

Optimal vorbereitet für Ihre ESET Lösungen

Verwenden Sie eine Firewall, stellen Sie bitte sicher, dass die ESET Lösungen Zugriff auf die folgenden Ports und URLs haben:

ESET PROTECT (Cloud und On-Prem):

- HTTP (Port 80)
- HTTPS (Port 443)
- UDP/TCP (Port 53535)
- *.eset.com
- *.eset.systems
- *.eset.eu
- *.e5.sk

ESET Inspect (Cloud und On-Prem):

- TCP (Port 8093)

Diese Verbindungen sind erforderlich, damit die ESET Lösungen vollständig und ordnungsgemäß funktionieren. Weitere Details finden Sie hier:

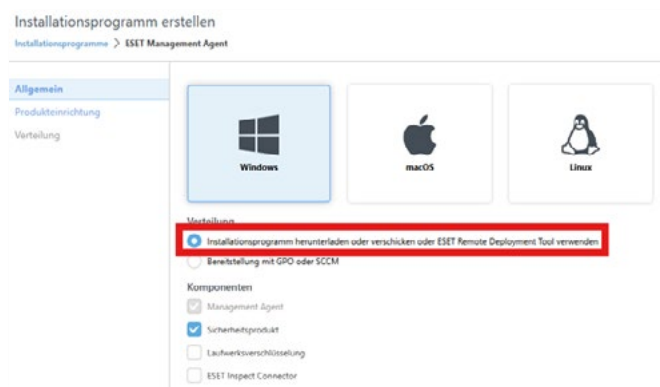
➤ <https://support.eset.com/en/kb332-ports-and-addresses-required-to-use-your-eset-product-with-a-third-party-firewall>

Sobald die zentrale Verwaltungskonsole ESET PROTECT eingerichtet ist, kann die Bereitstellung der ESET Endpoint-Lösungen starten. Dafür stehen drei verschiedene Methoden zur Auswahl.

Methode 1: Live Installer

Wenn Sie sich für die Installation über den Live Installer entscheiden, haben Sie die Möglichkeit, unser Remote Deployment Tool zu verwenden. Dieses steht ausschließlich für Windows-Systeme zur Verfügung. Mehr Informationen zum Remote Deployment Tool und Download finden Sie hier:

➔ <https://www.eset.com/de/business/download/eset-protect/#standalone>



Der Live Installer ist eine ausführbare .exe-Datei, die automatisch die aktuellen Agenten und Produktversionen aus dem ESET Repository herunterlädt.

Falls hierbei Probleme auftreten, liegt dies in den meisten Fällen daran, dass der Endpoint keinen Zugriff auf die erforderlichen ESET Ressourcen hat. Bitte überprüfen Sie daher, ob in der Firewall die oben genannten Ausnahmen korrekt definiert wurden.

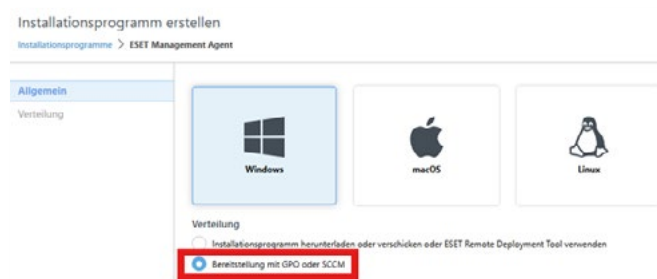
Während des Vorgangs werden Logs erstellt und unter folgendem Dateipfad abgelegt:

%temp%\eset*installer.log

Weitere Details finden Sie hier:

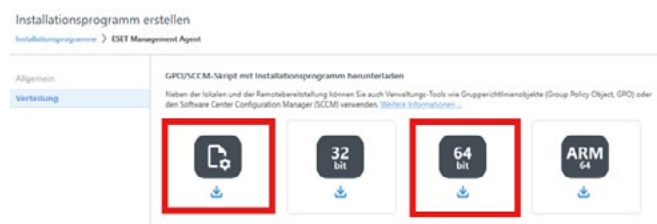
➔ https://help.eset.com/protect_cloud/de-DE/fs_local_deployment_aio_create.html

Methode 2: GPO Deployment (MSI + INI)



Hierbei wird die .msi-Datei des Agenten über eine Gruppenrichtlinie verteilt.

Eine begleitende .ini-Datei enthält Zertifikate sowie Verbindungsinformationen (Serveradresse, Port, etc.).



Falls hierbei Probleme auftreten, müssen die Logs manuell über den Command-Befehl erstellt werden:

msiexec /i agent_x64.msi /lvx* install.log

Dieser Befehl führt die Installation erneut aus, diesmal wird zusätzlich ein Log erstellt.

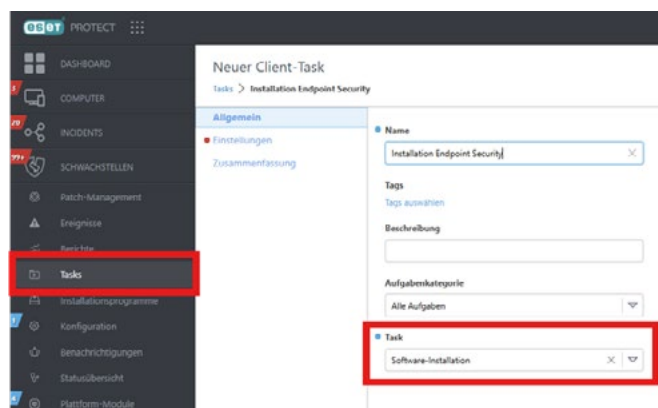
Weitere Details finden Sie hier:

➔ <https://support.eset.com/en/kb6864-deploy-the-eset-management-agent-using-a-group-policy-object-windows-8x9x>

➔ <https://support.eset.com/de/kb406-eset-smart-security-oder-eset-nod32-antivirus-installationsprobleme-wie-erzeuge-ich-ein-fehlerprotokoll>

Methode 3: Installation über bestehenden Agenten (Software-Installations-Task)

Wenn der Agent bereits installiert ist, kann die Software über einen Task ausgerollt werden.



Standardmäßig wird ESET Management Agent alle 10 Minuten mit ESET PROTECT synchronisiert.

Falls die Softwareinstallation aus irgendeinem Grund fehlschlägt, können Sie die Ursache in den Logs auf dem Endpoint unter folgendem Pfad einsehen:

Windows	C:\ProgramData\ESET\RemoteAdministrator\Agent\EraAgentApplicationData\Logs\software-install.log
Linux	/var/log/eset/RemoteAdministrator/Agent/var/log/eset/RemoteAdministrator/EraAgentInstaller.log
MacOs	/Library/Application Support/com.eset.remoteadministrator.agent/Logs/Users/%user%/Library/Logs/EraAgentInstaller.log

Beachten Sie, dass **ProgramData** ein vom Betriebssystem versteckter Ordner ist. Sie können ihn öffnen, indem Sie den Pfad direkt im Windows-Explorer eingeben oder die Anzeige für versteckte Ordner aktivieren.

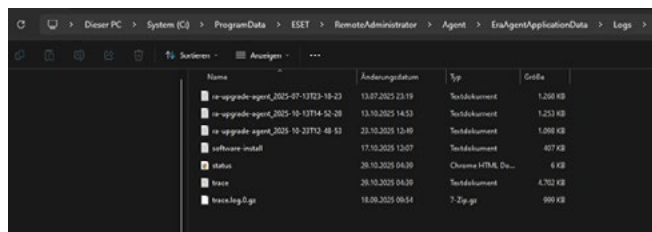
Im ESET Ordner befinden sich weitere wichtige Log-Dateien, die folgende Aufgaben erfüllen:

status.html – Dieses Protokoll zeigt den aktuellen Status der Kommunikation (Synchronisierung) zwischen ESET Management Agent und ESET PROTECT Server an. Das Log enthält außerdem die HTTP-Proxykonfiguration, eine Liste der angewendeten Policies (inklusive angewendeter Ausschlüsse) und eine Liste der dynamischen Gruppen, zu denen das Gerät gehört.

last-error.html – Dieses Protokoll zeigt den letzten aufgezeichneten Fehler an, während der ESET Management Agent aktiv war.

software-install.log – Dieses Protokoll zeigt den letzten Remote-Installations-Task, den der ESET Management Agent ausgeführt hat.

trace.log – Dieses ausführliche Protokoll zeigt alle Aktivitäten des ESET Management Agenten inklusive aller erfassten Fehler.



Weitere Details finden Sie hier:

➤ https://help.eset.com/protect_cloud/de-DE/admin_ct.html?client_tasks_software_install.html

➤ https://help.eset.com/protect_cloud/de-DE/fs_agent_connection_troubleshooting.html

ÜBER ESET

Als europäischer Hersteller mit mehr als 35 Jahren Erfahrung bietet ESET ein breites Portfolio an Sicherheitslösungen für jede Organisationsgröße. Wir schützen betriebssystemübergreifend sämtliche Endpoints und Server mit einer vielfach ausgezeichneten mehrschichtigen Technologie und halten Ihre Infrastruktur mithilfe von Cloud Sandboxing frei von Zero-Day-Bedrohungen. Mittels Multi-Faktor-Authentifizierung und zertifizierter Verschlüsselungslösungen unterstützen wir Sie bei der Umsetzung von Datenschutzbestimmungen sowie Compliance-Maßnahmen.

Unsere Endpoint Detection and Response-Lösung, dedizierte Services wie z.B. Managed Detection and Response und Frühwarnsysteme in Form von Threat Intelligence ergänzen das Angebot im Hinblick auf Incident Management sowie den Schutz vor gezielter Cyberkriminalität und APTs. Dabei setzt ESET nicht allein auf modernste KI-Technologie, sondern kombiniert Erkenntnisse aus der cloudbasierten Reputationsdatenbank ESET LiveGrid® mit Machine Learning und menschlicher Expertise, um Ihnen den besten Schutz zu gewährleisten.

3 VON ÜBER 500.000 ZUFRIEDENEN KUNDEN



**CHAMPION
PARTNER**

Seit 2019 ein starkes Team
auf dem Platz und digital



Seit 2016 durch ESET geschützt
Mehr als 4.000 Postfächer



ISP Security Partner seit 2008
2 Millionen Kunden

BEWÄHRT



ESET wurde das Vertrauensiegel
„IT Security made in EU“ verliehen



Unsere Lösungen sind nach den Qualitäts- und
Informationssicherheitsstandards ISO 9001:2015
und ISO/IEC 27001:2022 zertifiziert

KONTAKT

Bei Rückfragen können sich ESET Partner
an die Partnerbetreuung wenden.

Tel: +49 (0) 3641 / 31 14 - 220 (Mo - Fr 8 - 17 Uhr)
E-Mail: partner@eset.de



Digital Security
Guide