

Windows AppLocker - solis pretim drošākam datoram

Andris Medjānis

27.03.2025.



Kas ir AppLocker

- Iebūvēts Windows rīks, kas ļauj kontrolēt lietotnes/programmas
- Mērķis – bloķēt ļaunatūru, nevēlamu lietotni vai uzbrucēja darbību

* Mērķa auditorija: datoru lietotāji

* Darbojas Windows operētājsistēmā, Pro / Ent. / Edu. (Home)

Salīdzinājumam:



Ieviešana

- Iestatīšanas sarežģītība: vidēja
- Uzturēšana: (ne)regulāra

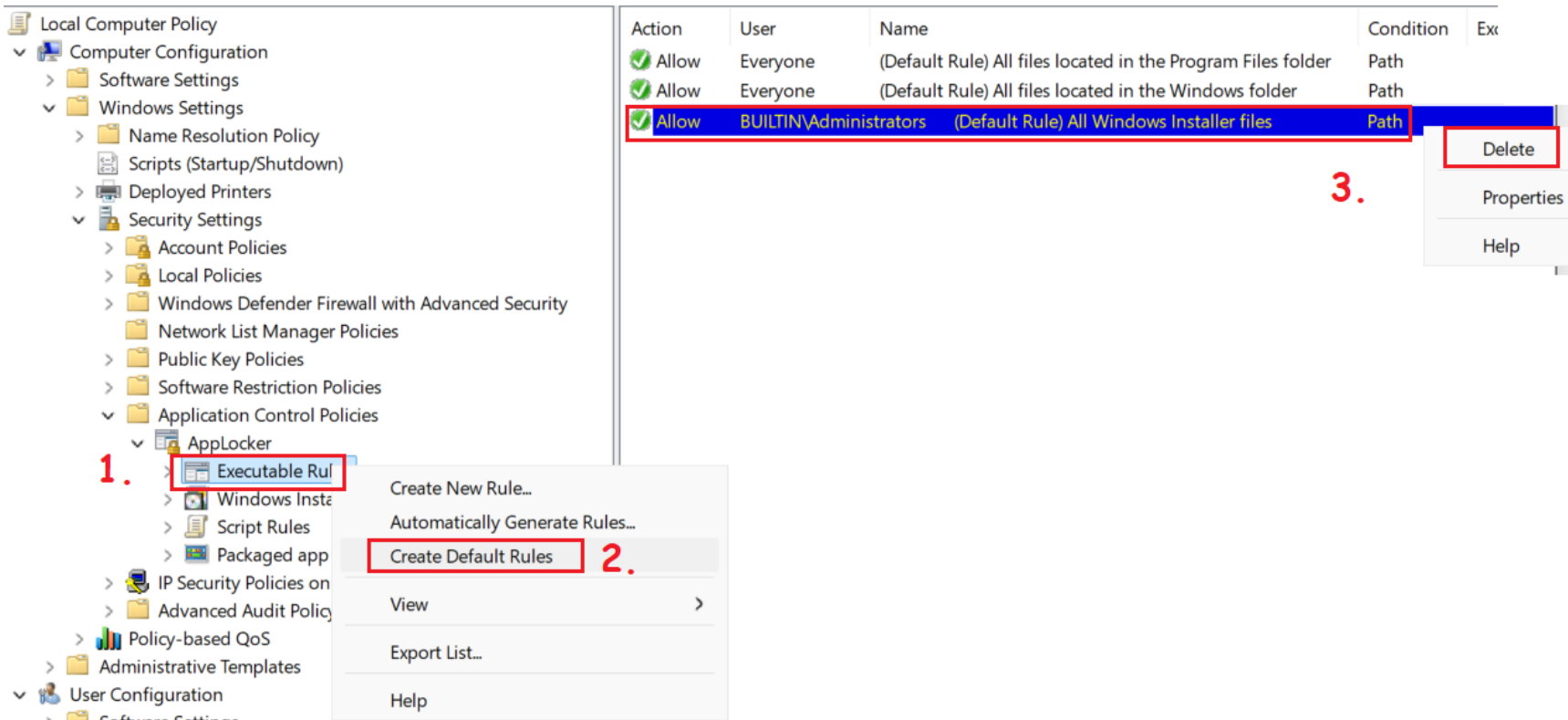
*Darbojas Windows operētājsistēmā, Pro / Ent. / Edu. (Home)

Iestatīšana - solis nr.1

The screenshot shows the Local Group Policy Editor window. The left-hand navigation pane is expanded to show the following path: Local Computer Policy > Computer Configuration > Windows Settings > Application Control Policies > AppLocker. A red box highlights this path, with a red number '2.' next to it. At the bottom of the window, a Run dialog box is open with 'gpedit.msc' entered in the text field, and a red number '1.' is placed above it.

The screenshot shows the 'AppLocker Properties' dialog box, specifically the 'Enforcement' tab. It contains four sections, each with a red box around the 'Configured' checkbox and a red number indicating the step: 'Executable rules:' (1), 'Windows Installer rules:' (2), 'Script rules:' (3), and 'Packaged app Rules:' (4). Each section also has a dropdown menu set to 'Audit only'. At the bottom of the dialog are 'OK', 'Cancel', and 'Apply' buttons.

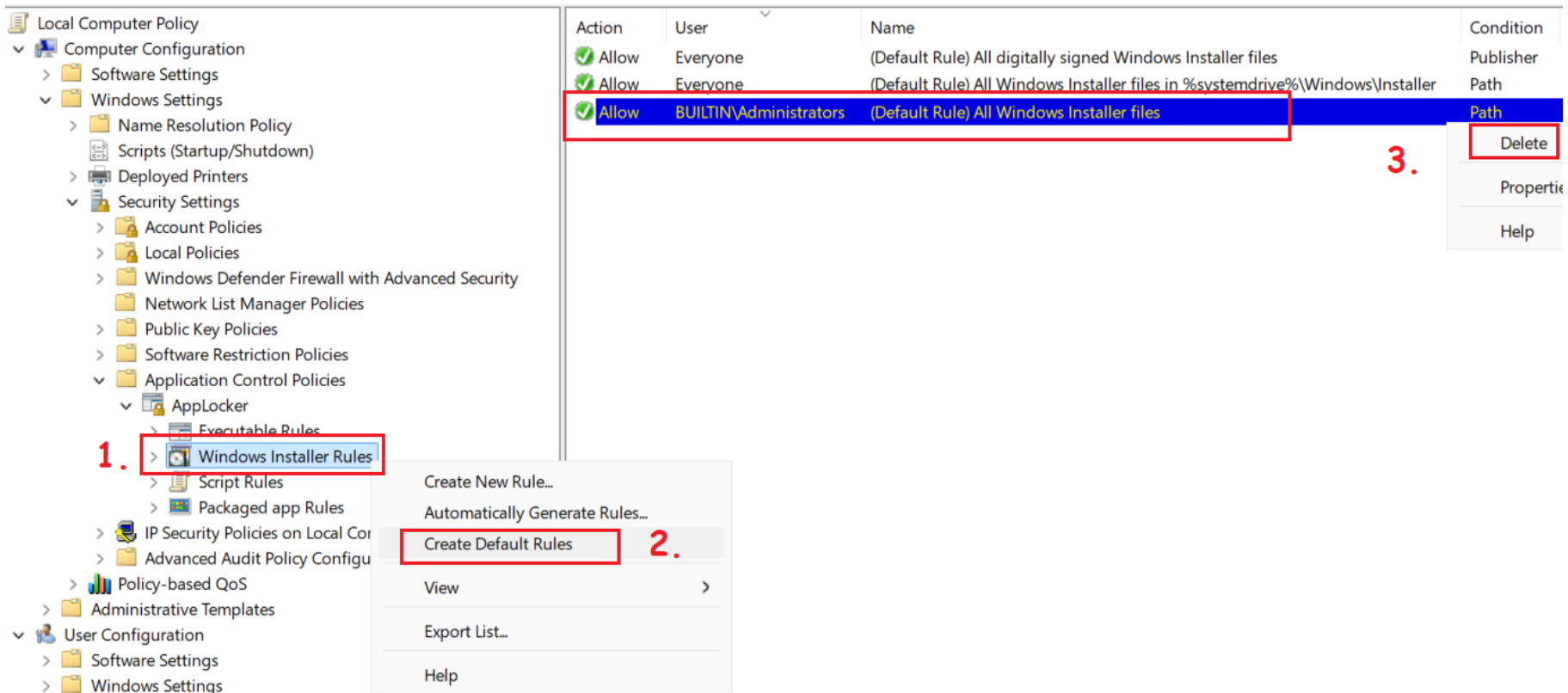
Iestatīšana - solis nr.2



The screenshot shows the Windows Local Computer Policy console. The left-hand tree view is expanded to 'AppLocker' > 'Executable Rules'. A red box labeled '1.' highlights the 'Executable Rules' folder. A context menu is open over this folder, with 'Create Default Rules' highlighted by a red box labeled '2.'. The main pane shows a table of existing rules, with the third rule selected and a context menu open over it, showing 'Delete' highlighted by a red box labeled '3.'.

Action	User	Name	Condition	Ex
✓ Allow	Everyone	(Default Rule) All files located in the Program Files folder	Path	
✓ Allow	Everyone	(Default Rule) All files located in the Windows folder	Path	
✓ Allow	BUILTIN\Administrators	(Default Rule) All Windows Installer files	Path	

Iestatīšana - solis nr.3

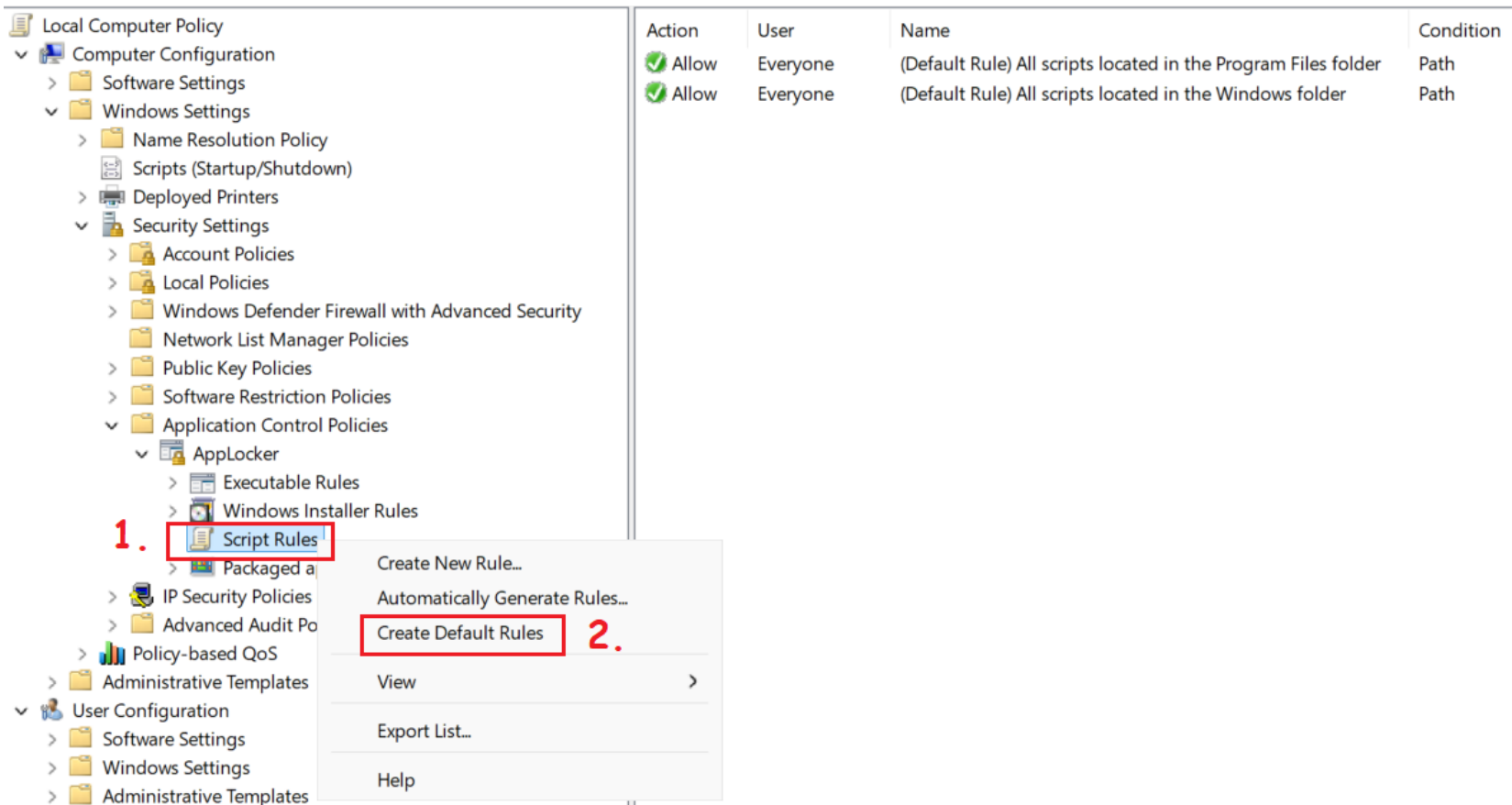


The screenshot shows the Windows Local Computer Policy console. The left-hand navigation pane is expanded to 'Application Control Policies' > 'AppLocker' > 'Executable Rules'. A red box labeled '1.' highlights the 'Windows Installer Rules' folder. A context menu is open over this folder, with 'Create Default Rules' highlighted by a red box labeled '2.'. The main pane displays a table of rules:

Action	User	Name	Condition
Allow	Everyone	(Default Rule) All digitally signed Windows Installer files	Publisher
Allow	Everyone	(Default Rule) All Windows Installer files in %systemdrive%\Windows\Installer	Path
Allow	BUILTIN\Administrators	(Default Rule) All Windows Installer files	Path

A red box labeled '3.' highlights the 'Delete' button in the context menu for the selected rule.

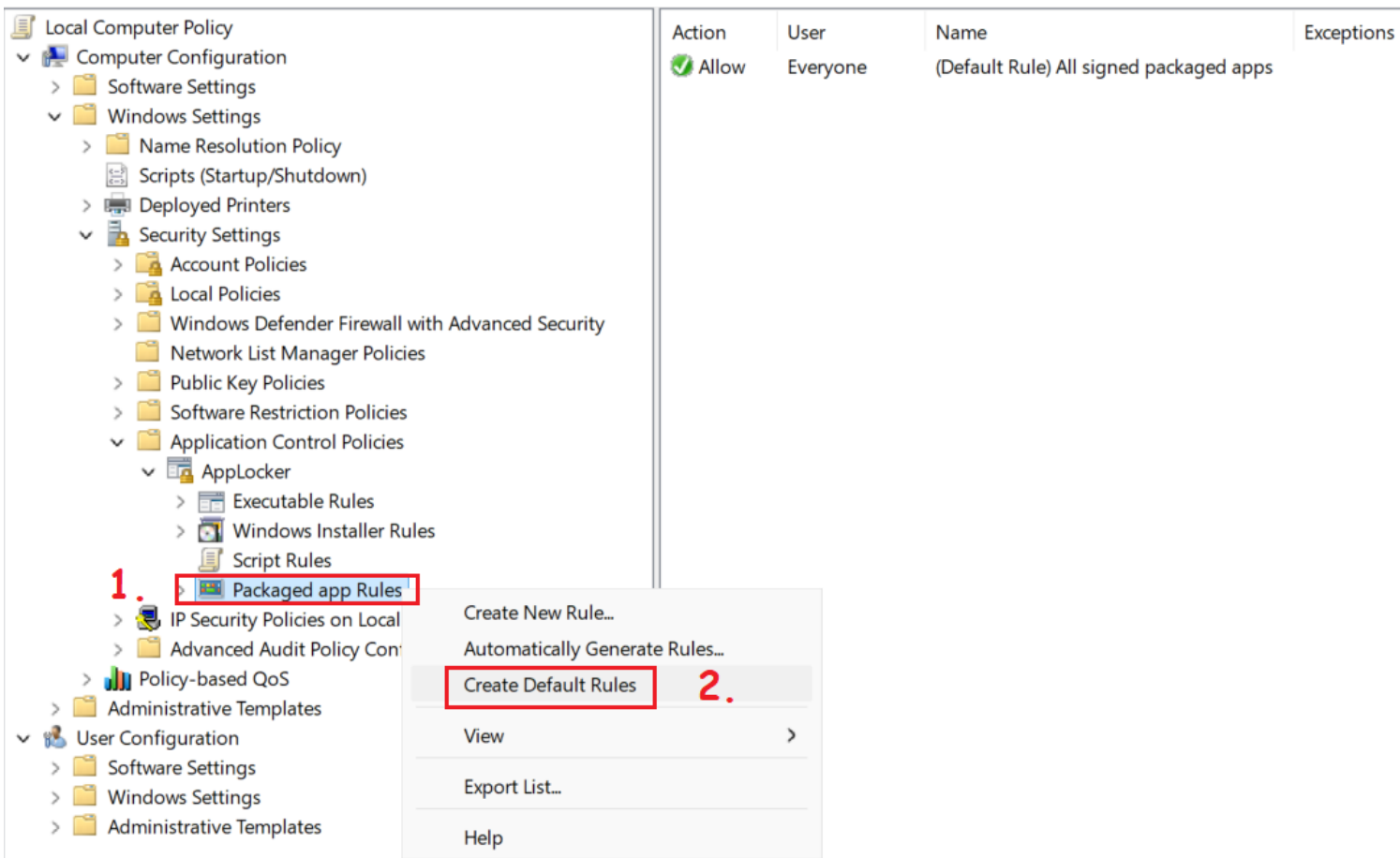
Iestatīšana - solis nr.4



The screenshot shows the Windows Local Computer Policy console. The left pane displays a tree view of policy settings, with 'Script Rules' selected and highlighted by a red box and the number '1.'. A context menu is open over 'Script Rules', with 'Create Default Rules' selected and highlighted by a red box and the number '2.'. The right pane shows a table of default rules.

Action	User	Name	Condition
✓ Allow	Everyone	(Default Rule) All scripts located in the Program Files folder	Path
✓ Allow	Everyone	(Default Rule) All scripts located in the Windows folder	Path

Iestatīšana - solis nr.5



The screenshot shows the Windows Local Computer Policy console. The left pane displays a tree view of policy categories. The right pane shows a table of existing rules.

1. In the left pane, the **Packaged app Rules** folder is selected and highlighted with a red box.

2. A context menu is open over the **Packaged app Rules** folder, and the **Create Default Rules** option is selected and highlighted with a red box.

Action	User	Name	Exceptions
✔ Allow	Everyone	(Default Rule) All signed packaged apps	

Iestatīšana - solis nr.6

The screenshot displays the Windows Group Policy Editor interface. On the left, the navigation tree shows the path to AppLocker under 'Application Control Policies', with a red box and the number '1.' highlighting it. The main pane shows the 'AppLocker provides access control for applications' window. A red box and the number '2.' highlight the 'Configure rule enforcement' button. The 'Configure Rule Enforcement' dialog is open, showing a warning icon and instructions. A red box and the number '3.' highlight the 'Enforce rules' dropdown menu for 'Executable rules'. The 'Advanced' tab is selected, showing 'Configured' for all rule types: Executable rules, Windows Installer rules, Script rules, and Packaged app Rules. A red box and the number '4.' highlight the 'Apply' button at the bottom right of the dialog.

Local Computer Policy

- Computer Configuration
 - Software Settings
 - Windows Settings
 - Name Resolution Policy
 - Scripts (Startup/Shutdown)
 - Deployed Printers
 - Security Settings
 - Account Policies
 - Local Policies
 - Windows Defender Firewall with Advanced Security
 - Network List Manager Policies
 - Public Key Policies
 - Software Restriction Policies
 - Application Control Policies
 - AppLocker** (1.)
 - Executable Rules
 - Windows Installer Rules
 - Script Rules
 - Packaged app Rules
 - IP Security Policies on Local Computer
 - Advanced Audit Policy Configuration
 - Policy-based QoS
 - Administrative Templates

- User Configuration
- Software Settings
- Windows Settings
- Administrative Templates

AppLocker provides access control for applications

Getting Started

AppLocker uses rules and the properties of files to provide access control for applications. If rules are present in a rule collection, only the files included in those rules will be permitted to run. AppLocker rules do not apply to all editions of Windows.

More about AppLocker

Which editions of Windows support AppLocker?

Configure Rule Enforcement

For the AppLocker policy to be enforced on a computer, the Application Identity service must be running.

Use the enforcement settings for each rule collection to configure whether rules are enforced or audited. If rule enforcement has not been configured, rules will be enforced by default.

Configure rule enforcement (2.)

More about rule enforcement

Overview

- Executable Rules
 - Rules: 3
 - Enforcement configured: Rules are enforced
- Windows Installer Rules
 - Rules: 3
 - Enforcement configured: Rules are enforced
- Script Rules
 - Rules: 2
 - Enforcement configured: Rules are enforced
- Packaged app Rules
 - Rules: 1
 - Enforcement configured: Rules are enforced

AppLocker Properties

Enforcement Advanced

Specify whether AppLocker rules are enforced for each rule collection.

Executable rules:
 Configured
Enforce rules

Windows Installer rules:
 Configured
Enforce rules (3.)

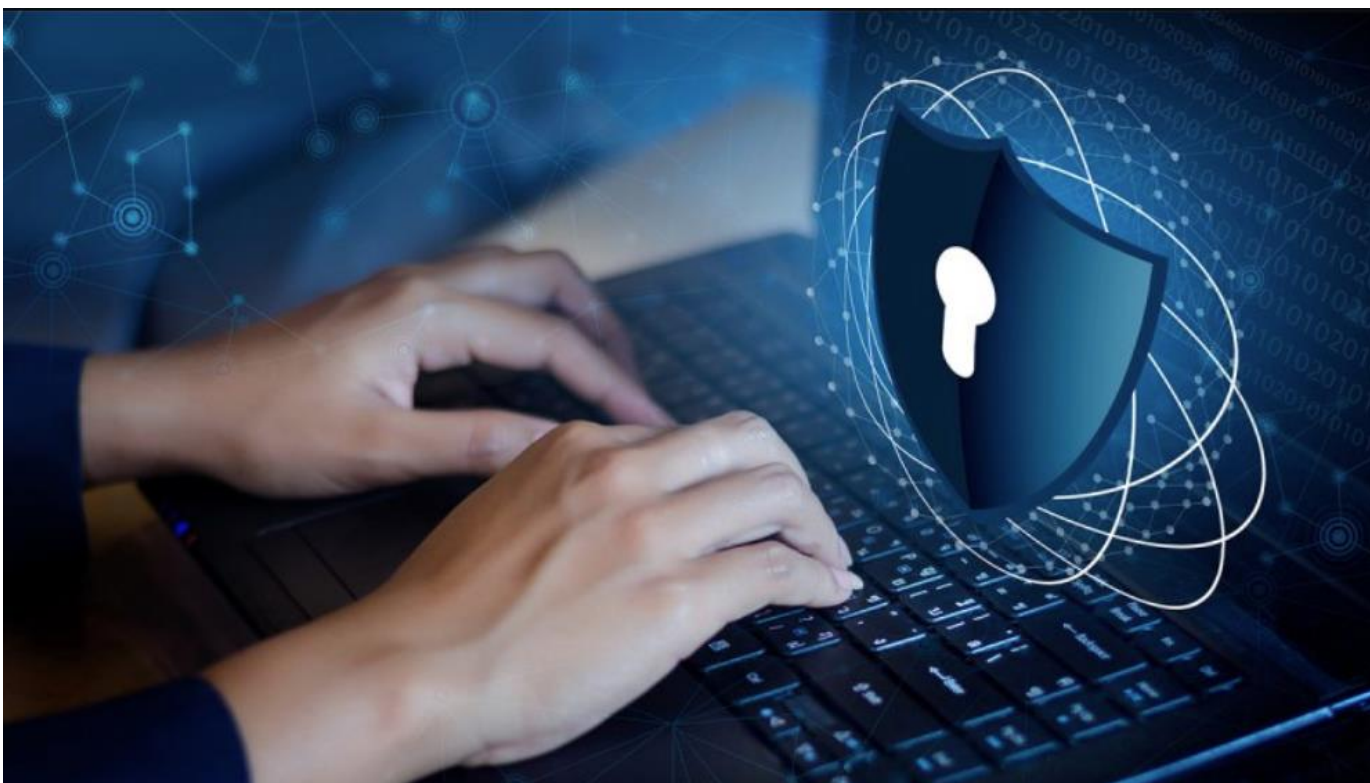
Script rules:
 Configured
Enforce rules

Packaged app Rules:
 Configured
Enforce rules

More about rule enforcement (4.)

OK Cancel Apply

Uzmanīgi!



Solis tuvāk mūsu datoru drošībai

- ...jo kibernetiķi ik dienu strādā, lai būtu soli tuvāk mūsu datoriem
- AppLocker bāzes konfigurācija.
 - Turpinājums sekos?



Paldies!

**Drošība = modrs lietotājs +
atjauninājumi**