

Step by step guide for Demo by Paula Januszkiewicz

1. On Windows 7 or windows 2008 R2 Run the applocker service. It is available in the Services.msc -> Application Identity. Start it and set to automatic.
2. Open Local Security Policy and in the Applocker configuration create the Deny rule for f.e. notepad.exe.
3. Click No in the "Create the default rules" window.
4. Reboot
5. Notice that even you log in the system - you will receive "nothing"
6. Boot with the Windows CD - go to the "repair mode".
7. Run the cmd console and type "regedit"
8. Pick the Local Machine registry key. In the Regedit menu choose Load Hive. Load the %systemdrive%\Windows\System32\config\ ==> SYSTEM.
9. Give the registry tree some name.
10. Go to this tree and choose between CurrentControlSet's -> You can find the informaiton about the current one in the Select container in the same tree. Should be the one with the "1".
11. Find the AppIDSvc in the services container in the current control set.
12. Change the start type from 2 to 4 (2 is automatic start, 4 is Disabled).
13. Restart the system.
14. Log in :) If everything was ok you should be able to log in!