Regeln angewendet werden sollen. Sie können auch eine einzige Gerätegruppe erstellen, die als **Lesen/Schreiben** oder **Schreibgeschützt** festgelegt wird. So werden nicht erkannte Geräte durch die Gerätesteuerung gesperrt, wenn sie an den Computer angeschlossen werden.

WARNUNG

Externe Geräte, die an Ihren Computer angeschlossen sind, können ein Sicherheitsrisiko darstellen.

Folgende Funktionen stehen zur Verfügung:

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 Herstellername, Modell und Seriennummer eingeben).

Bearbeiten

Mit dieser Option können Sie den Namen der ausgewählten Gruppe oder die Parameter der in der Gruppe enthaltenen Geräte (Hersteller, Modell, Seriennummer) ändern.

Löschen

Löscht die ausgewählte Gruppe bzw. das ausgewählte Gerät, je nachdem, in welchen Fensterbereich Sie geklickt haben. Alternativ können Sie eine Regel mit dem benachbarten Kontrollkästchen deaktivieren, falls Sie sie nicht dauerhaft löschen möchten, um sie später wieder verwenden zu können.

Importieren

Importiert eine Liste von Geräteseriennummern aus einer Datei.

Auslesen

Bietet einen Überblick über alle aktuell angeschlossenen Geräte nebst Informationen zu Gerätetyp, Gerätehersteller, Modell und Seriennummer (sofern verfügbar). Wenn Sie ein Gerät (in der Liste der erkannten Geräte) auswählen und auf **OK** klicken, wird ein Regel-Editorfenster mit vordefinierten Informationen angezeigt (Sie können alle Einstellungen anpassen).

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

HINWEIS

Beachten Sie, dass bestimmte Rechte (Aktionen) nur für bestimmte Gerätetypen verfügbar sind. Wenn das Gerät über Speicherplatz verfügt, sind alle vier Aktionen verfügbar. Bei anderen Geräten als Speichergeräten sind nur zwei Aktionen verfügbar. (Die Aktion Nur Lesezugriff ist für Bluetooth-Geräte nicht verfügbar. Diese Geräte können daher nur entweder gesperrt oder zugelassen werden).

Tool-Konfiguration

In diesem Abschnitt können Sie die folgenden erweiterten Einstellungen anpassen:

- [Zeitfenster](#)
- [Scan-Ziele für ERA/ESMC](#)
- [Override-Modus](#)
- [ESET CMD](#)
- [ESET RMM](#)
- [Lizenz](#)
- [WMI-Anbieter](#)
- [Log-Dateien](#)
- [Proxyserver](#)
- [E-Mail-Benachrichtigungen](#)
- [Präsentationsmodus](#)
- [Diagnose](#)
- [Cluster](#)

Zeitfenster

Zeitfenster werden in [Regeln für die Gerätesteuerung](#) verwendet, um festzulegen, wann die Regeln angewendet werden. Erstellen Sie ein Zeitfenster und wählen Sie es beim Erstellen oder Bearbeiten von Regeln aus (Parameter **Anwendungszeitraum**). Auf diese Weise können Sie häufig verwendete Zeitfenster (Geschäftszeiten, Wochenende usw.) definieren und für mehrere Regeln wiederverwenden. Zeitfenster sollten für alle relevanten Regeltypen anwendbar sein, die eine zeitbasierte Kontrolle unterstützen.

Microsoft Windows Update

Windows-Updates stellen wichtige Korrekturen für möglicherweise gefährliche Schwachstellen bereit und verbessern das allgemeine Sicherheitsniveau des Computers. Aus diesem Grund ist es essenziell, dass Sie verfügbare Microsoft Windows-Updates sofort installieren. Entsprechend der von Ihnen festgelegten Richtlinien benachrichtigt Sie ESET Security for Microsoft SharePoint 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. Die aktualisierten Systemdaten stehen möglicherweise nicht unmittelbar nach Speicherung der Änderungen zur Verfügung.

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 Security for Microsoft SharePoint-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 Security for Microsoft SharePoint-Konfigurationen über die Befehlszeile importieren und exportieren. Sie können diesen Vorgang manuell ausführen oder ein Skript für die Automatisierung erstellen.

WICHTIG

Sie müssen die erweiterten ecmd-Befehle entweder mit Administratorberechtigungen oder in einer Windows-Befehlszeile (cmd) mit der Option **Als Administrator ausführen** verwenden. Andernfalls erhalten Sie die Nachricht **Error executing command..** Außerdem muss der ausgewählte Zielordner beim Exportieren einer Konfiguration vorhanden sein. Der Befehl zum Exportieren funktioniert auch, wenn die ESET CMD-Einstellung deaktiviert ist.

BEISPIEL

Befehl zum Exportieren von Einstellungen:

```
ecmd /getcfg c:\config\settings.xml
```

Befehl zum Importieren von Einstellungen:

```
ecmd /setcfg c:\config\settings.xml
```

HINWEIS

Die erweiterten ecmd-Befehle können nur lokal ausgeführt werden. Der Client-Task **Befehl ausführen** in ESET Security Management Center unterstützt diese Befehle nicht.

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 von `xmlsigntool.exe`.
4. Führen Sie den Befehl zum Signieren der *.xml*-Konfigurationsdatei mit der folgenden Syntax aus:
`xmlsigntool /version 1|2 <xml_file_path>`

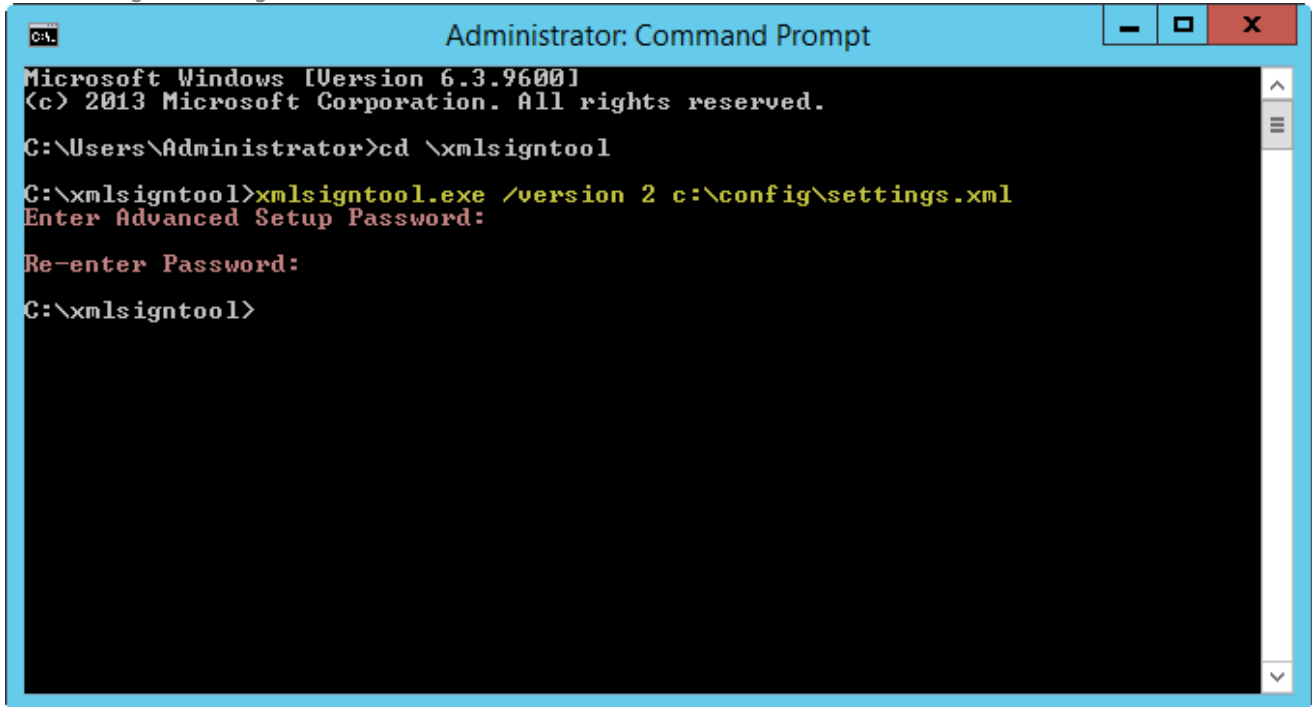
WICHTIG

Der Wert des Parameters `/version` hängt von Ihrer ESET Security for Microsoft SharePoint-Version ab. Verwenden Sie `/version 2` für ESET Security for Microsoft SharePoint 7 und neuere Versionen.

5. Geben Sie das Passwort für die [erweiterten Einstellungen](#) ein und bestätigen Sie es, wenn Sie vom XmlSignTool dazu aufgefordert werden. Ihre *.xml*-Konfigurationsdatei ist jetzt signiert und kann in einer anderen Instanz von ESET Security for Microsoft SharePoint mit ESET CMD und der Passwortautorisierungsmethode importiert werden.

BEISPIEL

Befehl zum Signieren einer exportierten Konfigurationsdatei: `xmldsigntool /version 2 c:\config\settings.xml`



```
Administrator: Command Prompt
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>cd \xmldsigntool
C:\xmldsigntool>xmldsigntool.exe /version 2 c:\config\settings.xml
Enter Advanced Setup Password:
Re-enter Password:
C:\xmldsigntool>
```

HINWEIS

Wenn sich das Passwort für die [erweiterten Einstellungen](#) geändert hat und Sie eine Konfiguration importieren möchten, die mit dem alten Passwort signiert wurde, können Sie die `.xml`-Konfigurationsdatei mit Ihrem aktuellen Passwort erneut signieren. Auf diese Weise können Sie eine ältere Konfigurationsdatei wiederverwenden, ohne sie vor dem Importieren auf einem anderen Computer mit ESET Security for Microsoft SharePoint erneut zu exportieren.

ESET RMM

Remote Monitoring and Management (RMM) bezieht sich auf die Überwachung und Kontrolle von Softwaresystemen (auf Desktops, Servern und Mobilgeräten) durch einen lokal installierten Agent, auf den über einen Verwaltungs-Dienstleister zugegriffen wird.

RMM aktivieren

Befehl zum Aktivieren von Remoteüberwachung und Verwaltung. Sie benötigen Administratorberechtigungen, um das RMM-Hilfsprogramm verwenden zu können.

Arbeitsmodus

Wählen Sie den RMM-Arbeitsmodus im Dropdownmenü aus.

- **Nur sichere Trennung** - Wenn Sie die RMM-Schnittstelle für sichere und schreibgeschützte Vorgänge aktivieren möchten
- **Alle Vorgänge** - Wenn Sie die RMM-Schnittstelle für alle Vorgänge aktivieren möchten


Autorisierungsmethode

Wählen Sie die RMM-Autorisierungsmethode im Dropdownmenü aus:

- **Keine** - Anwendungspfade werden nicht überprüft, Sie können *ermm.exe* mit beliebigen Anwendungen ausführen.
- **Anwendungspfad** - Geben Sie einen Anwendungspfad an, mit dem *ermm.exe* ausgeführt werden darf.

Die ESET Endpoint Security-Standardinstallation umfasst die Datei *ermm.exe* unter ESET Security for Microsoft SharePoint (Standardpfad: c:\Program Files\ESET\ESET Security for Microsoft SharePoint). *ermm.exe* tauscht Daten mit dem RMM-Plug-In aus, das mit dem RMM-Agent kommuniziert, der wiederum mit einem RMM-Server verbunden ist.

- *ermm.exe* - Ein von ESET entwickeltes Befehlszeilenhilfsprogramm zur Verwaltung von Endpoint-Produkten und für die Kommunikation ohne RMM-Plug-In.
- RMM-Plug-In - Eine externe Anwendung, die lokal auf dem Endpunkt-Windows-System ausgeführt wird. Das Plug-In wurde entwickelt, um mit einem bestimmten RMM-Agent (z. B. nur Kaseya) und mit *ermm.exe* zu kommunizieren.
- RMM-Agent - Eine externe Anwendung (z. B. von Kaseya), die lokal auf dem Endpunkt-Windows-System ausgeführt wird. Der Agent kommuniziert mit dem RMM-Plug-In und mit dem RMM-Server.
- RMM-Server - Wird als Dienst auf einem externen Server ausgeführt. Unterstützte RMM-Systeme sind von Kaseya, Labtech, Autotask, Max Focus und Solarwinds N-able verfügbar.

In unserem [Knowledgebase-Artikel](#)  finden Sie weitere Informationen zu ESET RMM in ESET Security for Microsoft SharePoint.

ESET Direct Endpoint Management-Plugins für RMM-Lösungen von Drittanbietern

Der RMM-Server wird als Dienst auf einem Drittanbieterserver gestartet. Weitere Informationen finden Sie in den folgenden Online-Anleitungen für ESET Direct Endpoint Management:

- [ESET Direct Endpoint Management-Plugin für die ConnectWise-Automatisierung](#) 
- [ESET Direct Endpoint Management-Plugin für DattoRMM](#) 
- [ESET Direct Endpoint Management für SolarWinds N-Central](#) 
- [ESET Direct Endpoint Management für NinjaRMM](#) 

Lizenz

ESET Security for Microsoft SharePoint verbindet sich mehrmals pro Stunde mit dem ESET-Lizenzserver, um Prüfungen auszuführen. Der Parameter **Intervallprüfung** ist standardmäßig auf **Automatisch** festgelegt. Wenn Sie den Netzwerkdatenverkehr für Lizenzprüfungen reduzieren möchten, ändern Sie die Intervallprüfung zu **eingeschränkt**, und die Lizenzprüfung wird nur noch einmal pro Tag (und nach Serverneustarts) ausgeführt.

Wenn die Intervallprüfung auf **Eingeschränkt** festgelegt ist, werden lizenzbezogene Änderungen an ESET Security for Microsoft SharePoint via ESET Business Account und am ESET MSP Administrator möglicherweise erst nach bis zu einem Tag übernommen.

WMI-Anbieter

Windows Management Instrumentation (WMI) ist die Microsoft-Implementierung von Web-Based Enterprise Management (WBEM), einer Brancheninitiative zur Entwicklung einer Standardtechnologie für den Zugriff auf Verwaltungsinformationen in einer Unternehmensumgebung.

Weitere Informationen zu WMI finden Sie bei

[http://msdn.microsoft.com/en-us/library/windows/desktop/aa384642\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/aa384642(v=vs.85).aspx) 

ESET WMI-Anbieter

Mit dem ESET WMI-Anbieter können Sie ESET-Produkte in einem Unternehmensnetzwerk ohne ESET-spezifische Software oder Tools remote überwachen. Die Bereitstellung von grundlegenden Produktinformationen, Statusinformationen und Statistiken über WMI bietet Administratoren umfangreiche neue Möglichkeiten bei der Überwachung von ESET-Produkten. Administratoren können die zahlreichen von WMI gebotenen Zugriffsmethoden nutzen (Befehlszeile, Skripte und Überwachungstools von Drittanbietern), um den Status ihrer ESET-Produkte zu überwachen.

In der aktuellen Bereitstellung steht ein Lesezugriff auf die grundlegenden Produktinformationen, auf Informationen zu installierten Funktionen und deren Schutzstatus, auf Statistiken einzelner Scan-Module und auf Produkt-Log-Dateien zur Verfügung.

Mit dem WMI-Anbieter können Sie die Windows WMI-Standardinfrastruktur und -Tools verwenden, um den Status von Produkt und Produkt-Logs auszulesen.

Bereitgestellte Daten

Alle WMI-Klassen in Bezug auf das ESET-Produkt befinden sich im Namespace „root\ESET“. Folgende Klassen sind derzeit implementiert und werden nachfolgend ausführlich beschrieben:

Allgemein

- ESET_Product
- ESET_Features
- ESET_Statistics

Logs

- ESET_ThreatLog
- ESET_EventLog
- ESET_ODFileScanLogs
- ESET_ODFileScanLogRecords
- ESET_ODServerScanLogs
- ESET_ODServerScanLogRecords
- ESET_HIPSLog
- ESET_URLLog
- ESET_DevCtrlLog
- ESET_GreylistLog
- ESET-MailServeg
- ESET_HyperVScanLogs
- ESET_HyperVScanLogRecords

ESET_Product-Klasse

Es darf nur eine Instanz der ESET_Product-Klasse vorhanden sein. Die Eigenschaften dieser Klasse beziehen sich auf grundlegende Informationen zum installierten ESET-Produkt:

- **ID** - Produkttyp-ID, zum Beispiel „esml“
- **Name** - Produktbezeichnung, zum Beispiel „ESET Mail Security“
- **FullName** - Vollständiger Name des Produkts, zum Beispiel „ESET Mail Security for IBM Domino“
- **Version** - Produktversion, zum Beispiel „6.5.14003.0“
- **VirusDBVersion** - Version der Signaturdatenbank, zum Beispiel „14533 (20161201)“
- **VirusDBLastUpdate** - Zeitstempel des letzten Update der Signaturdatenbank. Die Zeichenkette enthält den Zeitstempel im WMI-Format für Datum und Uhrzeit, zum Beispiel „20161201095245.000000+060“.
- **LicenseExpiration** - Lizenzablaufzeitpunkt. Die Zeichenkette enthält den Zeitstempel im WMI-Format
- **KernelRunning** - Boolescher Wert, der angibt, ob der ekrn-Dienst auf dem Computer ausgeführt wird, zum Beispiel „TRUE“
- **StatusCode** - Zahl, die den Schutzstatus des Produkts angibt: 0 - grün (OK), 1 - gelb (Warnung), 2 - rot (Fehler)
- **StatusText** - Beschreibung der Ursache, falls der StatusCode nicht null ist (andernfalls ist dieser Text leer)

ESET_Features-Klasse

Je nach Anzahl der Produktfunktionen hat die ESET_Features-Klasse mehrere Instanzen. Jede Instanz enthält Folgendes:

- **Name** - Name der Funktion (eine Liste der Namen finden Sie unten)
- **Status** - Status der Funktion: 0 - inaktiv, 1 - deaktiviert, 2 - aktiviert

Liste der Zeichenfolgen für aktuell erkannte Produktfunktionen:

- **CLIENT_FILE_AV** - Virenschutz des Echtzeit-Dateischutzes
- **CLIENT_WEB_AV** - Virenschutz für den Webzugriff des Client
- **CLIENT_DOC_AV** - Virenschutz für Dokumente auf dem Client
- **CLIENT_NET_FW** - Personal Firewall des Clients
- **CLIENT_EMAIL_AV** - Virenschutz für E-Mail-Programm auf dem Client
- **CLIENT_EMAIL_AS** - Spam-Schutz für E-Mail-Programm auf dem Client
- **SERVER_FILE_AV** - Echtzeit-Dateischutz für das geschützte Dateiserverprodukt, zum Beispiel Dateien in der SharePoint-Inhaltsdatenbank im Fall von ESET Security for Microsoft SharePoint
- **SERVER_EMAIL_AV** - Virenschutz für E-Mails auf dem geschützten Serverprodukt, zum Beispiel E-Mails in MS Exchange oder IBM Domino
- **SERVER_EMAIL_AS** - Spam-Schutz für E-Mails auf dem geschützten Serverprodukt, zum Beispiel E-Mails in MS Exchange oder IBM Domino
- **SERVER_GATEWAY_AV** - Virenschutz für geschützte Netzwerkprotokolle auf dem Gateway
- **SERVER_GATEWAY_AS** - Spam-Schutz für geschützte Netzwerkprotokolle auf dem Gateway

ESET_Statistics-Klasse

Je nach Anzahl der Scanner des Produkts hat die ESET_Statistics-Klasse mehrere Instanzen. Jede Instanz enthält Folgendes:

- **Scanner** - Zeichenkettencode für den bestimmten Scanner, zum Beispiel „CLIENT_FILE“
- **Total** - Gesamtzahl der gescannten Dateien
- **Infected** - Anzahl der gefundenen infizierten Dateien
- **Cleaned** - Anzahl der gesäuberten Dateien
- **Timestamp** - Zeitstempel der letzten Änderung dieser Statistik. Im WMI-Format für Datum und Uhrzeit, zum Beispiel „20130118115511.000000+060“
- **ResetTime** - Zeitstempel des letzten Zurücksetzens des Statistikzählers. Im WMI-Format für Datum und

Uhrzeit, zum Beispiel „20130118115511.000000+060“

Liste der Zeichenketten der derzeit erkannten Scanner:

- **CLIENT_FILE**
- **CLIENT_EMAIL**
- **CLIENT_WEB**
- **SERVER_FILE**
- **SERVER_EMAIL**
- **SERVER_WEB**

ESET_ThreatLog-Klasse

Die ESET_ThreatLog-Klasse hat mehrere Instanzen. Jede Instanz stellt einen Log-Eintrag aus dem Log „Erkannte Bedrohungen“ dar. Jede Instanz enthält Folgendes:

- **ID** - eindeutige ID dieses Prüfling-Eintrags
- **Timestamp** - Zeitstempel der Log-Erstellung (im WMI-Format für Datum/Uhrzeit)
- **LogLevel** - Schweregrad des Log-Eintrags, als Zahl zwischen 0 und 8. Die Werte entsprechen folgenden Schweregradstufen: Debug-Meldung, Information/Fußnote, Information, wichtige Information, Warnung, Fehler, Sicherheitswarnung, kritischer Fehler, kritische Sicherheitswarnung
- **Scanner** - Name des Scanners, der den Log-Eintrag erstellt hat
- **ObjectType** - Art des Objekts, das das Log-Ereignis ausgelöst hat
- **ObjectName** - Name des Objekts, das das Log-Ereignis ausgelöst hat
- **Threat** - Name der Bedrohung, die im Objekt mit den Eigenschaften „ObjectName“ und „ObjectType“ gefunden wurde
- **Action** - Aktion, die nach der Identifizierung der Bedrohung ausgeführt wurde
- **User** - Benutzerkonto, unter dem das Log-Ereignis erzeugt wurde
- **Information** - zusätzliche Beschreibung des Ereignisses
- **Hash** - Hash des Objekts, das das Log-Ereignis ausgelöst hat

ESET_EventLog

Die ESET_EventLog-Klasse hat mehrere Instanzen. Jede Instanz stellt einen Log-Eintrag aus dem Log „Ereignisse“ dar. Jede Instanz enthält Folgendes:

- **ID** - eindeutige ID dieses Prüfling-Eintrags
- **Timestamp** - Zeitstempel der Log-Erstellung (im WMI-Format für Datum/Uhrzeit)
- **LogLevel** - Schweregrad des Log-Eintrags, als Zahl zwischen 0 und 8. Die Werte entsprechen folgenden Schweregradstufen: Debug-Meldung, Information/Fußnote, Information, wichtige Information, Warnung, Fehler, Sicherheitswarnung, kritischer Fehler, kritische Sicherheitswarnung
- **Module** - Name des Moduls, das den Log-Eintrag erstellt hat
- **Event** - Beschreibung des Ereignisses
- **User** - Benutzerkonto, unter dem das Log-Ereignis erzeugt wurde

ESET_ODFileScanLogs

Die ESET_ODFileScanLogs-Klasse hat mehrere Instanzen. Jede stellt einen Eintrag des On-Demand-Datei-Scans dar. Dies entspricht der Log-Liste „On-Demand-Scan“ in der Benutzeroberfläche. Jede Instanz enthält Folgendes:

- **ID** - eindeutige ID dieses Prüfling-Eintrags
- **Timestamp** - Zeitstempel der Log-Erstellung (im WMI-Format für Datum/Uhrzeit)

- **Targets** - Zielordner/-objekte für die Prüfung
- **TotalScanned** - Gesamtzahl der geprüften Objekte
- **Infected** - Anzahl der gefundenen infizierten Objekte
- **Cleaned** - Anzahl der gesäuberten Objekte
- **Status** - Status des Scan-Vorgangs

ESET_ODFileScanLogRecords

Die ESET_ODFileScanLogRecords-Klasse hat mehrere Instanzen. Jede stellt einen Log-Eintrag in einem der Prüflogs dar, die jeweils einer Instanz der ESET_ODFileScanLogs-Klasse entsprechen. Die Instanzen dieser Klasse entsprechen den Log-Einträgen aller On-Demand-Scans/-Logs. Wenn nur die Instanz eines bestimmten Prüflogs benötigt wird, können Sie die Elemente über die Eigenschaft „LogID“ filtern. Jede Klasse enthält Folgendes:

- **LogID** - ID des Prüflogs, zu dem der Eintrag gehört (ID einer der Instanzen der ESET_ODFileScanLogs-Klasse)
- **ID** - eindeutige ID dieses Prüflog-Eintrags
- **Timestamp** - Zeitstempel der Log-Erstellung (im WMI-Format für Datum/Uhrzeit)
- **LogLevel** - Schweregrad des Log-Eintrags, als Zahl zwischen 0 und 8. Die Werte entsprechen folgenden Schweregradstufen: Debug-Meldung, Information/Fußnote, Information, wichtige Information, Warnung, Fehler, Sicherheitswarnung, kritischer Fehler, kritische Sicherheitswarnung
- **Log** - die eigentliche Log-Meldung

ESET_ODServerScanLogs

Die ESET_ODServerScanLogs-Klasse hat mehrere Instanzen. Jede stellt einen ausgeführten Lauf des On-Demand-Server-Scans dar. Jede Instanz enthält Folgendes:

- **ID** - eindeutige ID dieses Prüflog-Eintrags
- **Timestamp** - Zeitstempel der Log-Erstellung (im WMI-Format für Datum/Uhrzeit)
- **Targets** - Zielordner/-objekte für die Prüfung
- **TotalScanned** - Gesamtzahl der geprüften Objekte
- **Infected** - Anzahl der gefundenen infizierten Objekte
- **Cleaned** - Anzahl der gesäuberten Objekte
- **RuleHits** - Gesamtzahl der Regeltreffer
- **Status** - Status des Scan-Vorgangs

ESET_ODServerScanLogRecords

Die ESET_ODServerScanLogRecords-Klasse hat mehrere Instanzen. Jede stellt einen Log-Eintrag in einem der Prüflogs dar, die jeweils einer Instanz der ESET_ODServerScanLogs-Klasse entsprechen. Die Instanzen dieser Klasse entsprechen den Log-Einträgen aller On-Demand-Scans/-Logs. Wenn nur die Instanz eines bestimmten Prüflogs benötigt wird, können Sie die Elemente über die Eigenschaft „LogID“ filtern. Jede Klasse enthält Folgendes:

- **LogID** - ID des Prüflogs, zu dem der Eintrag gehört (ID einer der Instanzen der ESET_ODServerScanLogs-Klasse)
- **ID** - eindeutige ID dieses Prüflog-Eintrags
- **Timestamp** - Zeitstempel der Log-Erstellung (im WMI-Format für Datum/Uhrzeit)
- **LogLevel** - Schweregrad des Log-Eintrags, als Zahl zwischen 0 und 8. Die Werte entsprechen folgenden Schweregradstufen: Debug-Meldung, Information/Fußnote, Information, wichtige Information, Warnung, Fehler, Sicherheitswarnung, kritischer Fehler, kritische Sicherheitswarnung

- **Log** - die eigentliche Log-Meldung

ESET_SmtpProtectionLog

Die ESET_SmtpProtectionLog-Klasse hat mehrere Instanzen. Jede Instanz stellt einen Log-Eintrag aus dem „Smtp protection“-Log dar. Jede Instanz enthält Folgendes:

- **ID** - eindeutige ID dieses Prüfling-Eintrags
- **Timestamp** - Zeitstempel der Log-Erstellung (im WMI-Format für Datum/Uhrzeit)
- **LogLevel** - Schweregrad des Log-Eintrags, als Zahl zwischen 0 und 8. Die Werte entsprechen folgenden Schweregradstufen: Debug-Meldung, Information/Fußnote, Information, wichtige Information, Warnung, Fehler, Sicherheitswarnung, kritischer Fehler, kritische Sicherheitswarnung
- **HELODomain** - Name der HELO-Domäne
- **IP** - Quell-IP-Adresse
- **Sender** - Absender der E-Mail
- **Recipient** - Empfänger der E-Mail
- **Schutzart** – Art des verwendeten Schutzes
- **Action** - ausgeführte Aktion
- **Grund** – Grund für Aktion
- **TimeToAccept** - Anzahl der Minuten, nach der die E-Mail akzeptiert wird

ESET_HIPSLog

Die ESET_HIPSLog-Klasse hat mehrere Instanzen. Jede Instanz stellt einen Log-Eintrag aus dem „HIPS“-Log dar. Jede Instanz enthält Folgendes:

- **ID** - eindeutige ID des Log-Eintrags
- **Timestamp** - Zeitstempel der Log-Erstellung (im WMI-Format für Datum/Uhrzeit)
- **LogLevel** - Schweregrad des Log-Eintrags, als Zahl zwischen 0 und 8. Die Werte entsprechen folgenden Schweregradstufen: Debug-Meldung, Information/Fußnote, Information, wichtige Information, Warnung, Fehler, Sicherheitswarnung, kritischer Fehler, kritische Sicherheitswarnung
- **Application** - Quellenanwendung
- **Target** - Art der Operation
- **Action** - Von HIPS ausgeführte Aktion, z. B. erlauben, verweigern usw.
- **Rule** - Name der Regel, die für die Aktion verantwortlich ist
- **AdditionalInfo**

ESET_URLLog

Die ESET_URLLog-Klasse hat mehrere Instanzen. Jede Instanz stellt einen Log-Eintrag aus dem Log „Gefilterte Websites“ dar. Jede Instanz enthält Folgendes:

- **ID** - eindeutige ID des Log-Eintrags
- **Timestamp** - Zeitstempel der Log-Erstellung (im WMI-Format für Datum/Uhrzeit)
- **LogLevel** - Schweregrad des Log-Eintrags, als Zahl zwischen 0 und 8. Die Werte entsprechen folgenden Schweregradstufen: Debug-Meldung, Information/Fußnote, Information, wichtige Information, Warnung, Fehler, Sicherheitswarnung, kritischer Fehler, kritische Sicherheitswarnung
- **URL** - Die URL
- **Status** - Was ist mit der URL geschehen, z. B. „Gesperrt durch Web-Kontrolle“
- **Application** - Die Anwendung, die versucht hat, die URL zu öffnen
- **User** - Das Benutzerkonto, das die Anwendung ausgeführt hat

ESET_DevCtrlLog

Die ESET_DevCtrlLog-Klasse hat mehrere Instanzen. Jede Instanz stellt einen Log-Eintrag aus dem Log „Gerätesteuerung“ dar. Jede Instanz enthält Folgendes:

- **ID** - eindeutige ID des Log-Eintrags
- **Timestamp** - Zeitstempel der Log-Erstellung (im WMI-Format für Datum/Uhrzeit)
- **LogLevel** - Schweregrad des Log-Eintrags, als Zahl zwischen 0 und 8. Die Werte entsprechen folgenden Schweregradstufen: Debug-Meldung, Information/Fußnote, Information, wichtige Information, Warnung, Fehler, Sicherheitswarnung, kritischer Fehler, kritische Sicherheitswarnung
- **Device** - Gerätename
- **User** - Name des Benutzerkontos
- **UserSID** - SID des Benutzerkontos
- **Group** - Name der Benutzergruppe
- **GroupSID** - SID der Benutzergruppe
- **Status** - Was ist mit dem Gerät passiert, z. B. „Schreibzugriff gesperrt“
- **DeviceDetails** - Zusätzliche Informationen zum Gerät
- **EventDetails** - Zusätzliche Informationen zum Ereignis

ESET-MailServerLog

Die ESET-MailServerLog-Klasse hat mehrere Instanzen. Jede Instanz stellt einen Log-Eintrag aus dem „E-Mail-Server“-Log dar. Jede Instanz enthält Folgendes:

- **ID** - eindeutige ID des Log-Eintrags
- **Timestamp** - Zeitstempel der Log-Erstellung (im WMI-Format für Datum/Uhrzeit)
- **LogLevel** - Schweregrad des Log-Eintrags, als Zahl zwischen 0 und 8. Die Werte entsprechen folgenden Schweregradstufen: Debug-Meldung, Information/Fußnote, Information, wichtige Information, Warnung, Fehler, Sicherheitswarnung, kritischer Fehler, kritische Sicherheitswarnung
- **IPAddr** - Quell-IP-Adresse
- **HELODomain** - Name der HELO-Domäne
- **Sender** - Absender der E-Mail
- **Recipient** - Empfänger der E-Mail
- **Subject** - E-Mail-Betreff
- **ProtectionType** - Schutztyp, der die im aktuellen Logeintrag beschriebene Aktion ausgeführt hat, z. B. Malware-Schutz, Spam-Schutz oder Regeln.
- **Action** - ausgeführte Aktion
- **Reason** - Der Grund, aus dem die Aktion für den jeweiligen „ProtectionType“ auf dem Objekt ausgeführt wurde.

ESET_HyperVScanLogs

Die ESET_HyperVScanLogs-Klasse hat mehrere Instanzen. Jede stellt eine Ausführung des Hyper-V-Datei-Scans dar. Dies entspricht der Log-Liste „Hyper-V-Scan“ in der Benutzeroberfläche. Jede Instanz enthält Folgendes:

- **ID** - eindeutige ID des Log-Eintrags
- **Timestamp** - Zeitstempel der Log-Erstellung (im WMI-Format für Datum/Uhrzeit)
- **Targets** - Zielcomputer/-laufwerke/-volumes für die Prüfung
- **TotalScanned** - Gesamtzahl der geprüften Objekte
- **Infected** - Anzahl der gefundenen infizierten Objekte
- **Cleaned** - Anzahl der gesäuberten Objekte

- **Status** - Status des Scan-Vorgangs

ESET_HyperVScanLogRecords

Die ESET_HyperVScanLogRecords-Klasse hat mehrere Instanzen. Jede stellt einen Log-Eintrag in einem der Scan-Logs dar, die jeweils einer Instanz der ESET_HyperVScanLogs-Klasse entsprechen. Die Instanzen dieser Klasse entsprechen den Log-Einträgen aller Hyper-V-Scans/-Logs. Wenn Sie nur die Instanz eines bestimmten Scan-Logs benötigen, können Sie die Elemente über die Eigenschaft „LogID“ filtern. Jede Klasse enthält Folgendes:

- **LogID** - ID des Scan-Logs, zu dem der Eintrag gehört (ID einer der Instanzen der ESET_HyperVScanLogs-Klasse)
- **ID** - eindeutige ID des Log-Eintrags
- **Timestamp** - Zeitstempel der Log-Erstellung (im WMI-Format für Datum/Uhrzeit)
- **LogLevel** - Schweregrad des Log-Eintrags, als Zahl zwischen 0 und 8. Die Werte entsprechen folgenden Schweregradstufen: Debug-Meldung, Information/Fußnote, Information, wichtige Information, Warnung, Fehler, Sicherheitswarnung, kritischer Fehler, kritische Sicherheitswarnung
- **Log** - die eigentliche Log-Meldung

ESET_NetworkProtectionLog

Die ESET_NetworkProtectionLog-Klasse hat mehrere Instanzen. Jede Instanz stellt einen Log-Eintrag aus dem „Network protection“-Log dar. Jede Instanz enthält Folgendes:

- **ID** - eindeutige ID des Log-Eintrags
- **Timestamp** - Zeitstempel der Log-Erstellung (im WMI-Format für Datum/Uhrzeit)
- **LogLevel** - Schweregrad des Log-Eintrags, als Zahl zwischen 0 und 8. Die Werte entsprechen folgenden Schweregradstufen: Debug-Meldung, Information/Fußnote, Information, wichtige Information, Warnung, Fehler, Sicherheitswarnung, kritischer Fehler, kritische Sicherheitswarnung
- **Event** – Ereignis, das die Netzwerkschutzaktion auslöst
- **Action** – vom Netzwerkschutz ausgeführte Aktion
- **Source** – Quelladresse des Netzwerkgeräts
- **Target** – Zieladresse des Netzwerkgeräts
- **Protocol** – Netzworkkommunikationsprotokoll
- **RuleOrWormName** – Name der Regel oder des Wurms, die/der mit dem Ereignis verknüpft ist
- **Application** – Anwendung, die die Netzworkkommunikation initiiert hat
- **User** - Benutzerkonto, unter dem das Log-Ereignis erzeugt wurde

ESET_SentFilesLog

Die ESET_SentFilesLog-Klasse hat mehrere Instanzen. Jede Instanz stellt einen Log-Eintrag aus dem „Sent files“-Log dar. Jede Instanz enthält Folgendes:

- **ID** - eindeutige ID des Log-Eintrags
- **Timestamp** - Zeitstempel der Log-Erstellung (im WMI-Format für Datum/Uhrzeit)
- **LogLevel** - Schweregrad des Log-Eintrags, als Zahl zwischen 0 und 8. Die Werte entsprechen folgenden Schweregradstufen: Debug-Meldung, Information/Fußnote, Information, wichtige Information, Warnung, Fehler, Sicherheitswarnung, kritischer Fehler, kritische Sicherheitswarnung
- **Sha1** – SHA-1-Hash der gesendeten Datei
- **File** – gesendete Datei
- **Size** – Größe der gesendeten Datei
- **Category** – Kategorie der gesendeten Datei

- **Reason** – Grund für das Senden der Datei
- **SentTo** – ESET-Abteilung, an die die Datei gesendet wurde
- **User** - Benutzerkonto, unter dem das Log-Ereignis erzeugt wurde

ESET_OneDriveScanLogs

Die ESET_OneDriveScanLogs-Klasse hat mehrere Instanzen. Jede stellt eine Ausführung des OneDrive-Scans dar. Dies entspricht der Log-Liste „OneDrive Scan“ in der Benutzeroberfläche. Jede Instanz enthält Folgendes:

- **ID** – eindeutige ID des OneDrive-Logs
- **Timestamp** - Zeitstempel der Log-Erstellung (im WMI-Format für Datum/Uhrzeit)
- **Targets** - Zielordner/-objekte für die Prüfung
- **TotalScanned** - Gesamtzahl der geprüften Objekte
- **Infected** - Anzahl der gefundenen infizierten Objekte
- **Cleaned** - Anzahl der gesäuberten Objekte
- **Status** - Status des Scan-Vorgangs

ESET_OneDriveScanLogRecords

Die ESET_OneDriveScanLogRecords-Klasse hat mehrere Instanzen. Jede stellt einen Log-Eintrag in einem der Scan-Logs dar, die jeweils einer Instanz der ESET_OneDriveScanLogRecords-Klasse entsprechen. Die Instanzen dieser Klasse entsprechen den Log-Einträgen aller OneDrive-Scans/-Logs. Wenn nur die Instanz eines bestimmten Prüflogs benötigt wird, können Sie die Elemente über die Eigenschaft „LogID“ filtern. Jede Instanz enthält Folgendes:

- **LogID** – ID des Scan-Logs, zu dem der Eintrag gehört (ID einer der Instanzen der ESET_OneDriveScanLogs-Klasse)
- **ID** – eindeutige ID des OneDrive-Logs
- **Timestamp** - Zeitstempel der Log-Erstellung (im WMI-Format für Datum/Uhrzeit)
- **LogLevel** - Schweregrad des Log-Eintrags, als Zahl zwischen 0 und 8. Die Werte entsprechen folgenden Schweregradstufen: Debug-Meldung, Information/Fußnote, Information, wichtige Information, Warnung, Fehler, Sicherheitswarnung, kritischer Fehler, kritische Sicherheitswarnung
- **Log** - die eigentliche Log-Meldung

Zugriff auf die bereitgestellten Daten

Hier finden Sie einige Beispiele dazu, wie Sie über die Windows-Befehlszeile und PowerShell auf die ESET-WMI-Daten zugreifen können. Beide Methoden funktionieren in allen aktuellen Windows-Betriebssystemen. Es stehen jedoch mit anderen Skriptsprachen und Tools zahlreiche weitere Möglichkeiten für den Zugriff auf die Daten zur Verfügung.

Befehlszeile ohne Skripts

Mit dem `wmic`-Kommandozeilentool können Sie auf verschiedene vordefinierte und beliebige benutzerdefinierte WMI-Klassen zugreifen.

So zeigen Sie die vollständigen Informationen zum Produkt auf dem lokalen Computer an:

```
wmic /namespace:\\root\ESET Path ESET_Product
```

So zeigen Sie nur die Produktversion des Produkts auf dem lokalen Computer an:


```
wmic /namespace:\\root\ESET Path ESET_Product Get Version
```

So zeigen Sie die vollständigen Informationen zum Produkt auf dem Remote-Computer mit der IP-Adresse 10.1.118.180 an:

```
wmic /namespace:\\root\ESET /node:10.1.118.180 /user:Administrator Path ESET_Product
```

PowerShell

So rufen Sie die vollständigen Informationen zum Produkt auf dem lokalen Computer ab und zeigen Sie an:

```
Get-WmiObject ESET_Product -namespace 'root\ESET'
```

So rufen Sie die vollständigen Informationen zum Produkt auf dem Remote-Computer mit der IP-Adresse 10.1.118.180 ab und zeigen Sie an:

```
$cred = Get-Credential # fordert den Benutzer zur Eingabe der Anmeldedaten auf und speichert diese Informationen in einer Variable  
Get-WmiObject ESET_Product -namespace 'root\ESET' -computername '10.1.118.180' -cred $cred
```

Scan-Ziele für ERA/ESMC

Mit dieser Funktion kann [ESET Security Management Center](#) das Scan-Ziel (On-Demand-Postfachdatenbank-Scan und [Hyper-V-Scan](#)) verwenden, wenn der Client-Task **Server-Scan** auf einem Server mit ESET Security for Microsoft SharePoint ausgeführt wird. Die Einstellung für ERA/ESMC-Scan-Ziele ist nur verfügbar, wenn der ESET Management Agent installiert ist. Andernfalls ist die Funktion deaktiviert.


Mit der Funktion **Liste der Ziele generieren** erstellt ESET Security for Microsoft SharePoint eine Liste der aktuell verfügbaren Prüfziele. Diese Liste wird regelmäßig gemäß dem festgelegten **Updateintervall** erzeugt.

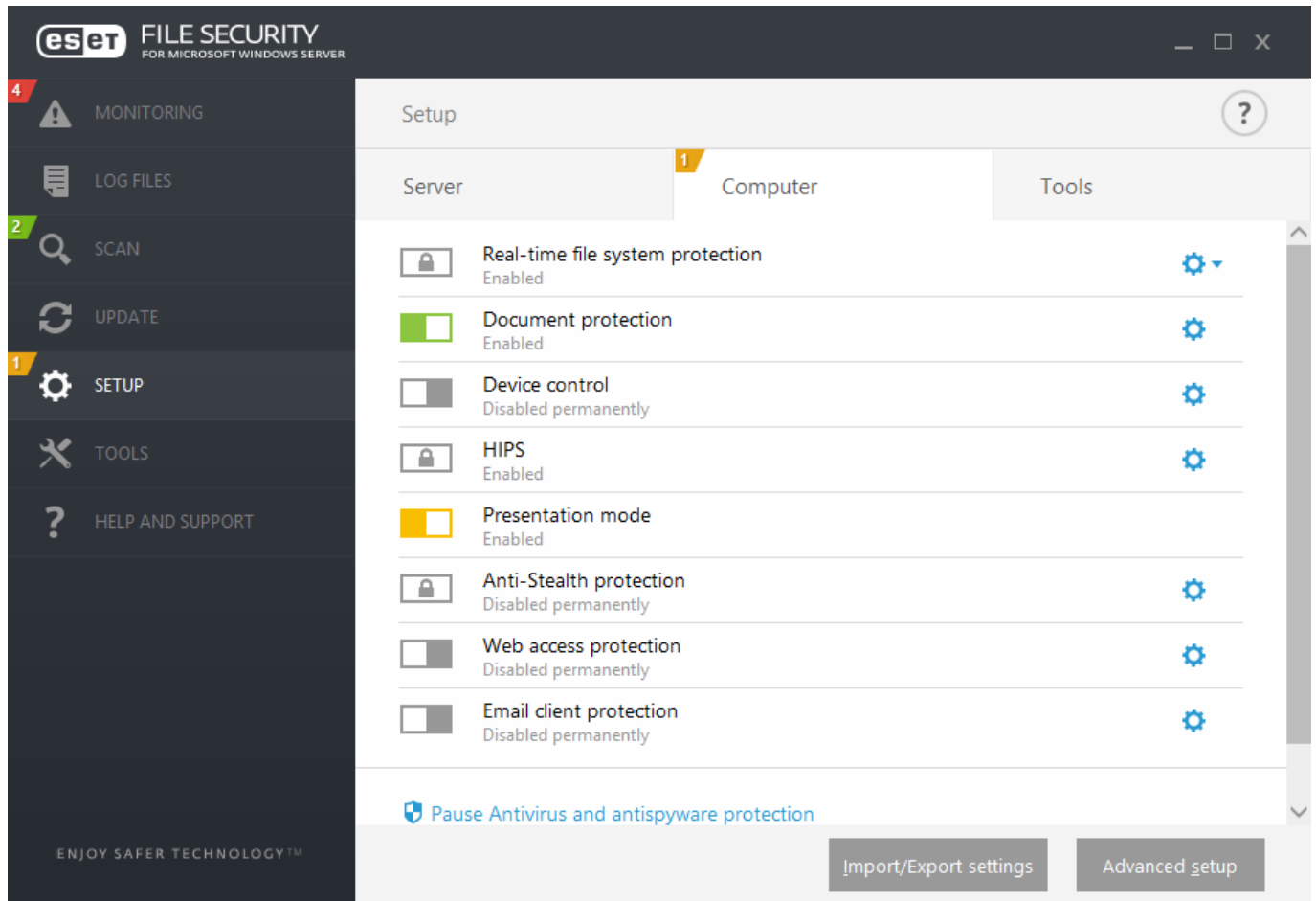
HINWEIS

Wenn Sie Option **Liste der Ziele generieren** zum ersten Mal aktivieren, braucht ESET Security Management Center ca. die Hälfte des angegebenen **Updateintervalls** für die Erfassung. Bei einem **Updateintervall** von 60 Minuten braucht ESMC also ca. 30 Minuten, um die Liste der Prüfziele zu empfangen. Falls ESET Security Management Center die Liste früher abrufen soll, können Sie ein kleineres Updateintervall festlegen. Sie können das Intervall später jederzeit verlängern.

Wenn ESET Security Management Center den Clienttask **Server-Scan** ausführt, wird die Liste abgerufen, und Sie können die Scan-Ziele für die [Hyper-V-Scan](#) auf dem entsprechenden Server auswählen.

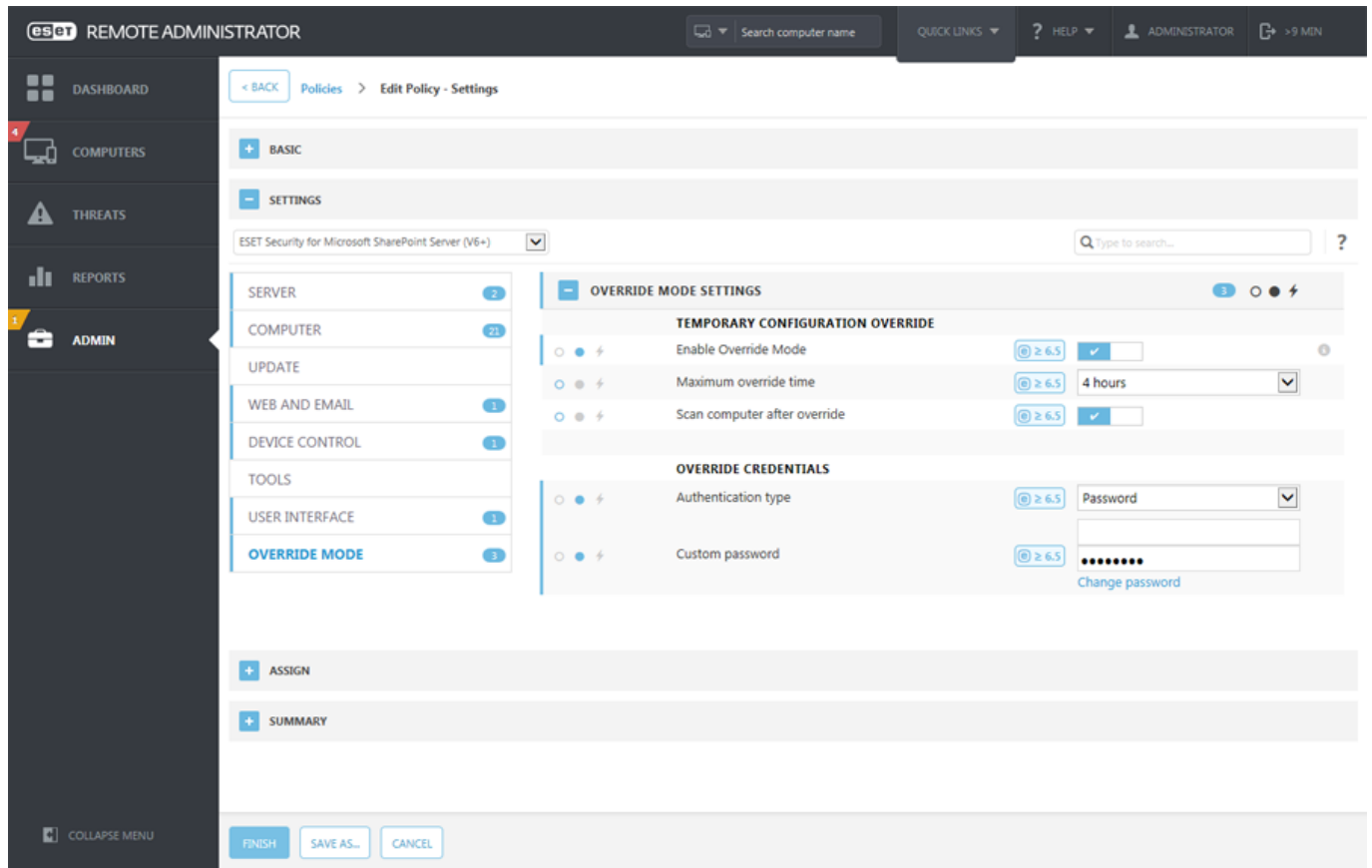
Override-Modus

Wenn Sie die ESET Security Management Center-Policy für ESET Security for Microsoft SharePoint anwenden, wird je ein Sperrsymbol  anstelle des Schalters zum Aktivieren und Deaktivieren in den [Einstellungen](#) und neben dem Schalter in den **Erweiterten Einstellungen** angezeigt.

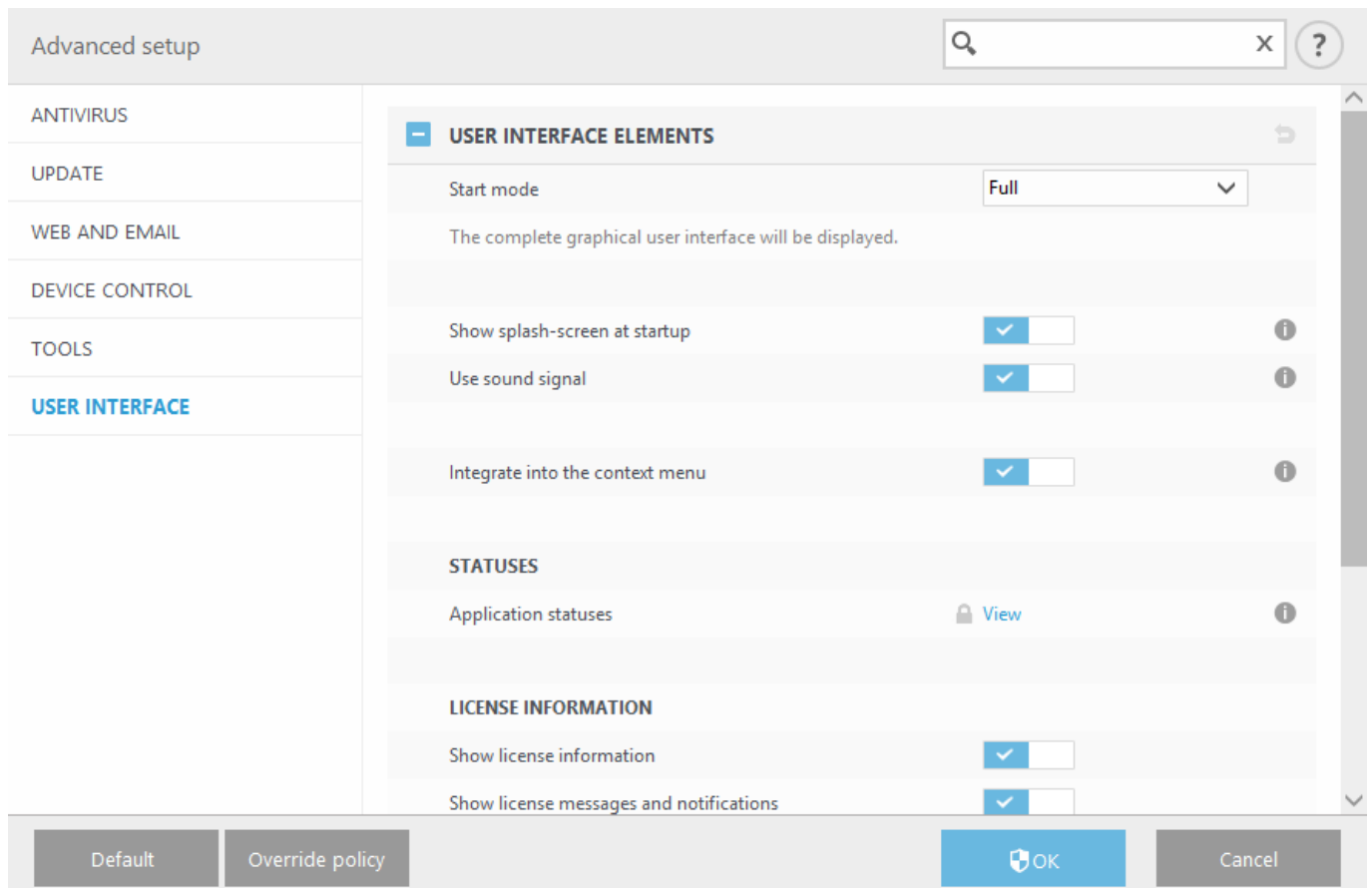


Einstellungen, die per ESET Security Management Center-Policy konfiguriert wurden, können normalerweise nicht geändert werden. Mit dem Override-Modus können Sie diese Einstellungen vorübergehend außer Kraft setzen. Dazu müssen Sie jedoch den **Override-Modus** mit einer ESET Security Management Center-Policy aktivieren.

Melden Sie sich bei der [ESMC-Web-Konsole](#) an, navigieren Sie zu **Policies**, und bearbeiten Sie entweder eine auf ESET Security for Microsoft SharePoint angewendete vorhandene Policy oder erstellen Sie eine neue Policy. Klicken Sie in den **Einstellungen** auf **Override-Modus**, aktivieren Sie den Modus, und konfigurieren Sie die restlichen Einstellungen inklusive des Authentifizierungstyps (**Active Directory-Benutzer** oder **Passwort**).

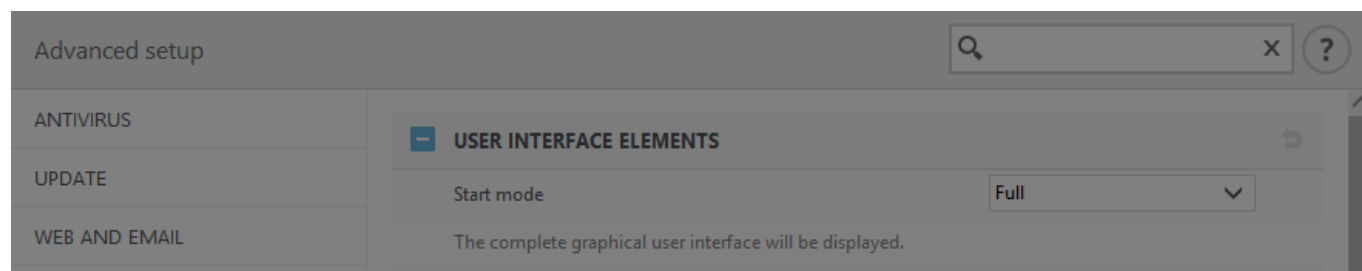


Nachdem Sie die Policy bearbeitet bzw. die neue Policy auf ESET Security for Microsoft SharePoint angewendet haben, wird die Schaltfläche Policy außer Kraft setzen im Fenster Erweiterte Einstellungen angezeigt.



Klicken Sie auf die Schaltfläche **Policy außer Kraft setzen**, legen Sie die Dauer fest und klicken Sie auf

Übernehmen.



Temporary policy override

Set the duration for which the policy settings can be overridden. After this duration the configuration will revert to the policy.

Override duration

4 hours ▼

10 min

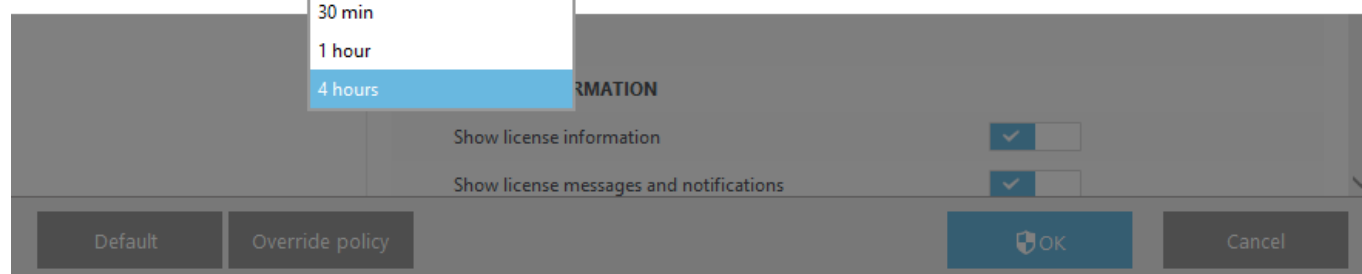
30 min

1 hour

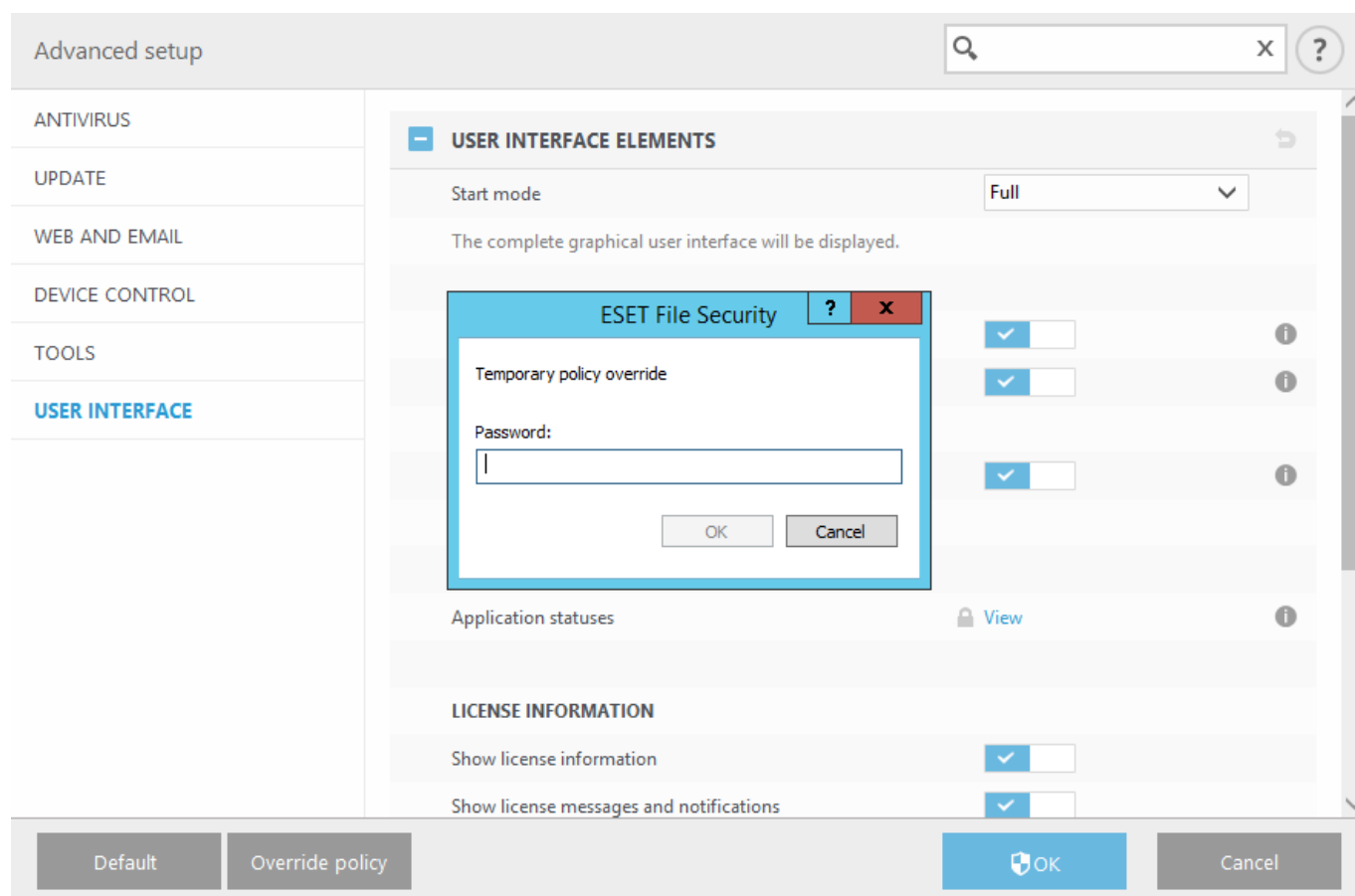
4 hours

Apply

Cancel



Falls Sie den Authentifizierungstyp **Passwort** ausgewählt haben, müssen Sie das Override-Passwort eingeben.



Nach Ablauf des Override-Modus werden alle vorgenommenen Konfigurationsänderungen wieder auf die ESET Security Management Center-Policeinstellungen zurückgesetzt. Vor dem Ablauf des Override-Modus wird eine Benachrichtigung angezeigt.

Sie können den **Override-Modus** jederzeit auf der [Überwachungsseite](#) oder in den **Erweiterten Einstellungen** vorzeitig beenden.

Log-Dateien

In diesem Bereich können Sie die Logging-Konfiguration von ESET Security for Microsoft SharePoint ändern.

[Loggingfilter](#)

Produziert eine große Menge an Daten, da standardmäßig alle Loggingoptionen aktiviert werden. Deaktivieren Sie nach Möglichkeit das Logging für die Komponenten, die für Ihr Problem nicht relevant sind.

HINWEIS

Um das allgemeine Logging zu aktivieren, müssen Sie die **Diagnose-Logs** im Hauptmenü unter **Einstellungen > Tools** aktivieren. Nachdem Sie die Loggingfunktion aktiviert haben, sammelt ESET Security for Microsoft SharePoint ausführliche Logs, je nachdem, welche Funktionen in diesem Bereich aktiviert sind.

Mit den Schaltern können Sie einzelne Features aktivieren oder deaktivieren. Diese möglichen Kombinationen für diese Optionen hängen von der Verfügbarkeit einzelner Komponenten in ESET Security for Microsoft SharePoint ab.

- **Diagnoseprotokollierung für SharePoint** - Schreibt ausführliche Informationen in die Logs, insbesondere für die Problembehandlung.
- **Cluster-Diagnose-Logging** - Das Cluster-Logging ist in den allgemeinen Diagnose-Logs enthalten.

[Log-Dateien](#)

Hier können Sie Einstellungen für Logs festlegen, um zu verhindern, dass die Festplatte vollläuft. Mit den Standardeinstellungen werden ältere Logs automatisch gelöscht, um Platz auf der Festplatte zu sparen.

Einträge automatisch löschen, die älter sind als (Tage)

Log-Einträge, die älter sind als die angegebene Anzahl an Tagen, werden automatisch gelöscht.

Bei Überschreitung der Log-Größe automatisch alte Einträge löschen

Wenn die Log-Größe **Max Log-Größe [MB]** überschreitet, werden alte Log-Einträge gelöscht, bis die **Reduzierte Log-Größe [MB]** erreicht ist.

Automatisch gelöschte Einträge sichern

Automatisch gelöschte Log-Einträge und -Dateien werden im angegebenen Verzeichnis gesichert und optional als ZIP-Datei komprimiert.

Diagnose-Logs sichern

Automatisch gelöschte Diagnose-Logs werden gesichert. Wenn diese Option nicht aktiviert ist, werden die Einträge der Diagnose-Logs nicht gesichert.

Sicherungsordner

Der Ordner, in dem die Log-Sicherungen gespeichert werden. Sie können festlegen, dass die Log-Sicherungen als ZIP-Datei komprimiert werden sollen.

Log-Dateien automatisch optimieren

Diese Option defragmentiert die Log-Dateien automatisch, wenn die Fragmentierung höher ist als der unter **Wenn ungenutzte Einträge größer als (%)** angegebene Wert. Klicken Sie zum Defragmentieren der Log-Dateien auf **Optimieren**. Bei diesem Prozess werden alle leeren Log-Einträge gelöscht, um Leistung und Log-Verarbeitung zu verbessern. Eine starke Verbesserung ist insbesondere dann erkennbar, wenn die Logs eine große Anzahl an Einträgen enthalten.

Textprotokoll aktivieren

Diese Option aktiviert die Speicherung von Logs in einem anderen, von den [Log-Dateien](#) getrennten Format:

- **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 Erkannte Bedrohungen in 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 (Sie finden dieses Log in der Ereignisanzeige in der Systemsteuerung).
- **Alle Log-Dateien löschen** – Löscht alle im Dropdownmenü **Typ** ausgewählten Logs.

HINWEIS

Um ein Problem schneller beheben zu können, werden Sie vom ESET-Support 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 unserem [Knowledgebase-Artikel](#).

Proxyserver

In großen lokalen Netzwerken wird die Verbindung zum Internet häufig über Proxyserver vermittelt. Wenn dies der Fall ist, müssen die nachfolgend beschriebenen Einstellungen vorgenommen werden. Andernfalls ist es unter Umständen nicht möglich, Updates automatisch über das Internet zu beziehen. Die Proxyserver-Einstellungen in ESET Security for Microsoft SharePoint können in zwei verschiedenen Bereichen der **erweiterten Einstellungen (F5)** konfiguriert werden:

1. **Erweiterte Einstellungen (F5) > Update > Profile > Updates > Verbindungsoptionen > HTTP-Proxy**

Diese Einstellung gilt für das entsprechende Update-Profil und wird für Laptops empfohlen, da diese die Updates der Signaturdatenbank oft aus verschiedenen Quellen beziehen.

2. Erweiterte Einstellungen (F5) > Tools > Proxyserver

Auf dieser Ebene können Sie die globalen Proxyservereinstellungen für alle Funktionen von ESET Security for Microsoft SharePoint festlegen. Diese Parameter werden von allen Modulen verwendet, die sich mit dem Internet verbinden.

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

Proxyserver erfordert Authentifizierung

Falls für die Netzwerkkommunikation über den Proxyserver eine Authentifizierung erforderlich ist, aktivieren Sie diese Option und geben Sie **Benutzername** und **Passwort** an.

Proxyserver automatisch erkennen

Klicken Sie auf **Erkennen**, wenn die Einstellungen des Proxyservers automatisch erkannt und ausgefüllt werden sollen. Die in Internet Explorer festgelegten Einstellungen werden kopiert.

HINWEIS

Diese Funktion ruft keine Anmeldedaten (Benutzername und Passwort) ab; Sie müssen diese Informationen selbst eingeben.

Direktverbindung verwenden, wenn der Proxy nicht verfügbar ist

Wenn in der Produktkonfiguration die Nutzung eines HTTP-Proxys vorgesehen ist und der Proxy nicht erreichbar ist, umgeht das Produkt den Proxy und kommuniziert direkt mit ESET-Servern.

Benachrichtigungen

Hinweise auf dem Desktop und Sprechblasen dienen ausschließlich zu Informationszwecken; Eingaben des Benutzers sind nicht erforderlich. Sie werden im Infobereich der Taskleiste rechts unten auf dem Bildschirm angezeigt. Weitere Optionen, wie Anzeigedauer und Transparenz können unten geändert werden. Aktivieren Sie **Desktopbenachrichtigungen nicht anzeigen, wenn Anwendungen im Vollbildmodus ausgeführt werden**, um keine nicht-interaktiven Benachrichtigungen anzuzeigen.

Benachrichtigungen über erfolgreiche Updates anzeigen

Wenn ein Update erfolgreich ausgeführt wurde, wird eine Popupnachricht angezeigt.

Ereignisbenachrichtigungen per E-Mail versenden

Diese Funktion aktiviert die E-Mail-Benachrichtigungen.

Anwendungsbenachrichtigungen

Klicken Sie auf [Bearbeiten](#), um Anwendungsbenachrichtigungen zu aktivieren oder zu deaktivieren.

Anwendungsbenachrichtigungen

Sie können festlegen, ob die ESET Security for Microsoft SharePoint-Benachrichtigungen auf dem Desktop angezeigt und/oder per E-Mail verschickt werden sollen.

HINWEIS

Achten Sie für E-Mail-Benachrichtigungen darauf, die Option **Ereignisbenachrichtigungen per E-Mail versenden** im Abschnitt **Einfach** zu aktivieren und den [SMTP-Server](#) und weitere Details nach Bedarf zu konfigurieren.

Selected application notifications will be displayed ?

Name	Show on desktop	Send by email
ANTIVIRUS		
Failed to initialize Anti-Stealth	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Initial scan has started	<input checked="" type="checkbox"/>	<input type="checkbox"/>
DEVICE CONTROL		
Device is allowed	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Device is blocked	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Device is blocked for writing	<input checked="" type="checkbox"/>	<input type="checkbox"/>
EMAIL		
Integration errors	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
GENERAL		
Advanced logging enabled	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Anonymous statistics was sent	<input type="checkbox"/>	<input checked="" type="checkbox"/>

OK **Cancel**

Desktophinweise

Sie können festlegen, wie ESET Security for Microsoft SharePoint Bedrohungswarnungen und Systembenachrichtigungen (z. B. erfolgreiche Updates) verarbeiten soll. Konfigurieren Sie die **Anzeigedauer** und **Transparenz** von Meldungen im Infobereich (nur für Systeme, die Benachrichtigungen im Infobereich der Taskleiste unterstützen).

Im Dropdownmenü **Mindestinformationen anzuzeigender Ereignisse** können Sie den Schweregrad für Warnungen und Benachrichtigungen auswählen. Die folgenden Optionen stehen zur Verfügung:

- **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.
- **Kritisch** - Nur kritische Fehler werden protokolliert.

Mit dem Feld **Auf Mehrbenutzersystemen Benachrichtigungen auf dem Bildschirm des folgenden Benutzers ausgeben** können Sie festlegen, bei welchem Benutzer Warnungen und Benachrichtigungen angezeigt werden, wenn mehrere Benutzer gleichzeitig angemeldet sind. Üblicherweise wird hier der System- oder Netzwerkadministrator gewählt. Besonders sinnvoll ist diese Option bei Terminalservern, sofern alle Systemmeldungen an den Administrator gesendet werden.

E-Mail-Benachrichtigungen

ESET Security for Microsoft SharePoint kann automatisch Ereignismeldungen senden, wenn ein Ereignis mit dem ausgewählten Informationsumfang auftritt.

HINWEIS

ESET Security for Microsoft SharePoint unterstützt keine SMTP-Server mit TLS-Verschlüsselung.

SMTP-Server

Der Name des SMTP-Servers für den Versand von Warnungen und Benachrichtigungen. Dies ist normalerweise der Name Ihres Microsoft Exchange-Servers.

Benutzername und Passwort

Falls für den SMTP-Server Zugangsdaten zur Authentifizierung erforderlich sind, geben Sie hier einen gültigen Benutzernamen und das Passwort ein.

Absenderadresse

Geben Sie die Absenderadresse ein, die in der Kopfzeile von Benachrichtigungs-E-Mails angezeigt werden soll. Diese Adresse wird dem Empfänger als **Absender** angezeigt.

Empfängeradresse

Geben Sie die **E-Mail-Adresse** ein, die Benachrichtigungen erhalten soll.

TLS aktivieren

Aktiviert die der TLS-Verschlüsselung unterstützten Warnungen und Benachrichtigungen.

E-Mail-Einstellungen

Informationsumfang der Meldungen

Gibt den Mindest-Informationsumfang für zu verschickende Benachrichtigungen an.

Intervall bis zum Senden neuer Benachrichtigungs-E-Mails (Min.)

Intervall in Minuten, nach dem neue Benachrichtigungen per E-Mail gesendet werden. Legen Sie für diese Einstellung den Wert „0“ fest, wenn die Benachrichtigungen sofort gesendet werden sollen.

Jede Benachrichtigung in einer getrennten E-Mail senden

Wenn diese Option aktiviert ist, erhält der Empfänger für jede einzelne Benachrichtigung eine separate E-Mail. Dies kann dazu führen, dass innerhalb kurzer Zeit eine große Anzahl E-Mails verschickt wird.

Format von Meldungen

Ereignismeldungen werden als E-Mails oder LAN-Nachrichten (Windows Messenger-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 für Ereignisse auf Remotecomputern.

Format der Meldungen bei Bedrohungen

Warnungen und Benachrichtigungen besitzen ein vordefiniertes Standardformat. Dieses Format sollte nicht geändert werden. Unter bestimmten Umständen (etwa, wenn Sie ein automatisiertes E-Mail-Verarbeitungssystem verwenden) ist es jedoch möglicherweise erforderlich, das Meldungsformat zu ändern.

Schlüsselwörter (durch %-Zeichen getrennte Zeichenfolgen) in der Meldung werden durch entsprechende Informationen ersetzt. Folgende Schlüsselwörter sind verfügbar:

- **%TimeStamp%** - Datum und Uhrzeit des Ereignisses
- **%Scanner%** - betroffenes Modul
- **%ComputerName%** - Name des Computers, auf dem die Warnmeldung aufgetreten ist
- **%ProgramName%** - Programm, das die Warnung erzeugt hat
- **%InfectedObject%** - Name der infizierten Datei, Nachricht usw.
- **%VirusName%** - Angabe des Infektionsverursachers
- **%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.

Zeichensatz

Wählen Sie eine Kodierung im Dropdownmenü aus. Die E-Mail-Nachricht wird gemäß der ausgewählten Zeichenkodierung konvertiert.

Quoted-Printable-Kodierung verwenden

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

Anpassen

Diese Nachricht wird in der Fußzeile aller ausgewählten Benachrichtigungen angezeigt.

Standardbenachrichtigung

Eine Standardnachricht, die in der Fußzeile von Benachrichtigungen angezeigt wird.

Bedrohungen

Warnhinweise für Bedrohungen nicht automatisch schließen

Benachrichtigungen für Schadsoftware müssen manuell geschlossen werden.

Standardnachricht verwenden

Sie können die Standardnachricht deaktivieren und eine benutzerdefinierte **Benachrichtigung** festlegen, die angezeigt wird, wenn eine Bedrohung blockiert wurde.

Bedrohungsbenachrichtigung

Geben Sie eine benutzerdefinierte Nachricht an, die beim Sperren einer Bedrohung angezeigt wird.

Präsentationsmodus

Der Präsentationsmodus ist eine Funktion für Benutzer, die ihre Software ununterbrochen nutzen, nicht durch Popup-Fenster gestört werden und die CPU-Auslastung reduzieren möchten. Der Präsentationsmodus kann auch für Präsentationen verwendet werden, die nicht durch Aktivitäten von ESET Security for Microsoft SharePoint unterbrochen werden dürfen. Wenn er aktiviert ist, werden alle Popup-Fenster deaktiviert und geplante Tasks werden nicht ausgeführt. Der Systemschutz läuft weiter im Hintergrund, aber es sind keine Eingaben durch den Benutzer erforderlich.

Präsentationsmodus automatisch aktivieren, wenn Anwendungen im Vollbildmodus ausgeführt werden

Der Präsentationsmodus wird automatisch aktiviert, wenn Sie eine Vollbildanwendung ausführen. Im Präsentationsmodus werden keine Benachrichtigungen oder [Statusänderungen](#) von ESET Security for Microsoft SharePoint angezeigt.

Präsentationsmodus automatisch deaktivieren nach

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

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 Security for Microsoft SharePoint Probleme.

Klicken Sie auf das Dropdownmenü neben **Typ des Speicherabbaus** und wählen Sie eine von drei Optionen aus:

- **Deaktivieren** – Deaktiviert diese Funktion.
- **Mini** – (Standardeinstellung) Protokolliert die kleinste Menge an Daten, die helfen könnten, die Ursache für den Absturz der Anwendung herauszufinden. Dieser Dumpdateityp ist eher zu empfehlen, wenn der Speicherplatz begrenzt 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 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 *Windows Explorer*-Fenster zu öffnen.

Diagnoseabbild erstellen

Klicken Sie auf **Erstellen**, um Diagnoseabbilder im Zielverzeichnis zu erstellen.

[Erweitertes Logging](#)

Erweitertes Logging für die Medienkontrolle aktivieren

Erfassen Sie alle in der Medienkontrolle aufgetretenen Ereignisse zu Diagnose- und Problembehebungszwecken.

Erweitertes Kernel-Logging aktivieren

Erfassen Sie alle im ESET-Kerneldienst (**ekrn**) aufgetretenen Ereignisse zu Diagnose- und Problembehebungszwecken.

Erweitertes Logging für Lizenzierung aktivieren

Gesamte Produktkommunikation mit dem Lizenzserver aufzeichnen.

Erweitertes Logging für den Netzwerkschutz aktivieren

Erfasst alle Daten, die den Netzwerkschutz durchlaufen, im PCAP-Format, um den Entwicklern bei der Diagnose und Behebung von Problemen im Zusammenhang mit dem Netzwerkschutz zu helfen.

Erweitertes Betriebssystem-Logging aktivieren

Zusätzliche Informationen zum Betriebssystem wie ausgeführte Prozesse, CPU-Aktivität und Laufwerksoperationen werden erfasst.

Erweitertes Logging für Protokollfilterung aktivieren

Erfasst alle Daten, die die Protokollfilterung durchlaufen, im PCAP-Format, um den Entwicklern bei der Diagnose und Behebung von Problemen im Zusammenhang mit der Protokollfilterung zu helfen.

Erweitertes Logging für Update-Modul aktivieren

Erfasst alle Ereignisse, die während des Updates auftreten, um den Entwicklern bei der Diagnose und Behebung von Problemen im Zusammenhang mit dem Update-Modul zu helfen.

Technischer Support

Systemkonfigurationsdaten senden

Wählen Sie **Immer senden** aus, um vor dem Senden Ihrer ESET Security for Microsoft SharePoint-Konfigurationsdaten nicht gefragt zu werden, oder verwenden Sie die Option **Vor dem Senden nachfragen**.

Cluster

„Cluster aktivieren“ wird automatisch aktiviert, wenn der ESET-Cluster konfiguriert wird. Sie können den Cluster manuell im Fenster **Erweiterte Einstellungen (F5)** deaktivieren, indem Sie auf das Schaltersymbol klicken (wenn Sie z. B. die Konfiguration ändern möchten, ohne andere Knoten im ESET-Cluster zu beeinflussen). Der Schalter dient nur dem Aktivieren und Deaktivieren der ESET-Clusterfunktion. Zum Einrichten oder Zerstören eines Cluster müssen Sie den [Clusterassistenten](#) verwenden bzw. die Option **Cluster zerstören** im Bereich **Tools > Cluster** im Hauptprogrammfenster.

ESET-Cluster nicht konfiguriert und deaktiviert:

Advanced setup

SERVER

COMPUTER

UPDATE 1

WEB AND EMAIL

DEVICE CONTROL

TOOLS

Log files

Proxy server

Email notifications

Presentation mode

Diagnostics

Cluster

USER INTERFACE

CLUSTER

Settings below are enabled only when the cluster is active.

Open port in Windows firewall ☒

Status refresh interval [sec] 10

Synchronize product settings ☒

CONFIGURATION INFORMATION

Settings below can be changed by the cluster wizard only.

Cluster name

Listening port 9777

List of cluster nodes

Default OK Cancel

ESET-Cluster richtig mit Details und Optionen konfiguriert:

Advanced setup

x
?

SERVER

COMPUTER

UPDATE

WEB AND EMAIL

DEVICE CONTROL

TOOLS

Log files

Proxy server

Email notifications

Presentation mode

Diagnostics

Cluster

USER INTERFACE

CLUSTER

Settings below are enabled only when the cluster is active.

Open port in Windows firewall

☒

i

Status refresh interval [sec]

i

Synchronize product settings

☒

i

CONFIGURATION INFORMATION

Settings below can be changed by the cluster wizard only.

Cluster name

termix

Listening port

9777

List of cluster nodes

W2012R2-NODE1;W2012R2-NODE2;W2012R2-NODE3;WIN-JDLB8CEUR5

Default

OK

Cancel

Benutzeroberfläche

Konfigurieren Sie das Verhalten der grafischen Benutzeroberfläche (GUI) von ESET Security for Microsoft SharePoint. Sie können das Erscheinungsbild und die grafischen Effekte des Programms anpassen.

[Elemente der Benutzeroberfläche](#)

Im Dropdownmenü „GUI-Startmodus“ können Sie die folgenden Startmodi für die grafische Benutzeroberfläche (GUI) auswählen:

- **Vollständig** - Die komplette Benutzeroberfläche wird angezeigt.
- **Terminal** - Es werden keine Warnungen und Benachrichtigungen angezeigt. Die grafische Benutzeroberfläche kann nur vom Administrator gestartet werden. Die Benutzeroberfläche sollte auf Terminal eingestellt werden, wenn die grafischen Elemente die Leistung des Computers beeinträchtigen oder andere Probleme auftreten. Außerdem können Sie die grafische Benutzeroberfläche für Terminalserver deaktivieren. Weitere Informationen zur Installation von ESET Security for Microsoft SharePoint auf einem Terminalserver finden Sie im Thema [Deaktivieren der Benutzeroberfläche auf Terminalserver](#).

Startbildschirm anzeigen

Deaktivieren Sie diese Option, wenn beim Start der GUI von ESET Security for Microsoft SharePoint kein Startbildschirm angezeigt werden soll, z. B. wenn Sie sich beim System anmelden.


Hinweistöne wiedergeben

ESET Security for Microsoft SharePoint spielt bei wichtigen Ereignissen wie z. B. der Erkennung einer Bedrohung oder nach Abschluss einer Prüfung einen Warnton ab.

In Kontextmenü integrieren

Diese Funktion integriert ESET Security for Microsoft SharePoint-Steuerelemente in das Kontextmenü. Das Kontextmenü wird angezeigt, wenn Sie mit der rechten Maustaste auf ein Element (eine Datei) klicken. Das Menü enthält alle Optionen, die auf das Objekt angewendet werden können.

Anwendungszustand

Klicken Sie auf [Bearbeiten](#), um die im Fenster [Überwachung](#) angezeigten Statusmeldungen auszuwählen. Alternativ können Sie [ESET Security Management Center-Policies](#)  verwenden, um Ihren Anwendungszustand zu konfigurieren. Ein Anwendungszustand wird auch angezeigt, wenn Ihr Produkt nicht aktiviert oder Ihre Lizenz abgelaufen ist.

Lizenzinformationen / Lizenzinformationen anzeigen

Wenn diese Option aktiviert ist, werden Nachrichten und Benachrichtigungen zu Ihrer Lizenz angezeigt.

[Warnungen und Hinweisfenster](#)

Konfigurieren Sie Warnungen und Benachrichtigungen, um festzulegen, wie Warnungen bei erkannten Bedrohungen und Systembenachrichtigungen angezeigt werden sollen. So können Sie diese Funktion an Ihre Anforderungen anpassen. Wenn Sie festlegen, dass bestimmte Benachrichtigungen nicht angezeigt werden sollen, werden diese in die Liste [Deaktivierte Nachrichten und Statusmeldungen](#) aufgenommen. Hier können Sie den Status der Hinweise abrufen, Details anzeigen oder sie aus dem Fenster entfernen.

[Einstellungen für den Zugriff](#)

Um einen maximalen Sicherheitsstandard zu gewährleisten, können Sie unbefugte Änderungen mit dem Tool „Einstellungen für den Zugriff“ verhindern.

[ESET-Shell](#)

Sie können die Zugriffsrechte auf Produkteinstellungen, Funktionen und Daten in eShell konfigurieren, indem Sie die ESET-Shell-Ausführungsrichtlinie ändern.

[Symbol im Infobereich der Taskleiste](#)

[Alle Einstellungen in diesem Bereich zurücksetzen](#)

Warnungen und Hinweisfenster

Sie können festlegen, wie ESET Security for Microsoft SharePoint Bedrohungswarnungen und Systembenachrichtigungen (z. B. erfolgreiche Updates) verarbeiten soll. Konfigurieren Sie die **Anzeigedauer** und **Transparenz** von Meldungen im Infobereich (nur für Systeme, die Benachrichtigungen im Infobereich der Taskleiste unterstützen).

Interaktive Warnungen anzeigen

Wenn Sie diese Funktion deaktivieren, zeigt ESET Security for Microsoft SharePoint keine Warnungen im

Windows-Benachrichtigungsbereich an.

Liste der interaktiven Warnungen

Nützlich für die Automatisierung. Deaktivieren Sie die Option **Benutzer fragen** für Elemente, die Sie automatisieren möchten, und wählen Sie die Aktion aus, die anstelle des Hinweisfensters ausgeführt werden soll.

Hinweisfenster enthalten kurze Textmitteilungen oder Fragen.

Hinweisfenster automatisch schließen

Popup-Fenster werden nach einer bestimmten Zeit automatisch geschlossen. Die Hinweise werden nach Ablauf der festgelegten Zeit automatisch geschlossen, sofern sie nicht bereits vom Benutzer geschlossen wurden.

Bestätigungsmeldungen

Klicken Sie auf **Bearbeiten**, um ein Pop-up-Fenster mit einer Liste der Bestätigungsmeldungen zu öffnen, die ESET Security for Microsoft SharePoint vor dem Ausführen einer Aktion anzeigt. Mit den Kontrollkästchen können Sie die Einstellungen für Bestätigungsmeldungen anpassen.

Einstellungen für den Zugriff

Um Ihr System optimal zu schützen ist es entscheidend, dass ESET Security for Microsoft SharePoint korrekt konfiguriert ist. Unbedachte Änderungen können zu Problemen oder sogar zum Verlust wichtiger Daten führen. Sie können Ihre ESET Security for Microsoft SharePoint-Konfiguration mit einem Passwort schützen, um unerwünschte Änderungen zu vermeiden.

WICHTIG

Falls Sie ESET Security for Microsoft SharePoint mit aktiviertem Sicherheitspasswort deinstallieren, werden Sie zur Eingabe des Passworts aufgefordert. Andernfalls können Sie ESET Security for Microsoft SharePoint nicht deinstallieren.

Einstellungen mit Passwort schützen

Sperrt/entsperrt die Programmeinstellungen. Klicken Sie auf diese Option, um das **Passwortfenster** zu öffnen.

Passwort festlegen

Klicken Sie auf **Passwort festlegen**, um ein Passwort für den Schutz der Einstellungen anzugeben oder um es zu ändern. Zum Schutz der Einstellungsparameter von ESET Security for Microsoft SharePoint vor unbefugten Änderungen muss ein neues Passwort festgelegt werden. Wenn Sie ein bestehendes Passwort ändern möchten, geben Sie Ihr altes Passwort in das Feld **Altes Passwort** und Ihr neues Passwort in die Felder **Neues Passwort** und **Neues Passwort bestätigen** ein. Klicken Sie anschließend auf **OK**. Um anschließend Änderungen an der Konfiguration von ESET Security for Microsoft SharePoint vorzunehmen, müssen Sie dieses Passwort eingeben.

Volle Administratorrechte für eingeschränkte Administratorkonten anfordern

Mit dieser Option werden Benutzer ohne Administratorrechte zur Eingabe von

Administratoranmeldeinformationen aufgefordert, wenn sie bestimmte Systemeinstellungen ändern möchten. Dazu gehört das Deaktivieren von Schutzmodulen.

HINWEIS

Wenn sich das Passwort für erweiterte Einstellungen geändert hat und Sie eine vorhandene *.xml*-Konfigurationsdatei importieren möchten, die vor der Passwortänderung signiert wurde, dann müssen Sie die Datei mit der [ESET CMD](#)-Befehlszeile erneut mit dem aktuellen Passwort signieren. Auf diese Weise können Sie eine ältere Konfigurationsdatei wiederverwenden, ohne sie vor dem Importieren auf einem anderen Computer mit ESET Security for Microsoft SharePoint erneut zu exportieren.

ESET-Shell

Sie können die Zugriffsrechte auf Produkteinstellungen, Funktionen und Daten in eShell konfigurieren, indem Sie die Einstellung **ESET-Shell-Ausführungsrichtlinie** ändern. Die Standardeinstellung ist **Eingeschränktes Scripting**. Sie können dies jedoch bei Bedarf zu „Deaktiviert“, „Nur Lesezugriff“ oder „Vollzugriff“ ändern.

Deaktiviert

eShell kann nicht verwendet werden. Nur die Konfiguration von eShell ist erlaubt - im `ui eshell`-Kontext. Sie können das Erscheinungsbild von eShell konfigurieren, jedoch nicht auf Produkteinstellungen oder Daten zugreifen.

Schreibgeschützt

eShell kann als Überwachungstool verwendet werden. Sie können alle Einstellungen im interaktiven und im Batch-Modus anzeigen, jedoch keinerlei Einstellungen, Features oder Daten bearbeiten.

Eingeschränktes Scripting

Im interaktiven Modus können Sie alle Einstellungen, Features und Daten bearbeiten. Im Batch-Modus verhält sich eShell wie im schreibgeschützten Modus. Sie können jedoch signierte Batchdateien verwenden, um Einstellungen und Daten zu bearbeiten.

Vollzugriff

Uneingeschränkter Zugriff auf alle Einstellungen im interaktiven und im Batch-Modus (bei der Ausführung von Batchdateien). Sie können alle Einstellungen anzeigen und bearbeiten. Sie benötigen ein Administratorkonto, um eShell mit Vollzugriff auszuführen. Falls UAC aktiviert ist, benötigen Sie außerdem erhöhte Rechte.

Deaktivieren der Benutzeroberfläche auf Terminalserver

In diesem Kapitel wird beschrieben, wie Sie die grafische Benutzeroberfläche von ESET Security for Microsoft SharePoint für Benutzersitzungen deaktivieren können, wenn das Produkt auf einem Windows-Terminalserver läuft.


Die Benutzeroberfläche von ESET Security for Microsoft SharePoint wird bei jeder Anmeldung eines Remote-Benutzers auf dem Terminalserver gestartet. Für gewöhnlich ist dies auf Terminalservern nicht erwünscht. Sie

können die Benutzeroberfläche für Terminalsitzungen deaktivieren, indem Sie in [eShell](#) den Befehl `set ui ui gui-start-mode none` ausführen. Dieser Befehl versetzt die Benutzeroberfläche in den Terminalmodus. Die Benutzeroberfläche kann in zwei verschiedenen Modi gestartet werden:

```
set ui ui gui-start-mode full
set ui ui gui-start-mode none
```

Führen Sie den Befehl `get ui ui gui-start-mode` aus, um den aktuellen Modus herauszufinden.

HINWEIS

Falls Sie ESET Security for Microsoft SharePoint auf einem Citrix-Server installiert haben, sollten Sie die in unserem [Knowledgebase-Artikel](#)  beschriebenen Einstellungen verwenden.

Deaktivierte Nachrichten und Statusmeldungen

Bestätigungsmeldungen



Zeigt eine Liste von Bestätigungsmeldungen an. Sie können auswählen, welche dieser Meldungen angezeigt werden sollen.

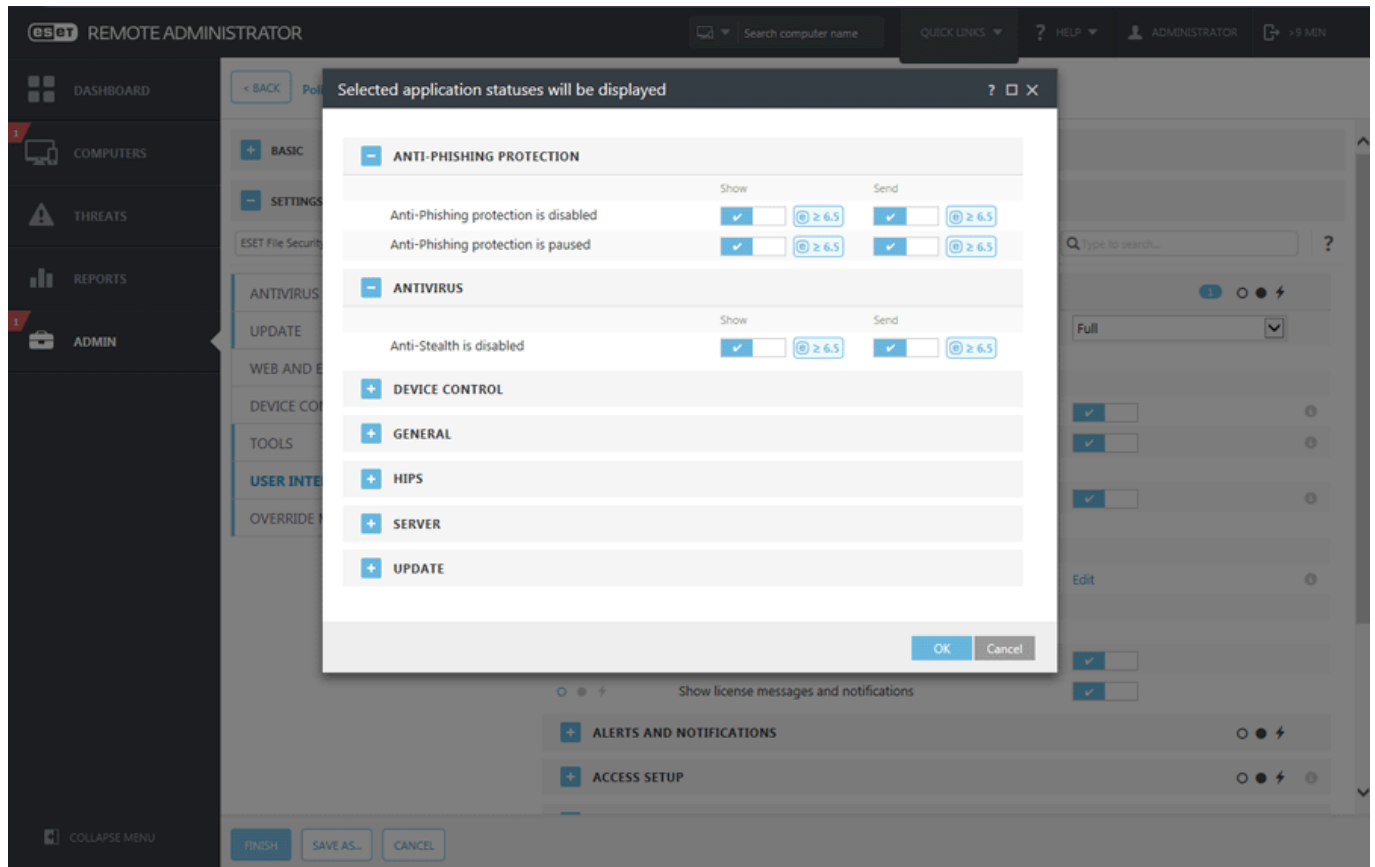
Anwendungsstatuseinstellungen

Mit dieser Option können Sie die Statusanzeige auf der Seite [Überwachung](#) im Hauptmenü aktivieren oder deaktivieren.


Anwendungsstatuseinstellungen

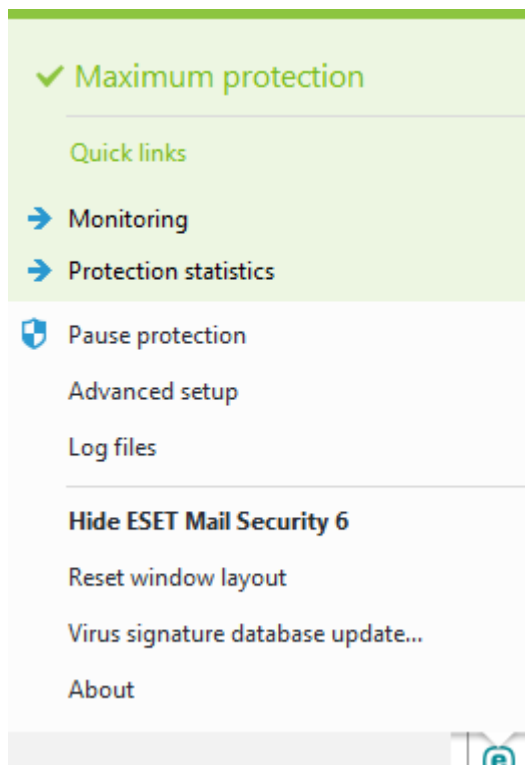
In diesem Fenster können Sie auswählen, welche Anwendungs-Statusmeldungen angezeigt werden sollen. Wenn Sie beispielsweise den Viren- und Spywareschutz anhalten, führt dies dazu, dass in der Seite [Überwachung](#) eine Änderung des Schutzstatus angezeigt wird. Wenn Ihr Produkt nicht aktiviert oder Ihre Lizenz abgelaufen ist, wird ebenfalls eine Anwendungs-Statusmeldung angezeigt.

Der Anwendungsstatus kann über [ESET Security Management Center-Policies](#)  verwaltet werden. Kategorien und Statusmeldungen erscheinen in einer Liste zusammen mit der Möglichkeit, den Status **anzuzeigen** und zu **versenden**. Die Spalte „Versenden“ wird für Statusmeldungen nur in der [ESET Security Management Center-Policy](#) -Konfiguration angezeigt. ESET Security for Microsoft SharePoint zeigt Einstellungen mit einem Sperrsymbol an. Sie können den [Override-Modus](#) verwenden, um einen Anwendungsstatus vorübergehend zu ändern.



Symbol im Infobereich der Taskleiste


Ermöglicht den schnellen Zugriff auf häufig verwendete Elemente und Funktionen von ESET Security for Microsoft SharePoint. Klicken Sie dazu mit der rechten Maustaste auf das Symbol im Infobereich der Taskleiste .



Weitere Informationen

Öffnet die Seite [Überwachung](#) mit dem aktuellen Schutzstatus und aktuellen Nachrichten.

Schutz vorübergehend deaktivieren

Zeigt ein Dialogfenster an, in dem Sie bestätigen müssen, dass der [Viren- und Spyware-Schutz](#) deaktiviert werden soll, der Dateivorgänge sowie die Internet- und E-Mail-Kommunikation überwacht und so Ihr System vor Angriffen schützt. Wenn Sie den Viren- und Spyware-Schutz vorübergehend über das Symbol  im Infobereich der Taskleiste deaktivieren, wird das Dialogfenster **Schutz vorübergehend deaktivieren** angezeigt. Der Malware-Schutz wird für die ausgewählte Dauer deaktiviert. Eine dauerhafte Deaktivierung des Schutzes ist nur über die **erweiterten Einstellungen** möglich. Verwenden Sie diese Möglichkeit mit Vorsicht, da sie Ihr System Bedrohungen aussetzen kann.

[Erweiterten Einstellungen](#)

Diese Option öffnet die **erweiterten Einstellungen**.

[Log-Dateien](#)

Log-Dateien enthalten Informationen zu allen wichtigen aufgetretenen Programmereignissen sowie einen Überblick über erkannte Bedrohungen.

ESET Security for Microsoft SharePoint Ausblenden

Blendet das ESET Security for Microsoft SharePoint-Fenster auf dem Bildschirm aus.

Fensterlayout zurücksetzen

Stellt die standardmäßige Fenstergröße und die Standardposition von ESET Security for Microsoft SharePoint auf dem Bildschirm wieder her.

[Nach Updates suchen](#)

Beginnt mit der Aktualisierung der Module, um den Schutz vor Schadcode zu gewährleisten.

[Über](#)

Enthält Systeminformationen zur installierten Version von ESET Security for Microsoft SharePoint und zu den installierten Programmmodulen und zeigt das Ablaufdatum der Lizenz an. Informationen zum Betriebssystem und zu den Systemressourcen befinden sich unten auf der Seite.

Auf Standardeinstellungen zurücksetzen

Sie können die Einstellungen in den **erweiterten Einstellungen** auf die Standardwerte zurücksetzen. Sie haben zwei Optionen zur Auswahl: Sie können entweder alles oder nur die Einstellungen in einem bestimmten Abschnitt zurücksetzen (die restlichen Einstellungen bleiben erhalten).

Alle Einstellungen zurücksetzen

Alle Einstellungen in sämtlichen Abschnitten der erweiterten Einstellungen werden auf die Standardwerte nach der Installation von ESET Security for Microsoft SharePoint zurückgesetzt. Dies entspricht dem

Zurücksetzen auf die Werkseinstellungen.

HINWEIS

Klicken Sie auf **Rückgängig machen**, um alle Änderungen zu verwerfen. Diese Aktion kann nicht rückgängig gemacht werden.

Alle Einstellungen in diesem Bereich zurücksetzen

Setzt die Moduleinstellungen im ausgewählten Abschnitt auf die Standardwerte zurück. Alle in diesem Abschnitt vorgenommenen Änderungen werden verworfen.

Revert to default settings



Revert all settings in this section?

This will revert the settings to their default values and any changes made after installation will be lost. This action cannot be undone.

Revert contents of tables

☐

Any data added to tables and lists (e.g. rules, tasks, profiles) either manually or automatically will be lost.

Revert to default

Cancel

Inhalte von Tabellen zurücksetzen

Wenn diese Option aktiviert ist, gehen manuell oder automatisch hinzugefügte Regeln, Tasks oder Profile verloren.

Hilfe und Support

ESET Security for Microsoft SharePoint enthält Tools für die Fehlerbehebung und Support-Informationen, die Ihnen bei der Lösung von möglichen Problemen behilflich sind.

Hilfe

[ESET Knowledgebase durchsuchen](#)

Die ESET-Knowledgebase enthält Antworten auf die am häufigsten gestellten Fragen sowie Lösungsvorschläge für zahlreiche Problemstellungen. Die Knowledgebase wird regelmäßig von den ESET-Supportmitarbeitern aktualisiert und eignet sich daher hervorragend für die Lösung verschiedenster Probleme.

Hilfe öffnen

Öffnet die Onlinehilfe für ESET Security for Microsoft SharePoint.

[Schnelle Lösung finden](#)

Wählen Sie diese Option aus, um Lösungen für die häufigsten Probleme zu finden. Bevor Sie sich an den Support wenden, sollten Sie diesen Abschnitt unbedingt lesen.

Technischer Support

[Supportanfrage senden](#)

Wenn Sie Ihr Problem nicht lösen konnten, können Sie sich auch über das Formular auf der ESET-Website schnell mit unserem technischen Support in Verbindung setzen.

[Details für den technischen Support](#)


Zeigt Detailinformationen (Produktname, Produktversion usw.) für den technischen Support an.

Support-Tools

[Virenenzyklopädie](#)

Öffnet die ESET-Virenenzyklopädie mit Informationen zu den Gefahren und Symptomen verschiedener Infiltrationsarten.

[ESET Log Collector](#)

Öffnet die [Downloadseite](#)  für den ESET Log Collector. Der Log Collector dient zum automatischen Erfassen von Informationen wie Konfigurationsdetails und Logs von Ihrem Server zur schnelleren Fehlerbehebung.

[Verlauf der Malware Scan Engine](#)

Öffnet den ESET-Virusradar mit Informationen zu Versionen der ESET-Erkennungsmodule.

[Spezielles ESET-Säuberungsprogramm](#)

Das spezielle ESET-Säuberungsprogramm ist ein Entfernungstool für bekannte Schadsoftware-Infektionen wie Conficker, Sirefef, Necurs usw.

Produkt- und Lizenzinformationen

[Produkt aktivieren](#) / [Lizenz ändern](#)

Klicken Sie hier, um das Produktaktivierungsfenster zu öffnen. Aktivieren Sie ESET Security for Microsoft SharePoint mit einer der verfügbaren Methoden.

[Über ESET Security for Microsoft SharePoint](#)

Informationen zu Ihrer Kopie von ESET Security for Microsoft SharePoint.

Supportanfrage senden

Um möglichst schnell und effizient Hilfe bieten zu können, benötigt der ESET-Support Informationen zu Ihrer Konfiguration von ESET Security for Microsoft SharePoint, detaillierte Systeminformationen, Informationen zu ausgeführten Prozessen ([ESET SysInspector-Log-Datei](#)) und Registrierungsdaten. ESET nutzt diese Daten ausschließlich zum Bereitstellen technischer Unterstützung für den Kunden. Sie können diese Einstellung auch in den **erweiterten Einstellungen (F5)** unter **Tools > Diagnose > Technischer Support** konfigurieren.

HINWEIS

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

Wenn Sie das Webformular übermitteln, werden Ihre Systemkonfigurationsdaten an ESET gesendet. Wählen Sie **Diese Informationen immer senden** aus, wenn Sie diese Aktion für den Prozess speichern möchten.

[Keine Daten senden](#)

Verwenden Sie diese Option, falls Sie keine Daten übermitteln möchten. Sie werden zur Webseite des technischen ESET-Supports weitergeleitet.


Über ESET Security for Microsoft SharePoint

Dieses Fenster enthält Details zur installierten Version von ESET Security for Microsoft SharePoint. Im oberen Fensterbereich sehen Sie Informationen zu Ihrem Betriebssystem und den Systemressourcen, den aktuell angemeldeten Benutzer und den vollständigen Computernamen.

Installierte Komponenten

Dieser Bereich enthält Informationen zu den Modulen, um eine Liste der Komponenten und deren Details zu öffnen. Klicken Sie auf **Kopieren**, um die Liste in Ihre Zwischenablage zu kopieren. Dies kann bei der Fehlerbehebung oder beim Kontakt zum Support hilfreich sein.

Glossar

Besuchen Sie die Seite [Glossar](#) , um weitere Informationen zu technischen Begriffen, zu Bedrohungen und zur Internetsicherheit zu erhalten.

Endbenutzer-Lizenzvereinbarung

WICHTIG: Vor dem Herunterladen, Installieren, Kopieren oder Verwenden des Produkts lesen Sie bitte die folgenden Nutzungsbedingungen. **DURCH DAS HERUNTERLADEN, INSTALLIEREN, KOPIEREN ODER VERWENDEN DER SOFTWARE ERKLÄREN SIE SICH MIT DEN NUTZUNGSBEDINGUNGEN EINVERSTANDEN UND AKZEPTIEREN DIE [DATENSCHUTZERKLÄRUNG](#).**

Endbenutzer-Lizenzvereinbarung

Diese Endbenutzer-Lizenzvereinbarung (die "Vereinbarung") zwischen ESET, spol. s r. o., mit Sitz in Einsteinova 24, 85101 Bratislava, Slovak Republic, Handelsregistereintrag 3586/B in der Rubrik Sro beim Amtsgericht Bratislava I, Firmennummer 31333532, (im Folgenden "ESET" oder "Anbieter") und Ihnen, einer natürlichen oder juristischen Person ("Sie" oder der "Endbenutzer"), berechtigt Sie zur Nutzung der in Abschnitt 1 dieser Vereinbarung definierten Software. Die in Abschnitt 1 dieser Vereinbarung definierte Software darf unter den im Folgenden aufgeführten Bedingungen auf einem Datenträger gespeichert, per E-Mail versendet, aus dem Internet oder von Servern des Anbieters heruntergeladen oder auf andere Weise beschafft werden.

DIESES DOKUMENT IST KEIN KAUFVERTRAG, SONDERN EINE VEREINBARUNG ÜBER DIE RECHTE DES ENDBENUTZERS. Der Anbieter bleibt Eigentümer des Exemplars der Software und, soweit vorhanden, des

physischen Mediums, auf dem die Software für den Verkauf vorliegt, sowie aller Kopien der Software, zu deren Erstellung der Endbenutzer unter den Bedingungen dieser Vereinbarung berechtigt ist.

Durch Klicken auf die Schaltfläche "Ich stimme zu" oder "Ich stimme zu..." beim Installieren, Herunterladen, Kopieren oder Verwenden der Software erklären Sie sich mit den Bestimmungen und Bedingungen dieser Vereinbarung einverstanden. Wenn Sie mit einer der Bestimmungen dieser Vereinbarung nicht einverstanden sind, klicken Sie auf die Schaltfläche "Ablehnen" oder "Ich stimme nicht zu". Brechen Sie den Download oder die Installation der Software ab, vernichten oder geben Sie die Software, das Installationsmedium, die zugehörige Dokumentation und den Erwerbsnachweis an den Anbieter oder an dem Ort, an dem Sie die Software erworben haben, zurück.

MIT DER NUTZUNG DER SOFTWARE ZEIGEN SIE AN, DASS SIE DIESE VEREINBARUNG GELESEN UND VERSTANDEN HABEN UND DASS SIE DIESER VEREINBARUNG ZUGESTIMMT HABEN.

1. Software. Mit "Software" wird in dieser Vereinbarung bezeichnet: (i) das mit dieser Vereinbarung ausgelieferte Computerprogramm und all dessen Komponenten; (ii) alle Inhalte der Disks, CD-ROMs, DVDs, E-Mails und Anlagen oder sonstiger Medien, denen diese Vereinbarung beigelegt 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 Schrift Dokumente und andere Dokumentationen in Bezug auf die Software, insbesondere Beschreibungen der Software und ihrer Spezifikationen, jede Beschreibung der Softwareeigenschaften oder -funktionen, Beschreibungen der Betriebsumgebung, in der die Software verwendet wird, Anweisungen zu Installation und zum Einsatz der Software ("Dokumentation"); (iv) Kopien der Software, Patches für mögliche Softwarefehler, Hinzufügungen zur Software, Erweiterungen der Software, geänderte Versionen und Aktualisierungen der Softwarebestandteile, sofern zutreffend, deren Nutzung der Anbieter gemäß Artikel 3 dieser Vereinbarung gewährt. Die Software wird ausschließlich in Form von ausführbarem Objektcode ausgeliefert.

2. Installation, Computer und ein Lizenzschlüssel. Die auf einem Datenträger bereitgestellte, per E-Mail verschickte, aus dem Internet oder von den Servern des Anbieters heruntergeladene oder auf anderem Weg beschaffte Software muss installiert werden. Sie müssen die Software auf einem korrekt konfigurierten Computer installieren, der die in der Dokumentation genannten Mindestvoraussetzungen erfüllt. Die Installationsmethode ist in der Dokumentation beschrieben. Auf dem Computer, auf dem Sie die Software installieren, darf kein Computerprogramm und keine Hardware vorhanden sein, die sich negativ auf die Software auswirken könnte. Die Bezeichnung "Computer" erstreckt sich auf Hardware inklusive, jedoch nicht ausschließlich, Personal Computer, Laptops, Arbeitsstationen, Palmtop-Computer, Smartphones, tragbare elektronische Geräte oder andere elektronische Geräte, für die die Software entwickelt wurde und auf denen die Software installiert und/oder eingesetzt wird. Der Begriff "Lizenzschlüssel" bezeichnet die eindeutige Abfolge von Symbolen, Buchstaben und Zahlen, die dem Endbenutzer bereitgestellt wird, um die legale Nutzung der Software in der jeweiligen Version bzw. die Verlängerung der Lizenz gemäß dieser Vereinbarung zu ermöglichen.

3. Lizenz. Unter der Voraussetzung, dass Sie dieser Vereinbarung zugestimmt haben und sämtliche darin enthaltenen Bestimmungen einhalten, gewährt Ihnen der Anbieter die folgenden Rechte (die "Lizenz"):

a) **Installation und Nutzung.** Sie erhalten das nicht exklusive und nicht übertragbare Recht, die Software auf der Festplatte eines Computers oder einem ähnlichen Medium zur dauerhaften Datenspeicherung zu installieren, die Software im Arbeitsspeicher eines Computers zu speichern und die Software auf Computern zu implementieren, zu speichern und anzuzeigen.

b) **Anzahl der Lizenzen.** Das Nutzungsrecht für die Software ist durch die Anzahl der Endbenutzer beschränkt. Unter einem "Endbenutzer" ist Folgendes zu verstehen: (i) die Installation der Software auf einem Computer; wenn der Umfang einer Lizenz sich nach der Anzahl von Postfächern richtet, ist ein Endbenutzer (ii) ein Computerbenutzer, der E-Mail über ein E-Mail-Programm empfängt. Wenn das E-Mail-Programm E-Mail

empfängt und diese anschließend automatisch an mehrere Benutzer weiterleitet, richtet sich die Anzahl der Endbenutzer nach der tatsächlichen Anzahl von Benutzern, an die auf diesem Weg E-Mail-Nachrichten gesendet werden. Wenn ein Mailserver die Funktion eines E-Mail-Gateways ausführt, entspricht die Zahl der Endbenutzer der Anzahl von Mailservern, für die dieses Gateway Dienste bereitstellt. Wenn mehrere E-Mail-Adressen (z. B. durch Aliasnamen) von einem Benutzer verwendet werden und nur ein Benutzer über diese Adressen E-Mail empfängt, während auf Clientseite keine E-Mail-Nachrichten automatisch an mehrere Benutzer verteilt werden, ist nur eine Lizenz für einen Computer erforderlich. Die gleichzeitige Nutzung derselben Lizenz auf mehreren Computern ist untersagt. Der Endbenutzer darf den Lizenzschlüssel für die Software nur in dem Umfang eingeben, für den er die entsprechende Anzahl von Lizenzen zur Nutzung der Software vom Anbieter erworben hat. Der Lizenzschlüssel ist vertraulich, und die Lizenz darf nicht mit Drittparteien geteilt oder von Drittparteien genutzt werden, sofern dies nicht in dieser Vereinbarung oder vom Anbieter erlaubt wurde. Benachrichtigen Sie den Anbieter unverzüglich, falls Ihr Lizenzschlüssel kompromittiert wurde.

c) **Business Edition.** Für die Verwendung der Software auf E-Mail-Servern, E-Mail-Relays, E-Mail- oder Internet-Gateways ist die Business Edition der Software erforderlich.

d) **Laufzeit der Lizenz.** Ihr Nutzungsrecht für die Software ist zeitlich beschränkt.

e) **OEM-Software.** OEM-Software darf ausschließlich auf dem Computer genutzt werden, mit dem Sie sie erhalten haben. Eine Übertragung auf einen anderen Computer ist nicht gestattet.

f) **Nicht für den Wiederverkauf bestimmte Software und Testversionen.** Nicht für den Wiederverkauf („not for resale“, NFR) oder als Testversion bereitgestellte Software darf nicht veräußert, sondern ausschließlich zum Vorführen oder Testen der Softwarefunktionen verwendet werden.

g) **Ablauf und Kündigung der Lizenz.** Die Lizenz läuft automatisch zum Ende des jeweiligen Lizenzzeitraums aus. Sollten Sie eine Ihrer Pflichten aus dieser Vereinbarung verletzen, ist der Anbieter berechtigt, diese außerordentlich zu kündigen und, ggf. auf dem Rechtsweg, etwaige weitere Ansprüche geltend zu machen. Bei Ablauf oder Kündigung der Lizenz müssen Sie die Software und ggf. alle Sicherungskopien sofort löschen, zerstören oder auf eigene Kosten an ESET oder das Geschäft zurückgeben, in dem Sie die Software erworben haben. Nach Ablauf oder Kündigung der Lizenz ist der Anbieter berechtigt, das Recht des Endbenutzers zur Nutzung der Softwarefunktionen zurückzuziehen, für die eine Verbindung zu Servern des Anbieters oder zu Servern von Drittanbietern erforderlich ist.

4. Funktionen mit Datenerfassung und Anforderungen an die Internetverbindung. Für den korrekten Betrieb benötigt die Software eine Internetverbindung und muss in der Lage sein, sich in regelmäßigen Abständen mit den Servern des Anbieters, Servern einer Drittpartei und entsprechenden Datenerfassungen gemäß der Datenschutzrichtlinie zu verbinden. Die Verbindung mit dem Internet und den entsprechenden Datenerfassungen ist für die folgenden Funktionen der Software erforderlich:

a) **Software-Updates.** Der Anbieter hat das Recht, von Zeit zu Zeit Aktualisierungen für die Software („Updates“) bereitzustellen, ist hierzu jedoch nicht verpflichtet. Diese Funktion ist in den Standardeinstellungen der Software aktiviert. Die Updates werden also automatisch installiert, sofern der Endbenutzer dies nicht deaktiviert hat. Zur Bereitstellung von Aktualisierungen muss die Echtheit der Lizenz überprüft werden. Dazu gehören Informationen über den Computer und/oder die Plattform, auf der die Software installiert wurde, in Übereinstimmung mit der Datenschutzrichtlinie.

b) **Weiterleitung von eingedrungener Schadsoftware und anderen Informationen an den Anbieter.** Die Software enthält Funktionen zur Erfassung neuer Computerviren und anderer schädlicher Computerprogramme sowie von verdächtigen, problematischen, potenziell unsicheren Objekten wie Dateien, URLs, IP-Pakete und Ethernet-Rahmen (im Folgenden "Infiltrationen"). Diese Daten werden zusammen mit Informationen über den Installationsprozess und die Plattform, auf der die Software installiert ist, oder anderen Informationen über

Betrieb und Funktionsweise der Software (im Folgenden "Informationen") an den Anbieter übertragen. Die Informationen und die Infiltrationen können Daten über den Endbenutzer oder andere Benutzer des Computers enthalten, auf dem die Software installiert ist (inklusive zufällig oder unbeabsichtigt erfasste personenbezogene Daten), sowie von eingedrungener Schadsoftware betroffene Dateien mit den entsprechenden Metadaten.

Die folgenden Funktionen der Software können Informationen und Infiltrationen sammeln:

- i. Das LiveGrid Reputationssystem sammelt und sendet Einweg-Hashes im Zusammenhang mit eingedrungener Schadsoftware an den Anbieter. Diese Funktion ist in den Standardeinstellungen der Software aktiviert.
- ii. Das LiveGrid-Reputationssystem erfasst Infiltrationen und überträgt diese zusammen mit den entsprechenden Metadaten und anderen Informationen an den Anbieter. Diese Funktion kann vom Endbenutzer bei der Installation der Software aktiviert werden.

Der Anbieter verwendet die erhaltenen Informationen und Infiltrationen ausschließlich zur Analyse und Erforschung der Infiltrationen, zur Verbesserung der Software und zur Überprüfung der Echtheit von Lizenzen und unternimmt angemessene Anstrengungen, um die erhaltenen Infiltrationen und Informationen zu schützen. Wenn diese Softwarefunktion aktiviert wird, darf der Anbieter gemäß der Datenschutzrichtlinie und gemäß geltender Gesetze Infiltrationen und Informationen erfassen und verarbeiten. Sie können diese Funktionen jederzeit deaktivieren.

Für die in dieser Vereinbarung festgelegten Zwecke werden Daten gesammelt, verarbeitet und gespeichert, mit denen der Anbieter Sie gemäß der Datenschutzrichtlinie identifizieren kann. Für die in dieser Vereinbarung festgelegten Zwecke werden Daten gesammelt, verarbeitet und gespeichert, mit denen der Anbieter Sie gemäß der Datenschutzrichtlinie identifizieren kann. Sie stimmen zu, dass der Anbieter mit eigenen Mitteln überprüfen darf, ob Sie die Software in Übereinstimmung mit den Bestimmungen dieser Vereinbarung nutzen. Sie erkennen an, dass es für die in dieser Vereinbarung festgelegten Zwecke erforderlich ist, dass Ihre Daten zwischen der Software und den Computersystemen des Anbieters bzw. denen seiner Geschäftspartner im Rahmen des Distributions- und Verteilungsnetzwerks des Anbieters übertragen werden, um die Funktionstüchtigkeit der Software und die Genehmigung zu deren Nutzung sowie die Rechte des Anbieters zu schützen.

Mit Abschluss dieser Vereinbarung willigen Sie zudem in die Übertragung, Verarbeitung und Speicherung Ihrer personenbezogenen Daten durch den Anbieter bzw. seine Geschäftspartner ein, soweit eine solche Nutzung zur Abrechnung und zur Erfüllung dieser Vereinbarung und zum Übertragen von Benachrichtigungen auf Ihren Computer erforderlich ist. Sie stimmen dem Empfang von Benachrichtigungen und Nachrichten zu, inklusive, jedoch nicht ausschließlich, Marketinginformationen.

Details zur Privatsphäre, zum Schutz persönlicher Daten und zu Ihren Rechten als betroffene Person finden Sie in der Datenschutzrichtlinie auf der Webseite des Anbieters oder direkt beim Installationsprozess. Sie finden diese Informationen außerdem im Hilfebereich der Software.

5. Ausübung der Rechte des Endbenutzers. Sie müssen Ihre Rechte als Endbenutzer selbst oder gegebenenfalls über Ihre Angestellten ausüben. Sie dürfen die Software ausschließlich zur Gewährleistung der Arbeitsfähigkeit und zum Schutz der Computer verwenden, für die Sie eine Lizenz erworben haben.

6. Beschränkungen der Rechte. Es ist untersagt, die Software zu kopieren, zu verbreiten oder aufzuteilen. Außerdem dürfen keine abgeleiteten Versionen erstellt werden. Für die Nutzung der Software gelten die folgenden Einschränkungen:

- a) Sie dürfen eine Kopie der Software auf einem Medium zur dauerhaften Speicherung als Sicherungskopie erstellen, vorausgesetzt die Sicherungskopien werden nicht auf einem anderen Computer installiert oder verwendet. Das Erstellen jeder weiteren Kopie der Software verstößt gegen diese Vereinbarung.

- b) Jegliche von den Bestimmungen dieser Vereinbarung abweichende Nutzung, Modifikation, Übersetzung oder Reproduktion der Software sowie die Einräumung von Rechten zur Nutzung der Software oder von Kopien der Software ist untersagt.
- c) Die Software darf nicht an andere Personen verkauft, sublizenziert oder vermietet werden. Ebenso darf die Software nicht von einer anderen Person gemietet, einer anderen Person ausgeliehen oder zur gewerbsmäßigen Erbringung von Dienstleistungen verwendet werden.
- d) Der Quellcode der Software darf nicht durch Reverse-Engineering analysiert, dekompiert 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, dekompileieren oder disassemblieren oder versuchen, sich den Quellcode auf andere Weise zu beschaffen, gehen automatisch sämtliche dadurch gewonnenen Informationen unwiderruflich und unmittelbar in das Eigentum des Anbieters über. Weiterhin ist der Anbieter in diesem Fall berechtigt, etwaige weitere Ansprüche aus Ihrem Verstoß gegen diese Vereinbarung geltend zu machen.

8. Rechtevorbehalt. Mit Ausnahme der Rechte, die Ihnen als Endbenutzer der Software in dieser Vereinbarung ausdrücklich gewährt werden, behält sich der Anbieter alle Rechte an der Software vor.

9. Versionen in verschiedenen Sprachen/auf mehreren Datenträgern, mehrere Exemplare. Wenn die Software mehrere Plattformen oder Sprachen unterstützt, oder wenn Sie mehrere Exemplare der Software erhalten haben, darf die Software nur auf derjenigen Anzahl von Computern und nur in den Versionen verwendet werden, für die Sie eine Lizenz erworben haben. Es dürfen keine Versionen oder Kopien der Software, die von Ihnen nicht verwendet werden, an andere Personen verkauft, vermietet, sublizenziert, verliehen oder auf diese übertragen werden.

10. Beginn und Gültigkeitsdauer der Vereinbarung. Diese Vereinbarung tritt an dem Tag in Kraft, an dem Sie sich mit ihren Bestimmungen einverstanden erklären. Sie können diese Vereinbarung jederzeit kündigen, indem Sie die Software, alle Sicherungskopien und, falls vorhanden, alle vom Anbieter oder seinen Geschäftspartnern zur Verfügung gestellten zugehörigen Materialien dauerhaft löschen, sie zerstören bzw. auf eigene Kosten zurückgeben. Unabhängig von der Gültigkeitsdauer dieser Vereinbarung und der Art und Weise ihres Ablaufs bzw. ihrer Kündigung behalten die Bestimmungen der Abschnitte 7, 8, 11, 13, 19 und 21 auf unbegrenzte Zeit ihre Gültigkeit.

11. AUSDRÜCKLICHE ERKLÄRUNGEN DES ENDBENUTZERS. ALS ENDBENUTZER ERKENNEN SIE AN, DASS DIE SOFTWARE IM JEWEILIGEN IST-ZUSTAND UND OHNE JEGLICHE AUSDRÜCKLICHE ODER KONKLUDENTE GEWÄHRLEISTUNG BEREITGESTELLT WIRD, SOWEIT DIES IM RAHMEN DER GELTENDEN GESETZE ZULÄSSIG IST. WEDER DER ANBIETER NOCH SEINE LIZENZGEBER ODER DIE RECHTEINHABER GEWÄHREN AUSDRÜCKLICHE ODER KONKLUDENTE ZUSICHERUNGEN ODER GEWÄHRLEISTUNGEN, INSBESONDERE KEINE ZUSICHERUNGEN HINSICHTLICH DER MARKTGÄNGIGKEIT, DER EIGNUNG FÜR EINEN BESTIMMTEN ZWECK ODER DER NICHTVERLETZUNG VON PATENTEN, URHEBER- UND MARKENRECHTEN ODER SONSTIGEN RECHTEN DRITTER. ES BESTEHT VON SEITEN DES ANBIETERS ODER DRITTER KEINERLEI GEWÄHRLEISTUNG, DASS DIE IN DER SOFTWARE ENTHALTENEN FUNKTIONEN IHREN ANFORDERUNGEN ENTSPRECHEN ODER DASS DIE SOFTWARE STÖRUNGS- UND FEHLERFREI AUSGEFÜHRT WIRD. SIE ÜBERNEHMEN DIE VOLLE VERANTWORTUNG UND DAS VOLLE RISIKO HINSICHTLICH DER AUSWAHL DER SOFTWARE ZUM ERREICHEN DER VON IHNEN BEABSICHTIGTEN ERGEBNISSE SOWIE FÜR INSTALLATION UND NUTZUNG DER SOFTWARE UND DEN MIT DIESER ERZIELTEN ERGEBNISSEN.

12. Keine weiteren Verpflichtungen. Aus dieser Vereinbarung ergeben sich für den Anbieter und seine Lizenzgeber keine weiteren Verpflichtungen außer den explizit aufgeführten.

13. HAFTUNGSAUSSCHLUSS. SOWEIT IM RAHMEN DER GELTENDEN GESETZE ZULÄSSIG, ÜBERNEHMEN DER ANBIETER, SEINE ANGESTELLTEN UND SEINE LIZENZGEBER KEINERLEI HAFTUNG FÜR ENTGANGENE GEWINNE, ERTRÄGE ODER VERKÄUFE. VON DER HAFTUNG AUSGESCHLOSSEN SIND AUSSERDEM DATENVERLUSTE, BESCHAFFUNGSKOSTEN FÜR ERSATZTEILE ODER DIENSTE, SACH- UND PERSONENSCHÄDEN, GESCHÄFTSUNTERBRECHUNGEN, DER VERLUST VON GESCHÄFTSINFORMATIONEN SOWIE JEGLICHE ANDERE NEBEN-, VERMÖGENS- ODER FOLGESCHÄDEN, DIE INFOLGE DER NUTZUNG ODER UNMÖGLICHKEIT DER NUTZUNG DER SOFTWARE ENTSTEHEN. DA IN BESTIMMTEN LÄNDERN UND UNTER BESTIMMTEN GESETZEN EIN HAFTUNGSAUSSCHLUSS NICHT ZULÄSSIG IST, EINE HAFTUNGSBESCHRÄNKUNG JEDOCH MÖGLICH, BESCHRÄNKT SICH DIE HAFTUNG DES ANBIETERS, SEINER ANGESTELLTEN UND LIZENZGEBER AUF DEN FÜR DIE LIZENZ ENTRICHTETEN PREIS.

14. Gesetzlich verankerte Verbraucherrechte haben im Konfliktfall Vorrang vor den Bestimmungen dieser Vereinbarung.

15. Technischer Support. ESET bzw. die von ESET beauftragten Dritten erbringen jeglichen technischen Support ausschließlich nach eigenem Ermessen und ohne diesbezügliche Zusicherungen oder Gewährleistungen. Endbenutzer sind verpflichtet, vor der Inanspruchnahme von Supportleistungen eine Sicherungskopie aller vorhandenen Daten, Softwareanwendungen und sonstigen Programme zu erstellen. ESET bzw. die von ESET beauftragten Dritten übernehmen keinerlei Haftung für Datenverluste, Sach- und Vermögensschäden (insb. Schäden an Software und Hardware) oder entgangene Gewinne infolge der Erbringung von Supportleistungen. ESET bzw. die von ESET beauftragten Dritten sichern nicht zu, dass ein bestimmtes Problem auf dem Wege des technischen Support gelöst werden kann, und behalten sich das Recht vor, die Arbeit an einem Problem ggf. einzustellen. ESET behält sich das Recht vor, die Erbringung von Supportleistungen nach eigenem Ermessen vorübergehend auszusetzen, ganz einzustellen oder im konkreten Einzelfall abzulehnen. Für die Bereitstellung des technischen Supports sind unter Umständen Lizenzinformationen, Informationen und andere Daten gemäß der Datenschutzrichtlinie erforderlich.

16. Übertragung der Lizenz. Die Software darf von einem Computersystem auf ein anderes übertragen werden,

sofern dabei nicht gegen Bestimmungen dieser Vereinbarung verstoßen wird. Sofern in dieser Vereinbarung nicht anderweitig geregelt, ist es dem Endbenutzer gestattet, die Lizenz und alle Rechte aus dieser Vereinbarung an einen anderen Endbenutzer zu übertragen, sofern der Anbieter dem zustimmt und die folgenden Voraussetzungen beachtet werden: (i) Der ursprüngliche Endbenutzer darf keine Kopien der Software zurückbehalten. (ii) Die Übertragung der Rechte muss direkt erfolgen, d. h. vom ursprünglichen Endbenutzer an den neuen Endbenutzer. (iii) Der neue Endbenutzer muss sämtliche Rechte und Pflichten des ursprünglichen Endbenutzers aus dieser Vereinbarung übernehmen. (iv) Der ursprüngliche Endbenutzer muss dem neuen Endbenutzer einen der in Abschnitt 17 genannten Nachweise für die Gültigkeit des Softwarelizenz übereignen.

17. Gültigkeitsnachweis für die Softwarelizenz. Der Endbenutzer kann seine Nutzungsrechte an der Software auf eine der folgenden Arten nachweisen: (i) über ein Lizenzzertifikat, das vom Anbieter oder einem von diesem beauftragten Dritten ausgestellt wurde; (ii) über eine schriftliche Lizenzvereinbarung, falls abgeschlossen; (iii) durch Vorlage einer E-Mail des Anbieters mit den Lizenzdaten (Benutzername und Passwort). Zur Überprüfung der Echtheit der Software sind unter Umständen Lizenzinformationen und Identifikationsdaten des Endbenutzers gemäß der Datenschutzrichtlinie erforderlich.

18. Lizenzvergabe an Behörden und die US-Regierung. Für die Lizenzvergabe an Behörden, insbesondere an Stellen der US-Regierung, gelten ausschließlich die in dieser Vereinbarung beschriebenen Lizenzrechte und Einschränkungen.

19. Einhaltung von Handelskontrollen.

a) Sie werden die Software nicht direkt oder indirekt an andere Personen exportieren, reexportieren, übertragen oder auf andere Arten verfügbar machen, auf eine Art verwenden oder sich an Handlungen beteiligen, die zu einer Verletzung der Handelskontrollgesetze durch oder zu sonstigen negativen Folgen für ESET oder eines der übergeordneten Unternehmen, die Tochtergesellschaften von ESET oder die Tochtergesellschaften der übergeordneten Unternehmen sowie die Entitäten unter der Kontrolle der übergeordneten Unternehmen (im Folgenden „angeschlossene Unternehmen“) führen könnten. Zu diesen Handelskontrollgesetzen zählen:

i. alle Gesetze, die Lizenzierungsanforderungen zum Export, Reexport oder zur Übertragung von Waren, Software, Technologie oder Dienstleistungen kontrollieren, einschränken oder auferlegen und die von Regierungen, Bundesstaaten/Bundesländern oder Regulierungsbehörden in den USA, in Singapur, in Großbritannien, der Europäischen Union oder ihren Mitgliedsstaaten oder in anderen Ländern eingeführt oder übernommen wurden, in denen die Verpflichtungen der Vereinbarung gelten, oder in denen ESET oder eines der angeschlossenen Unternehmen sesshaft oder tätig ist (im Folgenden „Exportkontrollgesetze“)

ii. alle sonstigen wirtschaftlichen, finanziellen oder handelsbezogenen Sanktionen, Einschränkungen, Embargos, Import- oder Exportbeschränkungen, Verbote von Vermögens- oder Assetübertragungen oder von Dienstleistungen sowie alle gleichwertigen Maßnahmen, die von Regierungen, Bundesstaaten/Bundesländern oder Regulierungsbehörden in den USA, in Singapur, in Großbritannien, der Europäischen Union oder ihren Mitgliedsstaaten oder in anderen Ländern eingeführt oder übernommen wurden, in denen die Verpflichtungen der Vereinbarung gelten, oder in denen ESET oder eines der angeschlossenen Unternehmen sesshaft oder tätig ist (im Folgenden „Sanktionsgesetze“).

b) ESET behält sich das Recht vor, die eigenen Verpflichtungen im Rahmen dieser Bestimmungen fristlos aufzuheben oder die Bestimmungen fristlos aufzukündigen, falls Folgendes eintritt:

i. ESET hat nach eigenem Ermessen festgestellt, dass ein Benutzer die Bestimmungen in Artikel 19.a dieser Vereinbarung verletzt hat oder vermutlich verletzt 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.

21. Geltendes Recht, Gerichtsstand. Diese Vereinbarung unterliegt slowakischem Recht. Endbenutzer und Anbieter vereinbaren, dass gesetzliche Bestimmungen zur Konfliktlösung und UN-Kaufrecht nicht zur Anwendung kommen. Sie erklären sich ausdrücklich damit einverstanden, dass als Gerichtsstand für alle Streitfälle mit dem Anbieter oder bezüglich Ihrer Verwendung der Software das Amtsgericht Bratislava I, Slowakische Republik vereinbart wird.

22. Allgemeine Bestimmungen. Wenn eine der Bestimmungen dieser Vereinbarung ungültig oder uneinklagbar ist, beeinträchtigt dies nicht die Gültigkeit der übrigen Bestimmungen der Vereinbarung. Diese bleiben unter den hier festgelegten Bedingungen gültig und einklagbar. Bei Widersprüchen zwischen übersetzten Versionen dieser Vereinbarung hat die englische Version Vorrang. Änderungen an dieser Vereinbarung bedürfen der Schriftform und müssen von einem bevollmächtigten Vertreter des Anbieters unterzeichnet werden.

Dies ist die vollständige Vereinbarung zwischen dem Anbieter und Ihnen in Bezug auf die Software. Sie ersetzt alle vorigen Darstellungen, Diskussionen, Unternehmungen, Kommunikationen und Werbungen in Bezug auf die Software.

EULA ID: BUS-STANDARD-20-01

Datenschutzerklärung

ESET, spol. s r. o., mit eingetragenem Firmensitz in Einsteinova 24, 851 01 Bratislava, Slowakei, eingetragen im Handelsregister Bratislava I, Abschnitt Sro, Eintragsnummer 3586/B, Firmenregisternummer 31333532 als Datenverarbeiter („ESET“ oder „Wir“) hat das Ziel, die persönlichen Daten und die Privatsphäre seiner Kunden transparent zu behandeln. Daher veröffentlichen wir diese Datenschutzerklärung mit dem ausschließlichen Ziel, unsere Kunden („Endkunde“ oder „Sie“) über die folgenden Themen zu informieren:

- Verarbeitung persönlicher Daten,
- Vertraulichkeit der Daten,
- Rechte betroffener Personen.

Verarbeitung persönlicher Daten

Die von ESET angebotenen und in unserem Produkt implementierten Dienste werden unter den Bestimmungen der Endbenutzer-Lizenzvereinbarung („EULA“) bereitgestellt. Einige dieser Dienste erfordern jedoch möglicherweise zusätzliche Aufmerksamkeit. Wir möchten Ihnen weitere Details zur Datensammlung im Zusammenhang mit der Bereitstellung unserer Dienste liefern. Wir bieten verschiedene in der EULA und der Produktdokumentation beschriebene Dienste an, darunter die Upgrade- und Updatedienste, ESET LiveGrid®, den Schutz vor dem Missbrauch von Daten, Support usw. Für die Erbringung dieser Dienste erfassen wir die folgenden Informationen:

- Update- und sonstige Statistiken und Informationen zum Installationsprozess und Ihrem Computer, z. B. die Plattform, auf der unser Produkt installiert wird, oder Informationen zum Betrieb und Funktionsumfang unserer Produkte wie Betriebssystem, Hardwareinformationen, Installations- und Lizenz-IDs, IP-Adresse, MAC-Adresse und Konfigurationseinstellungen des Produkts.
- Einweg-Hashes für Schadsoftware als Teil unseres LiveGrid®-Reputationssystems, das die Wirksamkeit der Sicherheitslösungen verbessert, indem es gescannte Dateien mit Positiv- und Negativlisten in einer Datenbank in der Cloud vergleicht.
- Verdächtige Samples und Metadaten „aus freier Wildbahn“ als Teil unseres ESET LiveGrid®-Reputationssystems, mit denen ESET unmittelbar auf die Anforderungen unserer Kunden reagieren und sie vor den neuesten Bedrohungen schützen kann. Wir benötigen die folgenden Daten von Ihnen:
 - oEingedrungene Schadsoftware, z. B. potenzielle Sample von Viren und anderen Schadprogrammen, sowie verdächtige, problematische, potenziell unerwünschte oder potenziell unsichere Objekte wie ausführbare Dateien oder E-Mail-Nachrichten, die von Ihnen als Spam markiert oder von unserem Produkt markiert wurden;
 - oInformationen zu Geräten im lokalen Netzwerk wie Art, Hersteller, Modell und/oder Name des Geräts;
 - oInformationen zur Internetnutzung wie IP-Adresse und geografische Informationen, IP-Pakete, URLs und Ethernet-Frames;
 - oAbsturzabbilder und darin enthaltenen Informationen.

Wir haben kein Interesse daran, Daten außerhalb des genannten Umfangs zu erfassen, allerdings lässt sich dies manchmal nicht vermeiden. Versehentlich erfasste Daten können in der Schadsoftware (ohne Ihr Wissen oder Ihre Zustimmung erfasst) oder als Teil von Dateinamen oder URLs enthalten sein. Es ist nicht unsere Absicht, diese Daten in unseren Systemen oder für die in dieser Datenschutzerklärung genannten Zwecke zu verarbeiten.

- Lizenzinformationen wie die Lizenz-ID und persönliche Daten wie Vor- und Nachname, Adresse und E-Mail-Adresse werden zu Abrechnungszwecken, zur Überprüfung der Echtheit der Lizenz und zur Erbringung unserer Dienste benötigt.
- Kontaktinformationen und andere Daten in Ihren Supportanfragen werden für möglicherweise für die Erbringung von Supportdiensten benötigt. Je nachdem, über welchen Kanal Sie uns kontaktieren, speichern wir möglicherweise Ihre E-Mail-Adresse, Telefonnummer, Lizenzinformationen, Produktdetails und eine Beschreibung Ihres Supportfalls. Möglicherweise werden Sie aufgefordert, uns weitere Informationen bereitzustellen, um die Bearbeitung der Supportanfrage zu erleichtern.

Vertraulichkeit der Daten

ESET ist ein weltweit operierendes Unternehmen über angeschlossene Unternehmen oder Partner im Rahmen unseres Distributions-, Dienst- und Supportnetzwerks. Die von ESET verarbeiteten Informationen können zur Erbringung der EULA von und zu angeschlossenen Unternehmen übertragen werden, beispielsweise für die Bereitstellung von Diensten, Supportleistungen oder Abrechnungen. Je nach Ihrem Standort und den von Ihnen ausgewählten Diensten müssen wir Ihre Daten unter Umständen in Länder ohne Gleichstellungsbeschluss der Europäischen Kommission übertragen. Selbst in diesem Fall unterliegen alle Datenübertragungen den Datenschutzbestimmungen und finden nur bei Bedarf statt. Übliche Vertragsklauseln, bindende Unternehmensregeln oder andere geeignete Mechanismen müssen ausnahmslos umgesetzt werden.

Wir unternehmen größte Anstrengungen, um zu verhindern, dass Ihre Daten bei der Bereitstellung von Diensten im Rahmen der EULA länger als notwendig gespeichert werden. Unser Aufbewahrungszeitraum ist unter Umständen länger als die Gültigkeitsdauer Ihrer Lizenz, um Ihnen eine problemlose und komfortable Erneuerung zu ermöglichen. Minimierte und pseudonymisierte Statistiken und sonstige Daten aus ESET LiveGrid® können zu

statistischen Zwecken weiterverarbeitet werden.

ESET implementiert angemessene technische und organisatorische Maßnahmen, um einen angemessenen Schutz vor potenziellen Risiken zu bieten. Wir bemühen uns nach Kräften, die fortlaufende Vertraulichkeit, Integrität, Verfügbarkeit und Ausfallsicherheit der Verarbeitungssysteme und Dienste zu gewährleisten. Falls jedoch Ihre Rechte und Freiheiten durch einen Datenangriff gefährdet sind, müssen wir die Aufsichtsbehörden sowie die betroffenen Personen informieren. Betroffene Personen haben das Recht, Beschwerde bei einer Aufsichtsbehörde einzulegen.

Rechte betroffener Personen

ESET unterliegt slowakischem Recht und ist als Teil der Europäischen Union an die Datenschutzgesetze gebunden. Im Rahmen der geltenden Datenschutzgesetze haben Sie als betroffene Person die folgenden Rechte:

- das Recht, Ihre persönlichen Daten von ESET anzufordern,
- das Recht, Ihre persönlichen Daten bei Bedarf zu berichtigen (Sie haben auch das Recht, unvollständige persönliche Daten zu vervollständigen),
- das Recht, die Löschung Ihrer persönlichen Daten anzufordern,
- das Recht, eine Einschränkung der Verarbeitung Ihrer persönlichen Daten anzufordern,
- Einlegen von Einspruch gegen die Verarbeitung
- Einlegen von Beschwerden sowie
- das Recht auf Übertragbarkeit der Daten.

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