THREATLOCKER

Default Deny

Default Deny is a solution that enables only allowed applications to run on your machine. When the agent is first installed it catalogs all of the files and applications that exist on the machine and creates policies automatically based around this. This is known as ThreatLockers learning mode. From here each application is assessed against the list of policies to see if they match. If they do not match, they will hit ThreatLockers default deny policy and will not be able to run on your machine.

Default Deny has long been considered the gold standard in protecting businesses from known and unknown executables. Unlike antivirus, Default Deny puts you in control over what software, scripts, executables, and libraries can run on your endpoints and servers. This approach not only stops malicious software, but it also stops other unpermitted applications from running. This process greatly minimizes cyber threats and other rouge applications running on your network.

Default Deny:

Using the threatlocker solution, you are able to default deny any application from running on your machine that is not part of the allow list. This helps to mitigate and stop cyber attacks from happening across your device and network.

Firewall like application policies:

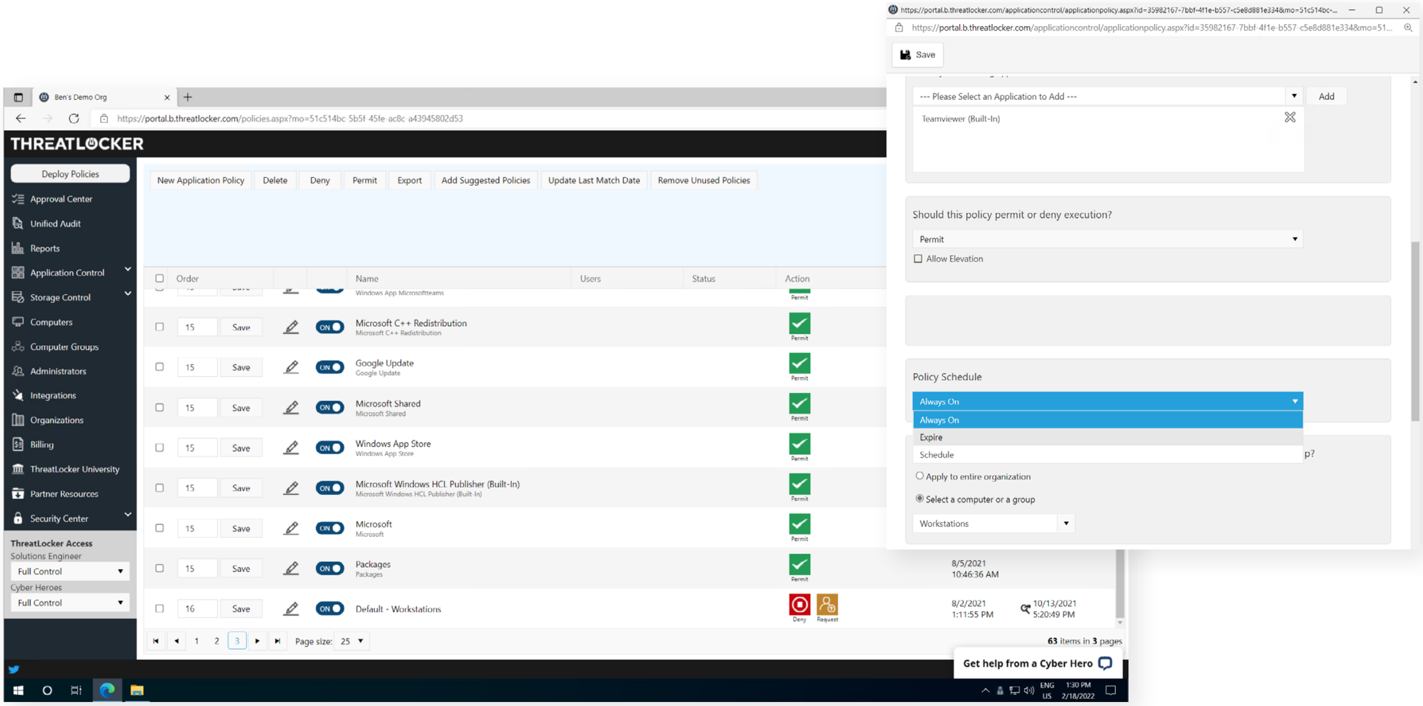
A powerful firewall like policy engine that allows you to permit, deny, or restrict application access at a granular level.

Time Based Policies:

Permit access to applications for a specified amount of time. Automatically block the application after the policy has expired.

Built-In Applications:

ThreatLocker automatically adds new hashes when application and system updates are released, allowing you to keep your applications up to date.



https://portal.b.threatlocker.com/policies.aspx?mo=51c514bc-5b5f-45fe-ac8c-a43945802d53

□	Order			Name	Users	Status	Action		
				Windows App Microsoftteams			Permit		
□	15	Save		ON	Microsoft C++ Redistribution Microsoft C++ Redistribution			✓ Permit		
□	15	Save		ON	Google Update Google Update			✓ Permit		
□	15	Save		ON	Microsoft Shared Microsoft Shared			✓ Permit		
□	15	Save		ON	Windows App Store Windows App Store			✓ Permit		
□	15	Save		ON	Microsoft Windows HCL Publisher (Built-In) Microsoft Windows HCL Publisher (Built-In)			✓ Permit		
□	15	Save		ON	Microsoft Microsoft			✓ Permit		
□	15	Save		ON	Packages Packages			✓ Permit	8/5/2021 10:46:36 AM	
□	16	Save		ON	Default - Workstations			Deny Request	8/2/2021 1:11:55 PM	10/13/2021 5:20:49 PM

1 2 3 Page size: 25 — 63 items in 3 pages

ThreatLocker Access
Solutions Engineer: Full Control
Cyber Heroes: Full Control

https://portal.b.threatlocker.com/applicationcontrol/applicationpolicy.aspx?id=35982167-7bbf-4f1e-b557-c5e8d881e334&mo=51c514bc-...

--- Please Select an Application to Add ---

Teamviewer (Built-In)

Should this policy permit or deny execution?

Permit

□ Allow Elevation

Policy Schedule

Always On

- Always On
- Expire
- Schedule

○ Apply to entire organization

● Select a computer or a group

Workstations

Ringfencing

Controlling what software can run should be the first line of defense when it comes to better protecting yourself against malicious software. Ringfencing adds a second line of defense for applications that are permitted. First, by defining how applications can interact with each other, secondly, by controlling what resources applications can access, such as network, files, and registry. Ringfencing is an invaluable tool in the fight against fileless malware and software exploits.

When you first deploy Ringfencing, your machine will automatically be aligned with the default ThreatLocker policies. These policies are then automatically applied to a list of default applications such as Microsoft Office, Powershell and virtual meeting applications. The aim of the default policies is to provide a baseline level of protection for all networks. Each of these policies can easily be manipulated to fit any environment at any time. ThreatLockers team of dedicated Cyber Heroes are always on hand to support any requests, 24/7/365.

Mitigate against fileless malware:

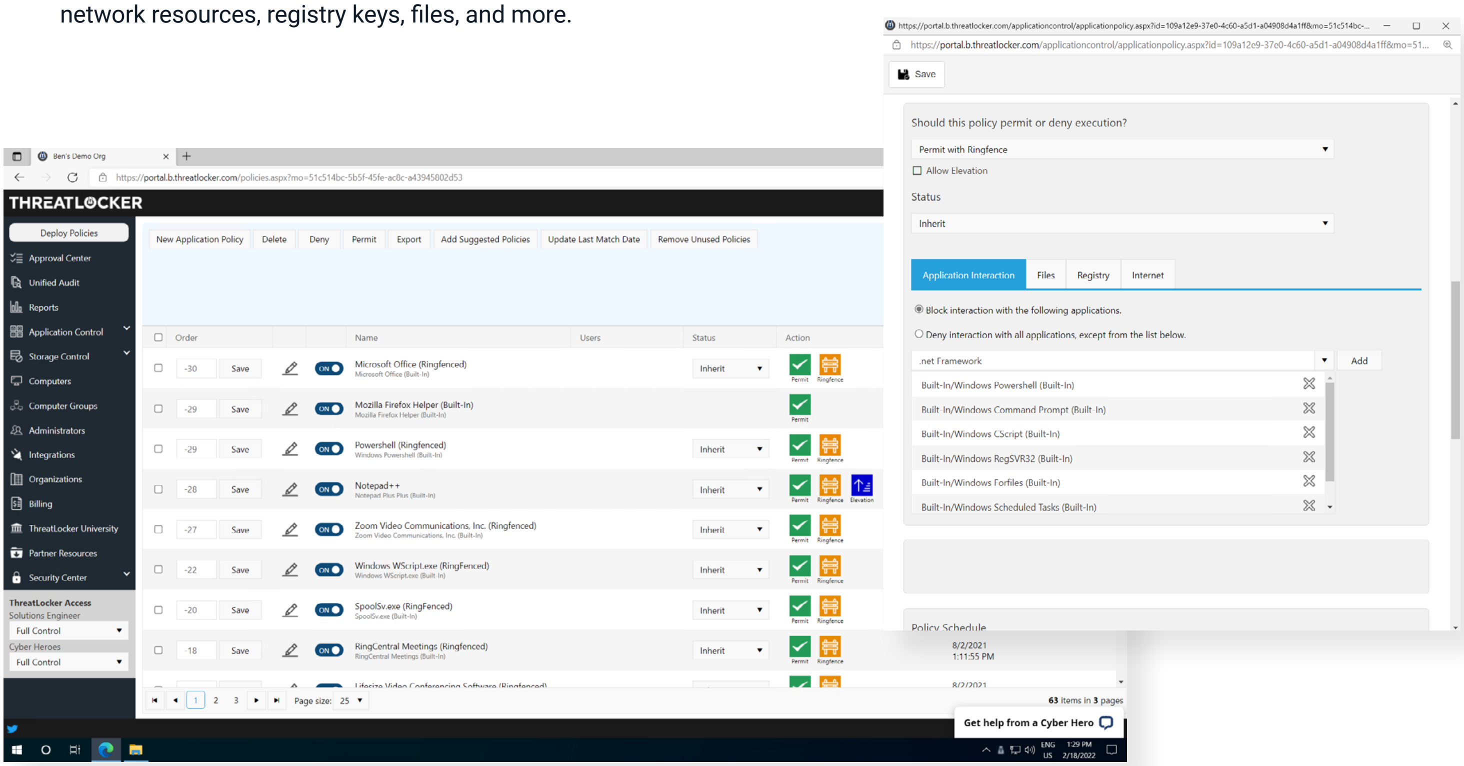
Stop fileless malware by limiting what applications are allowed to do.

Granular application policies:

Stop applications from interacting with other applications, network resources, registry keys, files, and more.

Limit application attacks:

Limit application attacks like application hopping by limiting what applications can access.



https://portal.b.threatlocker.com/policies.aspx?mo=51c514bc-5b5f-45fe-ac8c-a43945802d53

ThreatLocker Access
Solutions Engineer: Full Control
Cyber Heroes: Full Control

Order	Name	Users	Status	Action	
-30	Microsoft Office (Ringfenced) Microsoft Office (Built-In)		Inherit	Permit, Ringfence	
-29	Mozilla Firefox Helper (Built-In) Mozilla Firefox Helper (Built-In)			Permit	
-29	Powershell (Ringfenced) Windows Powershell (Built-In)		Inherit	Permit, Ringfence	
-28	Notepad++ Notepad Plus Plus (Built-In)		Inherit	Permit, Ringfence, Elevation	
-27	Zoom Video Communications, Inc. (Ringfenced) Zoom Video Communications, Inc. (Built-In)		Inherit	Permit, Ringfence	
-22	Windows WScript.exe (RingFenced) Windows WScript.exe (Built-In)		Inherit	Permit, Ringfence	
-20	SpoolSv.exe (RingFenced) SpoolSv.exe (Built-In)		Inherit	Permit, Ringfence	
-18	RingCentral Meetings (Ringfenced) RingCentral Meetings (Built-In)		Inherit	Permit, Ringfence	8/2/2021 1:11:55 PM
	Lifesize Video Conferencing Software (Ringfenced)			Permit, Ringfence	8/2/2021

Page 1 2 3 — Page size: 25 — **63** items in **3** pages

https://portal.b.threatlocker.com/applicationcontrol/applicationpolicy.aspx?id=109a12e9-37e0-4c60-a5d1-a04908d4a1ff&mo=51c514bc-...

Should this policy permit or deny execution?
Permit with Ringfence

☐ Allow Elevation

Status
Inherit

Application Interaction | Files | Registry | Internet

● Block interaction with the following applications.
○ Deny interaction with all applications, except from the list below.

.net Framework — Add

- Built-In/Windows Powershell (Built-In)
- Built-In/Windows Command Prompt (Built-In)
- Built-In/Windows CScript (Built-In)
- Built-In/Windows RegSVR32 (Built-In)
- Built-In/Windows Forfiles (Built-In)
- Built-In/Windows Scheduled Tasks (Built-In)

Policy Schedule

Elevation Control

When it comes to adding extra layers of security to your cyber security stack, it is important to always add a human layer. Users with admin access are often the weakest link across your network, so it is vital that their movements are monitored and tracked. ThreatLockers Elevation Control provides an additional layer of security by giving IT administrators the power to remove local admin privileges from their users, whilst allowing them to run individual applications as an administrator.

Elevation Control is easy to use, easy to implement, and will save you time and resources in the long run. Once you have implemented the ThreatLocker solution, the IT administrator can go through and choose specific applications for users to run as an administrator. Once this process has been set up the IT administrator can always edit the Elevation Control policy where needed.

Complete Visibility of Administrative Rights:

Gives you the ability to approve or deny an individual's access to specific applications within an organization even if the user is not a local administrator.

Streamlined Permission Requests:

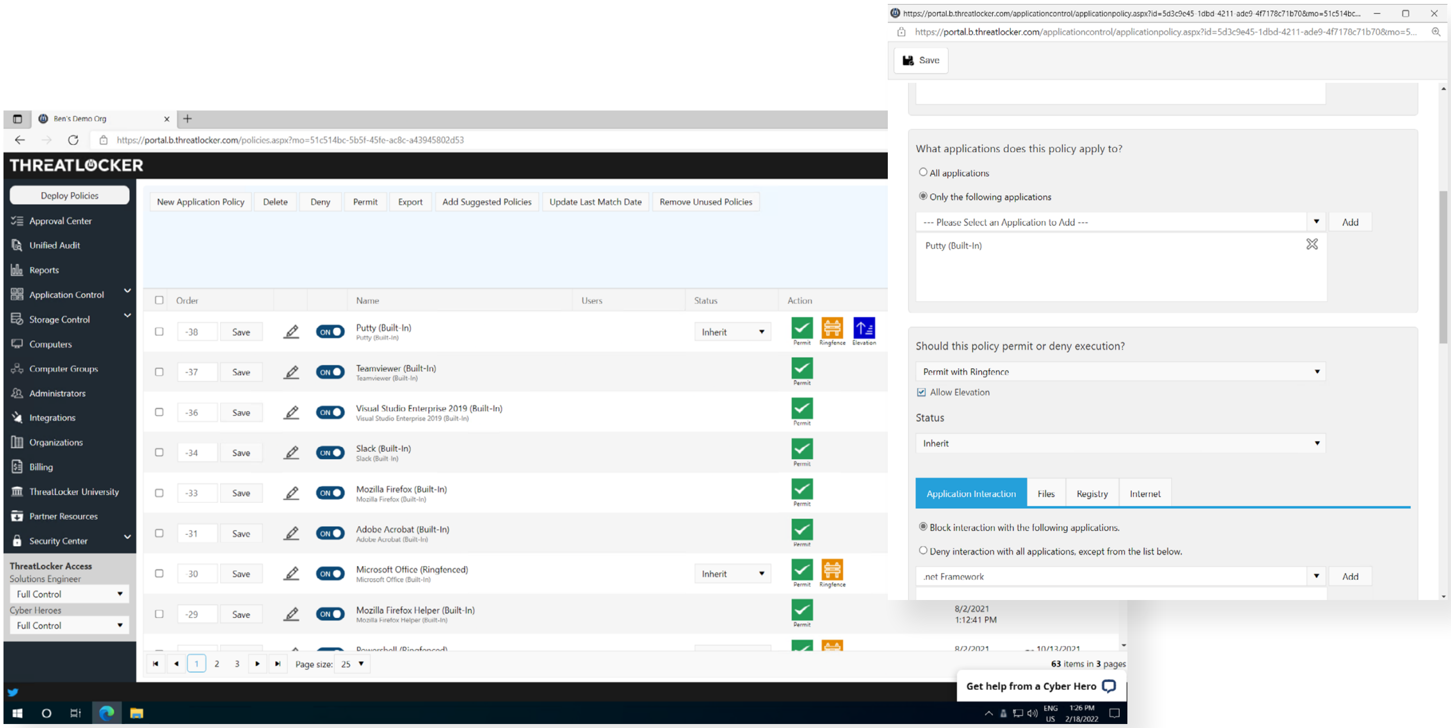
Users can request permission to elevate applications and attach files and notes to support their requests.

Varied Levels of Elevation:

Enables you to set durations for how long users are allowed access to specific applications by granting either temporary or permanent access.

Secure Application Integration

In combination with ThreatLocker Ringfencing™, ensures that once applications are elevated, users cannot jump to infiltrate connected applications within the network.



https://portal.b.threatlocker.com/policies.aspx?mo=51c514bc-5b5f-45fe-ac8c-a43945802d53

ThreatLocker Access
Solutions Engineer: Full Control
Cyber Heroes: Full Control

☐	Order			Name	Users	Status	Action
☐	-38	Save	ON	Putty (Built-In) Putty (Built-In)		Inherit	Permit, Ringfence, Elevation
☐	-37	Save	ON	Teamviewer (Built-In) Teamviewer (Built-In)			Permit
☐	-36	Save	ON	Visual Studio Enterprise 2019 (Built-In) Visual Studio Enterprise 2019 (Built-In)			Permit
☐	-34	Save	ON	Slack (Built-In) Slack (Built-In)			Permit
☐	-33	Save	ON	Mozilla Firefox (Built-In) Mozilla Firefox (Built-In)			Permit
☐	-31	Save	ON	Adobe Acrobat (Built-In) Adobe Acrobat (Built-In)			Permit
☐	-30	Save	ON	Microsoft Office (Ringfenced) Microsoft Office (Built-In)		Inherit	Permit, Ringfence
☐	-29	Save	ON	Mozilla Firefox Helper (Built-In) Mozilla Firefox Helper (Built-In)			Permit
				Powershell (Ringfenced)			Permit, Ringfence

1 2 3 Page size: 25

8/2/2021 1:12:41 PM
8/2/2021 10/13/2021
63 items in 3 pages

https://portal.b.threatlocker.com/applicationcontrol/applicationpolicy.aspx?id=5d3c9e45-1dbd-4211-ade9-4f7178c71b70&mo=51c514bc...

What applications does this policy apply to?

○ All applications
● Only the following applications

--- Please Select an Application to Add --- Add

Putty (Built-In)

Should this policy permit or deny execution?

Permit with Ringfence

☑ Allow Elevation

Status: Inherit

Application Interaction | Files | Registry | Internet

● Block interaction with the following applications.
○ Deny interaction with all applications, except from the list below.

.net Framework Add

Storage Control:

Most data protection programs on the market are butcher knife solutions to a problem that requires a scalpel. Blocking USB drives and encrypting data-storage servers can help secure your organization's private data, but these tools don't take into account that this data still needs to be utilized and quickly. Waiting for approval or trying to find a device that's allowed to access needed files can drain hours of productivity.

ThreatLocker® Storage Control is an advanced storage control solution that protects information. We give you the tools to control the flow and access of your data. This can be done in a variety of ways. You can control what USBs are permitted to be used   across your entire network, and you can choose what file and folder locations applications are allowed to access.

By using ThreatLocker®, you are in control of your file servers, USB drives, and your data which in turn will help you stay better protected against cyber threats.

Comprehensive Auditing:

A full audit of all file access on USB, Network and Local Hard Drives.

Granular access:

Restrict or deny access to external storage, including USB drives, network shares, or other devices.

Easy Approvals:

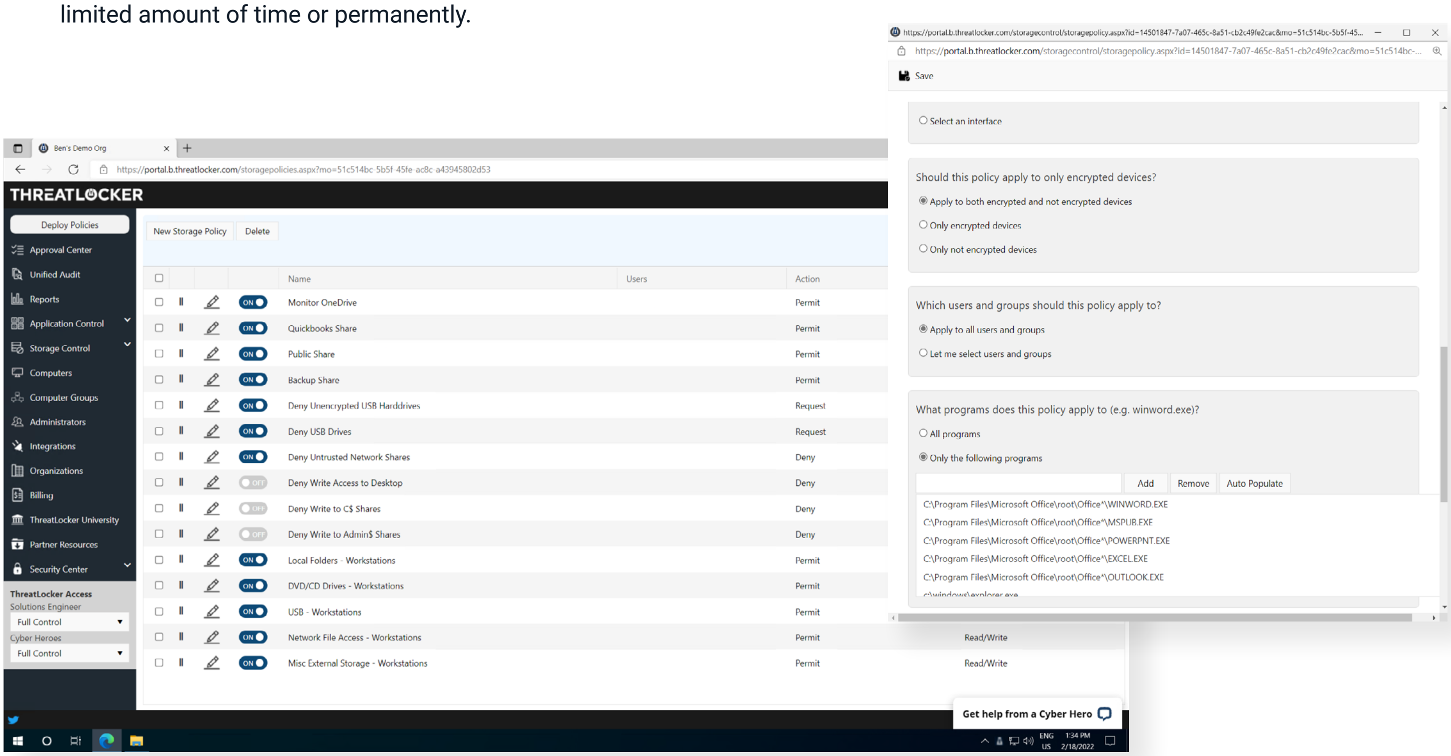
Single-click approval for specified devices or users for a limited amount of time or permanently.

Application file/folder Controls:

Limit access to a device or file share based on the application.

Total USB Control:

Enforce or audit the encryption status of USB hard drives and other external storage.



☐				Name	Users	Action	
☐	⏸	✎	ON	Monitor OneDrive		Permit	
☐	⏸	✎	ON	Quickbooks Share		Permit	
☐	⏸	✎	ON	Public Share		Permit	
☐	⏸	✎	ON	Backup Share		Permit	
☐	⏸	✎	ON	Deny Unencrypted USB Harddrives		Request	
☐	⏸	✎	ON	Deny USB Drives		Request	
☐	⏸	✎	ON	Deny Untrusted Network Shares		Deny	
☐	⏸	✎	OFF	Deny Write Access to Desktop		Deny	
☐	⏸	✎	OFF	Deny Write to C$ Shares		Deny	
☐	⏸	✎	OFF	Deny Write to Admin$ Shares		Deny	
☐	⏸	✎	ON	Local Folders - Workstations		Permit	
☐	⏸	✎	ON	DVD/CD Drives - Workstations		Permit	
☐	⏸	✎	ON	USB - Workstations		Permit	
☐	⏸	✎	ON	Network File Access - Workstations		Permit	Read/Write
☐	⏸	✎	ON	Misc External Storage - Workstations		Permit	Read/Write

https://portal.b.threatlocker.com/storagecontrol/storagepolicy.aspx?id=14501847-7a07-465c-8a51-cb2c49fe2cac&mo=51c514bc-5b5f-45...

Save

○ Select an interface

Should this policy apply to only encrypted devices?

● Apply to both encrypted and not encrypted devices
○ Only encrypted devices
○ Only not encrypted devices

Which users and groups should this policy apply to?

● Apply to all users and groups
○ Let me select users and groups

What programs does this policy apply to (e.g. winword.exe)?

○ All programs
● Only the following programs

Add | Remove | Auto Populate

C:\Program Files\Microsoft Office\root\Office*\WINWORD.EXE
C:\Program Files\Microsoft Office\root\Office*\MSPUB.EXE
C:\Program Files\Microsoft Office\root\Office*\POWERPNT.EXE
C:\Program Files\Microsoft Office\root\Office*\EXCEL.EXE
C:\Program Files\Microsoft Office\root\Office*\OUTLOOK.EXE
c:\windows\explorer.exe