

ACMP DEFENDER MANAGEMENT

Microsoft Defender Antivirus
im Unternehmen nutzen



Copyright

Alle Inhalte dieser Broschüre unterliegen dem deutschen Urheber- und Leistungsschutzrecht. Jede Art der Vervielfältigung, Bearbeitung, Verbreitung, Speicherung und jede Art der Verwertung außerhalb der Grenzen des Urheberrechts bedarf der vorherigen schriftlichen Zustimmung der Aagon GmbH. Das unerlaubte Kopieren/Speichern und Vervielfältigen der bereitgestellten Informationen dieser Broschüre ist nicht gestattet und strafbar.

Soest, September 2021.

ACMP Defender Management

Einführung

Die Nutzung von Microsoft Defender Antivirus kann ohne zentrale Verwaltung sehr zeitaufwendig sein. Die Konfigurationen über Microsoft-Management-Lösungen, wie Intune und SCCM, erschweren zusätzlich eine übersichtliche Organisation.

Mit ACMP Defender Management können Administratoren Microsoft Defender Antivirus zentral verwalten und konfigurieren. In der ACMP-Console bietet die Lösung alle Funktionen, um den Microsoft Defender zu managen und dadurch den administrativen Aufwand zu vereinfachen.



Was ist Microsoft Defender Antivirus?

Microsoft Defender Antivirus ist ein von Microsoft entwickelter Echtzeit-Virenschutz, um Bedrohungen wie Viren, Schadsoftware und Spyware in Apps, der Cloud und im Web zu erkennen. Das Programm ist standardmäßig unter Windows 10 vorinstalliert und soll Daten und Geräte mit einer Suite an erweiterten Sicherheitsmaßnahmen schützen. Die Software bietet umfassende Funktionen des Virenschutzes. Dazu zählen beispielsweise ein Event-Überblick über Funde, Bedrohungen und Updates, automatisierte Aktualisierungen der Bedrohungsdefinitionen und ein überwachter Ordnerzugriff. Die Grundfunktionalitäten von Microsoft Defender Antivirus sind Nutzer von Windows 10 ohne zusätzliche Kosten verfügbar.

Warum ACMP Defender Management?

ACMP Defender Management wurde entwickelt, um Administratoren die Möglichkeit zu geben, Microsoft Defender Antivirus in nur einer Oberfläche auf allen Clients und Servern zu verwalten.

So bildet ACMP Defender Management die Grundlage für einen umfassenden, vollintegrierten Antivirenschutz der Unternehmens-IT. ACMP Defender Management reduziert den Aufwand und sorgt für Kostenersparnisse.



Zentrale Verwaltung

Antivirus-Management über die ACMP-Console



Einfache Konfiguration

Leichte, komfortable Konfiguration über die bewährte ACMP Oberfläche



Größerer Funktionsumfang

Microsoft Defender Antivirus bietet – abhängig von der Lizenzierung – mehr Funktionen als vergleichbare Antivirenlösungen.



Zusammenspiel mit anderen ACMP-Modulen

Hohe Automatisierung durch die Kombination mit weiteren Lösungen in ACMP



Kostenersparnis

Zeitersparnisse und keine zusätzliche Antivirenlösung mehr nötig



Bereits im Betriebssystem integriert

Blitzschnelle Inbetriebnahme und bessere Performance



Dashboards und Reports

Security Audits und Management Reports dank Zusammenfassungen und Berichten unkompliziert meistern.



Konfigurationen für Signatur-Updates

Microsoft Defender Antivirus schnell und einfach so konfigurieren, dass Signatur-Updates von Ihrem WSUS-Server, aus dem Internet oder über ACMP CAWUM bezogen werden.

Funktionen

Abfragen, Dashboards und Reports

ACMP Defender Management zeigt den Defender-Status, Scan-Historien, neueste Bedrohungen sowie Infos zum nächsten anstehenden Scan an und bietet die Möglichkeit zur Abfrage der genutzten / nicht genutzten Konfigurationsprofile und vieles mehr.

Manipulationsschutz (Tamper Protection)

Der Manipulationsschutz verhindert das Setzen von diversen Einstellungen, sodass schädliche Apps wichtige Antivirus-Einstellungen des Microsoft Defenders nicht ändern können. Der Manipulationsschutz kann nicht automatisiert deaktiviert werden

Berechtigungs- und Benutzerrechteverwaltung

Administratoren können die Benutzerrechte für Konfigurationsprofile, Container und Query Actions konfigurieren. Außerdem lassen sich die Berechtigungen für Gruppen und deren Benutzer anpassen.

Ereignis-Überblick

Regelmäßig wird nach Funden, Bedrohungen und Updates gescannt. Benachrichtigungen über Funde erfolgen in Echtzeit. Zudem gibt es einen Überblick über alle gefundenen Bedrohungen, fehlgeschlagenen Updates und sonstigen Ereignisse. Die Anzeige der Ereignisse lässt sich konfigurieren. Außerdem besteht die Möglichkeit des Filterns, Sortierens und Löschens veralteter Ereignisse. Aus einem Ereignis kann direkt zum betroffenen Client navigiert werden.

Zentrale Quarantäne

Das Einsehen und Wiederherstellen von Quarantänedateien sowie Ausführen von Aktionen auf diesen ist ganz einfach zentral aus der ACMP-Console heraus möglich. Quarantänedateien lassen sich automatisiert nach Ablauf eines definierten Zeitraums löschen.

Antivirensan am Client starten

Sie können den Antivirus-Scan an einem Client starten und den Stand des Scans in den Logs anzeigen lassen. Zusätzlich gibt es die Möglichkeit, einem Client über ein Konfigurationsprofil geplante Scans zuzuweisen oder diese zu entfernen.

Management ohne Cloud-Anbindung

Microsoft bietet Unternehmen mit kritischen Infrastrukturen, welche aus Sicherheitsgründen nicht direkt mit dem Internet verbunden sind, keine Möglichkeit, das Management von Microsoft Defender ohne eine Cloud-Anbindung durchzuführen. Mit der Nutzung von ACMP Defender Management wird dieses Problem behoben, da ACMP einfach und unkompliziert direkt „on premises“ genutzt werden kann. Somit spricht auch in solchen Umgebungen nichts gegen den Einsatz des Microsoft Defender auf den Endgeräten.

Voraussetzungen

- Bereits ab Windows 10 Pro können Sie einen Großteil der Defender-Funktionen nutzen. Abhängig von der Größe Ihres Vertrags bei Microsoft kommen mit E3 oder E5 bzw. Education A5 noch weitere Enterprise-Funktionen hinzu. Den genauen Funktionsumfang von Microsoft Defender, abhängig von der Lizenzierung, hat Microsoft hier zusammengefasst.
- Das Modul ACMP Inventory ist eine Voraussetzung für das ACMP Defender Management.
- Die empfohlenen und erforderlichen Systemvoraussetzungen für ACMP finden Sie hier.

Häufig gestellte Fragen

Wo werden die Daten von MS Defender verarbeitet und gespeichert?

Die Daten werden zentral und nur in der ACMP-Datenbank gespeichert.

Wie wird das Modul lizenziert?

Das Modul wird auf Client-Basis als Mietlizenz lizenziert.

Was passiert mit Quarantänedateien?

Diese können wiederhergestellt oder mithilfe des Bereinigungsdienstes automatisch gelöscht werden. Außerdem können Ausnahmen für Quarantänedateien definiert werden.

Gibt es automatische Benachrichtigungen bei Funden?

Dies wird mithilfe von Reports umgesetzt. Sobald eine Benachrichtigung über einen Fund eingeht, kann automatisch ein Report verschickt werden.

Können feste Scanzeiten definiert werden?

Es können Zeitpunkte für Quick-, Full- und Custom-Scans definiert werden.

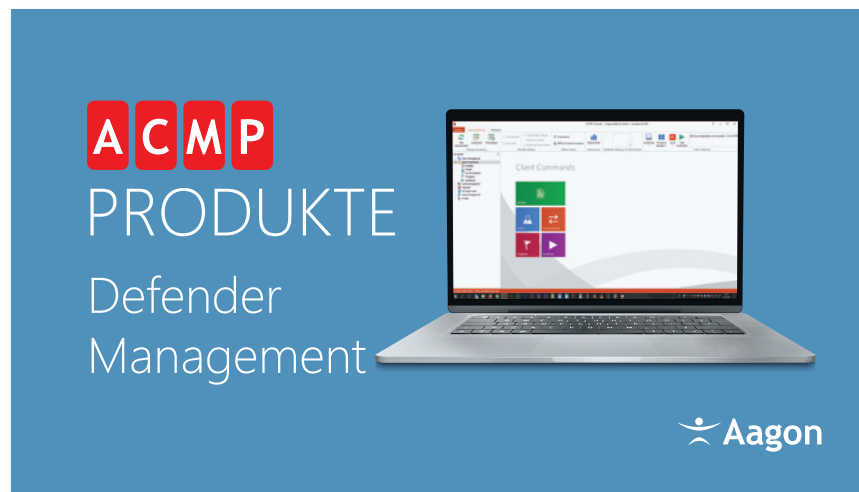
Ist es möglich, Defender-Profile dynamisch zuzuweisen?

Ja, Profile können über die Container dynamisch zugewiesen werden.

Video

Erfahren Sie im Video, welche Möglichkeiten Ihnen ACMP Defender Management bei der Verwaltung von Microsoft Defender Antivirus bietet.

Jetzt ansehen >



Überblick

ACMP Defender Management First Steps

Zurück nach
ACMP Lizenz

Ereignis-Scan-Einstellungen

Hier können Sie die Ereignistypen festlegen, die vom ACMP Agent gescannt werden sollen

⚡ Ereignistypen

Ereignistypen, die der ACMP Agent scannen soll

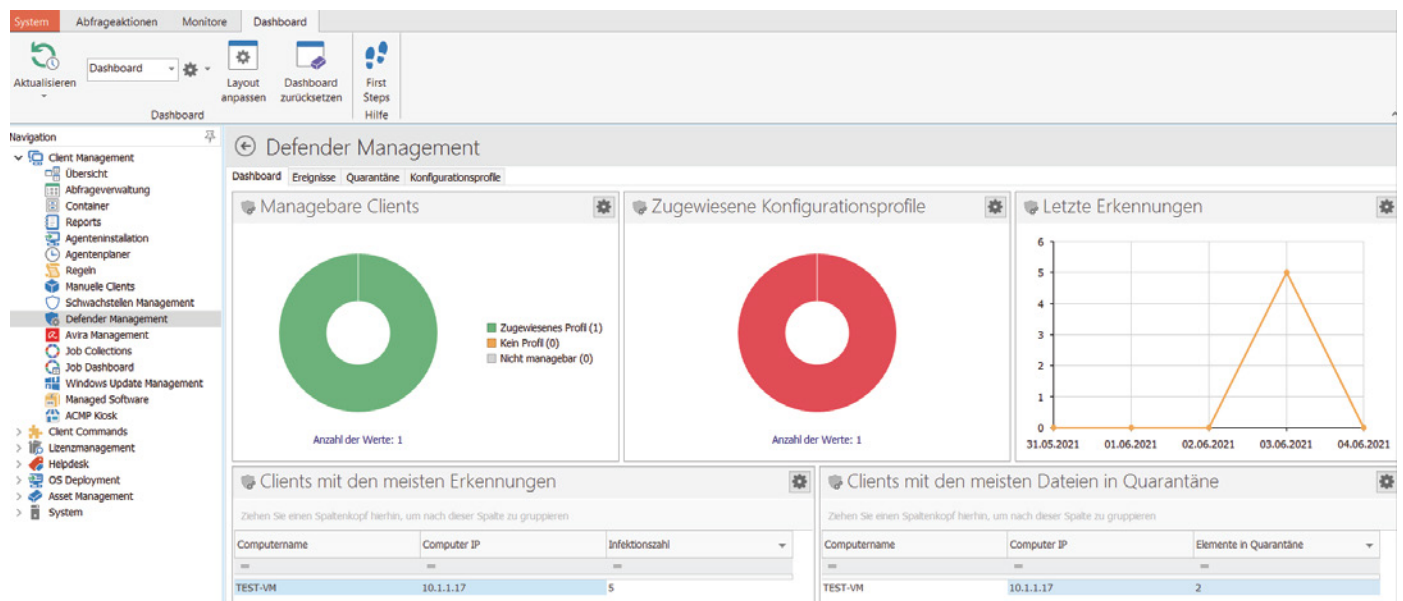
- ☒ Alarm
- ☒ Fehler
- ☒ Warnung
- ☒ Hinweis
- ☐ Information

Schritt 2 von 5
Ereignis Scan-Einstellungen

Nächster Schritt
Konfigurationsprofil Auswahl

< Zurück Weiter > Fertig Abbrechen

First Steps Wizard



Dashboard

TEST-VM

AI Clients TEST-VM

Defender Management

Defender Management

Dashboard Ereignisse Quarantäne Konfigurationsprofil

Modulinformationen

Modulname	Status
Anti Malware	Aktiviert
Anti Spyware	Aktiviert
Anti Virus	Aktiviert
Verhaltensüberwachung	Aktiviert
Internet-On-Demand-Antivirus-Schutz	Aktiviert
Network Inspection System	Aktiviert

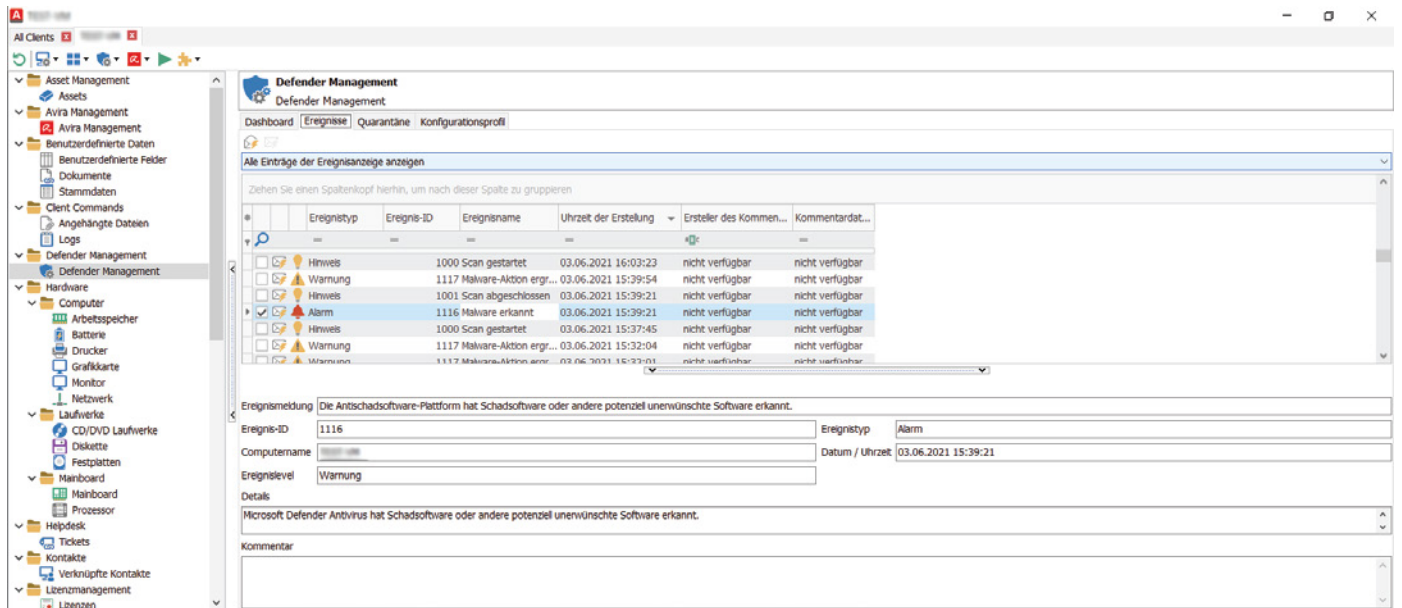
Signaturversionen

Modulname	Version	Letzte Aktualisierung	Signaturalter (Ta...
Anti Spyware	1.339.195...	03.06.2021 10:54:00	0
Anti Virus	1.339.195...	03.06.2021 10:54:00	0
Network Inspection System	1.339.195...	03.06.2021 10:54:00	0

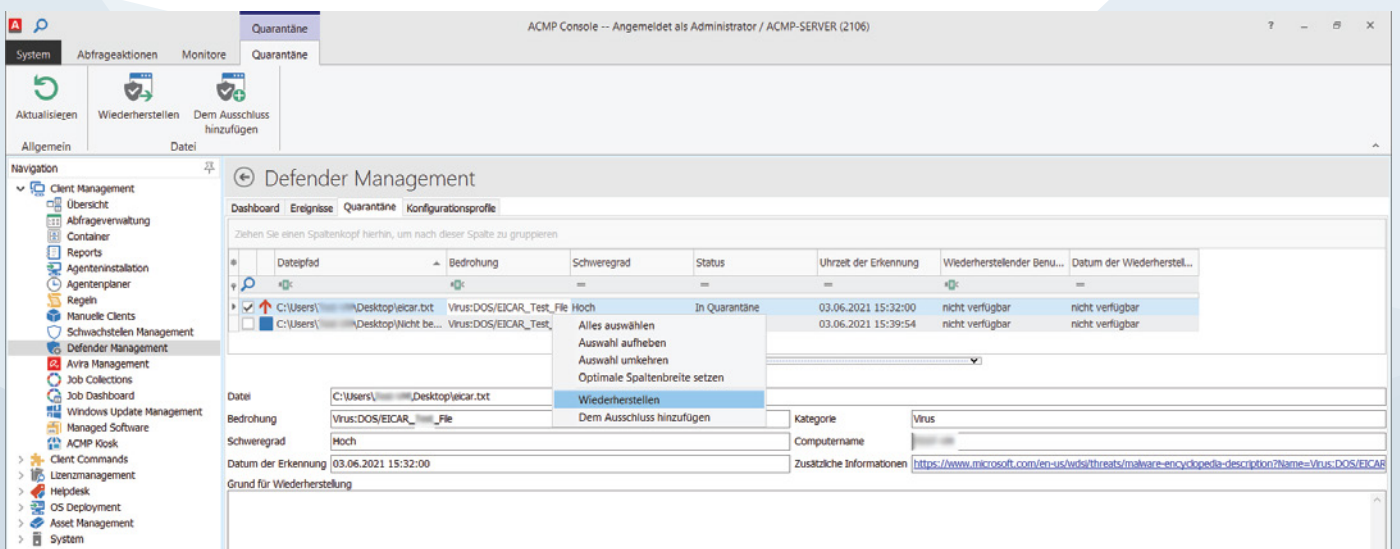
Letzte Scans

Scan-Typ	Alter des Scans (Tage)	Startzeit	Endzeit	Scan-Ursprung
Vollständiger System-Scan	nicht verfügbar	nicht verfügbar	nicht verfügbar	Unbekannt
System Schnellsan	0	03.06.2021 15:37:00	03.06.2021 15:39:00	System

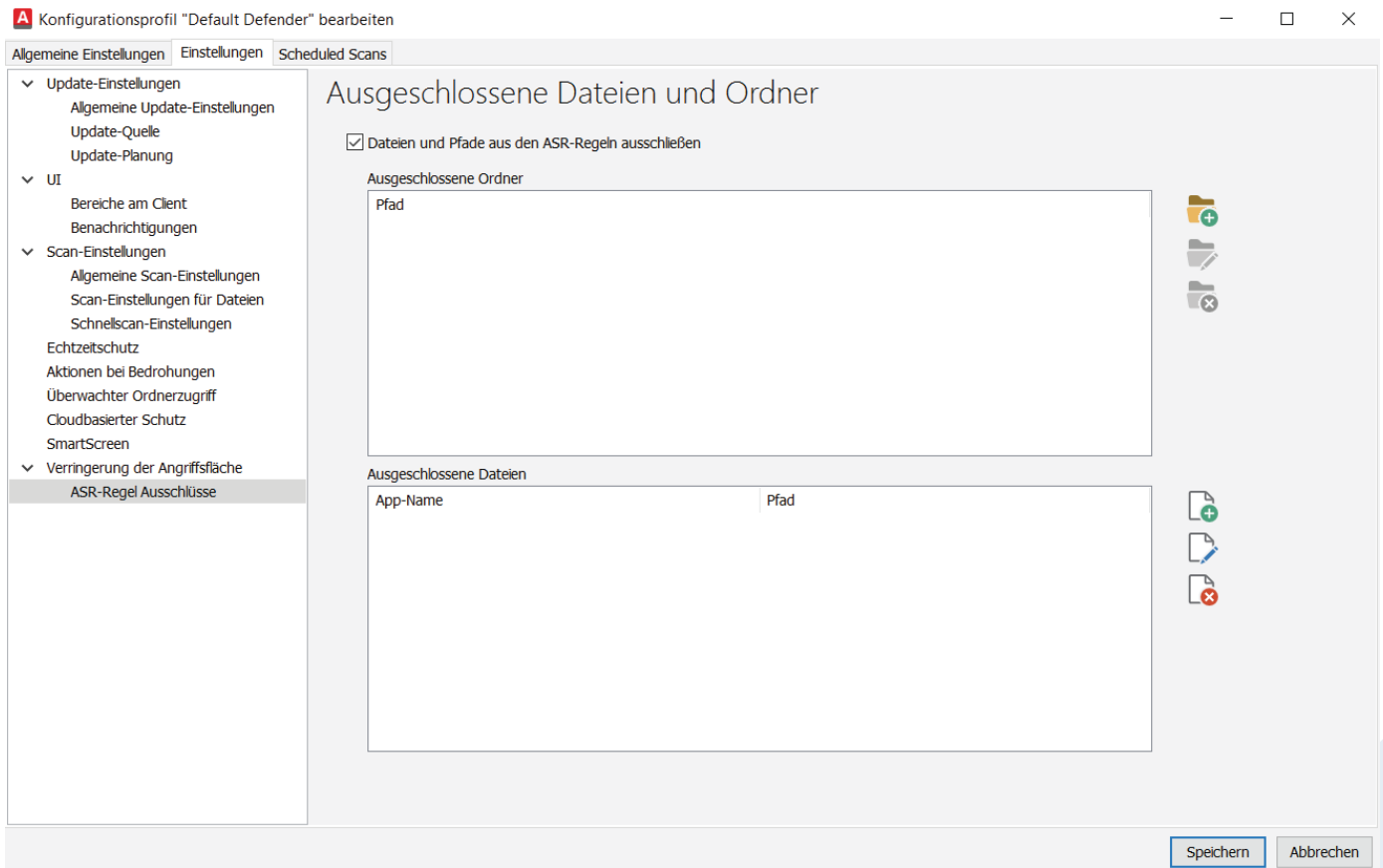
Client Details



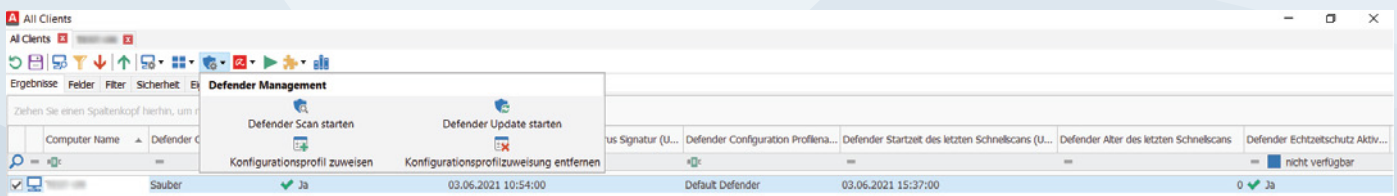
Defender-Events



Quarantänemanagement



Konfigurationsprofil



Query

EIN PRODUKT DER

Aagon GmbH

Lange Wende 33

D-59494 Soest

Fon: +49 (0)2921 - 789200

Fax: +49 (0)2921 - 789244

sales@aagon.com

www.aagon.com

