Information Systems Security

Group Project

Applocker

IS2109

Group No:21

Group Members

Name	Index Number	Registration Number
Dilshani J P E	17020247	2017/IS/024
Dilshan P A B	17020239	2017/IS/023
Shan W H P	17020786	2017/IS/078
Kalansooriya N N	17020395	2017/IS/039

Applocker

In many organizations , information is the most valuable asset, therefore access control technologies are used to restrict access from unauthorized users.

Applocker helps users control which apps and files they can run. When a user runs a process if he accidentally runs a malicious software he will lose the data . The data may be deleted or transmitted. Applocker will reduce these security issues by restricting the files that users and groups are allowed to run.

There are apps that can be installed by non-administrative users. This could be risky to an organization's written security policy and traditional app control solutions that rely on the inability of users to install apps. By creating an allowed list of apps and files Applocker prevents such types of apps running .

Applocker helps organizations to protect their digital assets and improve the management of application control policies

Scenarios of Applocker can be used

- When an app isn't no longer supported by your organization and if we need to prevent it from being accessed by everyone.
- When new version is app is deployed and prevent users from running the old version
- A group of users need to use a specific app that is restricted for others

- When you need to control the access to sensitive data
- When you need to prevent users from running unlicensed software
- When you need to prevent users from running revoked software
- When only specific users need to access the software

Applocker Security options

1. Protection against unwanted software

We can add our usable softwares to the applocker allow list, then the applocker is not allowed to be accessed and used to software other than in this list. It has the ability to deny apps from running. So no one can’t run an unauthorized application.

2. Application inventory

When we use Applocker, we can get information about all app access activities as an event log. We can use Windows PowerShell cmdlets to analyze this data programmatically.

3. Licensing conformance

AppLocker gives us the opportunity to add rules that preclude unlicensed software from running and set restrictions to authorized users while using licensed software.

4. Software standardization

When we use some computers as a business group, then using AppLocker policies we can be configured to allow only supported or approved apps in this group. This way we can set some standards for apps that we use.

Installing AppLocker

AppLocker is included with enterprise level editions of windows. We can use AppLocker for single computer as well as group of computers.

For single computer we have to author the rules by using the Local Security Policy editor

For a group of computers we have to author the rules within a Group Policy Object by using the Group Policy Management Console(GPMC)

Those are the baseline settings for a PC with AppLocker installed

Settings	Default Value
Accounts created	None
Authentication Method	Not applicable
Management interfaces	AppLocker can be managed by using a Microsoft Management Console snap-in, Group Policy Management, and Windows PowerShell
Ports opened	None
Minimum privileges required	Administrator on the local computer; Domain Admin, or any set of rights that allow you to create, edit and distribute Group Policy Objects.
Protocols used	Not applicable.
Scheduled tasks	Appidpolicyconverter.exe is put in a scheduled task to be run on demand.
Security policies	None required. Applocker creates security policies.
System services required	Applications identity service named as appidsvc runs under Local service and No impersonation.
Storage of credentials	none.