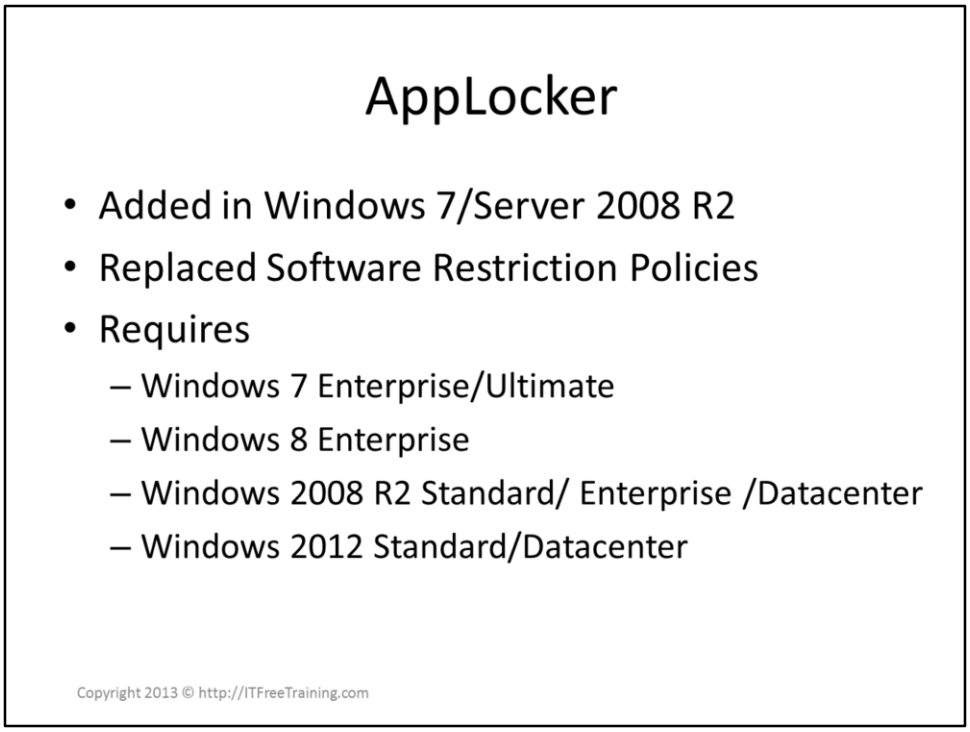
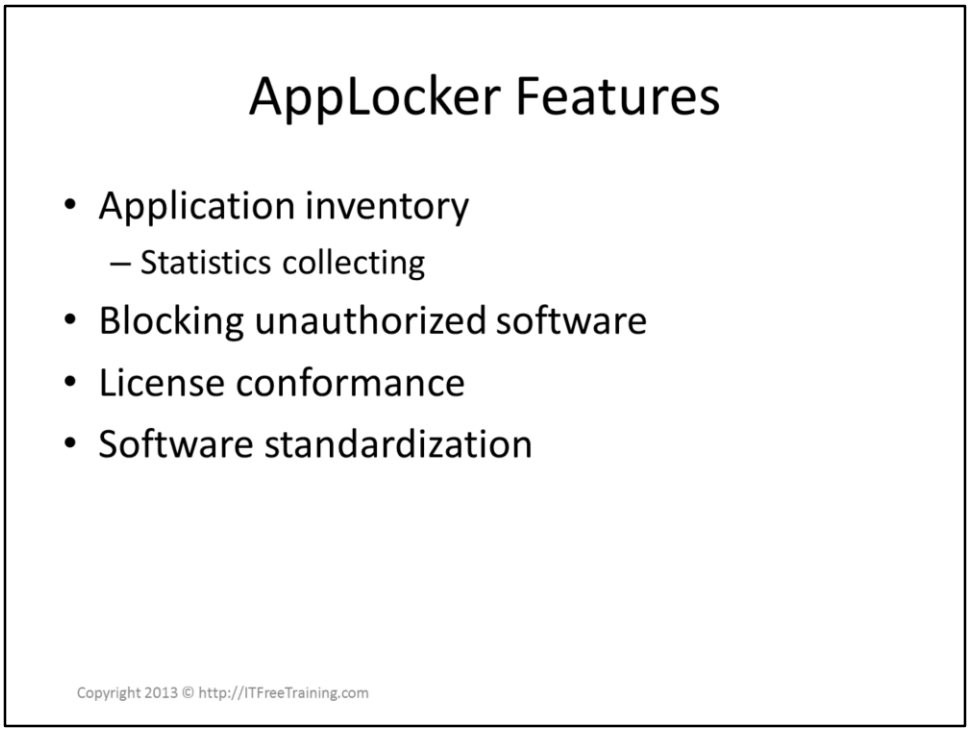
AppLocker allows the administrator to control which applications are run on the computers in your domain. The rules Applocker uses allow the scope of an application to be defined, like particular versions or newer version or can be narrowed down to a single application.



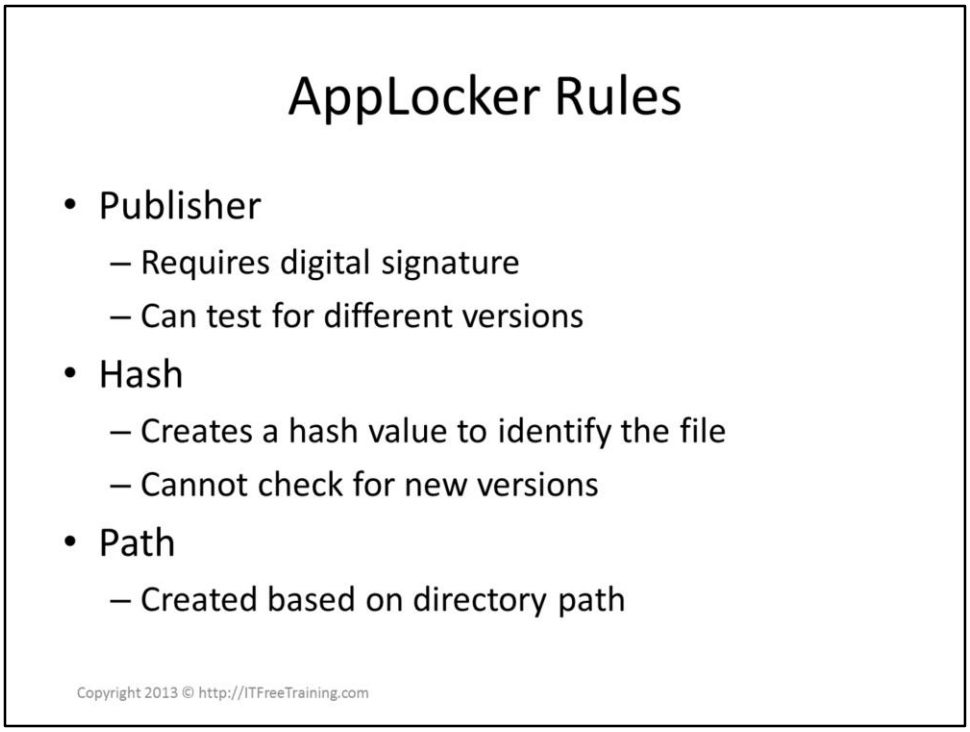
AppLocker

AppLocker was first added in Windows 7 and Windows Server 2008 R2 as a replacement for software restriction policies. Software restriction did not have any wizards and thus is hard to configure. AppLocker adds a wizard and is much easier to configure than Software restriction policies. Since it is aimed towards business, it only works on Windows operating systems that were targeted for business. For the client operating systems these are Windows 7 Enterprise/Ultimate and Windows 8 Enterprise. For server operating system these are Windows Server 2008 R2 Standard/Enterprise/Datacenter and Windows Server 2012 Standard/Datacenter.



AppLocker Features

Applocker can be used to monitor and control software. When AppLocker is in audit mode it will only report which software is run. If you put AppLocker in enforce mode this will allow the administrator to control which software is run. This allows a company to standardize which software is run and can be a tool used for software conformance.



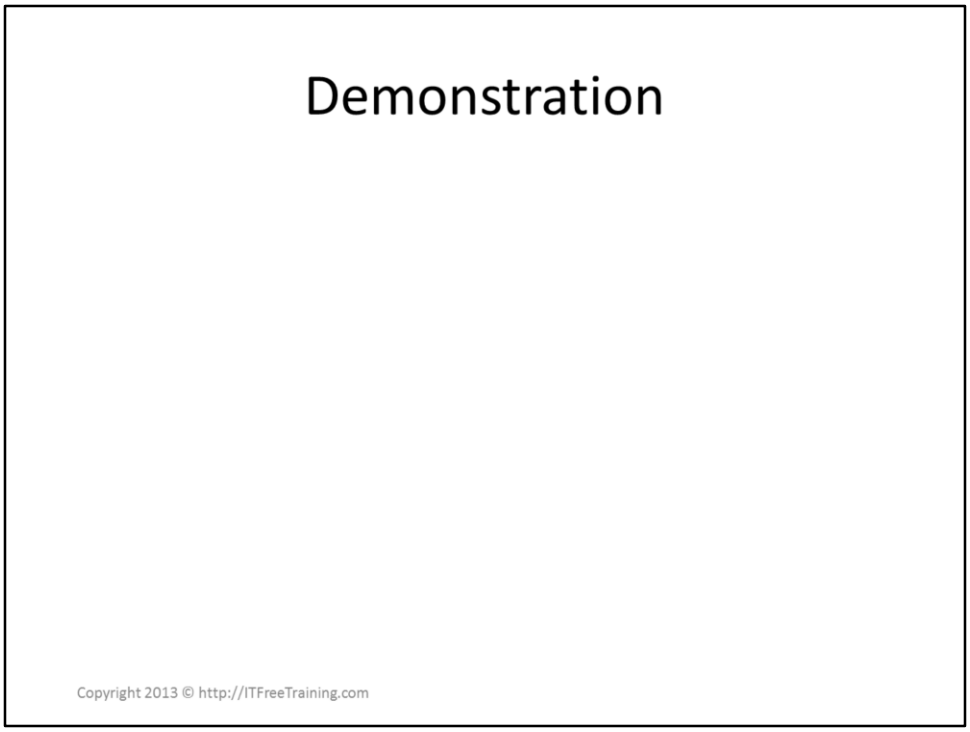
AppLocker Rules

In order for AppLocker to work out which software is allow to run and which software should be blocked, AppLocker supports 3 different types of rules.

Publisher: This rule relies on the executable being digitally signed. This allows Windows to determine the Vendor, Software Title and version of the software. Publisher rules allow you to create a rule that can work with new software that was not released when the rule was created.

Hash: A hash rule puts the file through a mathematical formula to determine a value. Each file should create a different hash value, kind of like a fingerprint. This rule type can only match that executable and thus does not account for new versions of the software.

Path: This checks the location the file was run from. For example, if the executable is located in the Program Files directory.



Demonstration

AppLocker requires the Application Identity service to be running on the client. If this is not running or stopped, AppLokcer will stop working. This service can be configured in Group Policy at the following location to start automatically.
Computer Configuration\Polices\Windows Settings\Security Setting\System Service\Application Identity

AppLocker is configured in Group Policy at the following location.
Computer Configuration\Polices\Windows Settings\Security Settings\Application Control Polices\AppLocker

To configure the default properties for AppLocker, select the

option “Configure rule enforcement”. Rules can be applied to executable, Windows Installer files and scripts. Once you enable the ones you want you can select AppLocker to run in Audit mode or Enforce mode.

AppLocker has the option to automatically create rules. This will examine the computer and create rules based on the executables found on it. This step can be run on any computer, this includes a computer that cannot run AppLocker. You are best to run this on a computer that has the software installed on it that you use in your company so AppLocker can create the correct rules.

You can also create default rules which will be used if no other rule matches. Without any default rules, if no match is found with the existing rules the software will not be allow to run. This can prevent software in the operating system from running.

References

“MCTS 70-640 Configuring Windows Server 2008 Active Directory Second edition” pg 361 - 362
“AppLocker” http://technet.microsoft.com/en-us/library/dd723678