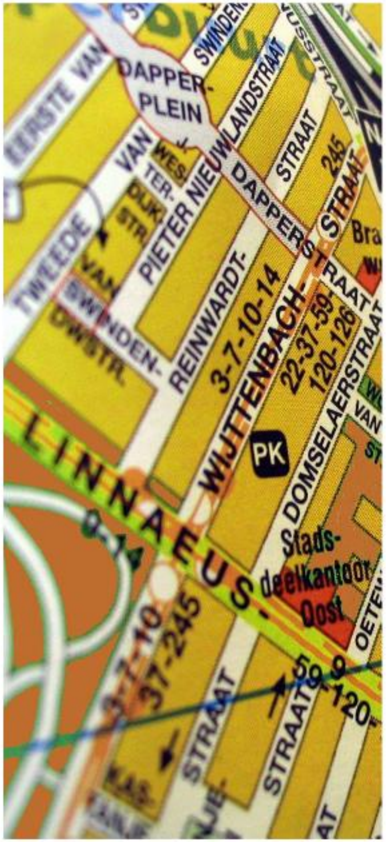
symantec.™

Confidence in a connected world.

Lesson 4

Configuring Application and Device Control Policies

Lesson Introduction



- Lesson 1: Introduction to Network Threat Protection and Application and Device Control
- Lesson 2: Configuring Firewall Policies
- Lesson 3: Managing Intrusion Prevention System Policies
- *Lesson 4: Configuring Application and Device Control Policies*
- Lesson 5: Customizing Network Threat Protection and Application and Device Control
- Lesson 6: Configuring Additional Protection
- Lesson 7: Monitoring and Reporting
- Lesson 8: Performing Server and Database Management
- Lesson 9: Installing Additional Management Components

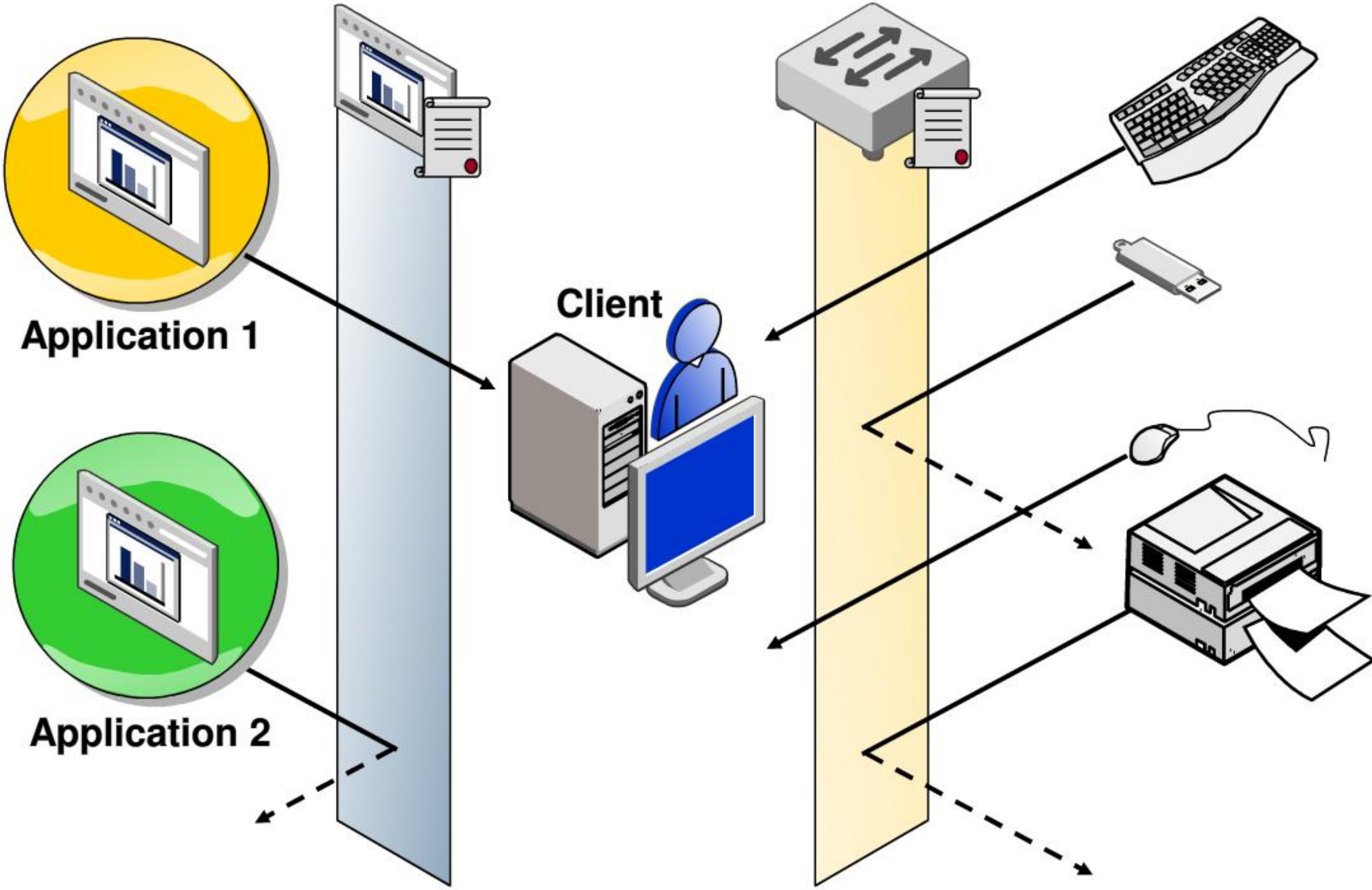
Lesson Topics and Objectives

Topic	After completing this lesson, you will be able to:
Creating Application and Device Control Policies	Describe application and device control policies.
Defining Application Control	Define application control settings.
Modifying Policy Rules	Add rule conditions with actions and change the rule order or rule set mode.
Defining Device Control	Define device control settings.

Topic 1: Creating Application and Device Control Policies

After completing this topic, you will be able to describe application and device control policies.

Application and Device Control Policies



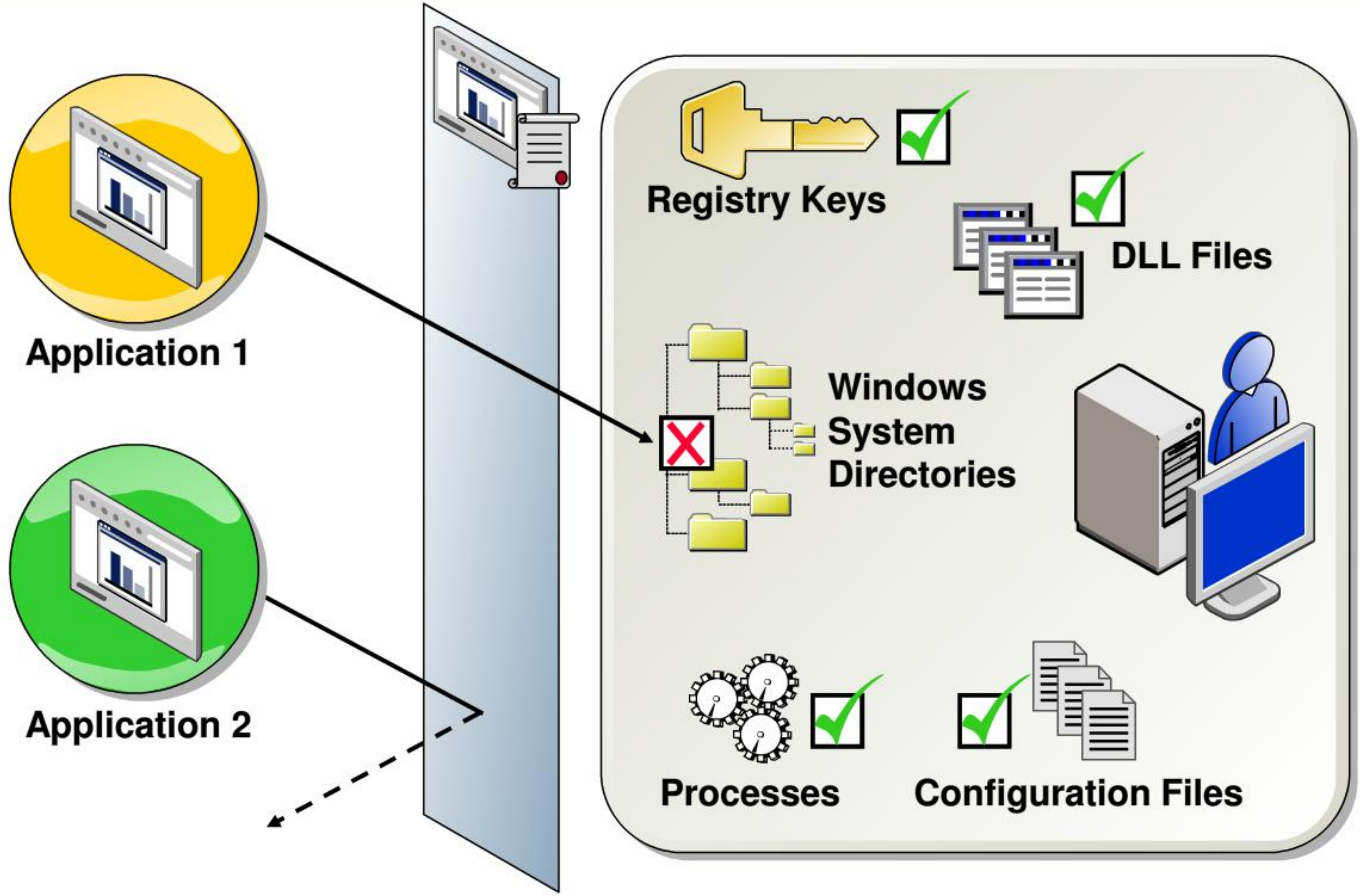
Creating a Policy

1. Create a new application and device control policy.
2. Create a rule set.
3. Define an application rule set.
4. Select processes to apply to, or exclude from, a rule set.
5. Define device control.

Topic 2: Defining Application Control

After completing this topic, you will be able to define Application Control.

Application Control



Creating a New Application and Device Control Policy

1 Create a new application and device control policy.

a Add an application and device control policy.

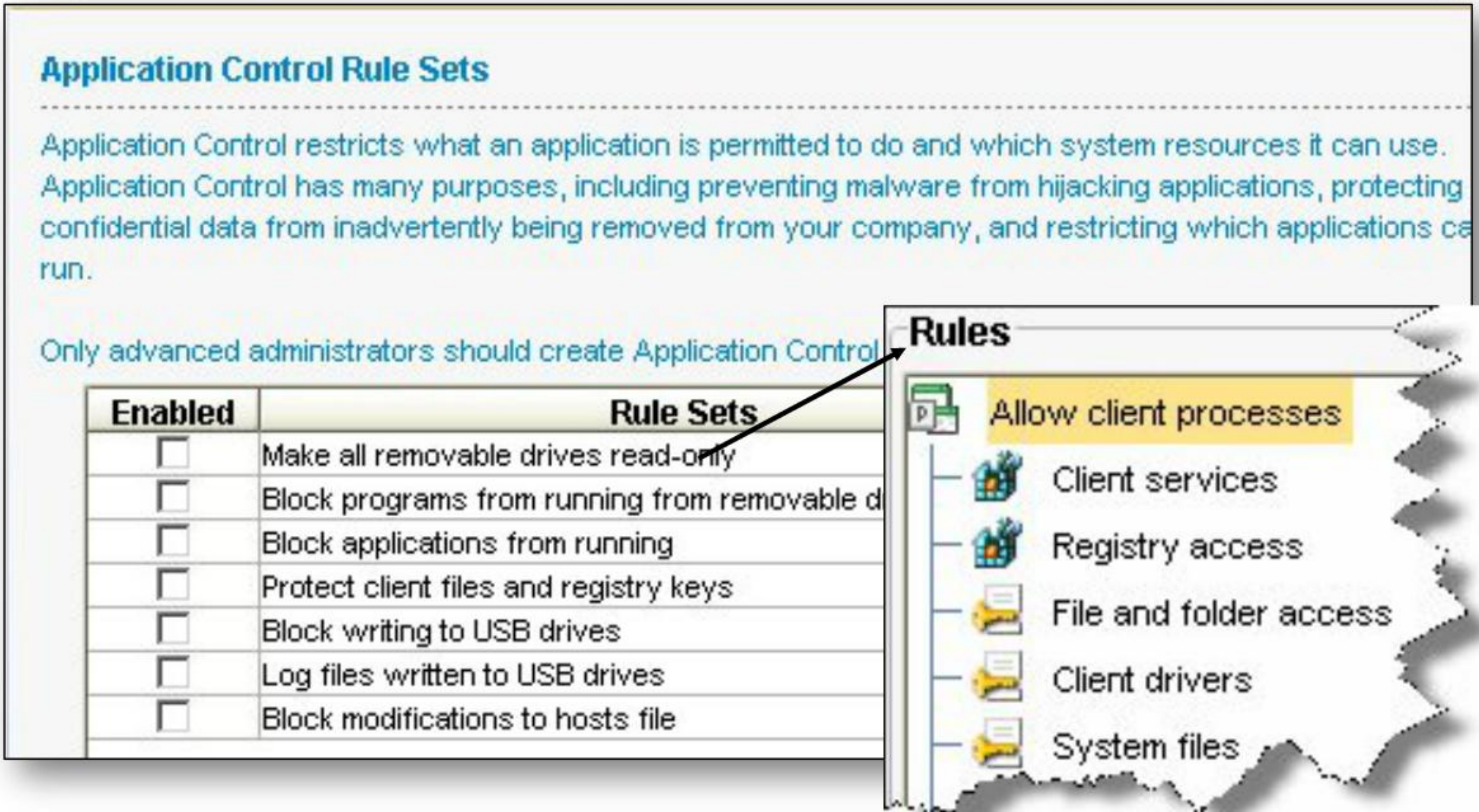
b Type the name and description.

c Enable the policy.

d Assign the policy.

Creating a Rule Set

2 Create a rule set.



Application Control Rule Sets

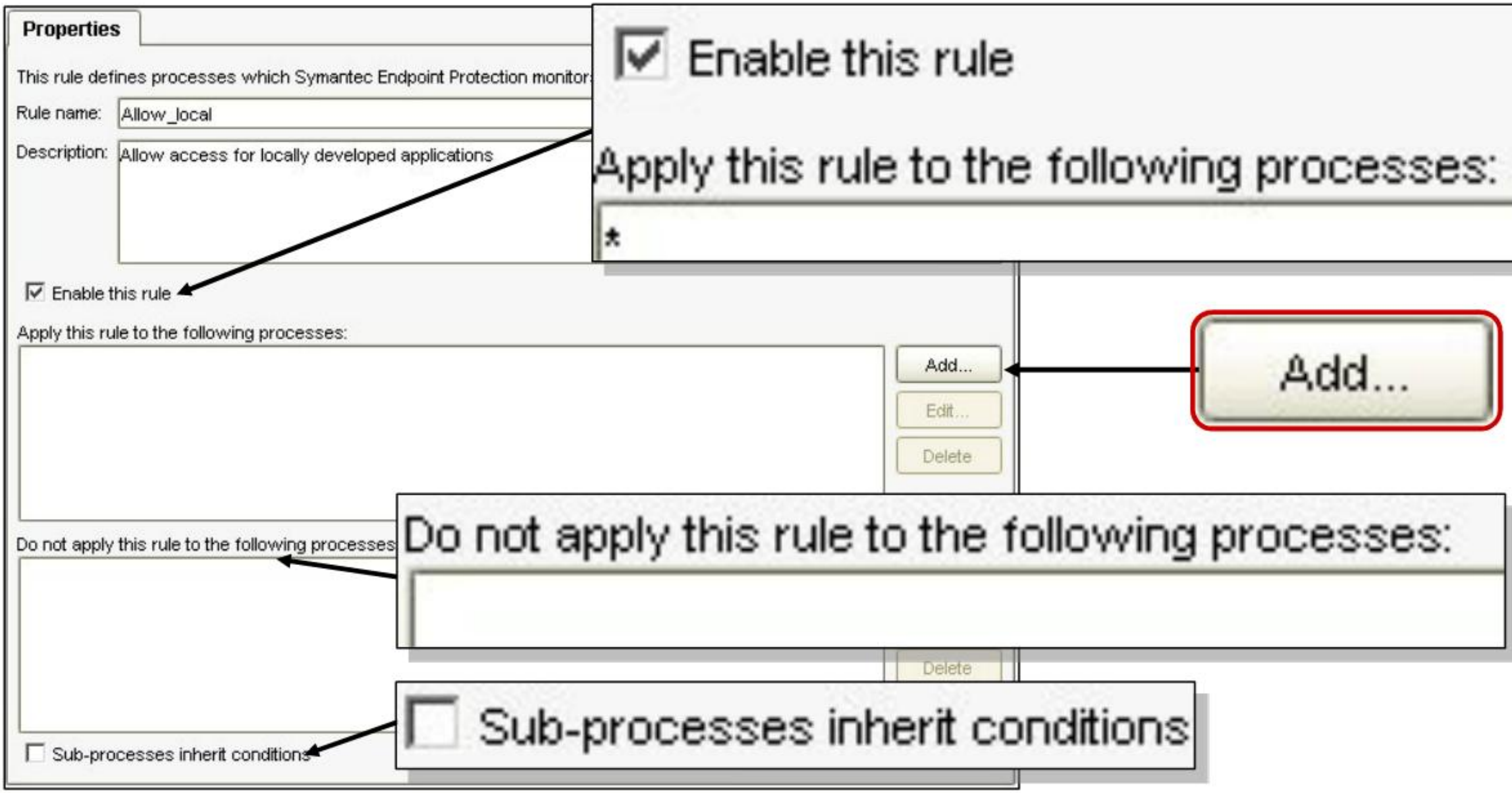
Application Control restricts what an application is permitted to do and which system resources it can use. Application Control has many purposes, including preventing malware from hijacking applications, protecting confidential data from inadvertently being removed from your company, and restricting which applications ca run.

Only advanced administrators should create Application Control

Enabled	Rule Sets
□	Make all removable drives read-only
□	Block programs from running from removable d
□	Block applications from running
□	Protect client files and registry keys
□	Block writing to USB drives
□	Log files written to USB drives
□	Block modifications to hosts file

Creating an Application Rule Set

3 Define an application rule set.



Properties

This rule defines processes which Symantec Endpoint Protection monitor

Rule name: Allow_local

Description: Allow access for locally developed applications

☑ Enable this rule

Apply this rule to the following processes:

Do not apply this rule to the following processes:

□ Sub-processes inherit conditions

☑ Enable this rule

Apply this rule to the following processes:

*

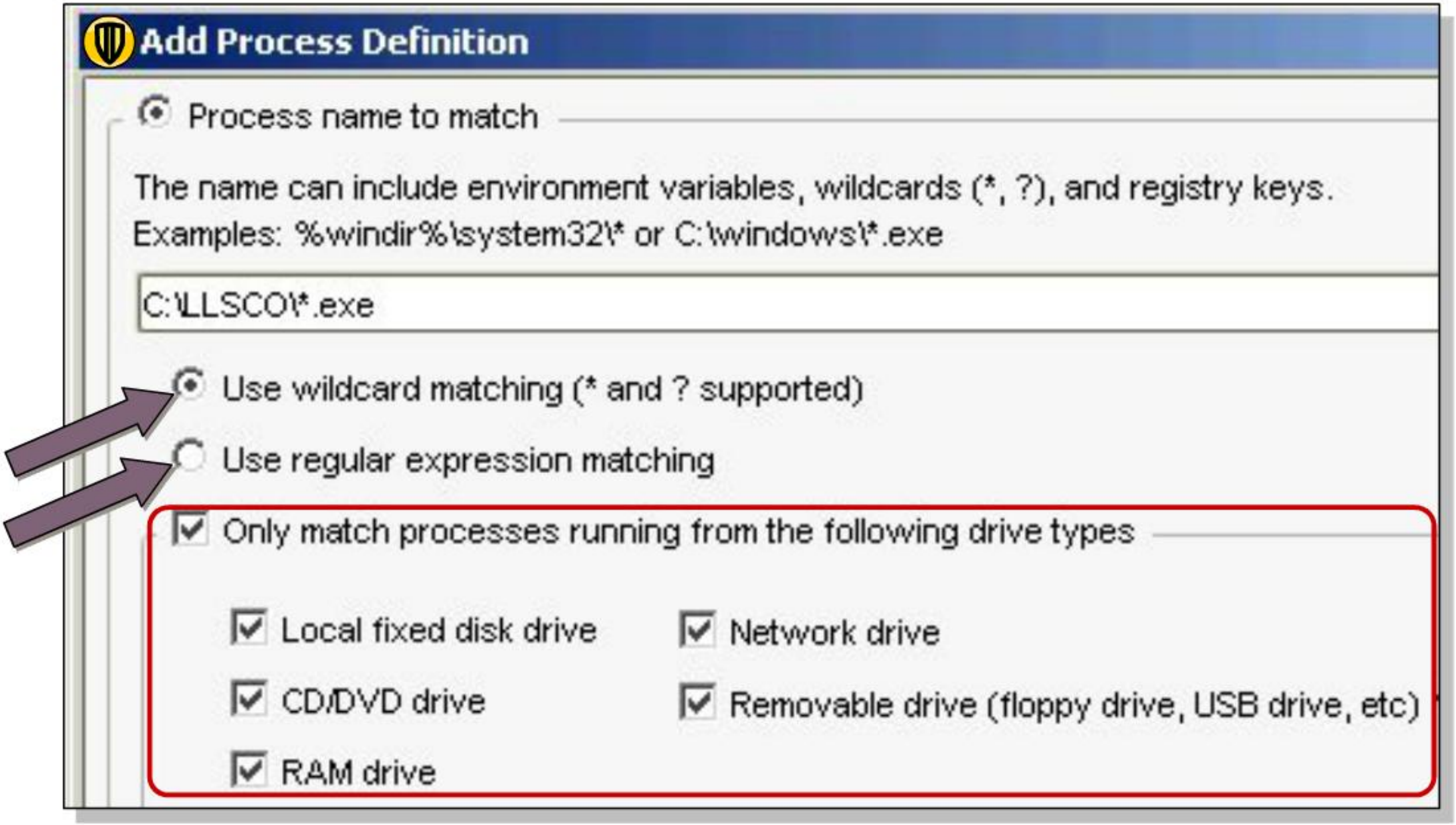
Add...

Do not apply this rule to the following processes:

□ Sub-processes inherit conditions

Selecting Processes

4 **Select processes to apply to, or exclude from, a rule set.**



Add Process Definition

● Process name to match

The name can include environment variables, wildcards (*, ?), and registry keys.
Examples: %windir%\system32\* or C:\windows\*.exe

C:\LLSCO\*.exe

● Use wildcard matching (* and ? supported)

○ Use regular expression matching

☑ Only match processes running from the following drive types

☑ Local fixed disk drive

☑ Network drive

☑ CD/DVD drive

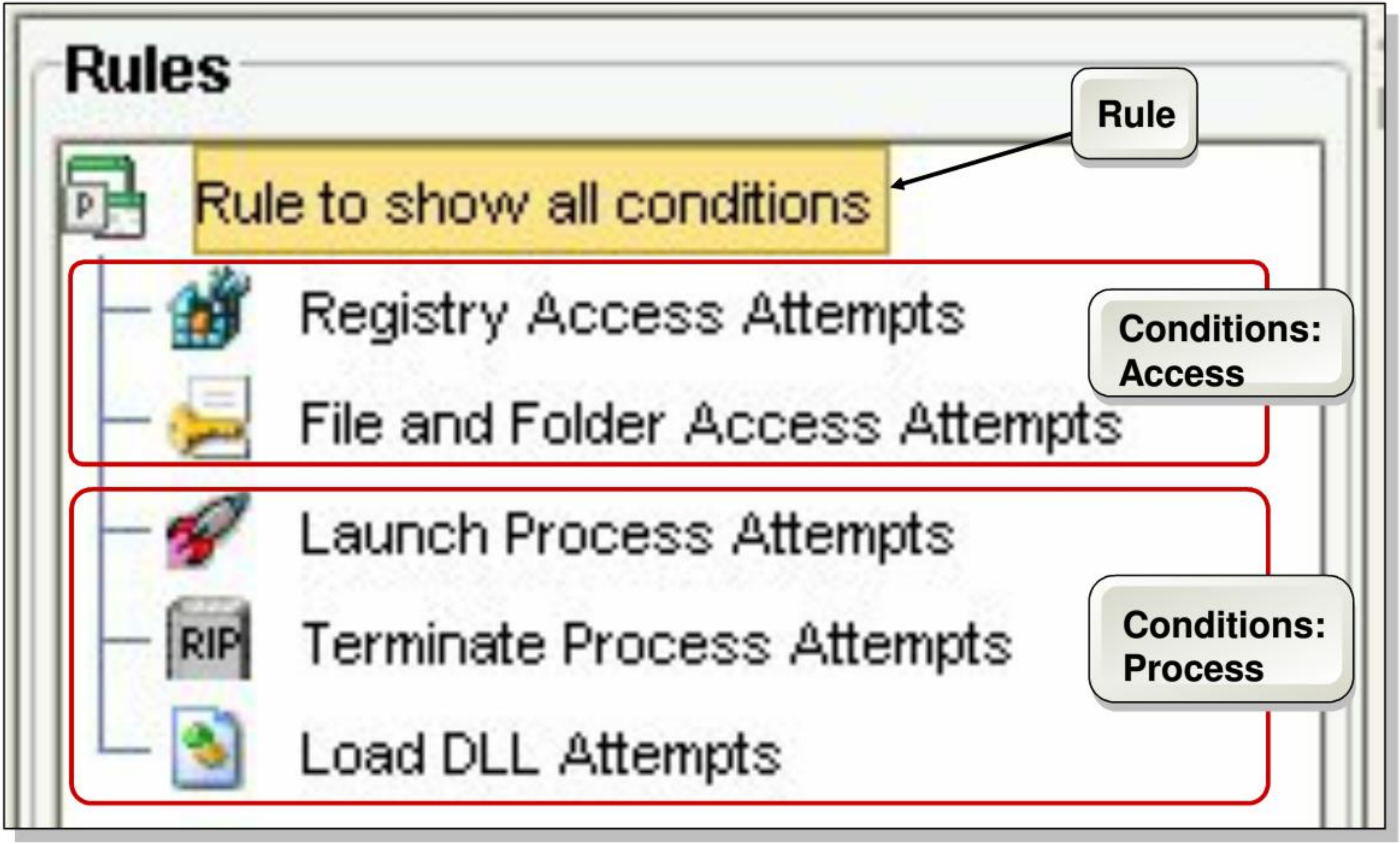
☑ Removable drive (floppy drive, USB drive, etc)

☑ RAM drive

Topic 3: Modifying Policy Rules

After completing this topic, you will be able to add rule conditions with actions and change the rule order or rule set mode.

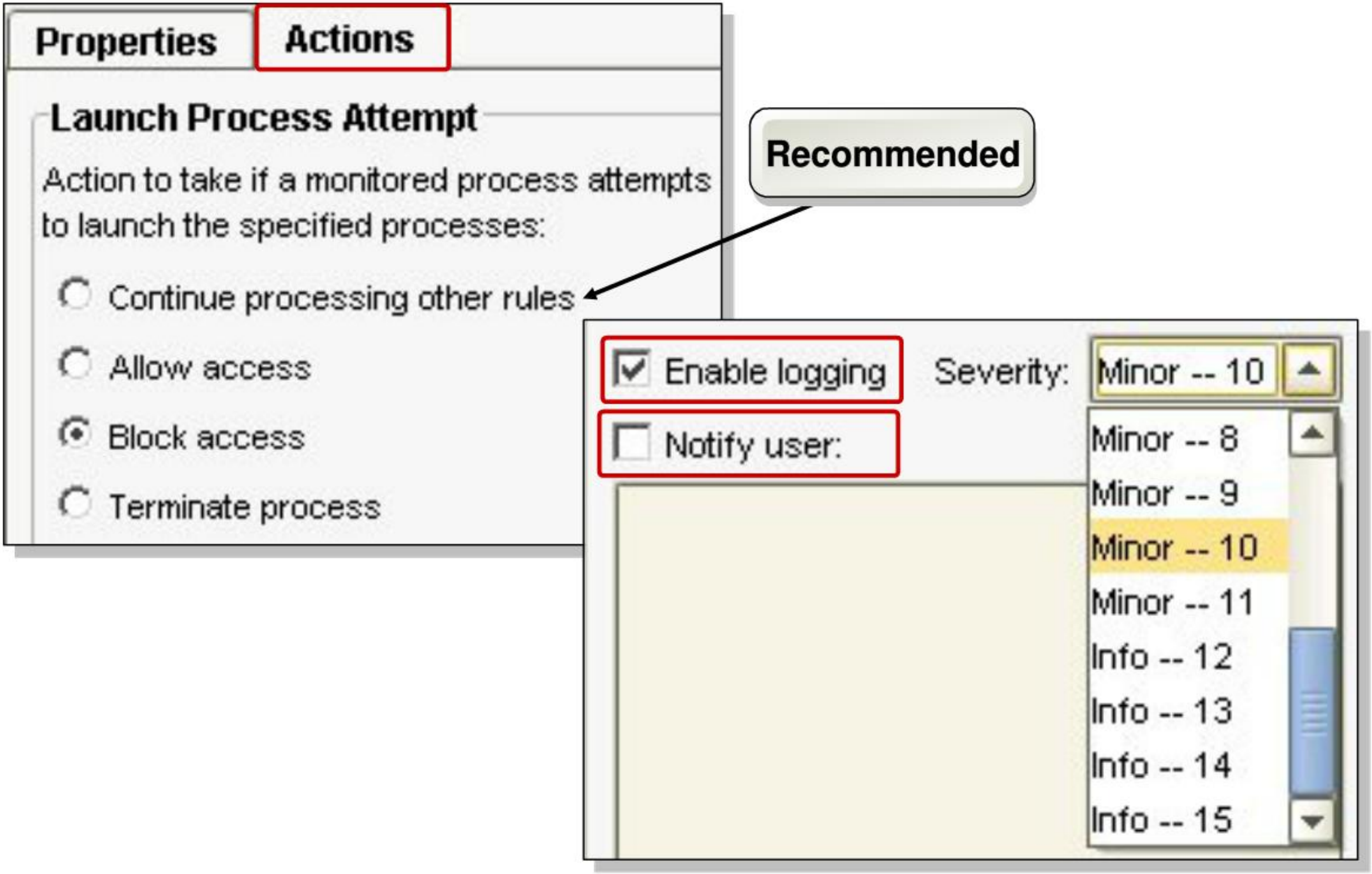
Adding Rule Conditions



Rules

- Rule to show all conditions
  - Registry Access Attempts
  - File and Folder Access Attempts
  - Launch Process Attempts
  - Terminate Process Attempts
  - Load DLL Attempts

Defining Rule Condition Actions: Process



Properties | Actions

Launch Process Attempt

Action to take if a monitored process attempts to launch the specified processes:

○ Continue processing other rules

○ Allow access

● Block access

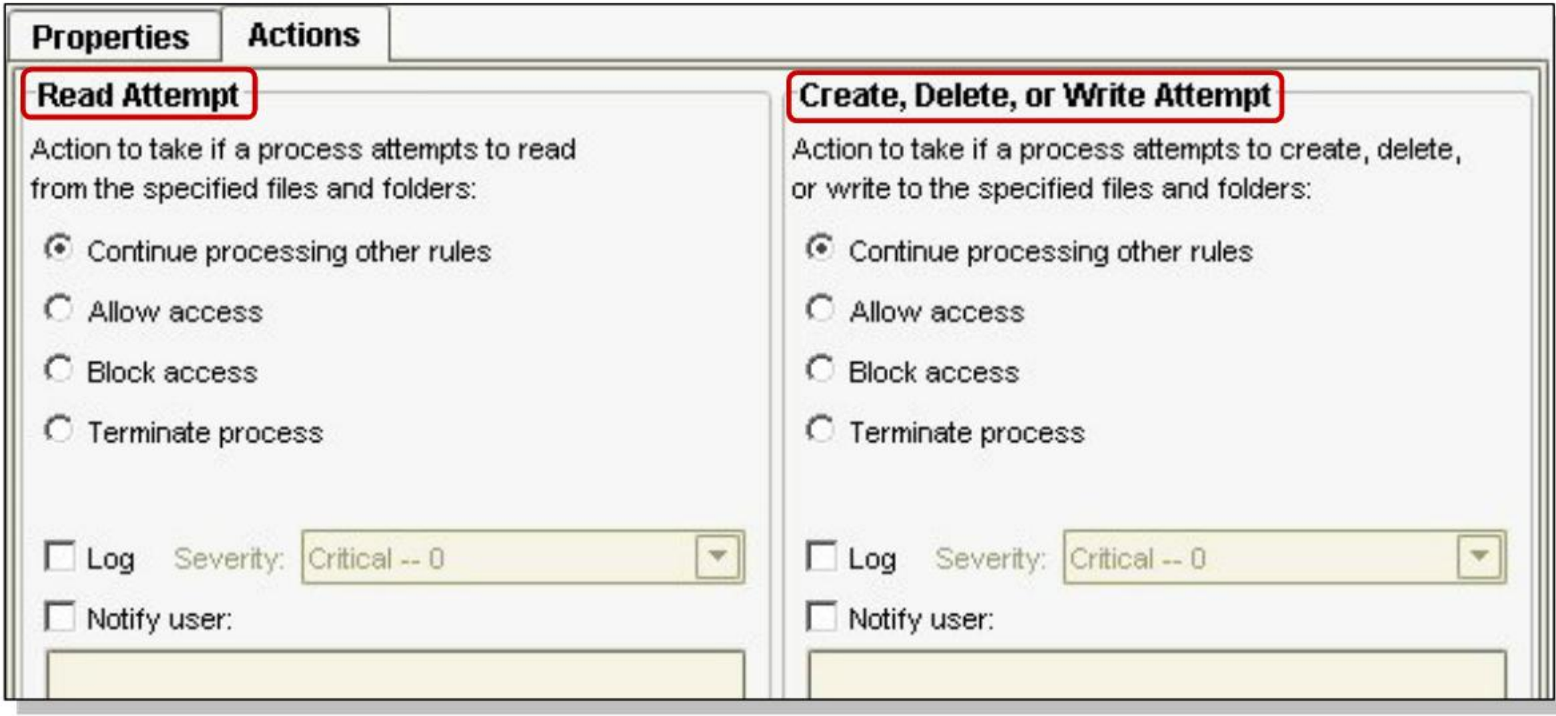
○ Terminate process

Recommended

☑ Enable logging Severity: Minor -- 10

□ Notify user:

Defining Rule Condition Actions: Access



Properties | Actions

Read Attempt

Action to take if a process attempts to read from the specified files and folders:

● Continue processing other rules

○ Allow access

○ Block access

○ Terminate process

□ Log Severity: Critical -- 0

□ Notify user:

Create, Delete, or Write Attempt

Action to take if a process attempts to create, delete, or write to the specified files and folders:

● Continue processing other rules

○ Allow access

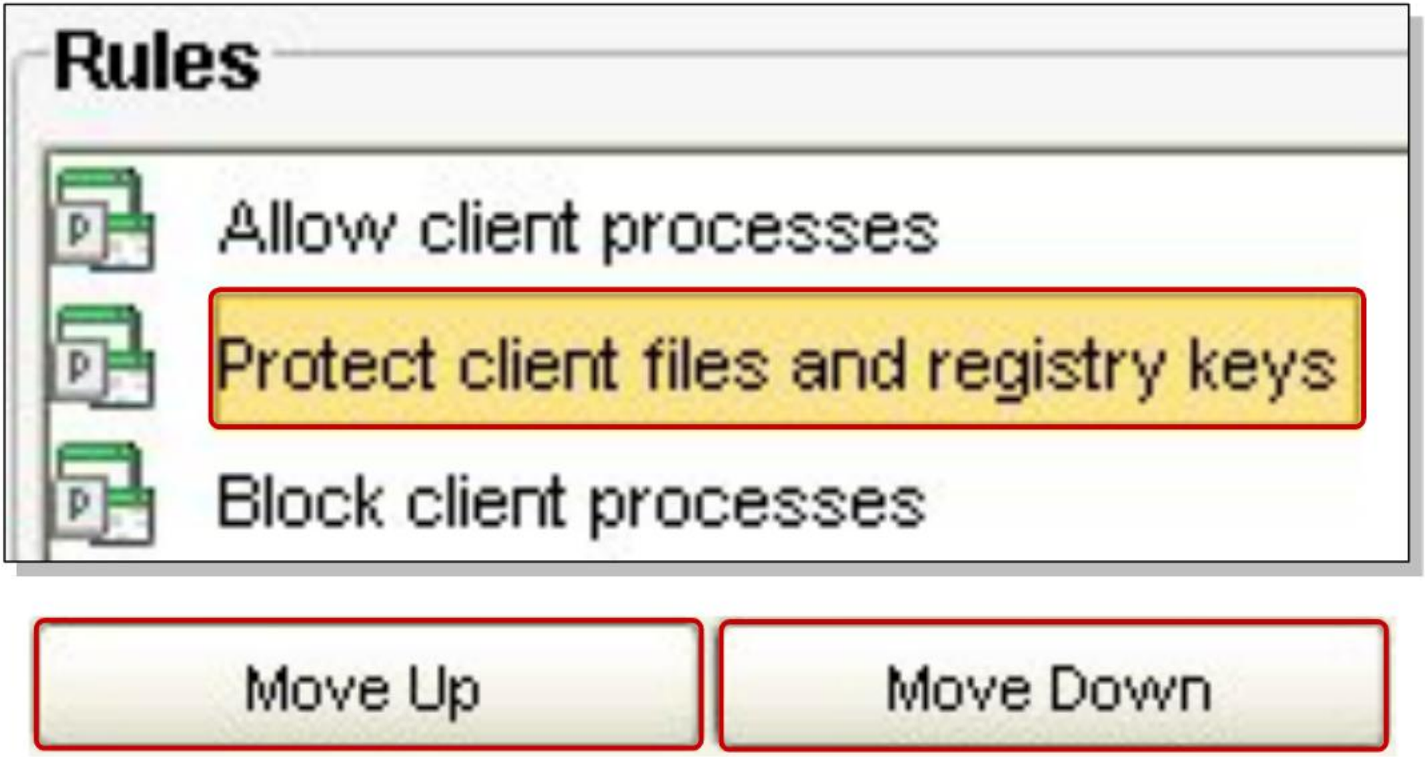
○ Block access

○ Terminate process

□ Log Severity: Critical -- 0

□ Notify user:

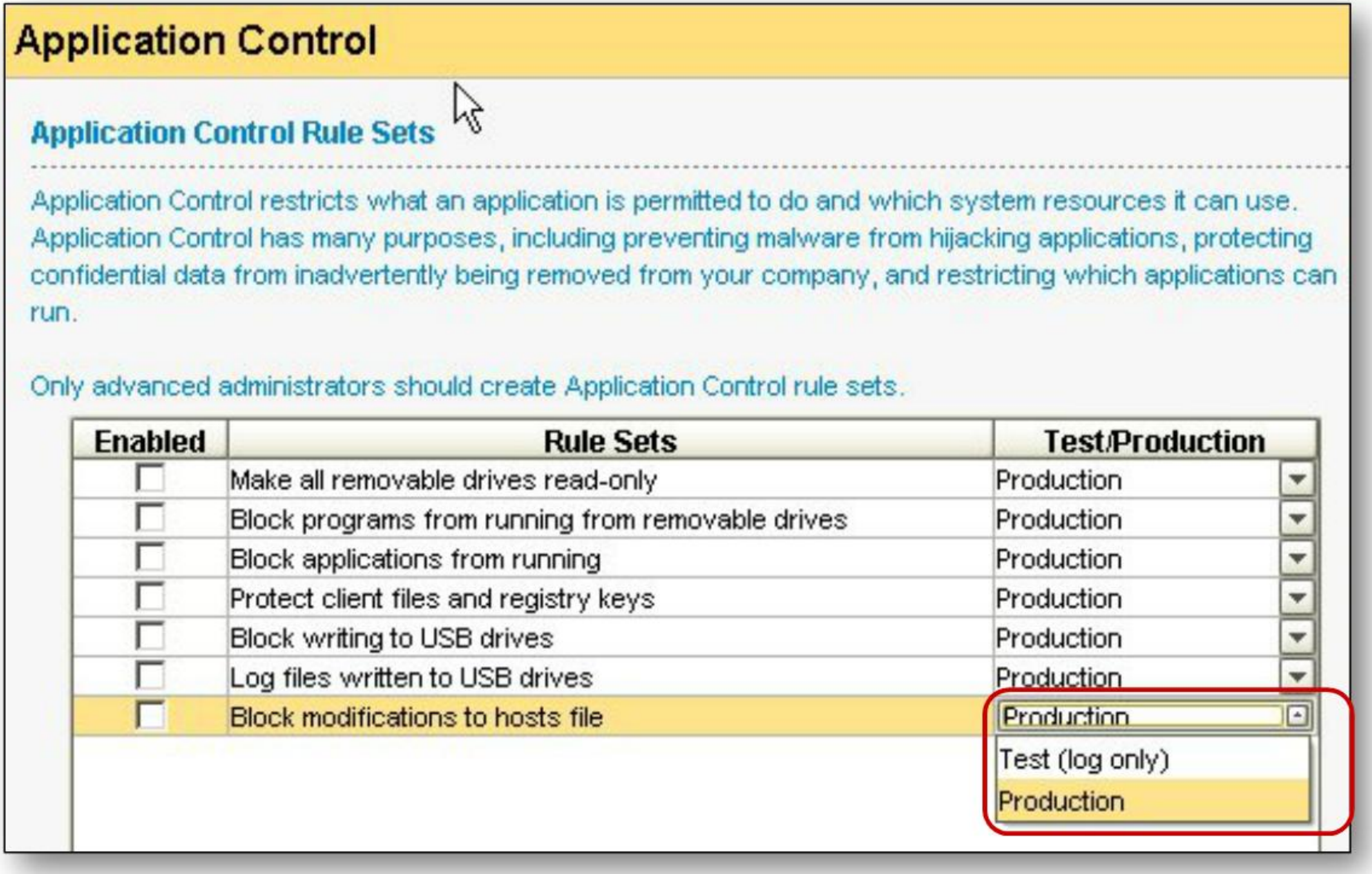
Changing the Rule Order



Rules

- Allow client processes
- Protect client files and registry keys
- Block client processes

Setting the Rule Set Mode



Application Control

Application Control Rule Sets

Application Control restricts what an application is permitted to do and which system resources it can use. Application Control has many purposes, including preventing malware from hijacking applications, protecting confidential data from inadvertently being removed from your company, and restricting which applications can run.

Only advanced administrators should create Application Control rule sets.

Enabled	Rule Sets	Test/Production
□	Make all removable drives read-only	Production
□	Block programs from running from removable drives	Production
□	Block applications from running	Production
□	Protect client files and registry keys	Production
□	Block writing to USB drives	Production
□	Log files written to USB drives	Production
□	Block modifications to hosts file	Production

Topic 4: Defining Device Control

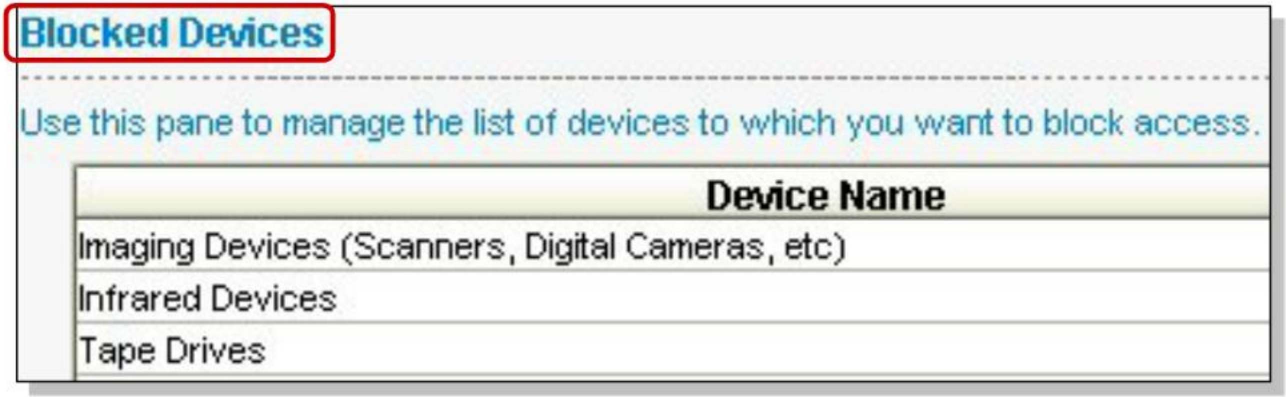
After completing this topic, you will be able to define device control.

Topic 4: Defining Device Control

After completing this topic, you will be able to define device control.

Defining Device Control

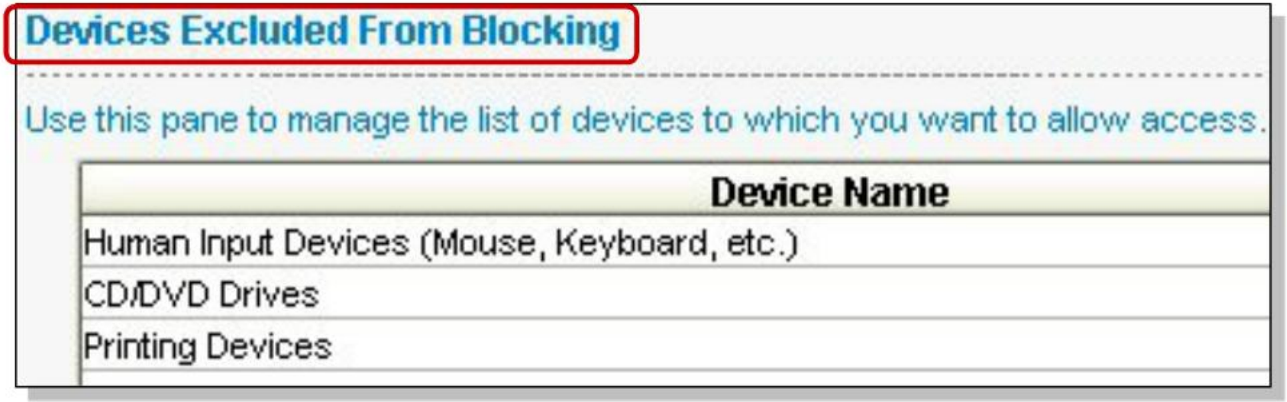
5 Define device control.



Blocked Devices

Use this pane to manage the list of devices to which you want to block access.

Device Name
Imaging Devices (Scanners, Digital Cameras, etc)
Infrared Devices
Tape Drives

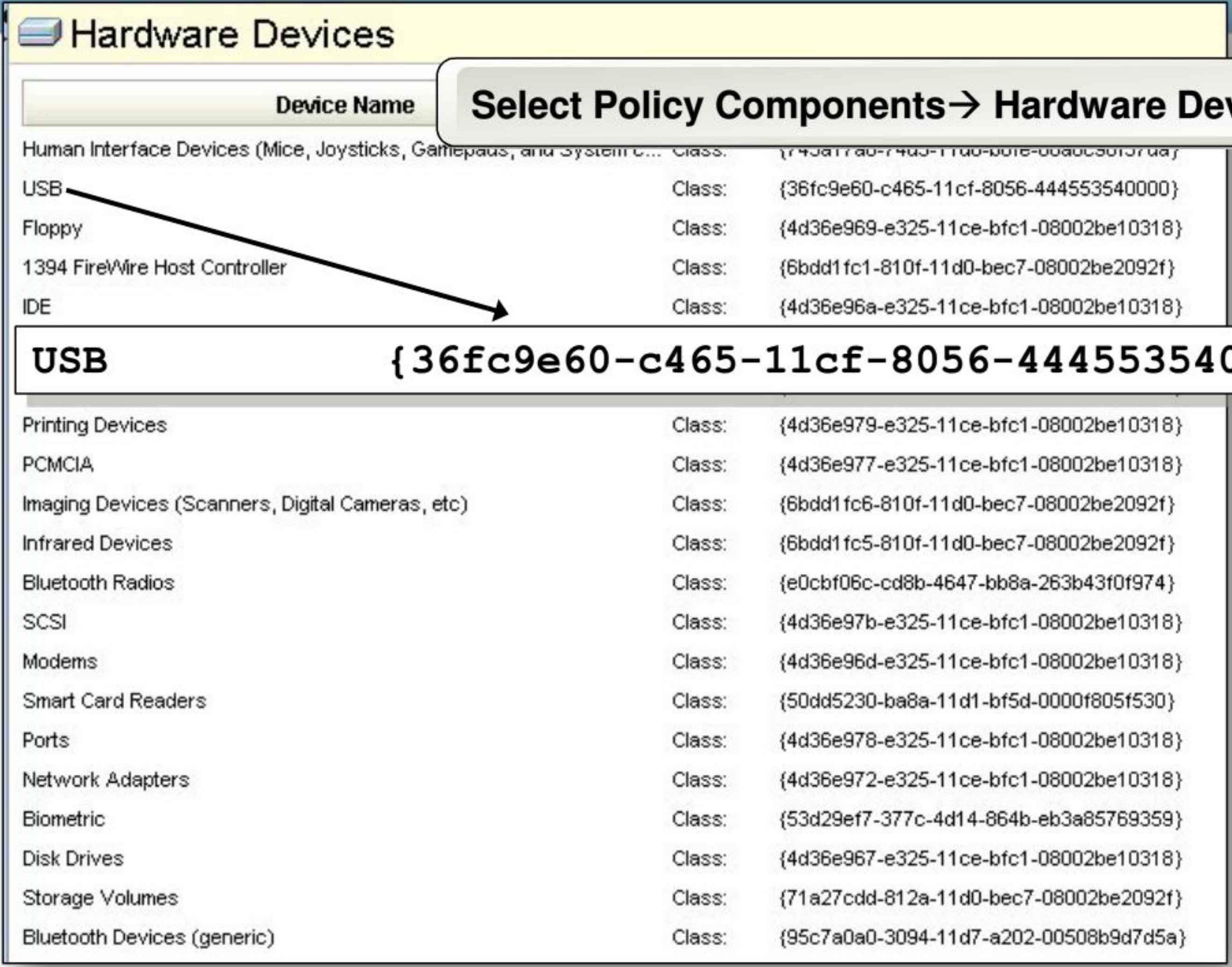


Devices Excluded From Blocking

Use this pane to manage the list of devices to which you want to allow access.

Device Name
Human Input Devices (Mouse, Keyboard, etc.)
CD/DVD Drives
Printing Devices

Defining Hardware Devices



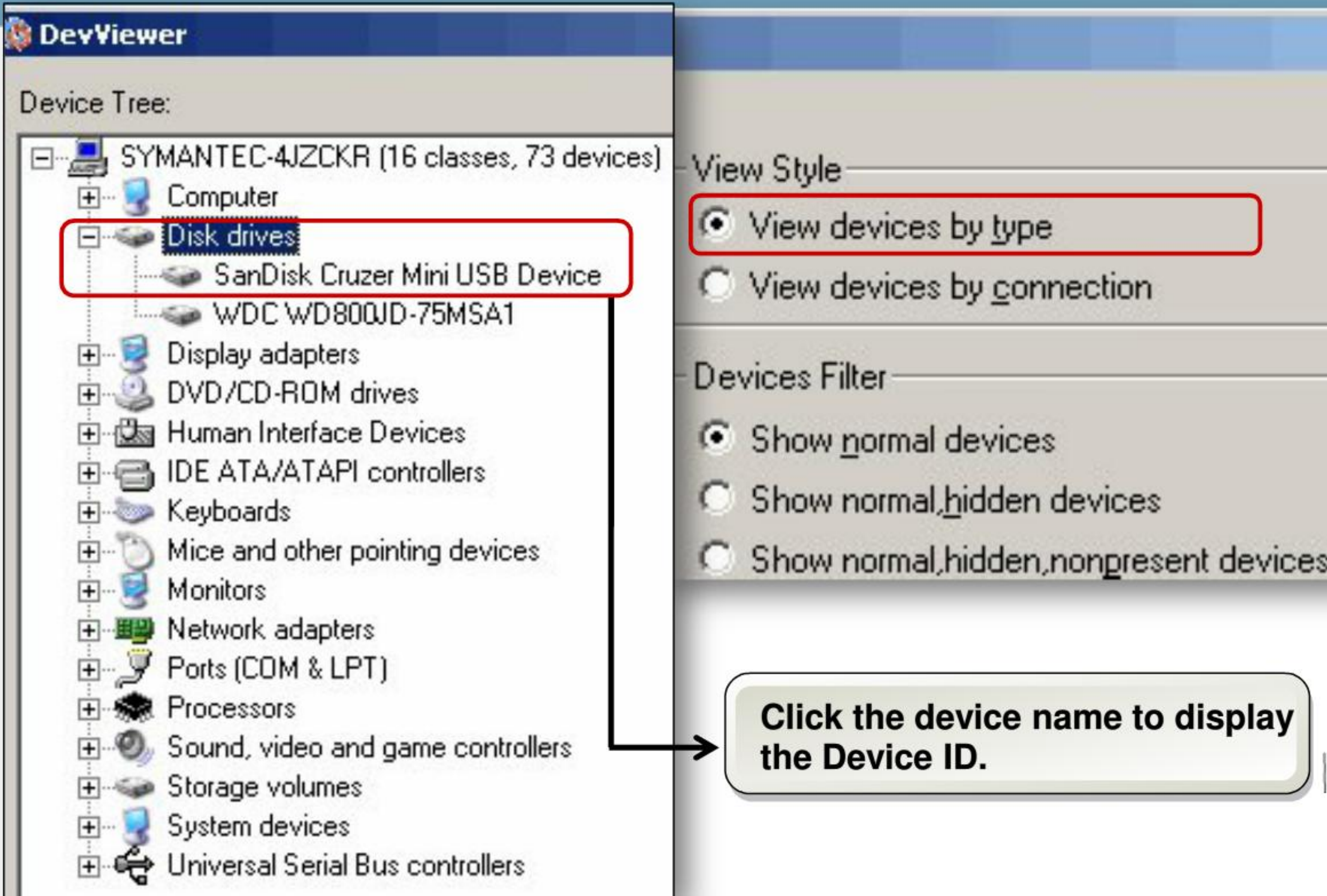
Hardware Devices

Select Policy Components→ Hardware Devices.

Device Name		
Human Interface Devices (Mice, Joysticks, Gamepads, and System c...	Class:	{745a17a0-74d3-11d0-b6fe-00a0c90f57da}
USB	Class:	{36fc9e60-c465-11cf-8056-444553540000}
Floppy	Class:	{4d36e969-e325-11ce-bfc1-08002be10318}
1394 FireWire Host Controller	Class:	{6bdd1fc1-810f-11d0-bec7-08002be2092f}
IDE	Class:	{4d36e96a-e325-11ce-bfc1-08002be10318}
Printing Devices	Class:	{4d36e979-e325-11ce-bfc1-08002be10318}
PCMCIA	Class:	{4d36e977-e325-11ce-bfc1-08002be10318}
Imaging Devices (Scanners, Digital Cameras, etc)	Class:	{6bdd1fc6-810f-11d0-bec7-08002be2092f}
Infrared Devices	Class:	{6bdd1fc5-810f-11d0-bec7-08002be2092f}
Bluetooth Radios	Class:	{e0cbf06c-cd8b-4647-bb8a-263b43f0f974}
SCSI	Class:	{4d36e97b-e325-11ce-bfc1-08002be10318}
Modems	Class:	{4d36e96d-e325-11ce-bfc1-08002be10318}
Smart Card Readers	Class:	{50dd5230-ba8a-11d1-bf5d-0000f805f530}
Ports	Class:	{4d36e978-e325-11ce-bfc1-08002be10318}
Network Adapters	Class:	{4d36e972-e325-11ce-bfc1-08002be10318}
Biometric	Class:	{53d29ef7-377c-4d14-864b-eb3a85769359}
Disk Drives	Class:	{4d36e967-e325-11ce-bfc1-08002be10318}
Storage Volumes	Class:	{71a27cdd-812a-11d0-bec7-08002be2092f}
Bluetooth Devices (generic)	Class:	{95c7a0a0-3094-11d7-a202-00508b9d7d5a}

```
USB          {36fc9e60-c465-11cf-8056-444553540000}
```

Locating the Device ID (`DevViewer.exe`)



DevViewer

Device Tree:

- SYMANTEC-4JZCKR (16 classes, 73 devices)
  - Computer
  - Disk drives
    - SanDisk Cruzer Mini USB Device
    - WDC WD800JD-75MSA1
  - Display adapters
  - DVD/CD-ROM drives
  - Human Interface Devices
  - IDE ATA/ATAPI controllers
  - Keyboards
  - Mice and other pointing devices
  - Monitors
  - Network adapters
  - Ports (COM & LPT)
  - Processors
  - Sound, video and game controllers
  - Storage volumes
  - System devices
  - Universal Serial Bus controllers

View Style

● View devices by type

○ View devices by connection

Devices Filter

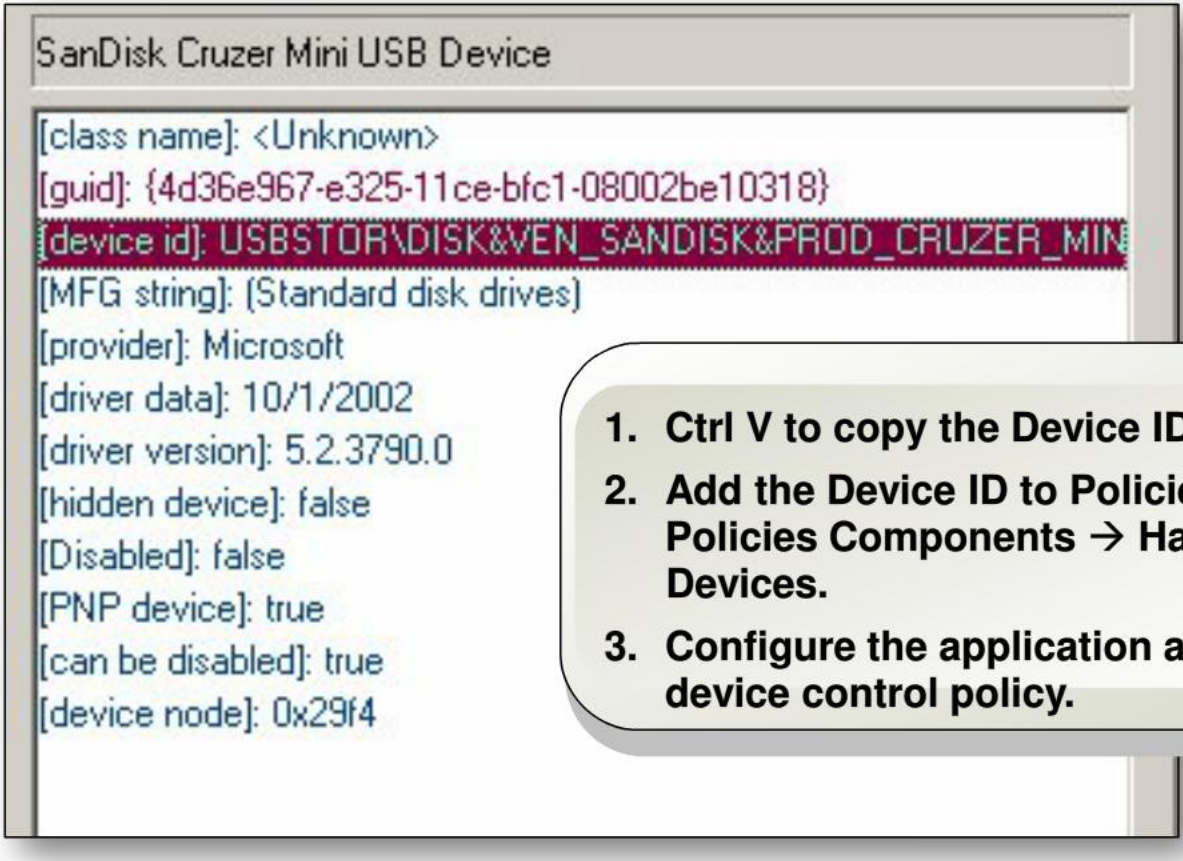
● Show normal devices

○ Show normal,hidden devices

○ Show normal,hidden,nonpresent devices

Click the device name to display the Device ID.

Adding the Device



```
SanDisk Cruzer Mini USB Device

[class name]: <Unknown>
[guid]: {4d36e967-e325-11ce-bfc1-08002be10318}
[device id]: USBSTOR\DISK&VEN_SANDISK&PROD_CRUZER_MIN
[MFG string]: (Standard disk drives)
[provider]: Microsoft
[driver data]: 10/1/2002
[driver version]: 5.2.3790.0
[hidden device]: false
[Disabled]: false
[PNP device]: true
[can be disabled]: true
[device node]: 0x29f4
```

1. **Ctrl V to copy the Device ID.**
2. **Add the Device ID to Policies → Policies Components → Hardware Devices.**
3. **Configure the application and device control policy.**

Lesson Summary

- **Key Points**
  - **In this lesson, you learned how to create application and device control policies.**
  - **You also learned how to modify application and device control policy rules.**
- **Reference Materials**

  Administration Guide for Symantec Endpoint Protection and Symantec Network Access Control

Lab 4: Configuring Application and Device Control Policies

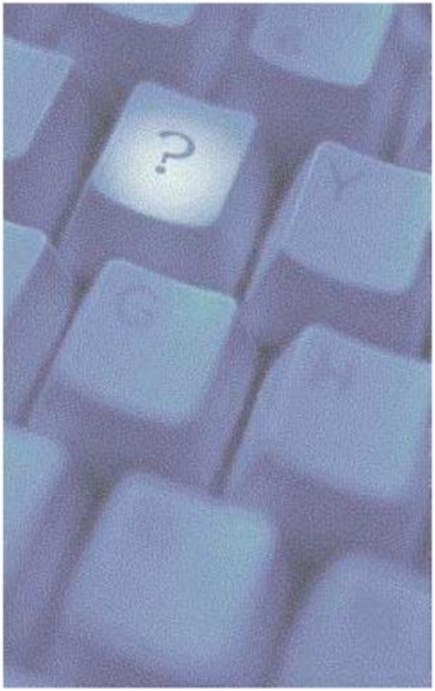
symantec.

In this lab, you:

- Create an application and device control policy.
- Test an application and device control policy.

- For Lab Details, see Appendix A.
- For Lab Solutions, see Appendix B.

What Did You Learn?



- You are about to be asked a series of questions related to the current topic.
- Read and try to answer each question.
- Click Answer at the bottom of the slide to view the correct answer.

Question 1

Creating an Application and Device Control policy includes all of the following steps, except:

A. Creating a new policy.

B. Defining an application rule set.

C. Defining a management server list.

D. Defining device control.

Answer

Answer 1

Creating an Application and Device Control policy includes all of the following steps, except:

A. Creating a new policy.

B. Defining an application rule set.

C. Defining a management server list.

D. Defining device control.

The correct answer is C. To create an Application and Device Control policy:

1. Create a new policy
2. Create a rule set.
3. Define an application rule set.
4. Select processes to apply or exclude.
5. Define device control.

Next >>

Question 2

A rule set defines:

A. The group a rule applies to.
B. The multiple rules within a policy.
C. What hardware devices are used in a rule.
D. The set of signatures applied to a rule.

Answer

Answer 2

A rule set defines:

A. The group a rule applies to.

B. The multiple rules within a policy.

C. What hardware devices are used in a rule.

D. The set of signatures applied to a rule.

The correct answer is B. A rule set defines a grouping of multiple rules within a policy.

Next >>

Question 3

symantec.

When defining rule conditions, you also define:

A. Hardware devices.
B. Rule order.
C. Rule set mode.
D. Actions for those conditions.

Answer

Answer 3

symantec.

When defining rule conditions, you also define:

A. Hardware devices.

B. Rule order.

C. Rule set mode.

D. Actions for those conditions.

The correct answer is D. When adding rule conditions, you then define the actions to take for the defined condition.

Next >>

Question 4

symantec.

Which of the following is true of the default Hardware Devices list?

A. Each device has only one device ID.

B. There is no default device list supplied.

C. The list is used only for devices connected to SEPMs.

D. No Device IDs can be added.

Answer

Answer 4

Which of the following is true of the default Hardware Devices list?

A. Each device has only one device ID.

B. There is no default device list supplied.

C. The list is used only for devices connected to SEPMs.

D. No Device IDs can be added.

The correct answer is A. There is a single device ID for each hardware device on the Symantec supplied default list. Additional devices can be added using device IDs from the:

- Registries of computers where devices are connected
- Internet
- Third-party tools

symantec™