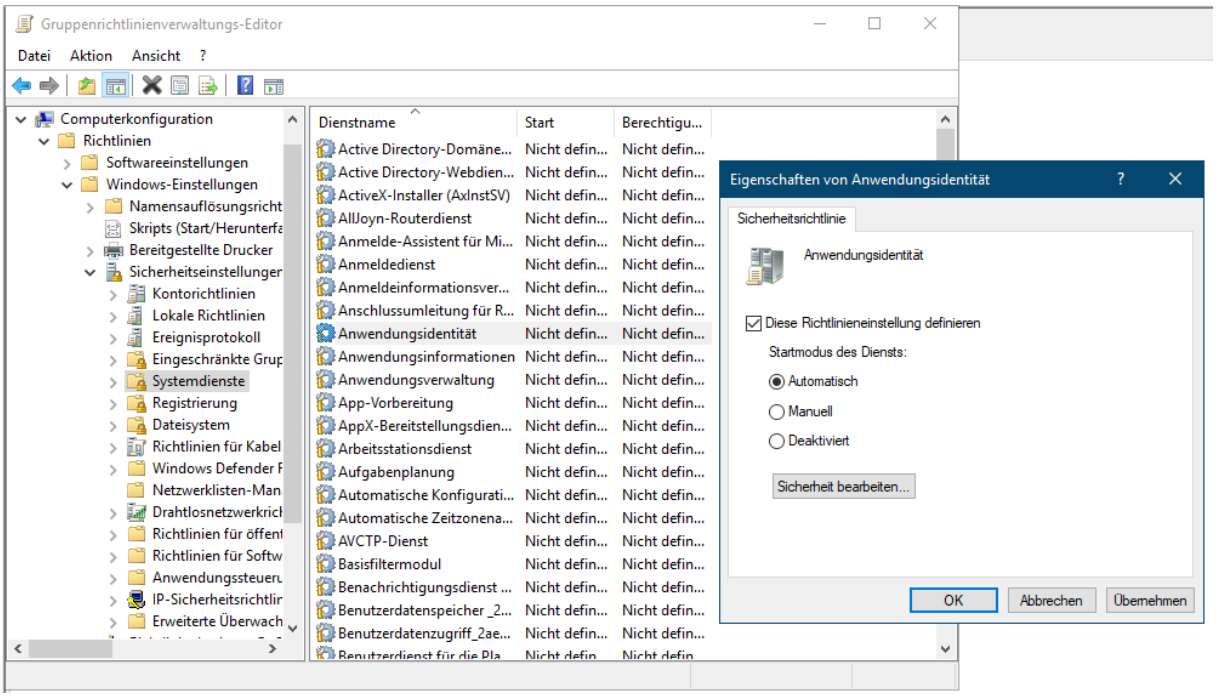
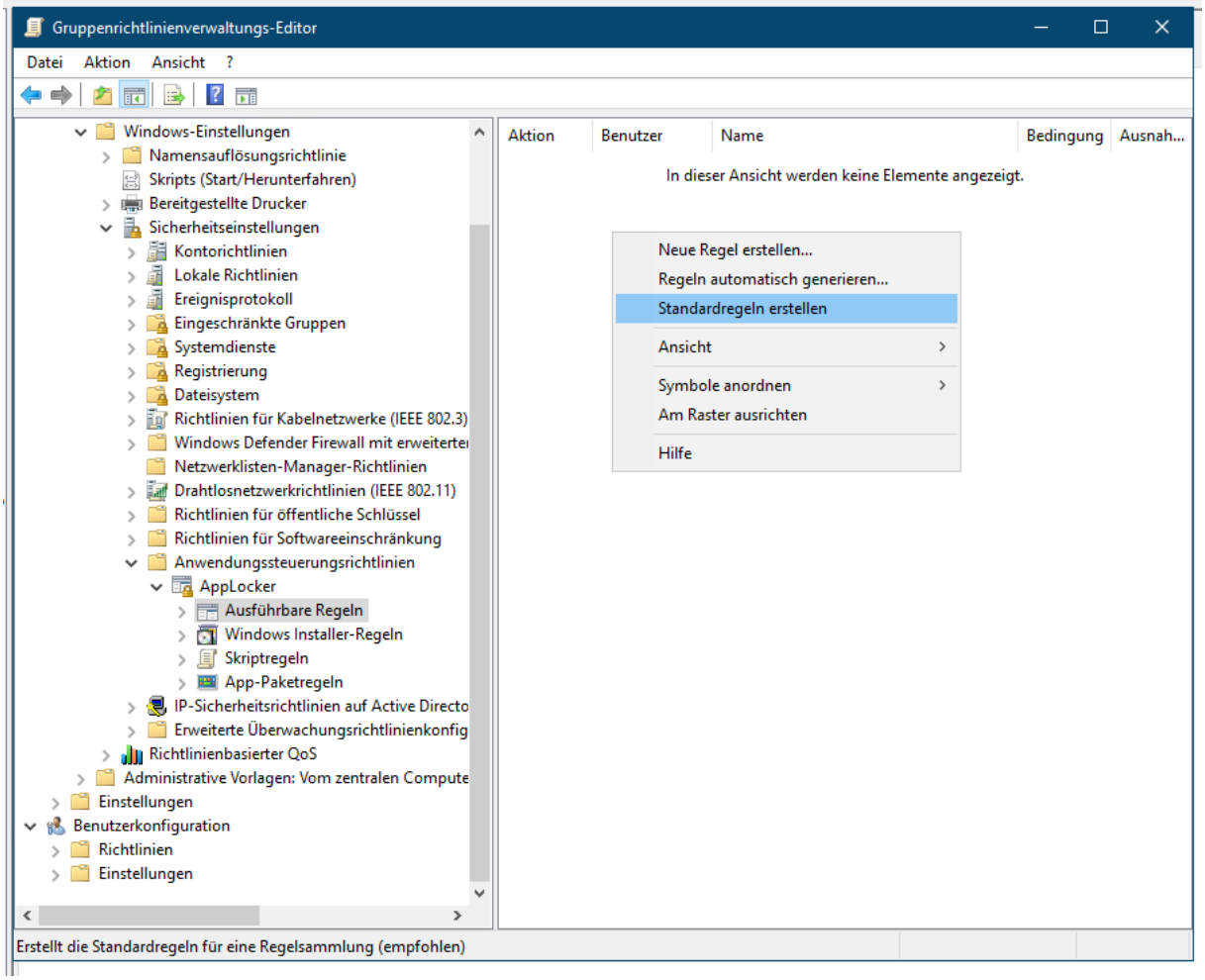
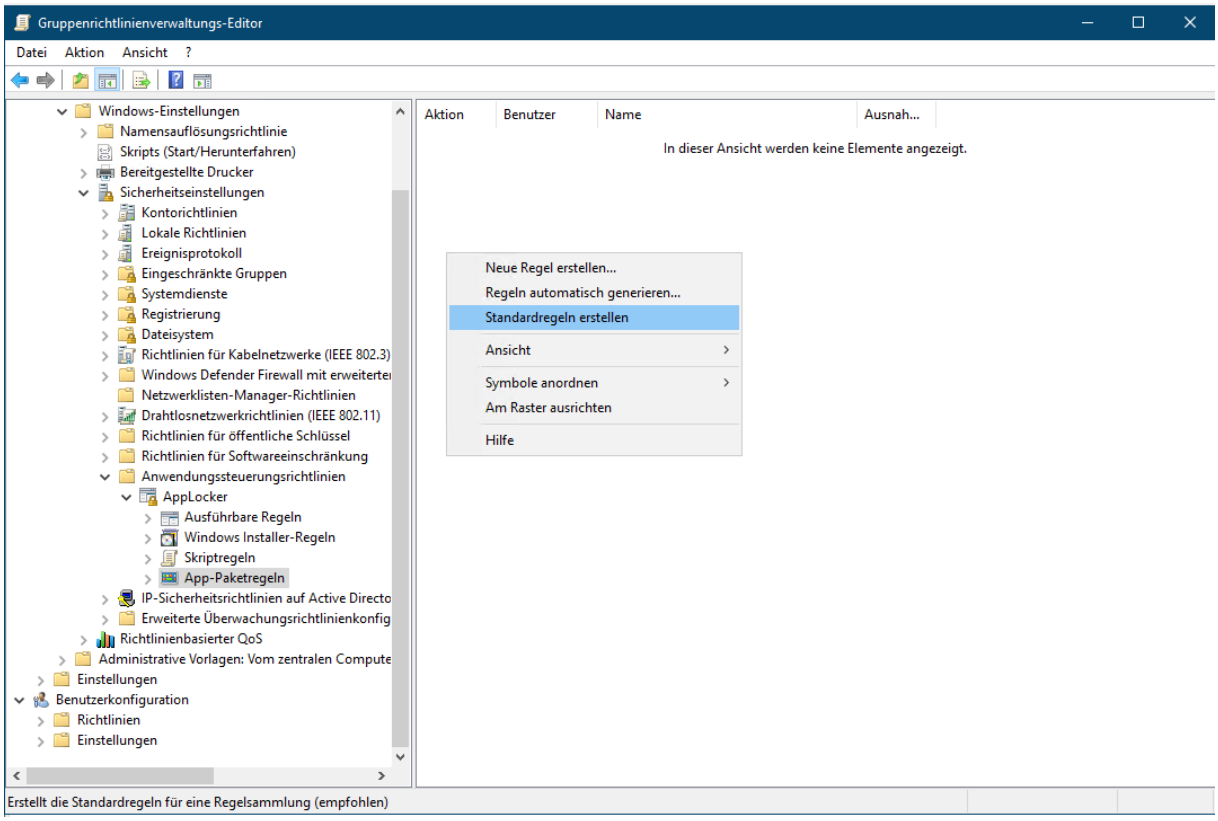
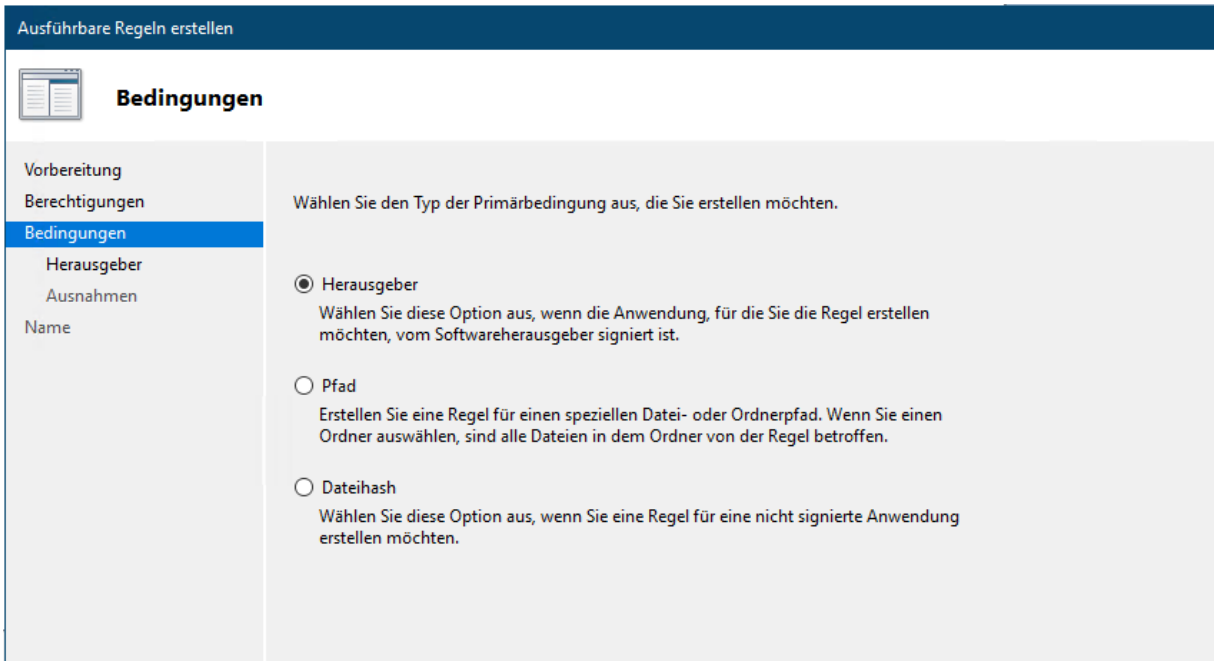

Gruppenrichtlinienverwaltungs-Editor
Datei Aktion Ansicht ?
Computerkonfiguration
Richtlinien
Softwareeinstellungen
Windows-Einstellungen
Namensauflösungsricht
Skripts (Start/Herunterfa
Bereitgestellte Drucker
Sicherheitseinstellunger
Kontorichtlinien
Lokale Richtlinien
Ereignisprotokoll
Eingeschränkte Grup
Systemdienste
Registrierung
Dateisystem
Richtlinien für Kabel
Windows Defender F
Netzwerklisten-Man
Drahtlosnetzwerkricl
Richtlinien für öffent
Richtlinien für Softw
Anwendungssteueru
IP-Sicherheitsrichtlir
Erweiterte Überwach
Dienstname
Start
Berechtigu...
Active Directory-Domäne...
Active Directory-Webdien...
ActiveX-Installer (AxInstSV)
AllJoyn-Routerdienst
Anmelde-Assistent für Mi...
Anmeldedienst
Anmeldeinformationsver...
Anschlussumleitung für R...
Anwendungsidentität
Anwendungsinformationen
Anwendungsverwaltung
App-Vorbereitung
AppX-Bereitstellungsdien...
Arbeitsstationsdienst
Aufgabenplanung
Automatische Konfigurati...
Automatische Zeitzonena...
AVCTP-Dienst
Basisfiltermodul
Benachrichtigungsdienst ...
Benutzerdatenspeicher _2...
Benutzerdatenzugriff_2ae...
Nicht defin...
Eigenschaften von Anwendungsidentität
Sicherheitsrichtlinie
Anwendungsidentität
Diese Richtlinieneinstellung definieren
Startmodus des Diensts:
Automatisch
Manuell
Deaktiviert
Sicherheit bearbeiten...
OK
Abbrechen
Übernehmen


Gruppenrichtlinienverwaltungs-Editor
Datei Aktion Ansicht ?
Windows-Einstellungen
Namensauflösungsrichtlinie
Skripts (Start/Herunterfahren)
Bereitgestellte Drucker
Sicherheitseinstellungen
Kontorichtlinien
Lokale Richtlinien
Ereignisprotokoll
Eingeschränkte Gruppen
Systemdienste
Registrierung
Dateisystem
Richtlinien für Kabelnetzwerke (IEEE 802.3)
Windows Defender Firewall mit erweiterter
Netzwerklisten-Manager-Richtlinien
Drahtlosnetzwerkrichtlinien (IEEE 802.11)
Richtlinien für öffentliche Schlüssel
Richtlinien für Softwareeinschränkung
Anwendungssteuerungsrichtlinien
AppLocker
Ausführbare Regeln
Windows Installer-Regeln
Skriptregeln
App-Paketregeln
IP-Sicherheitsrichtlinien auf Active Directo
Erweiterte Überwachungsrichtlinienkonfig
Richtlinienbasierter QoS
Administrative Vorlagen: Vom zentralen Compute
Einstellungen
Benutzerkonfiguration
Richtlinien
Einstellungen
Aktion
Benutzer
Name
Bedingung
Ausnah...
In dieser Ansicht werden keine Elemente angezeigt.
Neue Regel erstellen...
Regeln automatisch generieren...
Standardregeln erstellen
Ansicht
Symbole anordnen
Am Raster ausrichten
Hilfe
Erstellt die Standardregeln für eine Regelsammlung (empfohlen)





1. **Gruppenrichtlinienobjekt (GPO) erstellen/auswählen:**
    - Öffnet die "Gruppenrichtlinienverwaltung" (gpmc.msc).
    - Erstellt ein neues GPO (z.B. "AppLocker Richtlinien") oder wählt ein bestehendes GPO aus, das ihr für AppLocker verwenden möchtet. Verknüpft dieses GPO mit der Organisationseinheit (OU), die die Zielcomputer enthält.
2. **GPO bearbeiten:**

- Rechtsklickt auf das ausgewählte GPO und wählt "Bearbeiten...". Der "Gruppenrichtlinienverwaltungs-Editor" öffnet sich.

Schritt 1: Anwendungsidentitätsdienst konfigurieren

Der Dienst "Anwendungsidentität" (Application Identity) ist entscheidend für AppLocker. Er muss auf den Client-Computern laufen.

1. Navigiert im Gruppenrichtlinienverwaltungs-Editor zu:
   Computerkonfiguration -> Richtlinien -> Windows-Einstellungen -> Sicherheitseinstellungen -> Systemdienste.
2. Sucht in der Liste der Dienste den Dienst "**Anwendungsidentität**" (oder "Application Identity").
3. Doppelklickt darauf, um die "Eigenschaften von Anwendungsidentität" zu öffnen.
4. Setzt einen Haken bei "**Diese Richtlinieneinstellung definieren**".
5. Wählt als **Startmodus des Diensts: "Automatisch"**.
6. Klickt auf "Übernehmen" und dann auf "OK".

(Siehe oberer Screenshot auf Folie 1 der Anfrage)

Schritt 2: AppLocker Standardregeln erstellen

Bevor ihr eigene, restriktive Regeln erstellt, ist es **extrem wichtig**, die Standardregeln zu generieren. Diese erlauben es Windows und Programmen in Standardpfaden
(wie C:\Programme und C:\Windows) weiterhin zu funktionieren. Ohne diese kann euer System unbrauchbar werden!

1. Navigiert im Gruppenrichtlinienverwaltungs-Editor zu:
   Computerkonfiguration -> Richtlinien -> Windows-Einstellungen -> Sicherheitseinstellungen -> Anwendungssteuerungsrichtlinien -> AppLocker.
2. Klickt mit der rechten Maustaste auf den gewünschten Regeltyp (wir beginnen mit den wichtigsten):
   - **Ausführbare Regeln**: Rechtsklick -> "**Standardregeln erstellen**". Bestätigt die Auswahl.
   - **App-Paketregeln** (für Store-Apps): Rechtsklick -> "**Standardregeln erstellen**". Bestätigt die Auswahl.
3. **Wichtiger Hinweis von Folie 2:** *Nachdem der Dienst konfiguriert ist, müssen die beiden Standardregelgruppen erstellt werden. Einmal für Ausführbare Dateien und einmal AppPaketregeln, da sonst das Benutzerprofil unwiderruflich zerstört wird, oder das StartMenü sich nicht mehr benutzen lässt.*
   - Optional, aber oft empfohlen, könnt ihr auch Standardregeln für "Windows Installer-Regeln" und "Skriptregeln" erstellen, je nach euren Sicherheitsanforderungen.

(Siehe mittlerer Screenshot auf Folie 1 und oberer Teil von Folie 2 der Anfrage)

Schritt 3: AppLocker-Regeldurchsetzung konfigurieren

Nachdem die Standardregeln erstellt sind, müsst ihr festlegen, wie AppLocker die Regeln anwenden soll (z.B. nur überwachen oder tatsächlich blockieren).

1. Klickt im linken Bereich auf den Hauptknoten "**AppLocker**".
2. Klickt im rechten Bereich auf "**Eigenschaften von AppLocker konfigurieren**" (oder rechtsklickt auf AppLocker und wählt "Eigenschaften").
3. Im Tab "Durchsetzung":
    - Für jeden Regeltyp ("Ausführbare Regeln", "Windows Installer-Regeln", "Skriptregeln", "App-Paketregeln") könnt ihr wählen:
        - **Regeln erzwingen**: AppLocker blockiert aktiv Anwendungen, die nicht durch eine Regel erlaubt sind.
        - **Nur überwachen**: AppLocker blockiert nichts, protokolliert aber, was blockiert *würde*. **Dies ist der empfohlene Startmodus, um die Auswirkungen zu testen!**
    - Setzt für den Anfang bei "Ausführbare Regeln" und "App-Paketregeln" den Haken bei "Konfiguriert" und wählt "Nur überwachen".
4. Klickt auf "Übernehmen" und "OK".

Schritt 4: (Optional) Gezielte Anwendungsfreigaben erstellen

Die Standardregeln erlauben vieles aus den Windows- und Programme-Ordnern. Wenn Anwendungen von anderen Orten ausgeführt werden sollen oder ihr spezifische Anwendungen explizit erlauben (oder verbieten) wollt, müsst ihr eigene Regeln erstellen.

1. Rechtsklickt auf den entsprechenden Regeltyp (z.B. "Ausführbare Regeln") und wählt "**Neue Regel erstellen...**".
2. Folgt dem Assistenten:
    - **Vorbereitung:** Klickt auf "Weiter".
    - **Berechtigungen:** Wählt "Zulassen" oder "Verweigern". Wählt einen Benutzer oder eine Gruppe aus, für die die Regel gelten soll (standardmäßig "Jeder"). Klickt auf "Weiter".
    - **Bedingungen:** Hier wählt ihr den Typ der Regel (Primärbedingung):
        - **Herausgeber: Empfohlen, wenn die Anwendung digital signiert ist.** Basiert auf der Signatur des Softwareherstellers (z.B. "erlaube alle signierten Anwendungen von Microsoft Corp."). Sehr sicher und flexibel bei Updates.
        - **Pfad:** Erlaubt oder blockiert alles in einem bestimmten Ordner oder eine spezifische Datei. Vorsicht: Wenn der Benutzer Schreibrechte im Pfad hat, könnte er die Datei austauschen.
        - **Dateihash:** Erstellt einen eindeutigen "Fingerabdruck" (Hash) einer Datei. Sehr sicher für spezifische, unsignierte Dateien, aber bei jedem Update der Datei muss der Hash neu erstellt werden.

        - Wählt die passende Bedingung aus und klickt auf "Weiter". Konfiguriert die Details (z.B. den Pfad oder ladet die Referenzdatei für Herausgeber/Hash).
    - **(Optional) Ausnahmen:** Hier könntet ihr Ausnahmen für die Regel definieren.
    - **Name:** Gebt der Regel einen aussagekräftigen Namen und eine Beschreibung. Klickt auf "Erstellen".

(Siehe unterer Teil von Folie 2 der Anfrage)

Schritt 5: Überprüfung und Test auf dem Client

Bevor ihr AppLocker im "Regeln erzwingen"-Modus scharf schaltet, ist gründliches Testen unerlässlich!

1. **Dienst "Anwendungsidentität" prüfen:**
    - Stellt sicher, dass der Dienst "Anwendungsidentität" auf den Client-Computern gestartet ist und auf "Automatisch" steht.
2. **Gruppenrichtlinie aktualisieren:**
    - Führt auf einem Test-Client in der Kommandozeile (als Administrator) den Befehl gpupdate /force aus.
    - **Ein Neustart des Clients ist danach zwingend erforderlich**, damit AppLocker-Richtlinien (besonders die Dienstkonfiguration und die ersten Regeln) korrekt greifen.
3. **AppLocker-Ereignisprotokoll prüfen (im Überwachungsmodus):**
    - Öffnet die Ereignisanzeige (eventvwr.msc).
    - Navigiert zu: Anwendungs- und Dienstprotokolle -> Microsoft -> Windows -> AppLocker.
    - Hier seht ihr unter "EXE und DLL", "MSI und Skript" oder "Paket-App-Bereitstellung/Ausführung", welche Anwendungen blockiert *würden*. Analysiert diese Protokolle sorgfältig!
4. **Funktionalität testen:**
    - Versucht, verschiedene Anwendungen zu starten – sowohl erlaubte als auch solche, die (im Erzwingungsmodus) blockiert werden sollten.
5. **Anpassung der Regeln:**
    - Basierend auf den Testergebnissen und den Protokollen müsst ihr eure Regeln möglicherweise anpassen (weitere Ausnahmen hinzufügen, Pfade korrigieren etc.).
6. **Umstellung auf "Regeln erzwingen":**
    - Wenn ihr sicher seid, dass eure Regeln korrekt sind und nichts Wichtiges blockiert wird, könnt ihr in den AppLocker-Eigenschaften (siehe Schritt 3) von "Nur überwachen" auf "Regeln erzwingen" umstellen.
    - Wieder gpupdate /force und Neustart auf den Clients.