



Software Restriction for Zero Client Users (AppLocker Group Policy)

Software Restriction for Zero Client Users by Using AppLocker Group Policy

AppLocker Group policy Description:

AppLocker Group Policy for Windows system Applications can be used for restricting User or User Groups from running and installing programs.

Typically, only administrators have the permission to install programs. But green software and other software package do not necessarily need administrators' permission to be installed. So using AppLocker Group policy can directly limit the User from accessing and installing all programs.

AppLocker Group policy Configuration:

Tips:

- AppLocker Group Policy needs to be used in conjunction with User Account Control (**UAC**). Please refer to *User Account Control Guide* to turn on **UAC**.
- Before setting up AppLocker, please standardize the program installation path, be sure to install the required programs in C: \ Program Files or C: \ Program Files (x86) path. As Program Files folder is a kind of system file, which requires the administrator permission to make changes.
- Recommended operating systems: Windows 7 (Ultimate, Enterprise), Windows 8.1 Enterprise, Windows 10 Enterprise, Server 2008R2 Standard, Datacenter, Server 2012R2 (Standard, Datacenter), Server 2016 (Standard, Datacenter).

Environment of This Guide

System:

Windows 7 x64 Ultimate;

Disk partitions:

C disk - system & software partition

- D disk- public partition
- E disk private partition

The following guide applies to the above mentioned environment, configuration steps may vary depending on your actual application environment.

Content
AppLocker Quick Configuration Steps
AppLocker Detailed Configuration Steps
Remark 1: Allow software installation on other directories
Remark 2: Restrict a user from using a software
Remark 3: Enable Application Identity service in Windows 10/ Server 2016 25 -

AppLocker Quick Configuration Steps

- 1) Enter **Service**, set the **Application Identity** startup type to **automatic**
- 2) Enter the **local Group Policy Editor** → **AppLocker**
- 3) Executable rules→ Windows installer rules→ and script specifications create default rules
- 4) AppLocker open Configuration rules
- 5) Restart the host, Then the AppLocker settings will take effect.

AppLocker Detailed Configuration Steps

 Logon to the host system with the administrator account, run services.msc

	Type the name of a prog resource, and Windows	gram, folder, docun will open it for you.	nent, or Internet
pen:	services.msc		Ŧ
	OK	Cancel	Browse

2) Enter **services**, right-click on **Application Identity** and select **Properties**.



aeneral	Log On	Recovery Dependencies
Service	name:	AppIDSvc
Display	name:	Application Identity
Description:		Determines and verifies the identity of an application. Disabling this service will prevent AppLocker from
Path to	executabl	
C:\Win	dows\syst	tem32\svchost.exe +k LocalServiceAndNoImpersonation
Startup	type:	Manual
Help me	e configur	Automatic (layed Start)
Service	e state	Manual Disabled Stopped
Start		Stop Pause Resume
You can from he Start pa	n specify t re. arameters:	the start parameters that apply when you start the service

to Automatic, and start the service then click OK.

4) Logon to the host system with the administrator account, run gpedit.msc.

	Type the name of a program, for resource, and Windows will ope	older, document, or Interne en it for you.
pen:	gpedit.msc	
		Cancel

www.vcloudpoint.com

5) On Local Group Policy Editor open AppLocker through the path of Local Computer Policy -> Computer Configurations -> Windows settings -> Security Settings -> Application Control Policies -> AppLock



6) On **Local Group Policy Editor**, select the **Executable Rules**, right-click the right blank, **Create Default Rules** (default rule: user can only run the application under C:\Program Files or C:\Program Files (x86)).



www.vcloudpoint.com

7) On Local Group Policy Editor, select the Windows Installer Rules, right-click on the right blank, Create Default Rules.



Note: If you want to prevent users from installing programs more effectively, please follow steps 8-20 and manually set all disk installation restriction.

8) On Local Group Policy Editor Select Windows Installer Rules, right-click on the right blank, Create New Rule...



www.vcloudpoint.com

√*cloudpoint*

eate Windows Installer R	ules
Before Y	ou Begin
Before You Begin Permissions Conditions Publisher Exceptions Name	This wizard helps you create an AppLocker rule. A rule is based on file attributes, such as the file path or the software publisher contained in the file's digital signature. Before continuing, confirm that the following steps are complete: Install the applications you want to create the rules for on this computer. Back up your existing rules. Review the AppLocker documentation. To continue, click Next. Skip this page by default
	< Previous Next > Create Cancel

10) On **Create Executable Rules** Select **Deny**, and **select** a group.

Create windows installer Rules	
Permissions	
Before You Begin Permissions Conditions Publisher Exceptions Name	Select the action to use and the user or group that this rule should apply to. An allow action permits affected files to run, while a deny action prevents affected files from running. Action: Allow Allow
	Deny User or group: Everyone Select
	More about rule permissions
	< Previous Next > Create Cancel

11) Click Advanced.

Select this object type:	
User or Group	Object Types
From this location:	
VCLOUDPOINTDEMO	Locations
Enter the object name to select (<u>examples</u>):	
	Check Names

12) Click **Find Now**, select **vMatrixServerRemoteUsers**, and click **OK**.

alest this shipst type:		
leect this object type:		Object Trace
		Object Types
rom this location:		
VCLOUDPOINTDEMO		Locations
Common Queries		
Name: Starts with	-	Columns
Description: Starts with	r]	Find Now
Disabled accounts		Stop
Non expiring password		
Days since last logon:	*	P1
		OK Cancel
Search results:		OK Cancel
Search results: ame (RDN)	In Folde	OK Cancel
Gearch results: ame (RDN) suser30	In Folde VCLOUDPOINTDEMO	OK Cancel
Search results: ame (RDN) user30 user4	In Folde VCLOUDPOINTDEMO VCLOUDPOINTDEMO	OK Cancel
Search results: ame (RDN) user30 user4 user5 user5	In Folde VCLOUDPOINTDEMO VCLOUDPOINTDEMO VCLOUDPOINTDEMO	OK Cancel
Gearch results: ame (RDN) user30 user4 user5 user6 user7	In Folde VCLOUDPOINTDEMO VCLOUDPOINTDEMO VCLOUDPOINTDEMO VCLOUDPOINTDEMO VCLOUDPOINTDEMO	OK Cancel
Search results: ame (RDN) user30 user4 user5 user6 user7 user8	In Folde VCLOUDPOINTDEMO VCLOUDPOINTDEMO VCLOUDPOINTDEMO VCLOUDPOINTDEMO VCLOUDPOINTDEMO VCLOUDPOINTDEMO VCLOUDPOINTDEMO	OK Cancel
Search results: lame (RDN) user30 user4 user5 user6 user7 user8 user9	In Folde VCLOUDPOINTDEMO VCLOUDPOINTDEMO VCLOUDPOINTDEMO VCLOUDPOINTDEMO VCLOUDPOINTDEMO VCLOUDPOINTDEMO VCLOUDPOINTDEMO VCLOUDPOINTDEMO	OK Cancel
Search results: lame (RDN) user30 user4 user5 user6 user7 user8 user9 Users	In Folde VCLOUDPOINTDEMO VCLOUDPOINTDEMO VCLOUDPOINTDEMO VCLOUDPOINTDEMO VCLOUDPOINTDEMO VCLOUDPOINTDEMO VCLOUDPOINTDEMO VCLOUDPOINTDEMO	OK Cancel
Search results: lame (RDN) user30 user4 user5 user6 user7 user8 user9 Users VCP	In Folde VCLOUDPOINTDEMO VCLOUDPOINTDEMO VCLOUDPOINTDEMO VCLOUDPOINTDEMO VCLOUDPOINTDEMO VCLOUDPOINTDEMO VCLOUDPOINTDEMO VCLOUDPOINTDEMO VCLOUDPOINTDEMO VCLOUDPOINTDEMO	OK Cancel

13) Reconfirm the selection of the group and click **OK**.

Select this object type:	
User or Group	Object Types
From this location:	
VCLOUDPOINTDEMO	Locations
Enter the object name to select (<u>examples</u>):	
Enter the object name to select (<u>examples</u>): VCLOUDPOINTDEMO <mark>NMatrixServerRemoteUsers.</mark>	Check Names
Enter the object name to select (<u>examples</u>): VCLOUDPOINTDEMO <mark>NVMatrixServerRemoteUsers</mark>	Check Names

14) On **Create installer rules** select **Permission** Confirm the **Deny**, then click **Next.**

Create Windows Installer Rules	
Permissions	
Before You Begin Permissions Conditions Publisher Exceptions Name	Select the action to use and the user or group that this rule should apply to. An allow action permits affected files to run, while a deny action prevents affected files from running.
	More about rule permissions
	< Previous Next > Create Cancel

√*cloudpoint*

15) On **Create installer rules** Select **Path**, **Next>**.

Create Executable Rules	x.
Conditions	
Before You Begin Permissions	Select the time of mimory condition that you would like to create
Conditions	Select the type of prinnary condition that you would like to create.
Path Exceptions Name	Publisher Select this option if the application you want to create the rule for is signed by the software publisher.
	 Path Create a rule for a specific file or folder path. If you select a folder, all files in the folder will be affected by the rule. File hash Select this option if you want to create a rule for an application that is not signed.
	More about rule conditions < Previous Next > Create Cancel

16) On **Create installer rules** Select **Browse Folders...**

Create Windows Installer Rules	
Path	
Before You Begin Permissions Conditions Path Exceptions Name	Select the file or folder path that this rule should affect. If you specify a folder path, all files underneath that path will be affected by the rule. Path:
	More about path rules and path variables < Previous

17) Select **Disk(C:)**, limit the user to install the software in **disk C**, then click **OK**.



18) On **Create installer rules** Confirm the path,then click **Create**.

Create Windows Installer Rules		X
Path		
Before You Begin Permissions Conditions	Select the file or folder path that this rule should affect. If you specify a folder path, all files underneath that path will be affected by the rule.	
Exceptions Name	Path: %OSDRIVE%* Browse Folders	
	More about path rules and path variables	
	< Previous Next > Create Cancel	

19) You can see the path has been restricted (C for %OSDRIVE%).



In the same way, add other disks (public disk, private disk...) to the restriction list, which can limit the user to install the software under other disks.

20) All three Disk have been added to restriction list and (**C drive** appears as**% OSDRIVE%**).

File Action View Help				
 Local Computer Policy Computer Configuration Software Settings Windows Settings Name Resolution Policy Scripts (Startup/Shutdown) Deployed Printers Security Settings Account Policies Local Policies Local Policies Local Policies Local Policies Mondows Firewall with Advance Network List Manager Policies Public Key Policies Software Restriction Policies Applocker AppLocker Script Rules Soft Windows Installer Rules Soft Policies on Local Cor Avanced Audit Policy Configut Publicy-based OoS 	Action Allow Allow Allow Deny Deny Deny Deny	User Everyone BUILTIN\Ad VCLOUDPOI VCLOUDPOI	Name (Default Rule) All digitally signed Wind (Default Rule) All Windows Installer files (Default Rule) All Windows Installer files %OSDRIVE%* D:* E:*	Conditio Publisher Path Path Path Path
4 III +	•		ш	•

21) On **local group policy editor** Select **Script Rules**, right-click the right blank, **Create Default Rules**.





22) On local group policy editor, select AppLocker, click Configure rule enforcement.



23) On AppLocker Properties Tick all the rules then click OK.

for the second second		
nforcement	Advanced	
Specify wh each rule	ether AppLocker rules are enforced for collection.	
Executabl	le rules:	
Conf	igured	
R. f		1
Entorce	i i miez	J
Windows .	Installor rules:	
Conf	installer fules.	
V Com	rêm eu	÷
Enforce	e rules 💌 👻	
1		
Script r	ules:	
🔽 Conf	igured	
Enforce	rules 🔻	1
-		1
lore about	. rule forcement	
	OK Cancel App	oly

24) AppLocker Setup complete, restart the host.

Test:

- login a user at a vCloudPoint Zero Client, run the software that need to be used to see they run normally or not.
- When opening .exe file (program installation package or green program package), it will prompt and fail to open.

D:\AnyD	esk.exe
8	This program is blocked by group policy. For more information, contact your system administrator.
	ОК

Tips: Users can only open program shortcut on the user's desktop, please do not put.exe files on the user's desktop.

Remark 1: Allow software installation on other directories

If you have software to be installed in other directories but not C:\Program Files and C:\Program Files (x86) (for example, E:\Program Files), follow the following steps to create new rules.

1) On **local group policy editor**, select **Executable Rules**, right-click on right blank, **Create New Rule...**



2) On **Create Executable Rules**, select **Before You Begin** → **Next**.



3) On Permission select Allow→ Next.



Create Executable Rules	
Permissions	
Before You Begin Permissions Conditions Publisher Exceptions Name	Select the action to use and the user or group that this rule should apply to. An allow action permits affected files to run, while a deny action prevents affected files from running.
	More about rule permissions < Previous

4) On **Condition**, select **Path**→**Next**.





5) Path, select Browse Folders... Select the disk (D:) Program Files → Create.

Create Executable Rules	x - x - x - x - x - x - x - x - x - x -
Path	
Before You Begin Permissions Conditions Path	Select the file or folder path that this rule should affect. If you specify a folder path, all files underneath that path will be affected by the rule.
Exceptions Name	Path: D:\Program Files* Browse Files
	More about path rules and path variables
	< Previous Next > Create Cancel

6) After creating the new allowable custom rules will be shown.



Remark 2: Restrict a user from using a software

If a user (for example, user1) is required to be restricted from using a software, a denial rule should be created in the **Executable Rules**.

1) On **local group policy editor** Select **Executable Rules**, right-click the right blank, **Create New Rule...**



2) On **Executable Rules**, select **Deny**, and select the user.

Create Executable Rules		~
Permissions		
Before You Begin Permissions Conditions Publisher Exceptions Name	Select the action to use and the user or group that this rule should apply to. An allow action permits affected files to run, while a deny action prevents affected files from running.	
	More about rule permissions	
	< Previous Next > Create Cancel]

lect User or Group	8 2
Select this object type:	
User or Group	Object Types
From this location:	
VCLOUDPOINTDEMO	Locations
Enter the object name to select (<u>exan</u>	iples): Check Names
Advanced	OK Cancel

4) Click **Find Now**, select **user1**, **OK**.

Select this object ty	/pe:	
User or Group		Object Types
From this location:		
VCLOUDPOINTD	EMO	Locations
Common Queries]	
Name:	itarts with 💌	Columns
Description:	itarts with 👻	Find Now
Disabled acc	counts	Stop
Non expiring	password	
Days since last	logon:	<i>\$</i>
Days since last Search results:	logon:	OK Cancel
Days since last Search results: ame (RDN)	logon:	OK Cancel
Days since last Gearch results: ame (RDN)	logon:	OK Cancel
Days since last Gearch results: ame (RDN) Performance	logon:	OK Cancel
Days since last Gearch results: ame (RDN) Performance Performance Power Users	In Folder VCLOUDPOINT VCLOUDPOINT VCLOUDPOINT	OK Cancel
Days since last	In Folder VCLOUDPOINT VCLOUDPOINT VCLOUDPOINT VCLOUDPOINT VCLOUDPOINT	OK Cancel
Days since last Gearch results: ame (RDN) Performance Performance Power Users Remote Desk Replicator	In Folder VCLOUDPOINT VCLOUDPOINT VCLOUDPOINT VCLOUDPOINT VCLOUDPOINT VCLOUDPOINT	OK Cancel
Days since last Gearch results: lame (RDN) Performance Performance Power Users Remote Desk Replicator user 10	In Folder VCLOUDPOINT VCLOUDPOINT VCLOUDPOINT VCLOUDPOINT VCLOUDPOINT VCLOUDPOINT VCLOUDPOINT	OK Cancel
Days since last Gearch results: lame (RDN) Performance Performance Power Users Remote Desk Reolicator user10 user11	In Folder VCLOUDPOINT VCLOUDPOINT VCLOUDPOINT VCLOUDPOINT VCLOUDPOINT VCLOUDPOINT VCLOUDPOINT VCLOUDPOINT VCLOUDPOINT	OK Cancel
Days since last Search results: lame (RDN) Performance Performance Performance Remote Desk Replicator user1 user1 user11 user12	In Folder VCLOUDPOINT VCLOUDPOINT VCLOUDPOINT VCLOUDPOINT VCLOUDPOINT VCLOUDPOINT VCLOUDPOINT VCLOUDPOINT VCLOUDPOINT VCLOUDPOINT	OK Cancel

√*cloudpoint*

5) On **Create Executable Rules,** select **Permission→ Deny**, confirm User or User Group then click **Next**.

Create Executable Rules	
Permissions	
Before You Begin Permissions Publisher Exceptions Name	Select the action to use and the user or group that this rule should apply to. An allow action permits affected files to run, while a deny action prevents affected files from running. Action: Action: Callow Deny User or group: VCLOUDPOINTDEMO\user1 Select
	More about rule permissions
	< Previous Next > Create Cancel

6) On Create Executable Rules, select Condition, select Path, click Next.







Path		Browse For Folder
Before You Begin Permissions Conditions Path Exceptions Name	Select the file or folder path that this rule should affect. If you specify a folder path underneath that path will be affected by the rule. Path: Browse Files Browse Folders	all Select a folder containing the necessary files.
		< Previous Next > Create Cancel

√*cloudpoint*

8) A denial rule has been added.



9) When User1 runs the file, a pop-up prompt message will appear.

C:\Prog	gram Files\2345Soft\HaoZip\HaoZip.exe	×
8	This program is blocked by group policy. For more information, contact yo administrator.	our system
		ОК

10) If you need to restrict some users, you can first create a user group, add these users to the user group, and then restrict the user group.

Remark 3: Enable Application Identity service in Windows 10/ Server 2016

In Windows 10/Server 2016, Application Identity service cannot be set automatic startup at the **Services** console but the **Registry**.

1) Run **regedit** with an administrator account to open the Registry Editor.

		^
	Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.	
<u>O</u> pen:	regedit	~

2) Find AppIDSvc, right click Start to modify the value

(HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\AppIDSvc)



www.vcloudpoint.com



3)	Modify the value to be	e 2 , press Enter.
----	------------------------	---------------------------

Edit DWORD (32-bi	t) Value X
Value name:	
Start	
Value data:	Base Hexadecimal Decimal
	OK Cancel

4) The configuration of Application Identity service automatic startup is done.