

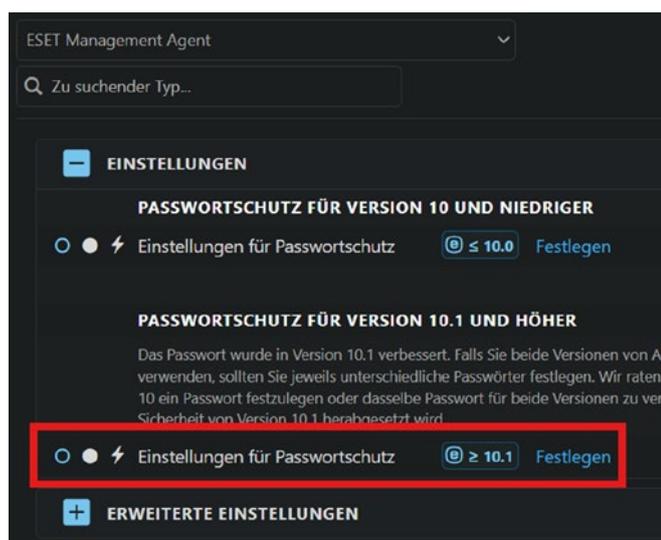
Best Practice für den ESET Management Agent (Version 12)

Diese Best-Practice-Anleitung gilt für den ESET Management Agent Version 12. Es ist möglich, dass sich diese Optionen in zukünftigen Versionen ändern. Alle Best-Practice-Empfehlungen sind mit einer Begründung versehen. Falls ein Vorschlag für Sie nicht relevant ist, können Sie diesen Punkt gerne überspringen.

Hinweis: Der ESET Management Agent ist nicht lizenzierungspflichtig. Sie können Agenten unabhängig von der Lizenz ausrollen. Der Agent wird mit SysAdmin-Rechten installiert, was bedeutet, dass er Tasks unabhängig vom später eingeloggten Benutzer ausführen kann. Wie den Software-Installations-Task, um im Nachgang weitere ESET Lösungen auf dem Endpoint zu installieren.

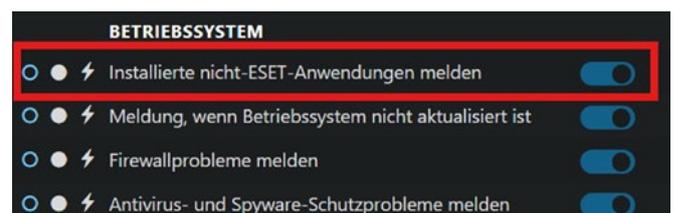
Vorschlag 1

Legen Sie ein Passwort fest, um eine ungewollte Deinstallation des *ESET Management Agent* zu verhindern.



Vorschlag 2

Aktivieren Sie die Option *Installierte Nicht-ESET-Anwendungen melden*. Dadurch können installierte Software und Anwendungen auf dem Gerät erfasst und angezeigt werden.



Vorschlag 3

Erstellen Sie ein neues Dashboard in *ESET PROTECT* und benennen Sie es *SW/HW-Inventar*.

Passen Sie das Layout so an, dass es aus maximal zwei Kacheln besteht. Diese belegen Sie mit den folgenden Berichten:

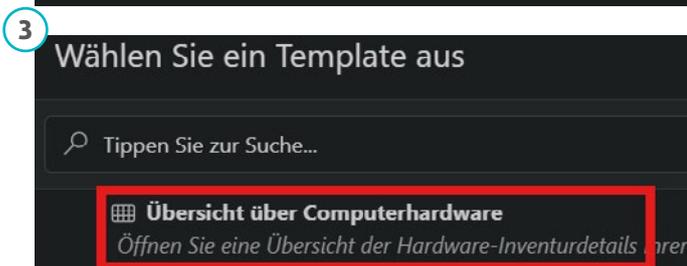
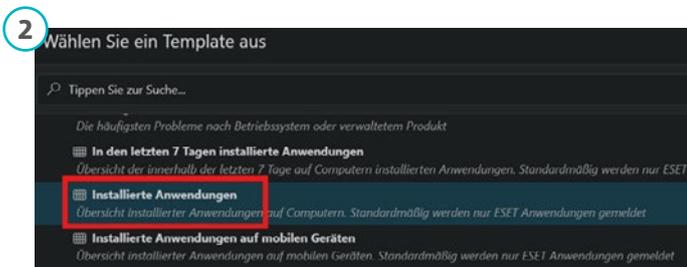
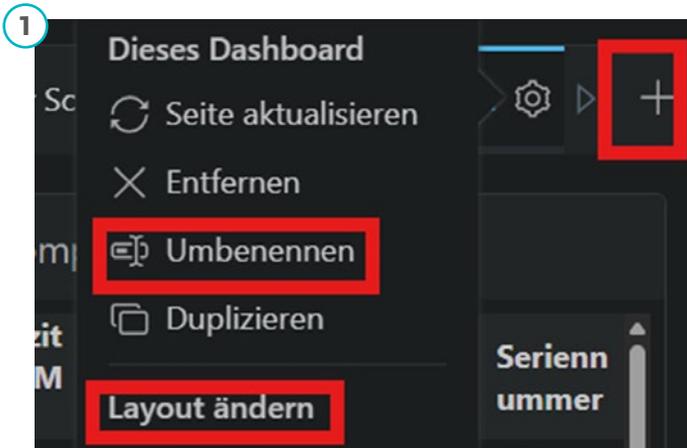
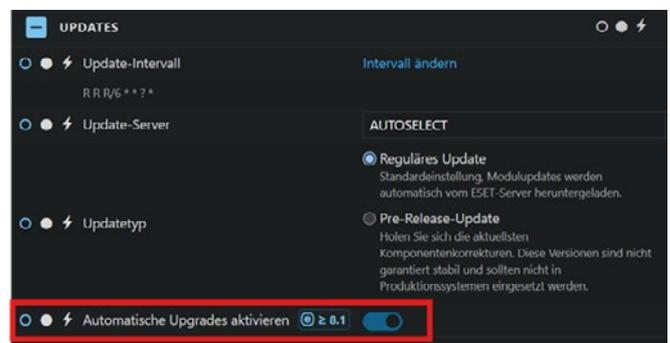
- Übersicht über Computerhardware
- Installierte Anwendungen

Durch diese beiden Berichte verfügen Sie nun über einen ausgezeichneten Überblick über Ihre Assets. Unser Agent ermöglicht Ihnen, sowohl Hardware- als auch Software-Attribute auszulesen – darunter verbaute Komponenten, angeschlossene Peripheriegeräte sowie Informationen zum Betriebssystem und den installierten Anwendungen. Dies ist besonders nützlich für die Umsetzung von Sicherheitsstrategien mithilfe von Policies und dynamischen Gruppen.

Vorschlag 4

Aktivieren Sie die Option *Automatische Updates*. Durch die Aktivierung der automatischen Upgrades bleibt das System stets auf dem neuesten Stand – so profitieren Sie von einem erhöhten Sicherheitsniveau.

Hinweis: Diese Option gilt ausschließlich für Agenten, die von einer On-Premises-Konsole verwaltet werden. Agenten in einer cloud-basierten ESET PROTECT Instanz benötigen diese Option nicht, da sie immer automatisch auf dem neuesten Stand gehalten werden.



ÜBER ESET

Als europäischer Hersteller mit mehr als 30 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



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

ESET IN ZAHLEN

110.000.000+

Geschützte Nutzer weltweit

500.000+

Geschützte Unternehmen

176

Länder & Regionen

11

Forschungs- und Entwicklungszentren weltweit

