



AppLocker Commander-Anleitung

1 Beschreibung.....	3
1.1 Was ist AppLocker?	3
1.2 Sicherheitsmechanismen im Vergleich	3
1.3 Warum AppLocker Commander?	3
1.4 Regeln verwalten	3
1.5 AppLocker pausieren	3
1.6 System härten	3
1.7 Events anzeigen	3
1.8 Import/Export	4
1.9 Software installieren	4
2 Anleitungen.....	5
2.1 Hauptansicht	5
2.2 Statusüberwachung	5
2.3 AppLocker pausieren	6
2.3.1 Dauer wählen	6
2.3.2 Module einzeln umschalten.....	6
2.3.3 Regel dauerhaft deaktivieren.....	7
2.3.4 Hinweis vor dem Pausieren	7
2.4 Regeln verwalten	8
2.4.1 Regelübersicht	8
2.4.2 Regeln löschen	8
2.4.3 Regeln gruppieren.....	9
2.4.4 XML anzeigen	9
2.4.5 Regel erstellen.....	9
2.4.5.1 Pfad	10
2.4.5.2 Herausgeber	11
2.4.5.3 Dateihash	12
2.4.5.4 App-Pakete	12
2.4.6 Regel bearbeiten	13
2.5 System härten	14
2.5.1 Stufen: System Rule, Data Rule, User Rule	14
2.5.2 Data-Rule-Feineinstellungen.....	15
2.5.3 User Rule	15
2.5.4 Win Tools Rule	16
2.5.5 System härten starten.....	18

2.6 Events anzeigen	20
2.6.1 Zeitraum und Suche	20
2.6.2 AppLocker-Selbsttest ausblenden	21
2.6.3 Duplikate zusammenfassen	21
2.6.4 Ereignis in die Zwischenablage kopieren	21
2.6.5 Regel aus Event erstellen	21
2.7 Import/Export	22
2.8 Software installieren	23
2.9 Einstellungen	24
2.9.1 UAC-Filter für lokale Administratoren	25
2.9.2 UAC-Grundfunktion	25
2.9.3 Anwendungsidentität	25
2.9.4 Windows starten	25
3 Lizenz	26

1 Beschreibung

1.1 Was ist AppLocker?

AppLocker ist ein Regelsystem nach dem Whitelisting-Prinzip: Es blockiert grundsätzlich alles, was nicht ausdrücklich erlaubt ist.

Dadurch schützt es auch vor Schadsoftware, die zum Zeitpunkt der Regelerstellung noch nicht existiert, ohne dass die Regeln laufend aktualisiert werden müssen.

Angepasst werden müssen die Regeln in der Regel nur bei Änderungen am System, etwa wenn Software installiert oder deinstalliert wird.

1.2 Sicherheitsmechanismen im Vergleich

Schutzsystem	Virusangriff	Start von Programmen	Funktionsprinzip
Virenschutz	● Wenn bekannt	● Immer erlaubt	Blacklisting Reagiert auf bekannte Signaturen
AppLocker	● Immer blockiert	● Wenn bekannt	Whitelisting Blockiert standardmäßig das Unbekannte

1.3 Warum AppLocker Commander?

AppLocker Commander macht die in Windows integrierte, aber schwer zugängliche AppLocker-Funktion über eine grafische Oberfläche nutzbar und vereint die dafür nötigen Werkzeuge an einem Ort.

Sicherheitsregeln lassen sich damit automatisiert erstellen, ohne die AppLocker-Konfiguration manuell bearbeiten zu müssen.

1.4 Regeln verwalten

- AppLocker-Regeln für Ausführbare Dateien, DLL-Dateien, Skripte, App-Pakete und Windows Installer erstellen, bearbeiten und löschen
- Regeln nach Pfad, Herausgeber oder Dateihash definieren

1.5 AppLocker pausieren

- AppLocker für alle oder einzelne Module vorübergehend auf Nur Überwachung schalten
- Zeitgesteuert (1–60 Minuten) oder dauerhaft, mit Restzeit-Anzeige

1.6 System härten

- Mit wenigen Klicks abgestufte AppLocker-Regeln für das gesamte System erzeugen
- Schutzgrad in Prozent zeigt die erreichte Absicherung an

1.7 Events anzeigen

- AppLocker-Ereignisse live überwachen, filtern und durchsuchen
- Aus einem blockierten Ereignis direkt eine passende Regel erstellen

1.8 Import/Export

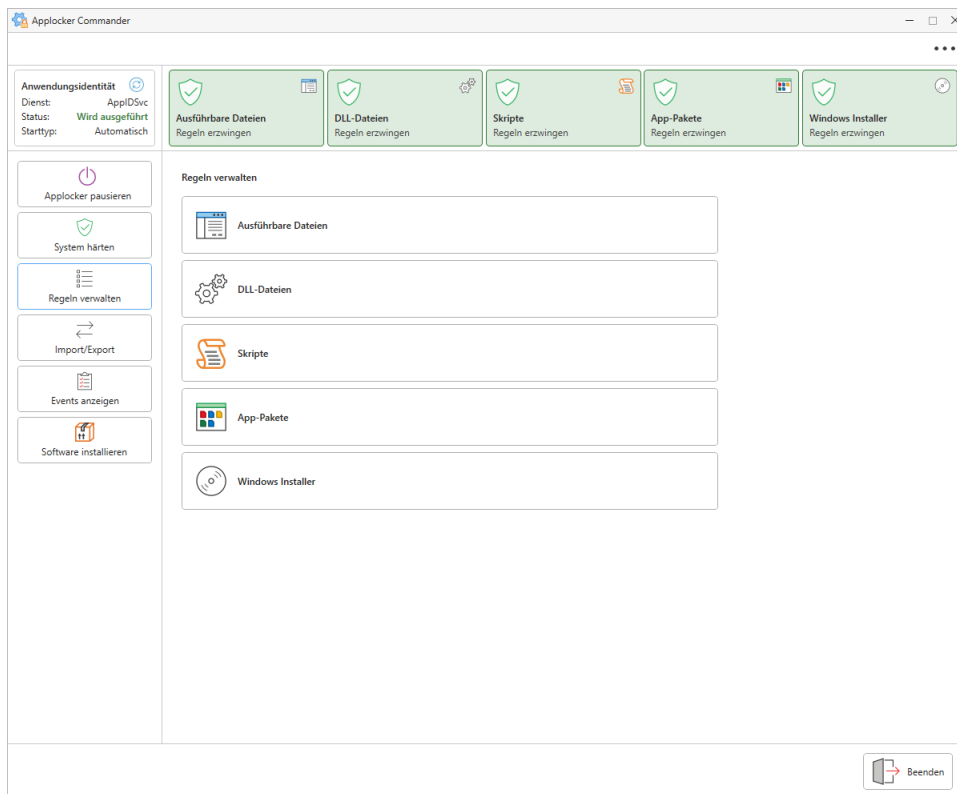
- Regeln als XML exportieren und einzeln oder komplett wieder importieren

1.9 Software installieren

- Installationsdateien kontrolliert ausführen, ohne von aktiven AppLocker-Regeln blockiert zu werden

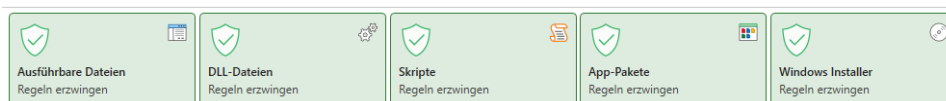
2 Anleitungen

2.1 Hauptansicht



- Oben links: Anwendungsidentität mit Dienststatus (AppIDSvc)
- Oben: Statusüberwachung
- Links: Hauptmenü mit allen Programmbereichen
- Mitte: Einstieg in die einzelnen Programmbereiche

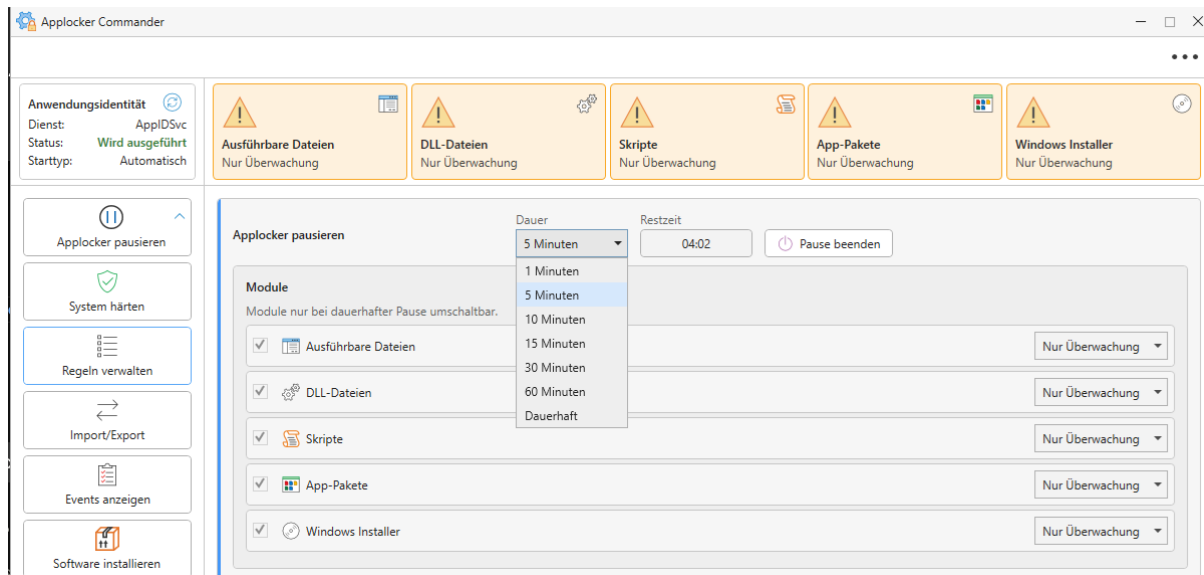
2.2 Statusüberwachung



- Grün mit Haken bedeutet, dass für dieses Modul Regeln erzwungen werden – blockierte Anwendungen werden aktiv verhindert.
- Gelb mit Ausrufezeichen bedeutet, dass sich das Modul im Modus 'Nur Überwachung' befindet – Verstöße werden protokolliert, aber nicht blockiert.
- Der Status wird laufend anhand der bestehenden Regeln geprüft.
- Das Abfrageintervall lässt sich in den Optionen anpassen.

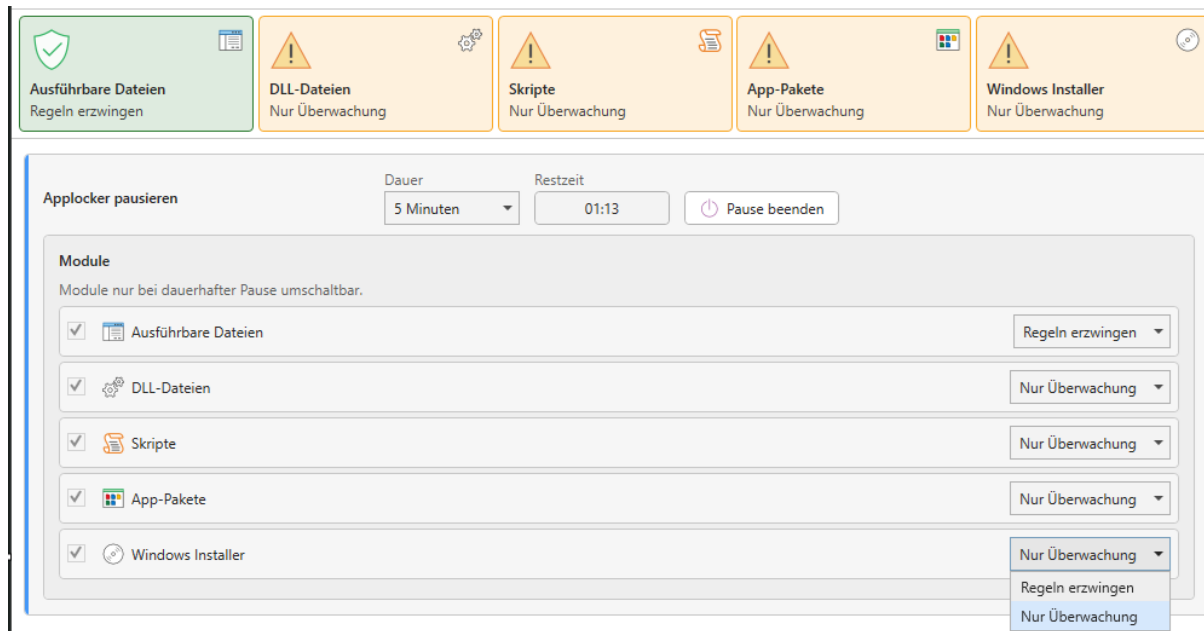
2.3 AppLocker pausieren

2.3.1 Dauer wählen



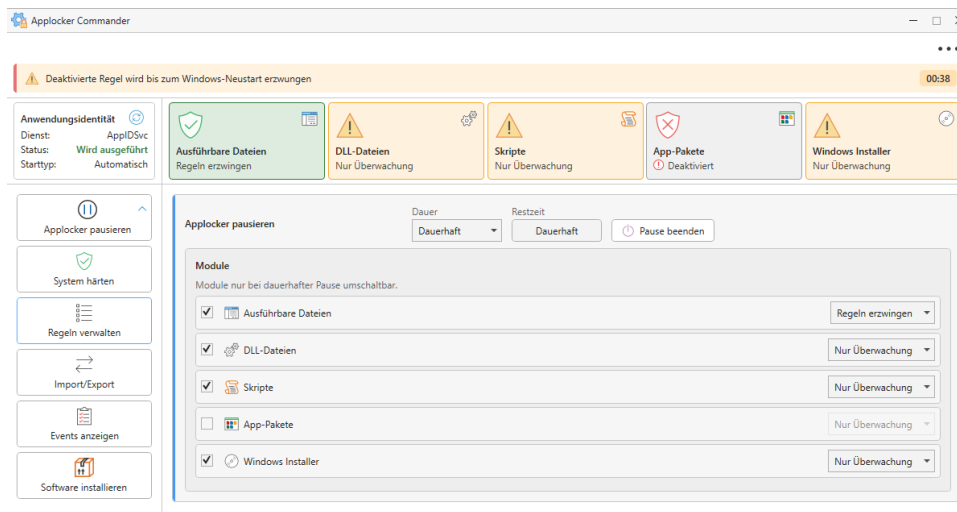
- Auswahl zwischen 1, 5, 10, 15, 30, 60 Minuten oder Dauerhaft
- Während der Pause zeigt Restzeit die verbleibende Dauer, Pause beenden stoppt sie vorzeitig

2.3.2 Module einzeln umschalten



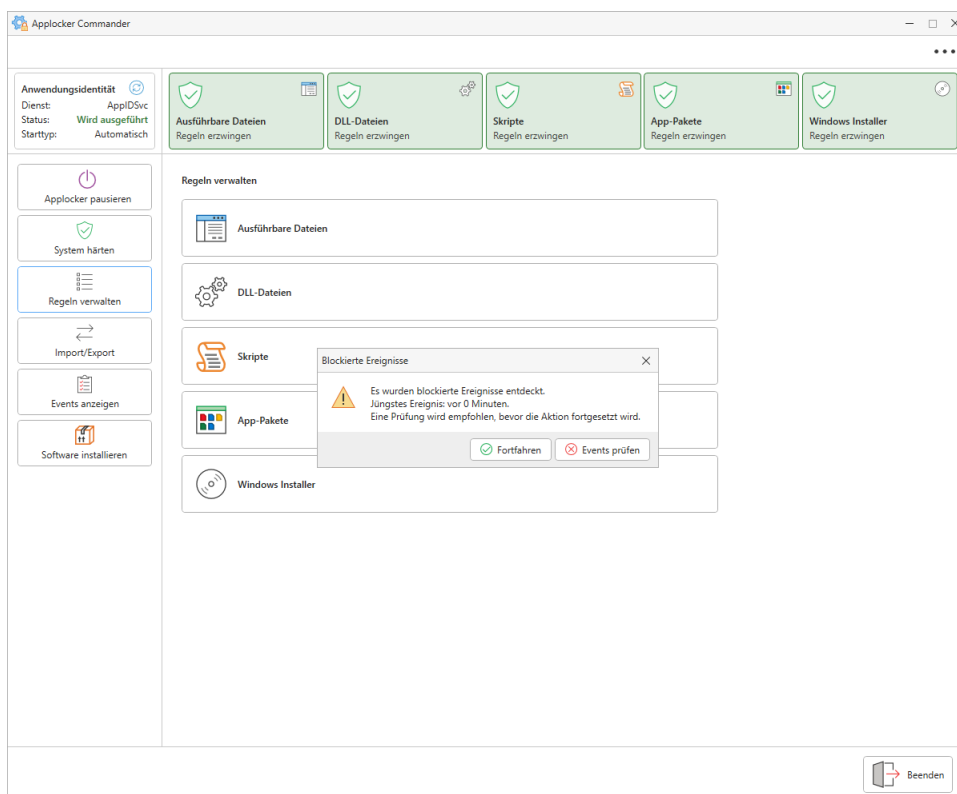
- Jedes Modul kann per Checkbox von der Pause ausgeschlossen werden
- Pro Modul wahlweise Regeln erzwingen oder Nur Überwachung –'Dauerhaft' umschaltbar

2.3.3 Regel dauerhaft deaktivieren



- Bei Dauer 'Dauerhaft' lässt sich ein Modul zusätzlich vollständig deaktivieren (Checkbox entfernen)
- Das Modul zeigt dann 'Deaktiviert' im oberen Status-Grid
- Warnhinweis: Die deaktivierte Regel wird spätestens bis zum nächsten Windows-Neustart automatisch durch AppLocker erzwungen (Countdown oben rechts)

2.3.4 Hinweis vor dem Pausieren



- Erscheint, wenn beim Start des Pausierens bereits blockierte Ereignisse vorliegen
- Fortfahren pausiert trotzdem, Events prüfen öffnet zuerst die Ereignisübersicht

2.4 Regeln verwalten

2.4.1 Regelübersicht

[Zurück](#) **Ausführbare Dateien** [XML anzeigen](#) ☐ Nur effektive Regeln anzeigen

[Hinzufügen](#) [Bearbeiten](#) [Löschen](#)

Name	Aktion	Regeltyp
▼ Sensor Rule (1)		
▲ System Rule (3)		
(System Rule) Allow %PROGRAMDATA%\Microsoft*	✓ Zulassen	Pfad
(System Rule) Allow %WINDIR%	✓ Zulassen	Pfad
(System Rule) Allow %PROGRAMFILES%	✓ Zulassen	Pfad

Vorschau
Name: (System Rule) Allow %WINDIR%
Aktion: Zulassen
Regeltyp: Pfad
Benutzer oder Gruppe: Jeder
Beschreibung: All files located in the Windows folder
FilePathCondition: Path=%WINDIR%*
Ausnahmen: Pfad: (18) Herausgeber: (0) Hash: (0)

- Regeln sind nach Herkunft gruppiert: Sensor Rule, System Rule, Data Rule, Event-based Rule, User Rule, Custom Rule
- Hinzufügen, Bearbeiten und Löschen über die Schaltflächen oben
- Nur effektive Regeln anzeigen: Blendet überschriebene oder inaktive Regeln aus und zeigt zusätzlich Regeln aus Gruppenrichtlinien an
- Vorschau unten zeigt alle Details der markierten Regel (Aktion, Regeltyp, Benutzer, Anzahl der Ausnahmen)

2.4.2 Regeln löschen

[Zurück](#) **Ausführbare Dateien** [XML anzeigen](#) ☐ Nur effektive Regeln anzeigen

[Hinzufügen](#) [Bearbeiten](#) [Löschen](#)

Name	Aktion	Regeltyp
▲ Data Rule (9)		
▼ Package Cache (9)		
(Data Rule) (Package Cache) Allow UninstallUI.exe	✓ Zulassen	Dateihash
(Data Rule) (Package Cache) Allow WINDSKSETUP.EXE	✓ Zulassen	Herausgeber
(Data Rule) (Package Cache) Allow WINDSKSETUP.EXE	✓ Zulassen	Herausgeber
(Data Rule) (Package Cache) Allow SMSZIP INSTALLER.EXE	✓ Zulassen	Herausgeber
(Data Rule) (Package Cache) Allow APPLOCKER COMMANDER INSTALLER.EXE	✓ Zulassen	Herausgeber
(Data Rule) (Package Cache) Allow WINDSKSETUP.EXE	✓ Zulassen	Herausgeber
(Data Rule) (Package Cache) Allow VC_REDIST.X86.EXE	✓ Zulassen	Herausgeber
(Data Rule) (Package Cache) Allow WIX314.EXE	✓ Zulassen	Herausgeber
(Data Rule) (Package Cache) Allow VC_REDIST.X64.EXE	✓ Zulassen	Herausgeber
▼ Event-based Rule (14)		
▼ Sensor Rule (1)		
▼ System Rule (3)		
▼ User Rule (24)		

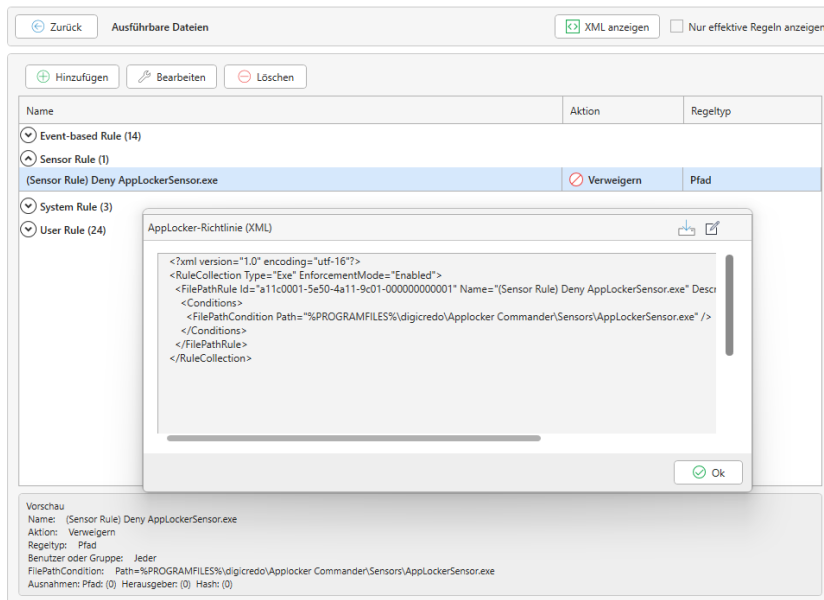
Vorschau
(Data Rule) (Package Cache) Allow UninstallUI.exe
(Data Rule) (Package Cache) Allow WINDSKSETUP.EXE
(Data Rule) (Package Cache) Allow WINDSKSETUP.EXE
(Data Rule) (Package Cache) Allow SMSZIP INSTALLER.EXE
(Data Rule) (Package Cache) Allow APPLOCKER COMMANDER INSTALLER.EXE
(Data Rule) (Package Cache) Allow WINDSKSETUP.EXE
(Data Rule) (Package Cache) Allow VC_REDIST.X86.EXE
(Data Rule) (Package Cache) Allow WIX314.EXE

- Mehrfachauswahl möglich, um mehrere Regeln gleichzeitig zu löschen

2.4.3 Regeln gruppieren

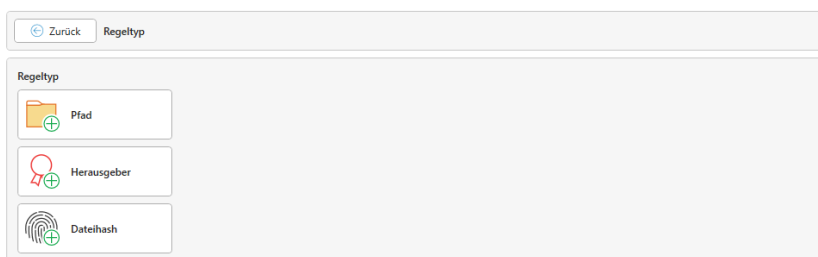
- Klammern im Regelnamen gruppieren die Regeln in der Übersicht – Regeln mit gleicher Klammer werden zusammen angezeigt.
- Name: (User Rule) (Desktop) Allow INSTALLER.EXE

2.4.4 XML anzeigen



- Zeigt die native AppLocker-Regel als XML an, inkl. Download- und Zwischenablage-Symbol

2.4.5 Regel erstellen



- Auswahl des Regeltyps: Pfad, Herausgeber oder Dateihash

2.4.5.1 Pfad

← Zurück Ausführbare Dateien\Pfad ✓ Speichern

Name

Beschreibung

Aktion

✓ Zulassen

Regeltyp: Pfad

Benutzer oder Gruppe:

Jeder

 Auswählen...

 Manuell eingeben...

Eigenschaften

Pfad Ausnahme

Pfad:

 Dateien durchsuchen...

 Ordner durchsuchen...

- Name, Beschreibung, Aktion (Zulassen/Verweigern), Benutzer oder Gruppe frei definierbar
- Pfad direkt eingeben oder über Dateien/Ordner durchsuchen auswählen
- Reiter Ausnahme erlaubt das Ausschliessen einzelner Unterpfade von der Regel

2.4.5.2 Herausgeber

Herausgeberausnahme

Referenzdatei: C:\Windows\regedit.exe Durchsuchen...

— Beliebiger Herausgeber

— Herausgeber:

— Produktname:

— Dateiname:

— Dateiversion:

O=MICROSOFT CORPORATION, L=REDMOND, S=WASHING

MICROSOFT® WINDOWS® OPERATING SYSTEM

REGEDIT.EXE

10.0.26100.9278 ↑ und höher

☐ Benutzerdefinierte Werte verwenden

Regelbereich:
Betrifft signierte Dateien
des Herausgebers O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US,
Produkts MICROSOFT® WINDOWS® OPERATING SYSTEM,
Dateinamens REGEDIT.EXE
und der angegebenen Version.

Ok Abbrechen

Zurück Ausführbare Dateien/Herausgeber Speichern

Name
REGEDIT.EXE

Beschreibung
C:\Windows\regedit.exe

Aktion
✓ Zulassen

Regeltyp: Herausgeber

Benutzer oder Gruppe:
Jeder Auswählen... Manuell eingeben...

Eigenschaften

Herausgeber

Ausnahme

Die unten aufgeführten Werte anpassen, um den Regelbereich zu verändern.

Hinzufügen

Herausgeber:
O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US

Produktname:
MICROSOFT® WINDOWS® OPERATING SYSTEM

Dateiname:
REGEDIT.EXE

Dateiversion:
10.0.26100.9278 ↑ und höher

[Weitere Informationen zu Herausgeberregeln](#)

- Werte (Herausgeber, Produktname, Dateiname, Version) können aus einer Referenzdatei automatisch übernommen werden
- Per Schieberegler lässt sich festlegen, wie granular die Regel greift (z. B. nur Herausgeber oder bis zur exakten Version)
- Benutzerdefinierte Werte verwenden erlaubt manuelle Anpassung einzelner Felder

2.4.5.3 Dateihash

Zurück Speichern

Name: PrintBrm.exe

Beschreibung: C:\Windows\System32\spool\tools

Aktion: ☒ Zulassen

Regeltyp: Dateihash

Benutzer oder Gruppe: Jeder Auswählen... Manuell eingeben...

Eigenschaften

Dateihash Ausnahme

Dateiname	Größe
PrintBrm.exe	76 KB
PrintBrmEngine.exe	300 KB

☒ Unterordner durchsuchen

- Eine oder mehrere Dateien per Hash erfassen (unabhängig von Pfad oder Signatur)
- Unterordner durchsuchen bezieht alle Dateien in Unterverzeichnissen mit ein

2.4.5.4 App-Pakete

Zurück Speichern

Name:

Beschreibung:

Aktion: ☒ Verweigern

Regeltyp: Herausgeber

Benutzer oder Gruppe: Jeder Auswählen... Manuell eingeben...

Eigenschaften

Herausgeber Ausnahme

Die unten aufgeführten Werte anpassen, um den

Herausgeber:

Paketname:

Paketversion: 0.0.0.0 und höher

App-Paket hinzufügen

☒ Ein installiertes App-Paket als Referenz verwenden

1527c705-839a-4832-9118-54d48d6a0c89 Auswählen...

☐ Installer für App-Pakete als Referenz verwenden

Durchsuchen...

Beliebiger Herausgeber: CN=Microsoft Windows, O=Microsoft Corporation, L=Redm...

Herausgeber: 1527c705-839a-4832-9118-54d48d6a0c89

Paketname: 10.0.19640.1000 und höher

Paketversion: und höher

☐ Benutzerdefinierte Werte verwenden

Regelbereich:
Betrifft signierte App-Pakete
des Herausgebers CN=Microsoft Windows, O=Microsoft Corporation, L=Redm...
Paketnamen 1527c705-839a-4832-9118-54d48d6a0c89
und der angegebenen Version.

- Dient vorwiegend dazu, eine einzelne App gezielt auszuschliessen (Aktion: Verweigern)
- Referenz entweder über ein installiertes App-Paket oder über dessen Installer

2.4.6 Regel bearbeiten

Zurück Ausführbare Dateien\Pfad Speichern

Name
(System Rule) Allow %WINDIR%

Beschreibung
All files located in the Windows folder

Aktion
Zulassen

Regeltyp: Pfad

Benutzer oder Gruppe:
Jeder Auswählen... Manuell eingeben...

Eigenschaften

Pfad Ausnahme

Pfad:
%WINDIR%*
Dateien durchsuchen... Ordner durchsuchen...

- Bestehende Regeln lassen sich vollständig nachbearbeiten (Name, Aktion, Pfad usw.)

Eigenschaften

Pfad Ausnahme

Ausnahme hinzufügen:
Pfad

Ausnahme:

Ausnahme	Typ
%WINDIR%\PLA\Reports*	Pfad
%WINDIR%\PLA\Rules*	Pfad
%WINDIR%\PLA\Templates*	Pfad
%WINDIR%\Registration\CRMLog*	Pfad
%WINDIR%\System32\Com\dmp*	Pfad
%WINDIR%\System32\FxsTmp*	Pfad
%WINDIR%\System32\LogFiles\WMI*	Pfad
%WINDIR%\System32\spool\drivers\color*	Pfad

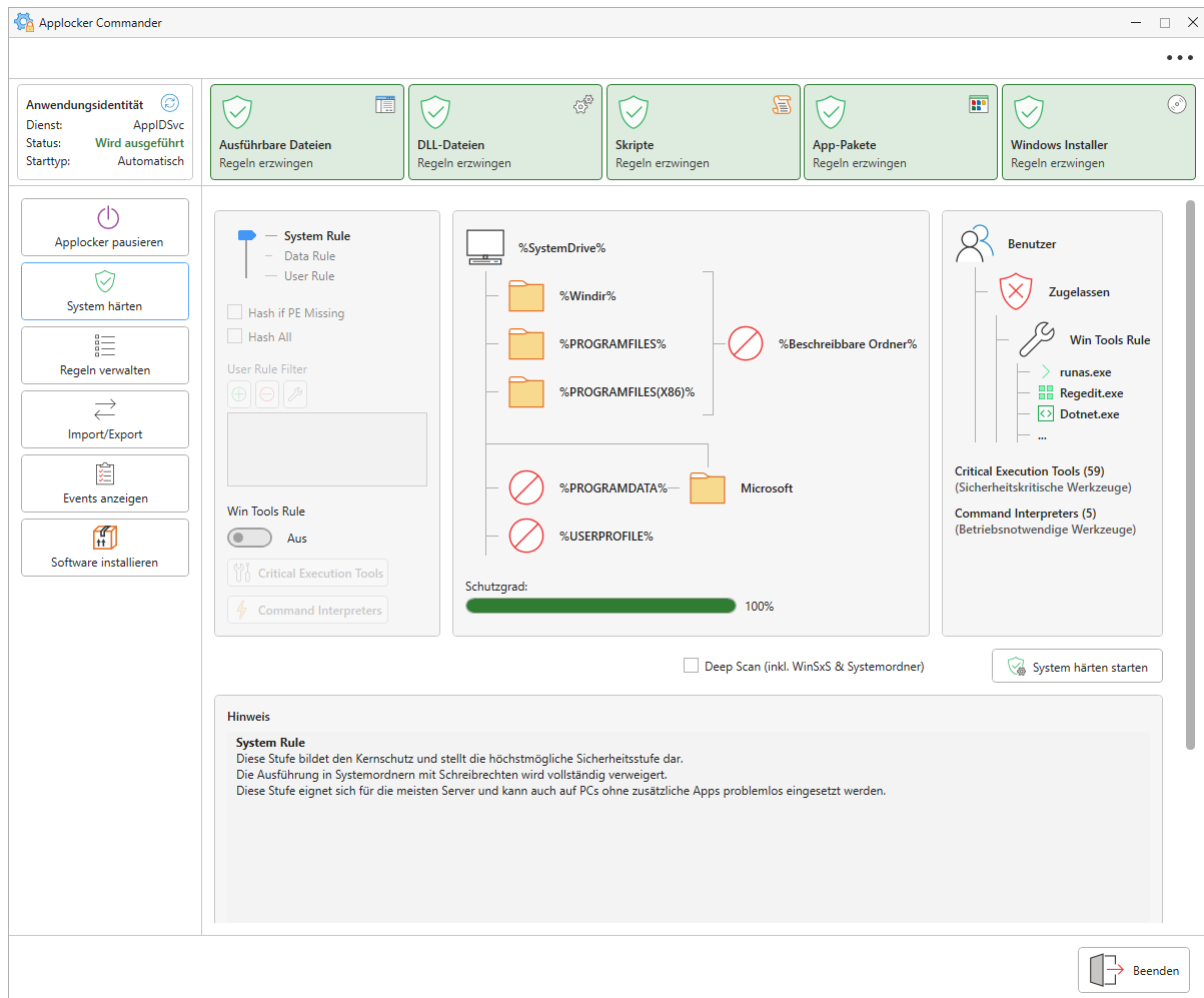
Hinzufügen
Bearbeiten
Löschen

Weitere Informationen zu Regelausnahmen

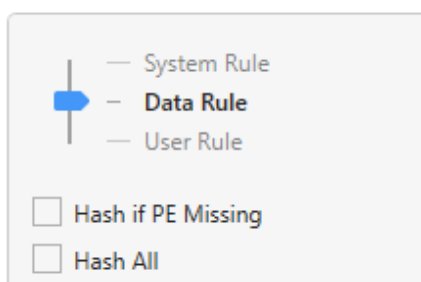
- Im Reiter Ausnahme können mehrere Ausnahmen verwaltet werden – Standardregeln bringen oft bereits vordefinierte Systemausnahmen mit

2.5 System härten

2.5.1 Stufen: System Rule, Data Rule, User Rule

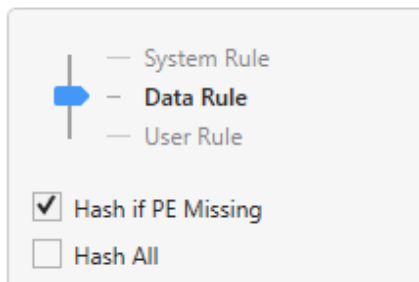


- System Rule: Kernschutz. Ausführung in Systemordnern mit Schreibrechten wird vollständig verweigert. Für die meisten Server geeignet, auch ohne Zusatz-Apps.

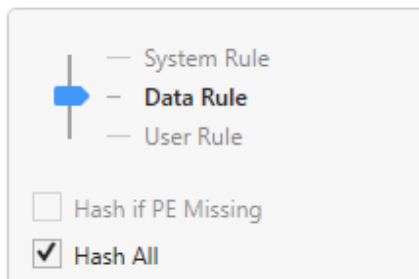


- Data Rule: schützt zusätzlich %PROGRAMDATA%, wo Windows- und Drittanbieterdaten liegen. Nur registrierte Signaturen/Hashes dürfen dort ausgeführt werden.
- User Rule: schützt zusätzlich den gesamten Benutzerbereich (%USERPROFILE%), in dem Anwendungen, Installer und Temp-Dateien liegen
- Der Schutzgrad-Balken zeigt die erreichte Absicherung in Prozent

2.5.2 Data-Rule-Feineinstellungen

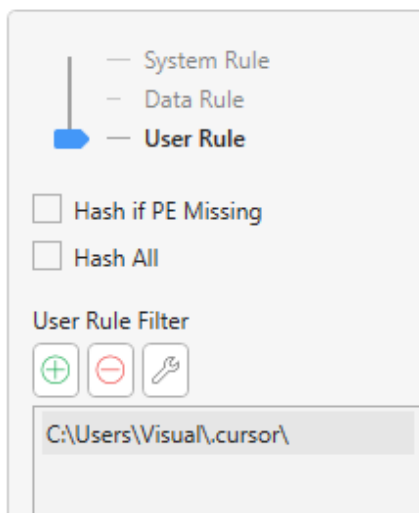


- Hash if PE Missing: signierte Dateien ohne PE-Produkt-/Binary-Metadaten werden per Hash statt nur nach Herausgeber erlaubt



- Hash All: höchstmögliche Integritätsprüfung per Hash-Regeln für alle Dateien in diesem Bereich
- Erfordert laufende Administration – nach jedem Update müssen betroffene Prozesse manuell neu freigegeben werden
- Eignet sich vor allem für Hochsicherheitsumgebungen mit fest definiertem Software-Stand

2.5.3 User Rule



- User Rule: schützt zusätzlich den gesamten Benutzerbereich (%USERPROFILE%), in dem Anwendungen, Installer und Temp-Dateien liegen. Nur registrierte Signaturen/Hashes dürfen dort ausgeführt werden.
- Eigene Pfade lassen sich über User Rule Filter dauerhaft von dieser Stufe ausschliessen

2.5.4 Win Tools Rule

System Rule
 - Data Rule
 - User Rule

☐ Hash if PE Missing
☐ Hash All

User Rule Filter

Win Tools Rule
☒ Ein

☒ Critical Execution Tools
☒ Command Interpreters

Benutzer

Blockiert

Win Tools Rule

runas.exe
 Regedit.exe
 Dotnet.exe
 ...

Critical Execution Tools (59)
 (Sicherheitskritische Werkzeuge)

Command Interpreters (5)
 (Betriebsnotwendige Werkzeuge)

Schutzgrad: 100%

☐ Deep Scan (inkl. WinSxS & Systemordner)

☒ System härten starten

Hinweis

System Rule
 Diese Stufe bildet den Kernschutz und stellt die höchstmögliche Sicherheitsstufe dar. Die Ausführung in Systemordnern mit Schreibrechten wird vollständig verweigert. Diese Stufe eignet sich für die meisten Server und kann auch auf PCs ohne zusätzliche Apps problemlos eingesetzt werden.

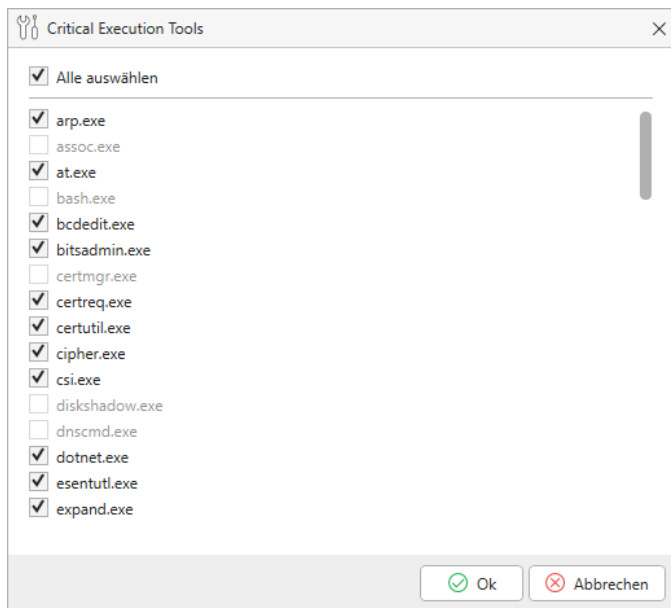
Win Tools Rule
 Diese Stufe dient als zweite Verteidigungslinie, falls die Pfad-Regel durchbrochen wird, und bietet durch spezifische Programm-Regeln zusätzlichen Schutz. Sie ist für Admins geeignet, die AppLocker-Events aktiv überwachen, um unbeabsichtigte Blockaden zu vermeiden.

Critical Execution Tools
 Hier kommen gezielte Programm-Regeln zum Einsatz, die zusätzlichen Schutz bieten, jedoch reguläre Windows-Prozesse beeinträchtigen können. Der Fokus liegt auf High-Risk-Werkzeugen, die typischerweise für unerwünschte Ausführung genutzt werden.

Command Interpreters
 In dieser Stufe greifen spezifische Regeln für Befehlszeilen- und Skript-Umgebungen, die ggf. an Ihre Umgebung angepasst werden müssen. Einige Aufgaben erfordern für einen reibungslosen Betrieb die Ausführung im SYSTEM-Kontext, welcher sich ausschließlich auf diese Shell- und Skript-Hosts bezieht.

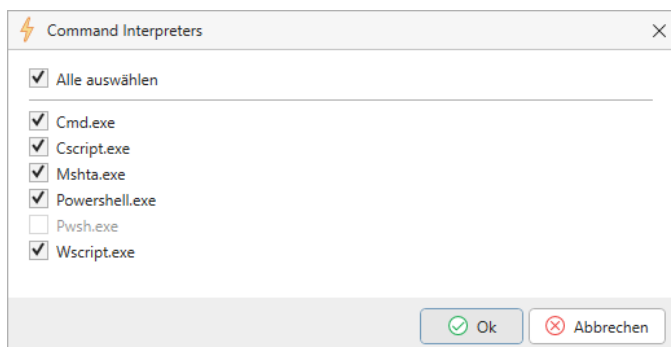
- Schliesst den häufigsten Umgehungsweg: den Missbrauch von Skript-Interpretern und Systemwerkzeugen, etwa wenn ein Office-Makro versucht, PowerShell oder Cmd zu starten, um eine dateilose Payload im Speicher nachzuladen
- Gilt für die Gruppe Jeder und damit auch für Prozesse im SYSTEM-Kontext (z. B. Wartungsaufgaben, Backup- oder Update-Software) – deshalb standardmässig deaktiviert und für Admins gedacht, die AppLocker-Events aktiv überwachen, um unbeabsichtigte Blockaden zu erkennen und zu vermeiden

2.5.4.1 Critical Execution Tools



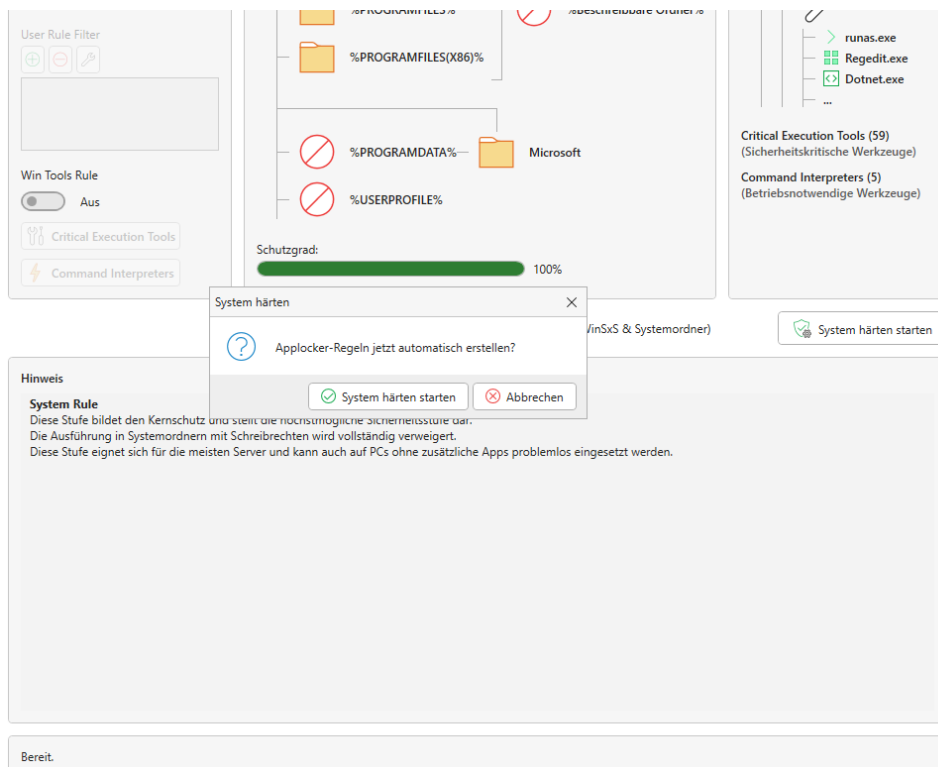
- Critical Execution Tools: gezielte Regeln für sicherheitskritische Windows-Werkzeuge (z. B. bcdedit.exe, certutil.exe), die für unerwünschte Ausführung missbraucht werden können
- Ausgegraute Einträge (z. B. assoc.exe, bash.exe) sind auf dem jeweiligen System nicht vorhanden

2.5.4.2 Command Interpreters



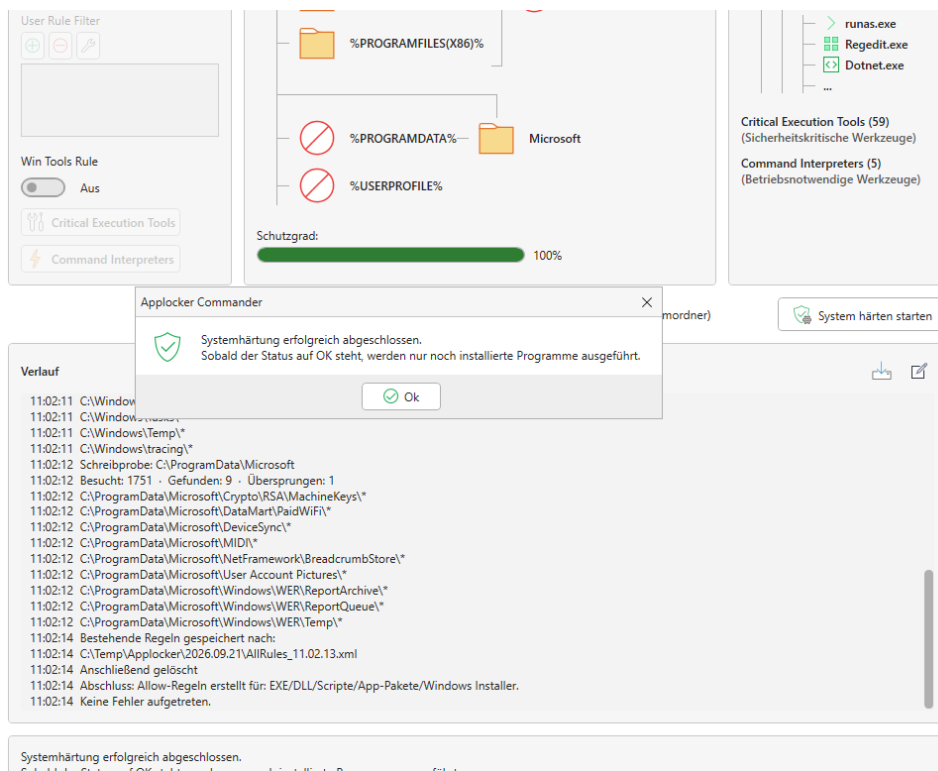
- Command Interpreters: Regeln für Befehlszeilen- und Skript-Umgebungen (Cmd, Cscript, Mshta, Powershell, Wscript)
- Für einen reibungslosen Betrieb greifen einige dieser Regeln im SYSTEM-Kontext, beschränkt auf diese Shell- und Script-Hosts

2.5.5 System härten starten



- Optional Deep Scan (inkl. WinSxS & Systemordner) für eine besonders gründliche Analyse aktivieren
- System härten starten fragt vor der Ausführung noch einmal explizit nach Bestätigung
- Jeder eingeschlossene Ordner wird auf Schreibrechte geprüft: In Ordnern, in die Benutzer schreiben können, liesse sich eine schädliche Datei einfach ablegen und ausführen – solche Verzeichnisse werden deshalb von der Ausführung ausgeschlossen
- Dateien, die dort trotzdem ausgeführt werden müssen, lassen sich gezielt per Herausgeber (Zertifikat) oder Hash freigeben

2.5.6 System härten abgeschlossen



- Der Verlauf protokolliert jeden Schritt: durchsuchte Pfade, gespeicherte Regel-Sicherung, Anzahl gefundener/übersprungener Objekte
- Abschlussmeldung bestätigt: Sobald der Status auf OK steht, werden nur noch installierte Programme ausgeführt

2.6 Events anzeigen

AppLocker Commander

Anwendungsidentität
Dienst: AppIDSvc
Status: Wird ausgeführt
Starttyp: Automatisch

Ausführbare Dateien
Regeln erzwingen

DLL-Dateien
Regeln erzwingen

Skripte
Regeln erzwingen

App-Pakete
Regeln erzwingen

Windows Installer
Regeln erzwingen

AppLocker pausieren

System härten

Regeln verwalten

Import/Export

Events anzeigen

Software installieren

Filter: Blockiert
Zeitraum: Letzte 5 Minuten
Suche:
Aktualisierung angehalten
Aktualisieren

Zeit	Ereignis-ID	Kanal	Nachricht (3)	Aktion
21.09.2026 16:49	8004	Micr	Die Ausführung von %PROGRAMFILES%\DIGICREDO\APPOCKER COMMANDER\SENSORS\APPOCKERSE...	
21.09.2026 16:49	8007	Micr	Die Ausführung von %PROGRAMFILES%\DIGICREDO\APPOCKER COMMANDER\SENSORS\APPOCKERSE...	
21.09.2026 16:49	8004	Micr	Die Ausführung von %PROGRAMFILES%\DIGICREDO\APPOCKER COMMANDER\SENSORS\APPOCKERSE...	

Zeit: 21.09.2026 16:49
Ereignis-ID: 8004
Kanal: Microsoft-Windows-AppLocker/EXE and DLL
Nachricht: Die Ausführung von %PROGRAMFILES%\DIGICREDO\APPOCKER COMMANDER\SENSORS\APPOCKERSENSOR.EXE wurde verhindert.
Pfad: C:\Program Files\digicredo\Aplocker Commander\Sensors\ApLockerSensor.exe

- Filter: Alle Ereignisse, Blockiert, Überwacht oder Zugelassen
- Durch klicken auf das Event werden alle Details angezeigt

2.6.1 Zeitraum und Suche

Filter: Blockiert
Zeitraum: Letzte 5 Minuten
Suche:
Aktualisierung angehalten
Aktualisieren

AppLocker-Events

Zeit	Ereignis-ID	Kanal	Nachricht	Aktion
21.09.2026 11:39	8004	Micr	PROGRAMFILES%\DIGICREDO\APPOCKER COMMANDER\SENSORS\APPOCKERSE...	
21.09.2026 11:39	8007	Micr	PROGRAMFILES%\DIGICREDO\APPOCKER COMMANDER\SENSORS\APPOCKERSE...	
21.09.2026 11:39	8004	Micr	PROGRAMFILES%\DIGICREDO\APPOCKER COMMANDER\SENSORS\APPOCKERSE...	
21.09.2026 11:38	8007	Micr	Die Ausführung von %OSDRIVE%\USERS\VISUAL\DESKTOP\APPOCKER.CMD wurde verhindert.	Erlauben

- Zeitraum wählbar von Letzte Minute bis Letzte 30 Tage
- Suche durchsucht die Ereignisliste als Volltext und zeigt die Events mit Treffer an
- Aktualisierung läuft automatisch und wird angehalten wenn ein Event ausgewählt wird

2.6.2 AppLocker-Selbsttest ausblenden



- AppLocker erstellt für Selbsttests temporäre PS1-Dateien, die ausgeblendet werden können.

2.6.3 Duplikate zusammenfassen



- Bei mehrfachem Aufkommen desselben Ereignisses zeigt der Filter nur das aktuellste an.

2.6.4 Ereignis in die Zwischenablage kopieren



- Das Ereignis wird in die Zwischenablage kopiert.

2.6.5 Regel aus Event erstellen

The screenshot shows the 'AppLocker-Events' window. At the top, there is a filter bar with 'Filter' set to 'Blockiert', 'Zeitraum' set to 'Letzte 5 Minuten', and a search field. Below the filter bar is a table of events. The table has columns: 'Zeit', 'Ereignis-ID', 'Kanal', 'Nachricht (4)', and 'Aktion'. The events are listed as follows:

Zeit	Ereignis-ID	Kanal	Nachricht (4)	Aktion
21.09.2026 11:39	8004	Micn	Die Ausführung von %PROGRAMFILES%\DIGICREDO\APPOCKER COMMANDER\SENSORS\APPOCKERSE...	
21.09.2026 11:39	8007	Micn	Die Ausführung von %PROGRAMFILES%\DIGICREDO\APPOCKER COMMANDER\SENSORS\APPOCKERSE...	
21.09.2026 11:39	8004	Micn	Die Ausführung von %PROGRAMFILES%\DIGICREDO\APPOCKER COMMANDER\SENSORS\APPOCKERSE...	
21.09.2026 11:38	8007	Micn	Die Ausführung von %OSDRIVE%\USERS\VISUAL\DESKTOP\APPOCKER.CMD wurde verhindert.	Erlauben

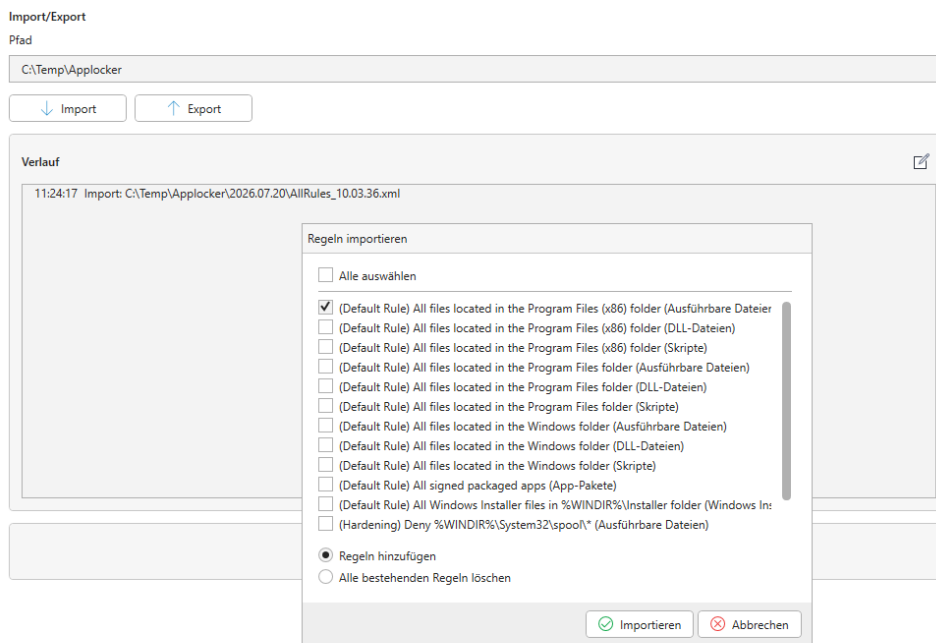
Below the table, there is a detailed view of the selected event (ID: 8007). It shows the following information:

- Zeit: 21.09.2026 11:38
- Ereignis-ID: 8007
- Kanal: Microsoft-Windows-AppLocker/MSI and Script
- Nachricht: Die Ausführung von %OSDRIVE%\USERS\VISUAL\DESKTOP\APPOCKER.CMD wurde verhindert.
- Pfad: C:\Users\Visual\Desktop\Applocker.cmd

A dialog box titled 'Erlauben' is open, showing the path 'C:\Users\Visual\Desktop\Applocker.cmd'. It has three radio buttons: 'Nur diese Datei', 'Alles in diesem Verzeichnis' (selected), and 'Herausgeber'. There is also a checkbox for 'Unterordner durchsuchen' which is checked. At the bottom of the dialog, there are two buttons: 'Erlauben' and 'Abbrechen'.

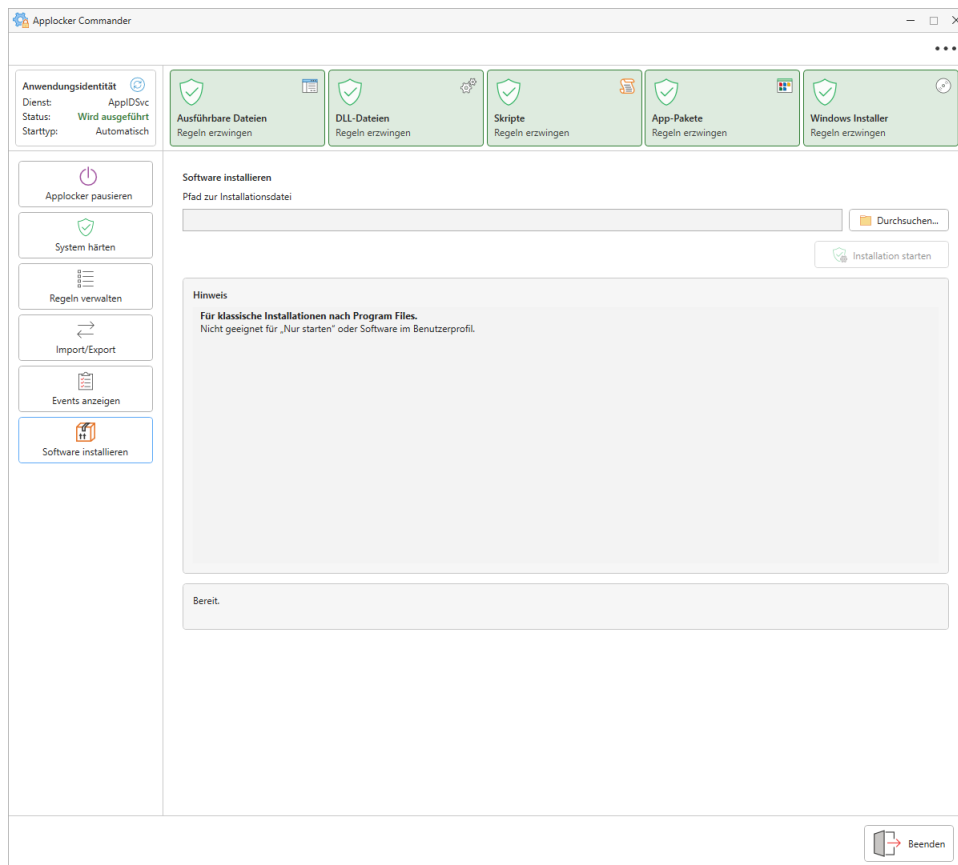
- Klick auf Erlauben bei einem blockierten Ereignis öffnet den Regel-Assistenten
- Geltungsbereich wählbar: Nur diese Datei, Alles in diesem Verzeichnis (optional inkl. Unterordner), Herausgeber oder Dateihash
- Erstellt automatisch eine passende AppLocker-Regel auf Basis des Ereignisses

2.7 Import/Export



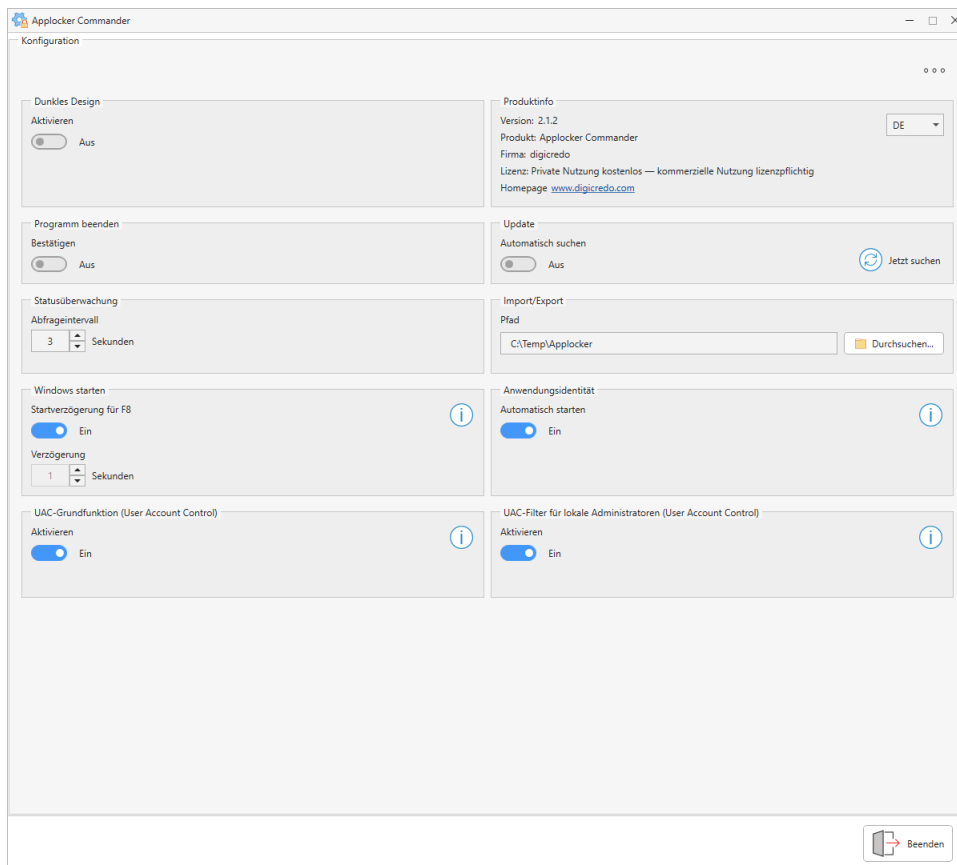
- Pfad für Import/Export frei wählbar
- Export sichert alle aktuellen Regeln als XML-Datei
- Import erlaubt die Auswahl einzelner Regeln aus einer XML-Datei per Checkbox
- Regeln hinzufügen ergänzt die Auswahl, Alle bestehenden Regeln löschen ersetzt den kompletten Regelbestand
- Verlauf protokolliert alle Import-/Export-Vorgänge mit Zeitstempel und Pfad

2.8 Software installieren



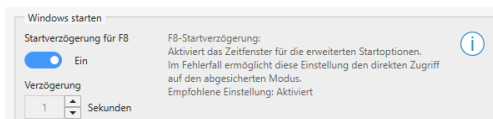
- Pfad zur Installationsdatei angeben und Installation starten
- Gedacht für klassische Installationen nach Program Files
- Nicht geeignet für portable Anwendungen ('Nur starten') oder Software, die ins Benutzerprofil installiert wird

2.9 Einstellungen



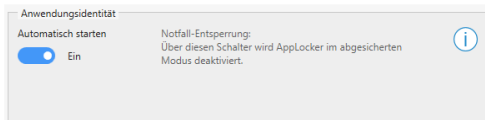
- Dunkles Design umschaltbar
- Produktinfo mit Version, Lizenzstatus, Sprache (DE) und Homepage-Link
- Programm beenden: Bestätigung beim Schliessen ein-/ausschaltbar
- Update: automatische Suche oder manuell über Jetzt suchen
- Statusüberwachung: Abfrageintervall in Sekunden
- Import/Export: Standardpfad für Regel-Dateien

2.9.1 Windows starten



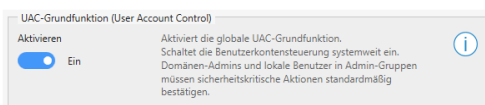
Startverzögerung für F8: Aktiviert das Zeitfenster für die erweiterten Startoptionen. Im Fehlerfall ermöglicht diese Einstellung den direkten Zugriff auf den abgesicherten Modus. Empfohlene Einstellung: Aktiviert.

2.9.2 Anwendungsidentität



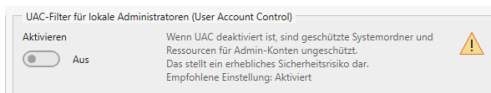
Automatisch starten (Notfall-Entsperrung): Blockiert eine fehlerhaft erstellte Regel den Systemstart, lässt sich AppLocker über diesen Schalter im abgesicherten Modus deaktivieren – danach startet das System wieder normal.

2.9.3 UAC-Grundfunktion



Aktiviert die Benutzerkontensteuerung systemweit. Domänen-Admins und lokale Benutzer in Admin-Gruppen müssen sicherheitskritische Aktionen standardmässig bestätigen.

2.9.4 UAC-Filter für lokale Administratoren



Schützt Systemordner und Ressourcen auch für Admin-Konten. Bei Deaktivierung erscheint ein Warnhinweis, da dies ein Sicherheitsrisiko darstellt. Empfohlene Einstellung: Aktiviert.

3 Lizenz

- Die private Nutzung von AppLocker Commander ist kostenlos.
- Für die kommerzielle Nutzung ist eine Lizenz erforderlich.

Lizenzinformationen: [AppLocker Commander License – digicredo](#)