opentext™

ZENworks
Endpoint Security Policies Reference

Legal Notice

For information about legal notices, trademarks, disclaimers, warranties, export and other use restrictions, U.S. Government rights, patent policy, and FIPS compliance, see https://www.microfocus.com/about/legal/.

© Copyright 2008 - 2024 Open Text

The only warranties for products and services of Open Text and its affiliates and licensors ("Open Text") are as may be set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Open Text shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Contents

About This Guide **7**

1 Concepts **9**

About Security and Configuration Policies . . . 9
Types of Security Policies . . . 9
How Network Locations Operate . . . 11
How User, Device, and Zone Policy Assignments Operate . . . 12
How the Effective Policy is Determined . . . 13
How Policy Precedence is Ordered . . . 13
Policy Merging Explained . . . 17
Policy Versioning . . . 19
Session Support . . . 19
Security Policy Summary . . . 20

2 Policy Deployment **23**

Deployment Best Practices . . . 23
Creating Security Policies . . . 26
Testing Security Policies . . . 27
Designate Test Devices . . . 27
Assign Policies to Test Devices . . . 27
Assigning Security Policies . . . 28
Assign Policies to Users . . . 28
Assign Policies to Devices . . . 29
Assign Policies to the Management Zone . . . 30
Viewing Effective Policies . . . 31

3 Policy Management **33**

Editing a Policy's Details . . . 33
Defining a Policy's System Requirements . . . 34
Configure Filter Conditions . . . 34
Define Filter Logic . . . 38
Publishing Policies . . . 39
Republish an Old Version . . . 39
Publish a Sandbox Version . . . 40
Renaming, Copying, and Moving Policies . . . 40
Rename a Policy . . . 40
Copy a Policy . . . 40
Move a Policy . . . 41
Enabling and Disabling Policies . . . 41
Disable a Policy . . . 41
Enable a Policy . . . 41
Replicating Policies to Content Servers . . . 42
Importing and Exporting Policies . . . 43

Export a Policy . . . 43
Import a Policy . . . 44
Managing Policy Groups . . . 44
Create Policy Groups . . . 44
Add Policies to Existing Groups . . . 45
Rename Policy Groups . . . 46
Move Policy Groups . . . 46
Delete Policy Groups . . . 46

4 Policy Removal 47

Removal Best Practices . . . 47
Removing Policy Assignments From Users and Devices . . . 48
Remove Multiple Policy Assignments From the Same Object . . . 48
Remove a Single Policy Assignment From Multiple Objects . . . 48
Removing Policy Assignments From the Management Zone . . . 49
Deleting Policies . . . 49
Deleting Versions of a Policy . . . 49

5 Policy Settings 51

Application Control Policy . . . 51
Configure Application Control Settings . . . 52
Communication Hardware Policy . . . 58
Configure Communication Hardware Settings . . . 58
Disable Adapter Bridging Control Settings . . . 59
Firewall Policy . . . 60
Configure the Default Behavior . . . 60
Disable Windows Firewall and Register Endpoint Security Management Firewall in Windows Security Center . . . 61
Configure Port/Protocol Rules . . . 61
Configure Standard Access Control Lists . . . 63
Create Custom Access Control Lists . . . 64
Location Assignment Policy . . . 67
Inherit from Policy Hierarchy . . . 67
Manage Allowed Locations . . . 69
Microsoft Data Encryption Policy . . . 70
General Information . . . 70
Removable Data Drives . . . 71
Fixed Disk Folders . . . 73
Scripting Policy . . . 75
Define Script Settings . . . 75
Define Trigger Settings . . . 76
Security Settings Policy . . . 78
Enable Client Self Defense for Endpoint Security Agent . . . 79
Enable Uninstall Password for Endpoint Security Agent . . . 79
Enable Password Override for Endpoint Security Agent . . . 79
Storage Device Control Policy . . . 80
Configure AutoPlay/AutoRun . . . 80
Configure Removable Storage Device Access . . . 81
USB Connectivity Policy . . . 85
Configure USB Devices . . . 86
Choose the Default Device Access . . . 86

Configure Device Group Access Settings 86
Configure USB Device Access Settings 87
VPN Enforcement Policy 90
Understanding the VPN Enforcement Policy 91
Configure Trigger Locations 95
Configure VPN Traffic. 97
Configure Pre-VPN Location 98
Configure VPN Location 99
Wi-Fi Policy 99
Configure General Settings 99
Define Access Points 100
Configure Minimum Security 102
Define the Minimum Security Message. 102

6 Data Encryption Key Management 103

About Data Encryption Keys. 103
Active Key 103
Multiple Zones 103
Key Security 104
Generating a New Encryption Key 104
Exporting Encryption Keys 104
Importing Encryption Keys 105

A Naming Conventions in ZENworks Control Center 107

B Troubleshooting Endpoint Security 109

Recovering Data in Folders Encrypted by the Microsoft Data Encryption Policy. 109
Other Troubleshooting Scenarios 110

About This Guide

This *ZENworks Endpoint Security Policies Reference* provides information to help you create, manage, and publish security policies.

Audience

This guide is written for the ZENworks Endpoint Security Management administrators.

Feedback

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the User Comments feature at the bottom of each page of the online documentation.

Additional Documentation

ZENworks Endpoint Security Management is supported by other documentation (in both PDF and HTML formats) that you can use to learn about and implement the product. For additional documentation, see the ZENworks documentation website.

1 Concepts

ZENworks Endpoint Security Management secures and protects Windows workstation devices from security risks regardless of their location. This protection is provided through security policies that you create and assign to workstation devices and users.

These sections provide an overview of security policy concepts that you need to understand to successfully protect your managed workstation devices.

- "About Security and Configuration Policies" on page 9
- "Types of Security Policies" on page 9
- "How Network Locations Operate" on page 11
- "How User, Device, and Zone Policy Assignments Operate" on page 12
- "How the Effective Policy is Determined" on page 13
- "Policy Versioning" on page 19
- "Session Support" on page 19
- "Security Policy Summary" on page 20

About Security and Configuration Policies

ZENworks includes three categories of policies: Windows security policies, Windows configuration policies, and Linux configuration policies. The security policies control security-related functionality for Windows workstation devices. The configuration policies control configuration settings for Windows and Linux devices.

ZENworks Endpoint Security Management uses all 11 security policies but only 3 of the configuration policies: Dynamic Local User policy, Windows Group policy, and ZENworks Explorer Configuration policy.

This guide helps you manage the security policies. For information about managing the configuration policies, see the *ZENworks Configuration Policies Reference*.

Types of Security Policies

There are 13 security policies that control a range of security-related functionality for Windows workstation devices. You can use all or some of the policies, depending on your organization's needs.

Policy	Purpose
Antimalware Enforcement	Installs the Antimalware Agent and configures the base on-access and on-demand scans that protect managed devices from malware threats. Because it is the base policy and installs the agent, it must be assigned to devices before any optional policies (Custom Scan Policy, Network Scan Policy, and Scan Exclusions Policy) can be assigned and enforced.

Policy	Purpose
Antimalware Custom Scan	Defines and schedules scans on local and network drives, other than the Full and Quick scans already defined in the Antimalware Policy. Provides the capability to target specific threats that may not be covered in the regularly scheduled scan using the Antimalware Policy.
Antimalware Network Scan	Defines and schedules scans on files from network drives only. This policy gives you the capability to target a network drive from a specific device. For example, you could use this policy to scan a file storage disk in an array of disks. Network credentials must be configured in the policy to access network files.
Antimalware Scan Exclusions	Customizes scan exclusions beyond those already configured in other Antimalware policies. Once this policy is created, you can add the Exclusions Policy option to the Custom Exclusions details of any of the three other Antimalware policies. The policy is then enforced based on having the same device assignment of the Exclusions Policy and the Antimalware policy that this option is configured in.
Application Control	Blocks execution of applications or denies Internet access to applications. You specify the applications that are blocked or denied Internet access.
Communication Hardware	Disables the following communication hardware: 1394-Firewire, IrDA-Infrared, Bluetooth, serial/parallel, dialup, wired, and wireless. Each communication hardware is configured individually, which means that you can disable some hardware types (for example, Bluetooth and dialup) while leaving others enabled.
Firewall	Controls network connectivity by disabling ports, protocols, and network addresses (IP and MAC).
Microsoft Data Encryption	Manages Microsoft's BitLocker and Encrypting File System (EFS) tools to encrypt removable drives and fixed disk folders, respectively.
Scripting	Runs a script (JScript or VBScript) on a device. You can specify the triggers that cause the script to run. Triggers can be based on Endpoint Security Agent actions, location changes, or time intervals.
Storage Device Control	Controls access to CD/DVD drives, floppy drives, and removable storage drives. Each storage device type is configured individually, which means that you can disable some and enable others.
USB Connectivity	Controls access to USB devices such as removable storage devices, printers, input devices (keyboards, mice, etc). You can specify individual devices or groups of devices. For example, you can disable access to a specific printer and enable access to all SanDisk USB devices.
VPN Enforcement	Enforces a VPN connection based on the device's location. For example, if the device's location is unknown, you can force a VPN connection through which all Internet traffic is routed.
Wi-Fi	Disables wireless adapters, blocks wireless connections, controls connections to wireless access points, and so forth.

In addition to the above security policies, the following security policies help protect and configure the ZENworks Endpoint Security Agent. The Endpoint Security Agent enforces security policies on a workstation device.

Policy	Purpose
Security Settings	Protects the Endpoint Security Agent from being tampered with and uninstalled. This policy is not used with the current Endpoint Security Agent. The ZENworks Endpoint Security Agent's security settings are not applied as a policy; instead, they are applied as ZENworks Agent settings (ZENworks Control Center > Configuration > Management Zone Settings > Device Management > ZENworks Agent). This policy is retained to provide support for devices that are still running the ZENworks 11 or ZENworks 11 SP1 Endpoint Security Agent. Those versions of the agent continue to use the Security Settings policy.
Location Assignment	Provides a list of predefined locations for the Endpoint Security Agent. ZENworks Endpoint Security Management lets you associate different security policies with different locations. For example, you might have an Office location and a Remote Office location; you also have a default Unknown location. The Endpoint Security Agent evaluates its current network environment to see if it matches any of the locations included in the Location Assignment policy. If so, the security policies associated with the matched location are applied. If not, the security policies associated with the Unknown location are applied.

How Network Locations Operate

The ZENworks Agent is location aware. This means that the agent can compare its current network environment against locations you defined. If the network environment matches one of the defined locations, the agent assigns that location to the device. If the network environment does not match a defined location, the agent assigns the Unknown location to the device.

The Endpoint Security Agent inherits the location assignment from the ZENworks Agent. This enables the Endpoint Security Agent to enforce different security policies at different locations. For example, you might choose to enforce different firewall settings for a stationary device located within your corporate office than for a mobile device that moves among less secure, unknown locations.

Several security policies can be designated as either location-based policies or global policies. A location-based policy is applied only if the device's location matches one of the locations identified in the policy. A global policy is applied regardless of the device's location.

NOTE: Ensure that you have assigned the Location Assignment Policy for the ZESM location-based policies to be enforced on the device.

Global-only Policies	Global or Location-based Policies
Antimalware Enforcement	Application Control
Antimalware Custom Scan	Communication Hardware
Antimalware Network Scan	Firewall
Antimalware Scan Exclusions	Storage Device Control
Location Assignment	USB Connectivity
Microsoft Data Encryption	Wi-Fi
Scripting	
Security Settings	
VPN Enforcement	

How User, Device, and Zone Policy Assignments Operate

You can assign security policies to users, workstation devices, and the Management Zone:

- **User assignment:** A user-assigned policy follows the user. When the user logs in through the ZENworks Agent on any device, the user-assigned policies are applied.
- **Device assignment:** A device-assigned policy follows the device. When the ZENworks Agent connects to the Management Zone, the device-assigned policies are applied.

  Security policies apply to workstation devices only. If you assign a security policy to a server device, it is not applied.
- **Zone assignment:** A zone-assigned policy is a default policy. It is evaluated after all user-assigned and device-assigned policies of that type.

Assignments to users and workstation devices are called *direct* assignments. You can also assign security policies to workstation folders and groups. When a user or workstation device is a member of a folder or a group, it inherits the assigned policies. These are called *inherited* assignments.

Assignments to the Management Zone can be made at the Management Zone, on a workstation device folder, and on a workstation device. This enables you to assign different default policies to different devices within your Management Zone.

Simply because a policy is assigned to a workstation device, the device's user, or the Management Zone does not mean that it will be enforced on the device. When multiple policies of the same type are applied to a workstation device through different assignments, the Endpoint Security Agent must determine a single *effective policy* to enforce on the device. Effective policies are discussed in How the Effective Policy is Determined.

How the Effective Policy is Determined

Because of the flexibility in assigning security policies (see How User, Device, and Zone Policy Assignments Operate), it is possible for multiple security policies of the same type to be applied to a device through different sources. For example, one Firewall policy might be assigned to a workstation device, a second Firewall policy to the device's user, and a third Firewall policy to a device group in which the device is a member. Because of multiple assignments, the ZENworks system must determine the **effective** policy for the device. The Endpoint Security Agent can then enforce the one effective policy on the device.

Determination of the effective policy is based on *ordering* and *merging* rules.

How Policy Precedence is Ordered

Policies are applied to a device through device assignments, user assignments, and zone assignments. Through the application of ordering rules, all of the assigned policies are combined into one list in order of precedence, from most important (highest priority) to least important (lowest priority). There are several steps involved in ordering:

- "Create Ordered Lists for Device-Assigned and User-Assigned Policies" on page 13
- "Create an Ordered List for Zone-Assigned Policies" on page 15
- "Resolve the Order of the Device-Assigned and User-Assigned Policy Lists" on page 16
- "Create Ordered Lists for Each Assigned Location" on page 17

Create Ordered Lists for Device-Assigned and User-Assigned Policies

The order of precedence for device-assigned policies and user-assigned policies is determined by where the assignment occurs in the ZENworks management hierarchy, using the following order of precedence:

1. Object
2. Group
3. Folder

A policy assigned to the object (device or user) precedes a policy assigned to the object's group or folder. Likewise, a policy assigned to an object's group precedes a policy assigned to the object's folder.

The order of precedence also takes into account that each level of the hierarchy includes multiple sub-levels. For example, if a device resides in a subfolder of the **Workstations** root folder, it might inherit assignments from both folders. Likewise, the device might be a member of multiple groups. The following table expands the levels to show the complete order of precedence:

Level	Order of Precedence	Example	Details
Object	1. First policy listed 2. Second policy listed 3. Third policy listed	1. Policy B 2. Policy A	The order of precedence for policies assigned to an object is determined by the object's **Assigned Policies** list in ZENworks Control Center. A policy at the top of the list has a higher priority than the same-type policies lower in the list. In the example, Policy B precedes Policy A.
Group	1. Object folder a. First group listed i. First policy ii. Second policy b. Second group listed i. First policy ii. Second policy 2. Parent folder a. First group listed i. First policy ii. Second policy b. Second group listed i. First policy ii. Second policy 3. Root folder a. First group listed i. First policy ii. Second policy b. Second group listed i. First policy ii. Second policy	1. Object folder a. Group 4 i. Policy D ii. Policy C b. Group 1 i. Policy F 2. Parent folder a. Group 3 i. Policy G ii. Policy J	The order of precedence for policies assigned to an object's groups is dependent on two factors: 1) the group locations in the folder hierarchy and 2) the policy ordering within the groups. The first factor is the group locations: ◆ For groups within the same folder, the order of precedence follows their order in the folder list, from top to bottom. ◆ For groups within different folders, the order of precedence follows the folders' order of precedence, with the object's folder preceding any of the object's parent folders. In the example, the resulting group order is 4, 1, 3. The second factor is the policy ordering within the group, which is determined by the group's **Assigned Policies** list. A policy at the top of the list has a higher priority than the same-type policies lower in the list. In the example, the resulting policy order is D, C, F, G, J.

Level	Order of Precedence	Example	Details
Folder	1. Object folder a. First policy listed b. Second policy listed 2. Parent folder a. First policy listed b. Second policy listed 3. Root folder a. First policy listed b. Second policy listed	1. Object Folder a. Policy I b. Policy H 2. Parent Folder a. Policy K 3. Root folder a. Policy R b. Policy S	The order of precedence for policies assigned to a folder corresponds to the order in the folder's **Policy Assignment**s list. In the example, Policy I has a higher precedence than Policy J. The precedence of an object's folders is determined by the folder hierarchy. The object's folder has precedence over folders located in folders higher in the folder hierarchy.

Using the example in the above table, the order of precedence for the policies assigned to the object (device or user) is:

1. Policy B
2. Policy A
3. Policy D
4. Policy C
5. Policy F
6. Policy G
7. Policy J
8. Policy I
9. Policy H
10. Policy K
11. Policy R
12. Policy S

Create an Ordered List for Zone-Assigned Policies

For policies assigned to the Management Zone, the order of precedence is determined by the position of the policies in the assignment list. The precedence is from the top to the bottom of the list. For example, if Policy A and Policy B are the same type and Policy B is higher in the list, the order of precedence is Policy B, Policy A.

Resolve the Order of the Device-Assigned and User-Assigned Policy Lists

After the ordered lists are created for each type of assignment (device-assigned, user-assigned, and zone-assigned), the three ordered lists for a single policy type look similar to the following example:

User Assignments	Device Assignments	Zone Assignments
1. Policy E	1. Policy H (Device Precedence)	1. Policy Q
2. Policy A	2. Policy B (User Only)	
3. Policy I	3. Policy R (Device Only)	
	4. Policy D (User Precedence)	

The goal of ordering is to have one ordered list per location, so the next step is to combine the three lists. By default, the zone-assignments list is always included as the last (lowest priority) list. The order of the user-assignments list and the device-assignments list is determined by the conflict resolution rules configured on the device assignments. There are four conflict resolution rules:

- **User Precedence:** The user-associated policies override device-associated policies. This means that the user-assigned policies have a higher priority than the device-assigned policies.
- **Device Precedence:** The device-associated policies override the user-associated policies. This means that the device-assigned policies have a higher priority than the user assigned policies.
- **User Only:** The user-assigned policies are applied and the device-assigned policies are ignored. However, if there are no user-assigned policies, the device-assigned policies are applied.
- **Device Only:** The device-assigned policies are applied and the user-assigned policies are ignored.

When there are multiple device assignments, the conflict resolution rule on the highest-priority device assignment is used. In the table above, Policy H is the highest-priority device assignment. Therefore, the Device Precedence rule is used and the result is the following ordered list:

1. Policy H (Device Assignment)
2. Policy B (Device Assignment)
3. Policy R (Device Assignment)
4. Policy D (Device Assignment)
5. Policy E (User Assignment)
6. Policy A (User Assignment)
7. Policy I (User Assignment)
8. Policy Q (Zone Assignment)

Create Ordered Lists for Each Assigned Location

At this point in the ordering process, the ordered list includes both location-based policies and global policies. Some policies might be applied in one location, others in another location, and some might be applied globally regardless of location.

Because the Endpoint Security Agent applies only the security policies assigned to the device's current security location, it requires separate ordered lists for each available location (as defined in the Location Assignment policy) and for the global "location." This results in lists similar to the following:

Location 1	Location 2	Location 3	Global
1. Policy H	1. Policy B	1. Policy R	1. Policy Q
2. Policy D	2. Policy D	2, Policy E	
3. Policy I	3. Policy A		
	4. Policy I		

Some policies might apply to multiple locations, such as Policy D that is included in the ordered lists for Location 2 and Location 3.

Creating the ordered lists for each location is the last step in the ordering process. With ordering complete, inheritance can be applied.

Policy Merging Explained

All security policies, except for the VPN Enforcement Policy, support merging of settings from multiple policies to create the effective policy.

After ordering is complete for a policy type, ordered lists exist for each assigned location and for the "global" location. The Endpoint Security Agent then completes the following process to merge policies and generate the final effective policy for each location:

- "Apply Inheritance to the Location Ordered Lists" on page 17
- "Merge the Location Effective Policies with the Global Effective Policy" on page 19
- "Merge Location Effective Policies with Default Effective Policy" on page 19

Apply Inheritance to the Location Ordered Lists

Security policies support inheritance, which is the passing of a setting from one policy to another policy of the same type. This allows settings from multiple policies to be merged into the single effective policy. Without inheritance, the effective policy would simply be the highest priority policy in the ordered list.

A policy setting is either single-valued, such as a Firewall policy's Default Behavior field, or is multi-valued, such as a Firewall policy's **Port/Protocol Rules** list. Single-valued settings can have assigned values, or they can inherit values from higher-level policies. Multi-valued settings can have their own values; in addition, they automatically inherit values from higher-level policies.

Consider the following example, where Policy A, B, and C are listed in order of precedence:

	Policy	Setting 1	Setting 2	List 3
1	A	Inherit	Disable	Item 1, Item 2
2	B	Inherit	Inherit	Item 1, Item 4
3	C	Enable	Enable	Item 3, Item 5
	Effective	Enable	Disable	Item 1, Item 2, Item 3, Item 4, Item 5

To determine the effective policy settings, the policies are evaluated and aggregated so that proper settings can be applied to the device. Higher priority settings take precedence over lower priority settings if there is a conflict.

For Setting 1 (a single-valued setting), Policy A inherits from Policy B, which inherits the Enable value from Policy C. Therefore, the effective value for Setting 1 is Enable.

For Setting 2 (a single-valued setting), Policy A is set to Disable, so the remaining policies are ignored. Therefore, the effective value for Setting 2 is Disable.

For List 3 (a multi-valued setting), the values from all three policy lists are used. Values that are exact matches, such as Item 1, are included only one time. Therefore, the effective values for List 3 are Item 1, Item 2, Item 3, Item 4, and Item 5.

Policy setting inheritance can be blocked at any policy. When it is blocked, inheritance stops at that policy. Consider the following example:

	Policy	Inheritance	Setting 1	Setting 2	List 3
1	D	Allowed	Inherit	Disable	Item 1, Item 2
2	E	Blocked	Enable	Disable	Item 1, Item 4
3	F	Allowed	Inherit	Enable	Item 3, Item 5
	Effective		Enable	Disable	Item 1, Item 2, Item 4

Policy E blocks setting inheritance from any lower priority policies.

For Setting 1 (a single-valued setting), Policy D inherits from Policy E, which blocks inheritance from F. Therefore, the effective value for Setting 1 is Enable.

For Setting 2 (a single-valued setting), Policy D is set to Disable, so the remaining policies are ignored. Therefore, the effective value for Setting 2 is Disable.

For List 3 (a multi-valued setting), the values from Policy D and Policy E are used. The values from Policy F are not used because Policy D blocks the inheritance of those values. Therefore, the effective values for List 3 are Item 1, Item 2, and Item 4.

Merge the Location Effective Policies with the Global Effective Policy

At this point, inheritance has been applied to all of the location ordered lists, including the global ordered list. The result is an effective policy for each location and for the global location.

When you assign policies to locations, you have the option of enabling the **Merge policy with assigned global policies** setting. When it is enabled, this setting causes an effective location policy to inherit any "unset" values from the effective global policy. Consider the following example:

Setting	Location 1 Policy	Location 2 Policy	Location 3 Policy	Global Policy
Setting 1	Enable	Disable	Inherit	Disable
Setting 2	Inherit	Disable	Disable	Disable
Setting 3	Enable	Inherit	Enable	Enable

Any location policy setting whose value is Inherit receives the value from the global policy setting.

Setting 1 in the Location 3 policy is set to Inherit. Therefore, it receives the value (Disable) assigned to Setting 1 in the Global policy. The same is true for Setting 2 in the Location 1 policy and Setting 3 in the Location 2 policy.

Merge Location Effective Policies with Default Effective Policy

The Endpoint Security Agent has a default policy of every type. Generally, the setting values for the default policy cause no change to the device.

If, after inheritance has been applied to all of the assigned policies, a setting value in the effective policy is still set to Inherit, the default value is used. The final result is that every setting value is defined for the effective policy.

Policy Versioning

A security policy can have multiple versions. Only one version, called the *published* version, is active at any one time.

When you change the published version of a policy, a Sandbox version is created. The published version remains active until you publish the Sandbox version, at which time it becomes active as the new published version. All old versions are retained until you delete them.

For information about publishing different versions of a policy, see Publishing Policies.

Session Support

Please be aware of security policy support for the following types of sessions:

- **Remote Sessions:** The Endpoint Security Agent does not support user-assigned security policies in remote (non-console) sessions. Only device-assigned policies are applied when logging in to a remote session.

- **Fast User Switching Sessions:** The Endpoint Security Agent does not support user-assigned security policies on devices when Fast User switching is used (that is, switching between user accounts without quitting applications and logging out). On devices where Fast User switching is employed, you should use device-assigned and zone-assigned policies only.

Security Policy Summary

The following chart provides a summary of location support (global or location-based), assignment support (device, user, or zone), and multiple-policy support (plural or singular).

	Global	Location Based	Device Assignment	User Assignment	Zone Assignment	Plural	Singular
Antimalware Enforcement	✓		✓		✓		✓
Antimalware Custom Scan	✓		✓		✓	✓	
Antimalware Network Scan	✓		✓		✓	✓	
Antimalware Scan Exclusions	✓		✓		✓	✓	
Application Control	✓	✓	✓	✓	✓	✓	
Communication Hardware	✓	✓	✓	✓	✓	✓	
Firewall	✓	✓	✓	✓	✓	✓	
Location Assignment	✓		✓	✓	✓	✓	
Microsoft Data Encryption	✓		✓		✓		✓
Security Setting	✓		✓	✓	✓	✓	
Scripting	✓		✓	✓	✓		✓
Storage Device Control	✓	✓	✓	✓	✓	✓	
USB Connectivity	✓	✓	✓	✓	✓	✓	
VPN Enforcement	✓		✓	✓	✓		✓
Wi-Fi	✓	✓	✓	✓	✓	✓	

Global: Can be created as a global policy. A global policy is available regardless of the device's location.

Location Based: Can be created as a location-based policy. A location-based policy is available only when the device's location matches a location defined in the policy.

Device Assignment: Can be assigned to a device, device folder, or device group.

User Assignment: Can be assigned to a user, user folder, or user group.

Zone Assignment: Can be assigned as a default policy at the Management Zone.

Plural: Supports merging of multiple policies (of the same type) into one effective policy to be enforced on a device. The effective policy is a determined by established ordering and merging rules. For details, see How the Effective Policy is Determined.

Singular: Supports enforcement of only one policy (of a single type) on a device. If multiple policies are assigned, the effective policy is determined by established ordering rules. For details, see How the Effective Policy is Determined.

2 Policy Deployment

These sections describe some best practices for deploying security policies and how to create, test, assign, and view them.

- "Deployment Best Practices" on page 23
- "Creating Security Policies" on page 26
- "Testing Security Policies" on page 27
- "Assigning Security Policies" on page 28
- "Viewing Effective Policies" on page 31

Deployment Best Practices

ZENworks management is based on a Manage by Exception model. This model assumes that a significant number of devices or users have the same base requirements; these base requirements become the rule and are applied to all (or most) devices or users, while the differences are handled as individual exceptions. The following practices provide the best approach to deploying security policies through the Manage by Exception model.

Practice 1: Define your security locations

The ZENworks Endpoint Security Agent is location aware. This allows it to apply different security policies based on its detected network environment matching defined locations or a default Unknown location.

If you have locations in which you want to enforce different security policies, you should define them before you begin creating policies. This allows you to design policies that best support your locations.

Because locations apply to multiple areas of ZENworks, creation of locations is not covered in this *ZENworks Endpoint Security Management Policies Reference*. For location information, see the *ZENworks Location Awareness Reference*.

Practice 2: Focus on one policy type at a time

There are 10 types of security policies. Each one covers a specific area of device security. Most contain multiple options and concepts that you need to clearly understand. Taken together, the policies can seem overwhelming. You should choose one policy type and focus on how it needs to be deployed in your organization. Then focus on the next one.

The Security Settings policy protects the Endpoint Security Agent. The Location Assignment policy determines which security locations are available to devices or users. Because of the nature of these two policies, we recommend that you address them first.

Practice 3: Decide on the best assignment method

ZENworks supports both device-assigned and user-assigned security policies. You can assign policies to any devices that are registered in your Management Zone. If your ZENworks system is connected to an LDAP user source, you can assign policies to users defined in the source.

As you plan the deployment of a security policy, you should consider whether it is best assigned to devices or to users:

- **Device Assignment:** Device-assigned policies are applied regardless of the user that is logged in. Be aware that security policies apply to workstation devices only. If you assign a security policy to a server device, it is not applied.
- **User Assignment:** User-assigned policies are applied only when the assigned user is logged in. If the user moves from one device to another, the policies move with the user and are applied when the user logs in to the device.

In some cases, you might need to use both types of assignments. For example, you could create a base Firewall policy and assign it to devices. Then, if you have specific users who have different firewall requirements, you could create the appropriate Firewall policy and assign it to the users.

When the same-type policy (such as a Firewall policy) is assigned to both a device and the device's user, you must decide which policy takes precedence. You do this by specifying the conflict resolution rule on the device-assignment. There are four rules:

- **User Precedence:** The user-assigned policy overrides the device-assigned policy.
- **Device Precedence:** The device-assigned policy overrides the user-assigned policy.
- **User Only:** Applies the user-assigned policy. If there is no user-assigned policy, the device-assigned policy is applied.
- **Device Only:** Applies the device-assigned policy. Ignores the user-assigned policy.

Practice 4: Utilize the management hierarchy for assignments

The ZENworks management hierarchy contains four levels:

1. Management Zone
2. Folder
3. Group
4. Object

A device or user (the object) is assigned policies directly. A device or user also inherits policies assigned to its zone or to a folder or group in which the device is a member.

Whenever possible, you should assign a policy at a level (or levels) that encompasses the majority of devices or users to whom the policy applies. For example, if all devices in your organization require data encryption, you might assign a Microsoft Data Encryption policy to the Management Zone and handle policy exceptions with assignments to device groups or individual devices. However, if only a specific group of devices require data encryption, you might decide to organize those devices into a device group and assign a Microsoft Data Encryption policy to the device group.

Practice 5: Utilize policy settings inheritance

When you create a policy, you provide each policy setting with a value. This is either an absolute value or the **Inherit** value. The **Inherit** value lets the setting value be inherited from the next higher policy in the policy hierarchy.

If, as suggested in Practice 4, you take advantage of the management hierarchy as you make policy assignments, policy settings inheritance becomes an important tool to successfully combine multiple policies into the one effective policy that is enforced on the device.

For example, assume that you create a base Firewall policy. You assign the policy to the Management Zone so that all devices inherit it. In the policy, you set the ACL value to allow 802.1x protocol packets. However, you have one group of devices for which you need to deny 802.1x protocol packets. You create a second Firewall policy, leave all setting values configured to **Inherit** except for the ACL value which you set to deny 802.1x protocol packets, and assign the Firewall policy to the device group. The Firewall policy assigned to the device group is closest to the device (in the policy hierarchy), so it takes precedence. All values are inherited from the zone Firewall policy except for the 802.1x ACL value, which uses the device group Firewall policy.

Multi-valued settings, such as the **Port/Protocol Rules** list in the Firewall policy, do not include an **Inherit** value. Instead, multi-valued settings are combined. In the previous example, the Port/Protocol Rules lists in the two Firewall policies (the zone policy and the device group policy) would be combined into one list in the effective Firewall policy.

In some cases, you might not want a policy to inherit values from a policy higher in the hierarchy. For example, you might not want the device group Firewall policy to inherit the **Port/Protocol Rules** list from the zone Firewall policy. Therefore, you can configure policies to block inheritance of higher-level policies.

Practice 6: Utilize global policies

A global policy is applied in all locations. A location-based policy is applied only in the locations specified in the policy.

If a policy's settings are not dependent on location, use a global policy. Even if some of the policy's settings are dependent on location, consider using a global policy to set the base policy and then creating location-based policies to override the location-dependent settings. When you use global and location-based policies together, the location-based policy settings override the global policy settings.

As you deploy security policies within your zone, we recommend that you create global policies and assign them at the highest level possible, preferably the zone. The global policies should include the policy settings that provide the base security required by the majority of your organization's devices.

Practice 7: Understand how effective policies are determined

The Endpoint Security Agent enforces one policy of each type on a device. This policy is the *effective* policy, which is determined by evaluating and manipulating all assigned policies (of the same type) according to *ordering* and *inheritance* rules.

To successfully deploy the intended policy to a device, you need to fully understand how assigned policies are going to be ordered based on assignment type (device or user), assignment level (zone, folder, group, and object), and policy location type (global or location-based). You also need to know how policy setting inheritance is applied once the order is determined. These concepts are covered in How the Effective Policy is Determined.

Practice 8: Test a policy before rolling it out to all users and devices

To ensure that security policies provide the results that you expect, we recommend that you test them on one or more devices before distributing them to all intended users and devices. For instructions, see Testing Security Policies.

Creating Security Policies

The following instructions explain how to create a new security policy by using the Create New Policy wizard. In addition to using the wizard, you can create policies by:

- Copying an existing security policy. All original system requirements, details, and settings are copied to the new policy. You can then make any desired modifications to the new policy. See Copy a Policy.
- Creating a Sandbox version of an existing security policy and then publishing it as a new policy. For information, see Publish a Sandbox Version.
- Importing a policy from another Management Zone. All original system requirements, details, and settings (if applicable) are imported to the new policy. For information, see Importing and Exporting Policies.

To create a security policy using the Create New Policy wizard:

1. In ZENworks Control Center, click **Policies** to display the Policies page.
2. In the Policies panel, click **New** > **Policy** to launch the Create New Policy wizard.
3. On the Select Platform page, select **Windows**, and click **Next**.
4. On the Select Policy Category page, select **Windows Endpoint Security Policies**, and click **Next**.
5. On the Select Policy Type page, select the type of policy you want to create, and click **Next**.

   For information about policy types, see Types of Security Policies.
6. On the Define Details page, specify a name for the policy, select the folder in which to place the policy, then click **Next**.

   The name must be unique among all other policies located in the selected folder. For additional requirements, see Naming Conventions in ZENworks Control Center.
7. (Conditional) If the Configure Inheritance and Location Assignments page is displayed, configure the following settings, then click **Next**.

   Inheritance: Leave the **Inherit from policy hierarchy** setting selected if you want to enable this policy to inherit settings from same-type policies that are assigned higher in the policy hierarchy. For example, if you assign this policy to a device and another policy (of the same type) to the device's folder, enabling this option allows this policy to inherit settings from the policy assigned to the device's folder. Deselect the **Inherit from policy hierarchy** setting if you don't want to allow this policy to inherit policy settings.

Location Assignments: Policies can be global or location-based. A global policy is applied regardless of location. A location-based policy is applied only when the device detects that it is within the locations assigned to the policy.

Select whether this is a global or location-based policy. If you select location-based, click **Add**, select the locations to which you want to assign the policy, then click **OK** to add them to the list.

8 Configure the policy-specific settings, then click **Next** until you reach the Summary page.

For information about a policy's settings, you can click **Help** > **Current Page** in ZENworks Control Center, or you can see Policy Settings.

9 On the Summary page, review the information to make sure it is correct. If it is incorrect, click the **Back** button to revisit the appropriate wizard page and make changes. If it is correct, select either of the following options (if desired), then click **Finish**.

- **Create as Sandbox:** Select this option to create the policy as a Sandbox version. The Sandbox version is isolated from users and devices until you publish it. For example, you can assign it to users and devices, but it is applied only after you publish it. You can also use the Sandbox version to test the policy on devices you've designated as test devices. For information, see Testing Security Policies.
- **Define Additional Properties:** Select this option to display the policy's property pages. These pages let you define system requirements that must be met before the policy can be assigned to a device, assign the policy to users and devices, and add the policy to policy groups.

10 To test the policy before assigning it to users and devices, see Testing Security Policies

11 To assign the policy to users and devices, see Assigning Security Policies.

Testing Security Policies

To ensure that security policies provide the results that you expect, we recommend that you test them on one or more devices before distributing them to all intended users and devices.

The best way to test a policy on a device is to apply a Sandbox version of the policy to a test device. The following sections explain how to do this.

Designate Test Devices

You can designate any managed device in your ZENworks Management Zone as a test device. When a policy is assigned to a test device, the Sandbox version of the policy is applied, not the Published version. If no Sandbox version exists, the Published policy is applied.

To designate a managed device as a test device:

1 In ZENworks Control Center, click **Devices**.

2 In the **Devices** list, select the check box next to the target device, then click **Action** > **Set as Test**.

Assign Policies to Test Devices

1 In ZENworks Control Center, click **Policies** to display the Policies page.

2 Click the policy you want to assign to test devices.

3 Make sure the policy you want to test has a Sandbox version. If it does not, create a Sandbox version by editing an item on the Details page (you can change an item and then change it back) and clicking **Apply**.

4 Assign the policy to test devices:

   4a Click the **Relationships** tab.

   4b In the Device Assignments panel, click **Add**, browse for and select the test devices, then click **OK**.

   4c Select **Device Only** as the policy conflict resolution, then click **Next**.

   4d Select **Enforce policies immediately on all assigned devices**, then click **Finish**.

5 Go to a test device and verify that the policy has been applied and is being enforced as expected.

   In addition to performing actions on the device that allow you to observe whether or not the policy is being enforced correctly, you can view the effective policies for the device. This is helpful if multiple policies of the same type are assigned to the device; in this case, the policies are merged into one effective policy that is then enforced. For information about viewing a device's effective policies, see Viewing Effective Policies.

Assigning Security Policies

You can assign security policies to users, workstation devices, and the Management Zone. Security policies do not apply to server devices; if you assign a security policy to a server or server folder, the policy is not applied.

When you assign a policy to a user, it is applied when the user is logged in to a ZENworks Server. When you assign a policy to a device, it is applied when the device starts, regardless of whether or not a user is logged in. When you assign a policy to the Management Zone, it becomes a default policy that is only applied after user-assigned and device-assigned policies.

Assign Policies to Users

You can assign policies and policy groups to users. This section assumes that you have already created any policy groups you want to assign. If not, see Managing Policy Groups.

The policy assignment can be directly to a user or indirectly to a user through a group or folder in which the user is a member.

1 In ZENworks Control Center, click the **Policies** tab.

2 In the **Policies** list, select the check box next to policies and policy groups you want to assign.

3 Click **Action** > **Assign to User**.

4 Browse for and select the user, user groups, and user folders to which you want to assign the group:

   4a Click next to a folder to navigate through the folders until you find the user, group, or folder you want to select.

   If you are looking for a specific item, such as a User or a User Group, you can use the **Items of type** list to limit the types of items that are displayed. If you know the name of the item you are looking for, you can use the **Item name** box to search for the item.

4b Click the underlined link in the **Name** column to select the user, group, or folder and display its name in the **Selected** list box.

4c Click **OK** to add the selected devices, folders, and groups to the **Users** list.

5 Click **Next** to display the Finish page.

6 Review the information and, if necessary, use the **Back** button to make corrections to the information.

7 If you want the selected policies to be immediately enforced, select the **Enforce policies immediately on all assigned devices**.

This option causes the policy to be immediately distributed to the assigned users' devices and enforced. If you don't select this option, the policy is distributed and enforced the next time the users' device refreshes its policy information from the ZENworks system, either through a manual refresh or a scheduled refresh.

8 Click **Finish**.

The policies or policies groups are assigned to the selected users, user groups, and user folders. You can view the assignments on the Relationships page of the policies or policy groups.

Assign Policies to Devices

Security policies apply to workstation devices only. If you assign a security policy to a server device, it is not applied.

1 In ZENworks Control Center, click the **Policies** tab.

2 In the **Policies** list, select the check box next to the policies and policy groups you want to assign.

3 Click **Action** > **Assign to Device**.

4 Browse for and select the devices, device groups, and device folders to which you want to assign the group:

4a Click next to a folder to navigate through the folders until you find the device, group, or folder you want to select.

If you are looking for a specific item, such as a Workstation or a Workstation Group, you can use the **Items of type** list to limit the types of items that are displayed. If you know the name of the item you are looking for, you can use the **Item name** box to search for the item.

4b Click the underlined link in the **Name** column to select the device, group, or folder and display its name in the **Selected** list box.

4c Click **OK** to add the selected devices, folders, and groups to the **Devices** list.

5 Click **Next** to display the Policy Conflict Resolution page.

This page lets you select how to resolve conflicts if another policy of the same policy type is assigned to one of the selected devices' users. For example, assume that UserA is assigned WirelessPolicy1. You are now assigning WirelessPolicy2 to DeviceA. If UserA logs in to DeviceA, a decision must be made about which policy (WirelessPolicy1 or WirelessPolicy2) to apply.

6 Select one of the following policy conflict resolution methods:

User Precedence: The user-associated policies override device-associated policies. This means that the user-assigned policies have a higher priority than the device-assigned policies.

Device Precedence: The device-associated policies override the user-associated policies. This means that the device-assigned policies have a higher priority than the user assigned policies.

Device Only: Applies the device-associated policy only. If a user-associated policy exists, it is not applied.

User Only: If a user-associated policy exists, applies the user-associated policy. If no user-associated policy exists, applies the device-associated policy.

7 Click **Next** to display the Finish page, review the information and, if necessary, use the **Back** button to make changes to the information.

If you want the policies to be immediately enforced on all the assigned devices, select **Enforce Policies Immediately on all Assigned Devices**.

8 Click **Finish**.

The policies or policies groups are assigned to the selected devices, device groups, and device folders. You can view the assignments on the Relationships page of the policies or policy groups.

Assign Policies to the Management Zone

You can assign security policies to the Management Zone. When determining the effective policies to be enforced on a device, the Zone policies are evaluated after all other assigned policies. For more information about how an effective policy is determined, see How the Effective Policy is Determined.

Consider the following situations:

- No Firewall policies are assigned to a device or the device's user (either directly or through a group or folder). The Zone Firewall policy becomes the effective policy for the device and is enforced on the device.
- Firewall policies are assigned to a device and the device's user. Both policies are evaluated and manipulated to determine the effective Firewall policy to apply to the device. After the effective policy is determined from the user-assigned and device-assigned policies, the Zone Firewall policy is used to supply any values that 1) are unset in the effective Firewall policy and 2) are additive (such as the multi-valued Port/Protocol Rules tables).

You can assign Zone policies at three levels. This enables you to assign different Zone policies to different devices within your Management Zone.

- **Management Zone:** The policies you assign at the Management Zone become the Zone policies for all devices, unless you assign different Zone policies at the device folder or device level.
- **Device Folder:** The policies you assign at a device folder override the Management Zone (and any parent device folders) and become the Zone policies for all devices contained within the folder structure, unless you assign different Zone policies for a subfolder or an individual device.

  Security policies apply to workstation devices only. If you assign a security policy to a Server device folder, the policy is not applied to any servers located in the folder.
- **Device:** The policies you assign for an individual device override the Management Zone and device folder and become the Zone policies for the device.

  Security policies apply to workstation devices only. If you assign a security policy to a server device, it is not applied.

NOTE: System requirements that are defined in a security policy are ignored when the policy is assigned as a Zone policy.

In ZENworks Control Center:

1. To assign a Zone policy to the Management Zone, click the **Configuration** tab, click **Endpoint Security Management** (in the Management Zone Settings panel), then click **Zone Policy Settings**.

   or

   To assign a Zone policy to a device folder, click the **Devices** tab, locate the folder in the **Devices** list, then click **Details** > **Settings** > **Endpoint Security Management** > **Zone Policy Settings**.

   or

   To assign a Zone policy to a device, click the **Devices** tab, click the device in the **Devices** list, then click **Settings** > **Endpoint Security Management** > **Zone Policy Settings**.

2. If you are assigning a Zone policy to a device folder or device, click **Override settings** to activate the panel.

3. In the list, click **Add**, browse for and select the policy you want to add as a default policy, then click **OK** to add it to the list.

4. After you finish adding default policies, click **Apply** to save the settings.

   By default, Management Zone settings are cached on the ZENworks Server and the cache is updated every 10 minutes. Because of this, if a change is made to a zone setting, devices do not receive the changes until the next cache update, which might be as long as 10 minutes.

   For ZENworks Endpoint Security Management, the following are stored as zone settings:

   - Zone security policies
   - Location and network environment settings
   - Effective policy report settings
   - Data encryption keys

   If you change any of these settings and you want to apply them immediately to a device, you must use the zac command line utility on the device to bypass the ZENworks Server cache and retrieve the new settings. To do so, run the following command on the device:

   ```
   zac ref general bypasscache
   ```

Viewing Effective Policies

Because of the flexibility in assigning security policies to users, devices, and the Management Zone, it is possible for multiple security policies of the same type to be applied to a device through different sources. For example, one Firewall policy might be assigned to a device, a second Firewall policy to the device's user, and a third Firewall policy to a device group in which the device is a member. Because of multiple assignments, the ZENworks system must determine the **effective** policy for the device. The Endpoint Security Agent can then enforce the one effective policy on the device. How the Effective Policy is Determined explains the process used to determine an effective policy.

You can view a device's effective policies through the Agent Status in the Endpoint Security Agent on the device. This requires the Endpoint Security Agent to have an override password assigned through a Security Settings policy.

For information about using the Endpoint Security Agent to view effective policies, see "Viewing Effective Policies" in the *ZENworks Endpoint Security Agent Reference*.

3 Policy Management

These sections explain how to perform common management tasks for existing security policies. For information about creating security policies, see Policy Deployment.

- "Editing a Policy's Details" on page 33
- "Defining a Policy's System Requirements" on page 34
- "Publishing Policies" on page 39
- "Renaming, Copying, and Moving Policies" on page 40
- "Enabling and Disabling Policies" on page 41
- "Replicating Policies to Content Servers" on page 42
- "Importing and Exporting Policies" on page 43
- "Managing Policy Groups" on page 44

Editing a Policy's Details

After creating a policy, you can make changes to the policy's details if necessary. Changing a policy's details creates a Sandbox version of the policy. For the changes to be applied, you must publish the Sandbox version.

To edit a policy's details:

1. In ZENworks Control Center, click **Policies** to display the Policies page.
2. In the **Policies** list, click the policy you want to edit.
3. Click the **Details** tab.
4. Make the desired changes.

   For information about the policy's details, click the Help button in ZENworks Control Center or see Policy Settings.
5. Click **Apply** to save the changes.
6. To publish the changes, click **Publish**, then follow the wizard prompts.

   For more information about publishing changes to a policy, see Publishing Policies.

Defining a Policy's System Requirements

You can define requirements, such as operating system, total memory, and processor speed, that a device must meet for the policy to be applied to it. These requirements are in addition to any location-based requirements. For example, consider a policy that is associated with the Office location. When the device is in the Office location, the policy is only applied if it meets the system requirements defined in the policy.

You define requirements through the use of filters. A filter is a condition that must be met by a device in order for the policy to be applied. For example, you can add a filter to specify that the device must have exactly 512 MB of RAM in order for the policy to be applied, and you can add another filter to specify that the hard drive be at least 20 GB in size.

NOTE: System requirements you define for a security policy are ignored when the policy is assigned to the management zone (see Assign Policies to the Management Zone).

To create system requirements for a policy:

1. In ZENworks Control Center, click the **Policies** tab.
2. Click the policy to display the policy's Summary page.
3. Click the **Requirements** tab.
4. Click **Add Filter**, select a filter condition from the drop-down list, then fill in the fields.

   As you construct filters, you need to know the conditions you can use and how to organize the filters to achieve the desired results. For more information, see Configure Filter Conditions and Define Filter Logic.
5. (Optional) Add additional filters and filter sets.
6. Click **Apply** to save the settings.

   Creating or changing system requirements creates a Sandbox version of the policy. For the requirements to be applied, you must publish the Sandbox version.
7. To publish the Sandbox version, click **Publish**, then follow the wizard prompts.

   For more information about publishing the Sandbox version of a policy, see Publishing Policies.

Configure Filter Conditions

You can choose from any of the following conditions when creating a filter:

- **Architecture:** Determines the architecture of Windows running on the device, either 32-bit or 64-bit. The condition you use to set the requirement includes a property, an operator, and a property value. The possible operators are equals (=) and does not equal (<>). For example, if you set the condition to architecture = 32, the device's Windows operating system must be 32-bit to meet the requirement.
- **Bundle Installed:** Determines if a specific bundle is installed. After specifying the bundle, the two conditions you can use to set the requirement are **Yes** and **No**. If you select **Yes**, the specified bundle must already be installed to meet the requirement. If you select **No**, the bundle must not be installed.

- **Connected:** Determines if the device is connected to a network. The two conditions you can use to set the requirement are **Yes** and **No**. If you select **Yes**, the device must be connected to the network to meet the requirement. If you select **No**, it must not be connected.
- **Connection Speed:** Determines the speed of the device's connection to the network. The condition you use to set the requirement includes an operator and a value. The possible operators are equals (**=**), does not equal (**<>**), is greater than (**>**), is greater than or equal to (**>=**), is less than (**<**), and is less than or equal to (**<=**). The possible values are bits per second (**bps**), kilobits per second (**Kbps**), megabits per second (**Mbps**), and gigabits per second (**Gbps**). For example, if you set the condition to `>= 100 Mbps`, the connection speed must be greater than or equal to 100 megabits per second to meet the requirement.
- **Disk Space Free:** Determines the amount of free disk space on the device. The condition you use to set the requirement includes a disk designation, an operator, and a value. The disk designation must be a local drive map (for example, c: or d:). The possible operators are equals (**=**), does not equal (**<>**), is greater than (**>**), is greater than or equal to (**>=**), is less than (**<**), and is less than or equal to (**<=**). The possible values are bytes (**Bytes**), kilobytes (**KB**), megabytes (**MB**), and gigabytes (**GB**). For example, if you set the condition to `c: >= 80 MB`, the free disk space must be greater than or equal to 80 megabytes to meet the requirement.
- **Disk Space Total:** Determines the amount of total disk space on the device. The condition you use to set the requirement includes a disk designation, an operator, and a value. The disk designation must be a local drive map (for example, c: or d:). The possible operators are equals (**=**), does not equal (**<>**), is greater than (**>**), is greater than or equal to (**>=**), is less than (**<**), and is less than or equal to (**<=**). The possible values are bytes (**Bytes**), kilobytes (**KB**), megabytes (**MB**), and gigabytes (**GB**). For example, if you set the condition to `c: >= 40 GB`, the total disk space must be greater than or equal to 40 gigabytes to meet the requirement.
- **Disk Space Used:** Determines the amount of used disk space on the device. The condition you use to set the requirement includes a disk designation, an operator, and a value. The disk designation must be a local drive map (for example, c: or d:). The possible operators are equals (**=**), does not equal (**<>**), is greater than (**>**), is greater than or equal to (**>=**), is less than (**<**), and is less than or equal to (**<=**). The possible values are bytes (**Bytes**), kilobytes (**KB**), megabytes (**MB**), and gigabytes (**GB**). For example, if you set the condition to `c: <= 10 GB`, the used disk space must be less than or equal to 10 gigabytes to meet the requirement.
- **Environment Variable Exists:** Determines if a specific environment variable exists on the device. After specifying the environment variable, the two conditions you can use to set the requirement are **Yes** and **No**. If you select **Yes**, the environment variable must exist on the device to meet the requirement. If you select **No**, it must not exist.
- **Environment Variable Value:** Determines if an environment variable value exists on the device. The condition you use to set the requirement includes the environment variable, an operator, and a variable value. The environment variable can be any operating system supported environment variable. The possible operators are **equal to**, **not equal to**, **contains**, and **does not contain**. The possible variable values are determined by the environment variable. For example, if you set the condition to `Path contains c:\windows\system32`, the Path environment variable must contain the `c:\windows\system32` path to meet the requirement.
- **File Date:** Determines the date of a file. The condition you use to set the requirement includes the filename, an operator, and a date. The filename can be any filename supported by the operating system. The possible operators are **on**, **after**, **on or after**, **before**, and **on or before**. The possible dates are any valid dates. For example, if you set the condition to `app1.msi on or after 6/15/07`, the `app1.msi` file must be dated 6/15/2007 or later to meet the requirement.

- **File Exists:** Determines if a file exists. After specifying the filename, the two conditions you can use to set the requirement are **Yes** and **No**. If you select **Yes**, the specified file must exist to meet the requirement. If you select **No**, the file must not exist.
- **File Size:** Determines the size of a file. The condition you use to set the requirement includes the filename, an operator, and a size. The filename can be any filename supported by the operating system. The possible operators are equals (**=**), does not equal (**<>**), is greater than (**>**), is greater than or equal to (**>=**), is less than (**<**), and is less than or equal to (**<=**). The possible sizes are designated in bytes (**Bytes**), kilobytes (**KB**), megabytes (**MB**), and gigabytes (**GB**). For example, if you set the condition to `doc1.pdf <= 3 MB`, the `doc1.pdf` file must be less than or equal to 3 megabytes to meet the requirement.
- **File Version:** Determines the version of a file. The condition you use to set the requirement includes the filename, an operator, and a version. The filename can be any file name supported by the operating system. The possible operators are equals (**=**), does not equal (**<>**), is greater than (**>**), is greater than or equal to (**>=**), is less than (**<**), and is less than or equal to (**<=**).

  Be aware that file version numbers contain four components: Major, Minor, Revision, and Build. For example, the file version for `calc.exe` might be 5.1.2600.0. Each component is treated independently. For this reason, the system requirements that you set might not provide your expected results. If you do not specify all four components, wildcards are assumed.

  For example, if you set the condition to `calc.exe <= 5`, you are specifying only the first component of the version number (Major). As a result, versions 5.0.5, 5.1, and 5.1.1.1 also meet the requirement.

  However, because each component is independent, if you set the condition to `calc.exe <= 5.1`, the `calc.exe` file must be less than or equal to version 5.1 to meet the requirement.
- **IP Segment:** Determines the device's IP address. After specifying the IP segment name, the two conditions you can use to set the requirement are **Yes** and **No**. If you select **Yes**, the device's IP address must match the IP segment. If you select **No**, the IP address must not match the IP segment.
- **Logged On To Primary Workstation:** Determines whether the user is logged on to his or her primary workstation. The two conditions you can use to set the requirement are **Yes** and **No**. If you select **Yes**, the user must be logged on to his or her primary workstation to meet the requirement. If you select **No**, and no user is logged on to the workstation, the requirement is not met. However, if a user other than the primary user is logged on to the workstation, the requirement is met.
- **Memory:** Determines the amount of memory on the device. The condition you use to set the requirement includes an operator and a memory amount. The possible operators are equals (**=**), does not equal (**<>**), is greater than (**>**), is greater than or equal to (**>=**), is less than (**<**), and is less than or equal to (**<=**). The memory amounts are designated in megabytes (**MB**) and gigabytes (**GB**). For example, if you set the condition to `>= 2 GB`, the device must have at least 2 gigabytes of memory to meet the requirement.
- **Novell Client Installed:** Determines if the device is using the Novell Client for its network connection. The two conditions you can use to set the requirement are **Yes** and **No**. If you select **Yes**, the device must be using the Novell Client to meet the requirement. If you select **No**, it must not be using the Novell Client.
- **Operating System - Windows:** Determines the architecture, service pack level, type, and version of Windows running on the device. The condition you use to set the requirement includes a property, an operator, and a property value. The possible properties are **architecture**, **service pack**, **type**, and **version**. The possible operators are equals (**=**), does not equal (**<>**), is

greater than (>), is greater than or equal to (>=), is less than (<), and is less than or equal to (<=). The property values vary depending on the property. For example, if you set the condition to `architecture = 32`, the device's Windows operating system must be 32-bit to meet the requirement.

Be aware that operating system version numbers contain four components: Major, Minor, Revision, and Build. For example, the Windows 2000 SP4 release's number might be 5.0.2159.262144. Each component is treated independently. For this reason, the system requirements that you set might not provide your expected results.

For example, if you specify **Operating System - Windows** in the first field, **Version** in the second field, **>** in the third field, and **5.1 -Windows XP Versions** in the last field, you are specifying only the first two components of the version number: Major (Windows) and Minor (5.0). As a result, for the requirement to evaluate to true, the OS must be at least 5.1 (Windows XP). Windows 2003 is version 5.2, so specifying > 5.1 also evaluates to True.

However, because each component is independent, if you specify the version = 5.1, Windows XP SP2 evaluates to False because the actual version number might be 5.1.2159.262144. You can specify the version >= 5.1 to make the requirement evaluate as True because the actual revision component is greater than 0.

When you select the OS version from the drop-down, the Major and Minor components are populated. The Revision and Build components must be typed manually.

- **Primary User Is Logged In:** Determines if the device's primary user is logged in. The two conditions you can use to set the requirement are **Yes** and **No**. If you select **Yes**, the primary user must be logged in to meet the requirement. If you select **No**, the user must not be logged in.
- **Processor Family:** Determines the device's processor type. The condition you use to set the requirement includes an operator and a processor family. The possible operators are equals (=) and does not equal (<>). The possible processor families are **Pentium**, **Pentium Pro**, **Pentium II**, **Pentium III**, **Pentium 4**, **Pentium M**, **WinChip**, **Duron**, **BrandID**, **Celeron**, and **Celeron M**. For example, if you set the condition to <> `Celeron`, the device's processor can be any processor family other than Celeron to meet the requirement.
- **Processor Speed:** Determines the device's processor speed. The condition you use to set the requirement includes an operator and a processor speed. The possible operators are equals (=), does not equal (<>), is greater than (>), is greater than or equal to (>=), is less than (<), and is less than or equal to (<=). The possible processor speeds are hertz (**Hz**), kilohertz (**KHz**), megahertz (**MHz**), and gigahertz (**GHz**). For example, if you set the condition to `>= 2 GHz`, the device's speed must be at least 2 gigahertz to meet the requirement.
- **Registry Key Exists:** Determines if a registry key exists. After specifying the key name, the two conditions you can use to set the requirement are **Yes** and **No**. If you select **Yes**, the specified key must exist to meet the requirement. If you select **No**, the key must not exist.
- **Registry Key Value:** Determines if a registry key value exists on the device. The condition you use to set the requirement includes the key name, the value name, an operator, a value type, and a value data. The key and value names must identify the key value you want to check. The possible operators are equals (=), does not equal (<>), is greater than (>), is greater than or equal to (>=), is less than (<), and is less than or equal to (<=). The possible value types are **INT_TYPE** and **STR_TYPE**. The possible value data is determined by the key, value name, and value type.

- **Registry Key and Value Exists:** Determines if a registry key and value exists. After specifying the key name and value, the two conditions you can use to set the requirement are **Yes** and **No**. If you select **Yes**, the specified key and value must exist to meet the requirement. If you select **No**, the key and value must not exist.
- **Service Exists:** Determines if a service exists. After specifying the service name, the two conditions you can use to set the requirement are **Yes** and **No**. If you select **Yes**, the service must exist to meet the requirement. If you select **No**, the service must not exist.
- **Specified Devices:** Determines if the device is one of the specified devices. After specifying the devices, the two conditions you can use to set the requirement are **Yes** and **No**. If you select **Yes**, the device must be included in the specified devices list to meet the requirement (an inclusion list). If you select **No**, the device must not be included in the list (an exclusion list).
- **ZENworks Agent Version:** Determines the ZENworks Agent version for a ZENworks Endpoint Security Management System. The condition you use to set the requirement includes an operator and a version. The possible operators are equals (**=**), does not equal (**<>**), is greater than (**>**), is greater than or equal to (**>=**), is less than (**<**), and is less than or equal to (**<=**).

  Be aware that the file version numbers contain four components: Major, Minor, Revision, and Build. For example, the file version for calc.exe might be 5.1.2600.0. Each component is treated independently. For this reason, the system requirements that you set might not provide your expected results. If you do not specify all four components, wild cards are assumed.

  For example, if you set the condition to calc.exe <= 5, you are specifying only the first component of the version number (Major). As a result, versions 5.0.5, 5.1, and 5.1.1.1 also meet the condition.

  However, because each component is independent, if you set the condition to calc.exe <= 5.1, the calc.exe file must be less than or equal to version 5.1 to meet the requirement.

Define Filter Logic

You can use one or more filters to determine whether the policy should be applied to a device. A device must match the entire filter list (as determined by the logical operators that are explained below) for the policy to be applied to the device.

There is no technical limit to the number of filters you can use, but there are practical limits, such as designing a filter structure that is easy to understand and organizing the filters so that you do not create conflicting filters.

Filters, Filter Sets, and Logical Operators

You can add filters individually or in sets. Logical operators, either **AND** or **OR**, are used to combine each filter and filter set. By default, filters are combined using **OR** (as determined by the **Combine Filters Using** field) and filter sets are combined using **AND**. You can change the default and use **AND** to combine filters, in which case filter sets are automatically combined using **OR**. In other words, the logical operator that is to combine individual filters (within in a set) must be the opposite of the operator that is used between filter sets.

You can easily view how these logical operators work. Click both the **Add Filter** and **Add Filter Set** options a few times each to create a few filter sets, then switch between **AND** and **OR** in the **Combine Filters Using** field and observe how the operators change.

As you construct filters and filter sets, you can think in terms of algebraic notation parentheticals, where filters are contained within parentheses, and sets are separated into a series of parenthetical groups. Logical operators (**AND** and **OR**) separate the filters within the parentheses, and the operators are used to separate the parentheticals.

For example, "(u AND v AND w) OR (x AND y AND z)" means "match either uvw or xyz." In the filter list, this looks like:

```
u  AND
v  AND
w
OR
x  AND
y  AND
z
```

Nested Filters and Filter Sets

Filters and filter sets cannot be nested. You can only enter them in series, and the first filter or filter set to match the device is used. Therefore, the order in which they are listed does not matter. You are simply looking for a match to cause the policy to be applied to the device.

Publishing Policies

A policy can include multiple versions:

- **Published version:** The currently active version of the policy. This version is applied to any assigned users and devices.
- **Old versions:** Previously published versions that are not currently active.
- **Sandbox version:** A version that is currently being worked on and has not yet been published as the active version. The Sandbox version is not applied to assigned users and devices until it is published. A Sandbox version can be applied to devices that are designated as test devices. For more information, see Testing Security Policies.

The following sections explain how to republish an old version and publish a Sandbox version:

Republish an Old Version

1. In ZENworks Control Center, click **Policies** to display the Policies page.
2. In the **Policies** list, click the policy for which you want to publish a previous version.
3. In the **Displayed Version** list, select the version you want to publish.
4. After the page refreshes, click **Create Sandbox**.
5. (Optional) Make changes to the Sandbox version.
6. Click **Publish**, then follow the wizard prompts.

Publish a Sandbox Version

When you publish a Sandbox version of a policy, you have the option to publish it as a new version of the current policy or as a completely new policy.

1. In ZENworks Control Center, click **Policies** to display the Policies page.
2. In the **Policies** list, click the policy for which you want to publish a previous version.
3. In the **Displayed Version** list, select **Sandbox**.
4. Click **Publish** to display the Publish Wizard.
5. If you want to publish the Sandbox version as a new version of the current policy, select **Publish as new version**, then click **Finish**.

   or

   If you want to publish the Sandbox version as a new policy, select **Publish as new policy**, fill in the new policy information, then click **Next** and follow the prompts to assign the policy to users and devices before clicking **Finish** to create the new policy.

Renaming, Copying, and Moving Policies

The following sections provide information to help you rename, copy, and move existing security policies in your ZENworks system:

Rename a Policy

If necessary, you can change a policy's name. Renaming a policy does not affect its assignments. However, it must be republished for the name change to be reflected on devices.

1. In ZENworks Control Center, click the **Policies** tab.
2. Select the check box next to the policy you want to rename, then click **Edit** > **Rename**.
3. In the **Name** field, type the new name.
4. Select the **Publish changed display name immediately** check box to make the change immediately available to devices.

   This increments the published policy version and ensures that devices see the name change when the next device refresh occurs. If you do not select this check box, a Sandbox version of the policy is created; the change is not available on devices until after you publish the Sandbox version.
5. Click **OK**.

Copy a Policy

You can copy a policy to create a new policy. All of the policy's system requirements, details, and settings are copied to the new policy. The relationships (device assignments, user assignments, and policy groups) are not copied.

1. In ZENworks Control Center, click the **Policies** tab.
2. Select the check box next to the policy you want to copy, then click **Edit** > **Copy**.

3 In the **Name** field, type the name for the new policy.

4 Click **OK**.

Move a Policy

You can move a policy from one folder in the **Policies** list to another. Moving a policy does not affect the policy's direct assignments to users and devices. It does, however, affect any assignments inherited from its current folder hierarchy.

1 In ZENworks Control Center, click the **Policies** tab.

2 Select the check box next to the policy you want to move, then click **Edit** > **Move**.

3 Browse for and select the destination folder, then click **OK**.

Enabling and Disabling Policies

A security policy can either be enabled or disabled. When a device receives an enabled policy, the Endpoint Security Agent applies the policy. When a device receives a disabled policy, the Endpoint Security Agent ignores the policy.

By default, a security policy is enabled during creation of the policy. The following sections explain how to disable a policy and enable it again.

Disable a Policy

When you disable a policy that is currently assigned to users or devices, the policy is ignored after the next device refresh. When you assign a disabled policy to users or devices, it is not applied until you enable it.

1 In ZENworks Control Center, click the **Policies** tab.

2 Select the check box next to the policy that you want to disable.

3 Click **Action > Disable**.

   In the **Policies** list, the **Enabled** status for the selected policy is changed to **No**.

Enable a Policy

The Endpoint Security Agent does not apply disabled policies that are assigned to the device or the device's user. To have the policy applied, you must enable it:

1 In ZENworks Control Center, click the **Policies** tab.

2 Select the check box next to the policy that you want to enable.

3 Click **Action > Enable**.

   In the **Policies** list, the **Enabled** status for the selected policy is changed to **Yes**.

Replicating Policies to Content Servers

If you have multiple ZENworks Servers or Satellites functioning as content servers, you can choose to replicate a security policy to all content servers or selected content servers. If a security policy is not replicated to a content server, the policy is not available to any devices that connect to that content server for their policies.

A security policy inherits its content replication settings from its policy folder hierarchy or from the Management Zone. If you do not want it to use the inherited replication settings, you can override the settings on the policy.

The following instructions explain how to override the content replication settings for an individual policy. For information about configuring content replication settings on a policy folder or the Management Zone, see "Content" in the *ZENworks Primary Server and Satellite Reference*.

To define the replication settings for a security policy:

1. In ZENworks Control Center, click the **Policies** tab.
2. In the **Policies** list, click the policy to display its properties.
3. Click the **Settings** tab.
4. Configure the content replication settings for the Primary Servers:
   - **4a** In the Policy Management panel, click **Primary Server Replication**.
   - **4b** Click **Override Settings** to activate the Primary Server Replication Status panel.
   - **4c** Select whether or not the policy is replicated to new Primary Servers added to the system.
   - **4d** In the list of existing Primary Servers, select the servers that you want to receive the policy, then click **Include**.

     A check mark appears in the **Included** column for the selected servers.
   - **4e** In the list of existing Primary Servers, select the servers that you don't want to receive the policy, then click **Exclude**.

     The **Included** column is left blank to indicate that the servers are not included in the replication of this policy.
   - **4f** Click **OK** to save the changes.
5. Configure the content replication settings for Satellites:
   - **5a** In the Policy Management panel, click **Satellite Server Replication**.
   - **5b** Click **Override Settings** to activate the Satellite Server Replication Status panel.
   - **5c** Select whether or not the policy is replicated to new Satellite Servers added to the system.
   - **5d** In the list of existing Satellite Servers, select the servers that you want to receive the policy, then click **Include**.

     A check mark appears in the **Included** column for the selected servers.
   - **5e** In the list of existing Satellite Servers, select the servers that you don't want to receive the policy, then click **Exclude**.

     The **Included** column is left blank to indicate that the servers are not included in the replication of this policy.
   - **5f** Click **OK** to save the changes.

The policy's content replication settings are used only by the ZENworks system and do not affect the actual policy. Therefore, changing the replication settings does not require you to republish the policy to assigned devices and users.

Importing and Exporting Policies

You can export security policies from your Management Zone and then import them into another zone or the same zone. This can be useful for exchanging security policies between zones or for backing up important security policies for a single zone.

Exporting and importing is performed through the zman command line utility on the ZENworks Server. The following sections provide instructions:

Export a Policy

When you export a policy, all of the policy data except the relationships (user assignments, device assignments, and policy group membership) is written to an export file. The export file is encrypted so that the data is secure outside of the ZENworks system. Because it is encrypted, you also need to export the policy encryption key with the policy.

Exporting a Policy

1 At a ZENworks Server command prompt, run the following command:

```
zman petf (policy path) (XML policy filepath)
```

(policy path) - The path (including the filename) of the policy object relative to the Policies root folder. For example, FWpolicy1 or ESMpolicies/DEpolicy4.

(XML policy filepath) - The path (including the filename) where you want to save the XML policy file. If you specify only a filename, the file is saved to the current directory. For example, `firewallpolicy.xml` or `c:\firewallpolicy.xml`.

Examples:

```
zman petf FWPolicy1 c:\FWpolicy1.xml
```

```
zman petf ESMpolicies/DEpolicy4 DEpolicy4.xml
```

Exporting the Policy Encryption Key

1 At a ZENworks Server command prompt, run the following command:

```
zman epektf (policy encryption key filepath)
```

(policy encryption key file path) - The path (including filename) where you want to save the security policy encryption key file. If you specify only a filename, the file is saved to the current directory. Use any supported filename for the file. The extension is not important; you can use any extension or no extension. For example, `key.txt`, `key.xml`, and `decryption.file` are all valid filenames.

Examples:

```
zman epektf c:\key.txt
```

```
zman epektf EncryptionKey.xml
```

Import a Policy

When you import a policy from an XML policy file, you can specify the name for the policy and the folder in which to place it.

1 At a ZENworks Server command prompt, run the following command:

```
zman epi (policy name) (policy encryption key filepath) (XML policy
file path) [parent folder]
```

(policy name) - The name to assign to the policy object.

(policy encryption key filepath) - The full path (including the filename) of the security policy encryption key (KMK) file for the Management Zone from which the policy was exported. This file is required to decrypt the encrypted XML file. If the key file is in the current directory, specify only the filename.

(XML policy filepath) - The full path (including the filename) of the encrypted XML policy file. If the file is in the current directory, specify only the filename.

[parent folder] - The Policies folder in which to create the policy object. If you want to create the object in the root folder, ignore this option.

Examples:

```
zman epi FWPolicy c:\key.txt c:\FWpolicy.xml
```

```
zman epi DEPolicy key.txt encryptionpolicy.xml esmpolicies/encryption
```

Managing Policy Groups

If you have multiple policies that you always want assigned together, you can create a policy group and add the policies as group members. Then, rather than assigning the individual policies, you can assign the policy group.

A policy can be a member of more than one policy group. For example, assume that you have 10 policy groups to accommodate the unique firewall and wireless access needs of various groups within your organization. However, all organizations require the same security for data encryption, so you add the same Microsoft Data Encryption policy to all of the policy groups.

The sections in this chapter provide instructions for managing policy groups.

You assign and remove policy groups for users and devices the same way that you assign and remove policies. For information, see Assigning Security Policies and Removing Policy Assignments From Users and Devices.

Create Policy Groups

1 In ZENworks Control Center, click the **Policies** tab.

2 Click **New** > **Policy Group**.

3 Fill in the fields:

Group Name: Provide a name for the policy group. The name must be different than the name of any other item (policy, group, folder, and so forth) that resides in the same folder. The name you provide displays in ZENworks Control Center.

For more information, see Naming Conventions in ZENworks Control Center.

Folder: Type the name or browse to and select the ZENworks Control Center folder where you want the policy to reside. The default is `/policies`, but you can create additional folders to organize your policies.

Description: Provide a short description of the policy group's contents. This description displays in ZENworks Control Center.

4 Click **Next** to display the Add Group Members page, then add the policies you want to be members of the group:

4a Click **Add** to display the Select Members dialog box.

Because you are adding policies to the group, the Select Members dialog box opens with the `Policies` folder displayed.

4b Click next to a folder to navigate through the folders until you find the policy you want to select.

If you know the name of the policy you are looking for, you can use the **Item name** box to search for the item. You can add only policies to the group. You cannot add other policy groups to the group.

4c Click the underlined link in the **Name** column to select the policy and display its name in the **Selected** list box.

4d (Optional) Repeat Step 4b and Step 4c to select additional policies.

4e Click **OK** to add the selected policies.

5 Click **Next** to display the Summary page, review the information and, if necessary, use the **Back** button to make changes to the information.

6 (Optional) Select the **Define Additional Properties** option to display the group's properties page after the group is created. You can then configure additional policy group properties, such as assigning the policy group to devices and users.

7 Click **Finish** to create the group.

Add Policies to Existing Groups

1 In ZENworks Control Center, click the **Policies** tab.

2 Click the policy group to display its properties.

3 In the Members panel, click **Add** to display the Select Members dialog box.

Because you are adding policies to the group, the Select Members dialog box opens with the `Policies` folder displayed.

4 Click next to a folder to navigate through the folders until you find the policy you want to select.

If you know the name of the policy you are looking for, you can use the **Item name** box to search for the item. You can add only policies to the group. You cannot add other policy groups to the group.

5 Click the underlined link in the **Name** column to select the policy and display its name in the **Selected** list box.

6 (Optional) Repeat Step 4 and Step 5 to select additional policies.

7 Click **OK** to add the selected policies to the **Members** list.

8 Click **OK** to save the policy group.

Rename Policy Groups

You can rename a policy group. Renaming a group does not affect the group's assignments to users and devices.

1 In ZENworks Control Center, click the **Policies** tab.

2 In the **Policies** list, select the check box next to the policy group you want to rename.

3 Click **Edit**, then click **Rename**.

4 Type the new name in the **Name** field, then click **OK**.

Move Policy Groups

You can move a policy group from one folder in the **Policies** list to another. Moving a group does not affect the group's assignments to users and devices.

1 In ZENworks Control Center, click the **Policies** tab.

2 In the **Policies** list, select the check box next to the policy group you want to move.

3 Click **Edit**, then click **Move**.

4 Select the destination folder for the policy group, then click **OK**.

Delete Policy Groups

Deleting a policy group does not delete its policies. It does remove all assignments of the policy group to devices and users.

1 In ZENworks Control Center, click the **Policies** tab.

2 In the **Policies** list, select the check box next to the policy group.

3 Click **Delete**, then click **OK** to confirm the deletion.

4 Policy Removal

These sections provide information for removing policy assignments and deleting policies.

- "Removal Best Practices" on page 47
- "Removing Policy Assignments From Users and Devices" on page 48
- "Removing Policy Assignments From the Management Zone" on page 49
- "Deleting Policies" on page 49
- "Deleting Versions of a Policy" on page 49

Removal Best Practices

The following practices provide the best approach to removing security policies that have been deployed to devices.

Practice 1: Remove policy assignments before deleting a policy

Deleting a policy automatically removes the policy assignments. However, we recommend that you remove policy assignments before you delete a policy to see if the policy removal has any negative effects on the device. If so, the policy is still available to reassign.

Practice 2: Ensure removable data drives are accessible post policy removal

When you remove a Microsoft Data Encryption policy from a device, folders encrypted by the policy are decrypted. However, removable data drives encrypted by the policy remain encrypted until they are decrypted using BitLocker management after providing the Unlock Password or a recovery key generated by BitLocker. The recovery key is not automatically generated when deploying the Microsoft Data Encryption Policy.

If you have user password control for removable data drives enabled in the policy at the time you disable or remove the policy, end users can use native BitLocker management to access or decrypt the drive at any time on any computer, whether managed by ZENworks or not, so long as they still know the password. If you have "No unlock password" set in the policy upon policy removal, any new login sessions following policy removal would require the BitLocker recovery key to access or decrypt the drive, which the user may not have.

We recommend the following best practice before removing the Microsoft Data Encryption Policy or any equivalent action such as policy deletion or agent removal:

- Ensure one of the password options below is enabled in the policy and all policy assigned devices are refreshed if this is a change from the **No unlock password** setting.
  - **Always prompt for the unlock password**
  - **Prompt for the password on first use**

- Notify all end users that use managed devices with the Microsoft Data Encryption Policy that mandatory encryption of removable drives by ZENworks via BitLocker will be disabled on their devices, and they should take one of the following actions after policy removal (which might require the Unlock Password) for any removable drives encrypted by ZENworks:
  - Generate and save a BitLocker recovery key for each encrypted drive to an accessible location after policy removable
  - Decrypt encrypted drives after policy removal
  - Move or copy any required files from the encrypted drives to an alternate and accessible location, which would make drive reformatting feasible

Removing Policy Assignments From Users and Devices

When a policy is assigned to an object (device, user, folder, or group), the assignment is reflected as a *relationship* in the policy's properties and in the object's properties. You can edit the relationships for either the policy or the object to remove the assignment.

The following sections provide instructions for two common assignment removal scenarios:

Remove Multiple Policy Assignments From the Same Object

The following instructions explain how to remove multiple policy assignments from a single object such as a device, device folder, device group, user, user folder, or user group. For example, these instructions can be used to remove both an Application Control policy assignment and a Firewall policy assignment from a single device.

1. In ZENworks Control Center, click the object (device, device folder, device group, user, user folder, or user group) from which you want to remove policy assignments.

   For device and user folders, you need to click **Details** next to the folder name rather than click the name.
2. Click **Assignments**.
3. In the Assigned Policies panel, click the **Direct** tab to ensure that it is active.

   The **Direct** tab displays all policies that are assigned directly to the object. Direct assignments are the only assignments you can remove for the object.
4. Select the check box next to the assignments you want to remove, then click **Remove**.

Remove a Single Policy Assignment From Multiple Objects

The following instructions explain how to remove a single policy assignment from multiple objects such as devices, device folders, device groups, users, user folders, or user groups. For example, these instructions can be used to remove an Application Control policy assignment from a device, a device group, and a user at the same time.

1. In ZENworks Control Center, click the **Policies** tab.
2. In the **Policies** list, click the policy for which you want to remove assignments.
3. Click **Relationships.**

4 In the Device Assignments panel, select the check boxes next to the devices, device groups, and device folders that you no longer want the policy assigned to, then click **Remove**.

5 In the User Assignments panel, select the check boxes next to the users, user groups, and user folders that you no longer want the policy assigned to, then click **Remove**.

Removing Policy Assignments From the Management Zone

If you no longer want a policy assigned to the Management Zone, you can remove the policy assignment.

Deleting a policy from the **Policies** list does not remove it from the Zone policy list. When you add a policy to the Zone policy list, a copy of the policy is created for the zone. To remove the assignment from the zone, you must remove the policy from the Zone policy list.

1 If the policy is assigned at the Management Zone, click the **Configuration** tab, click **Endpoint Security Management** (in the Management Zone Settings panel), then click **Zone Policy Settings**.

   or

   If the Zone policy assignment is on a device folder, click the **Devices** tab, locate the folder in the **Devices** list, then click **Details** > **Settings** > **Endpoint Security Management** > **Zone Policy Settings** > **Override** settings.

   or

   If the Zone policy assignment is on a device, click the **Devices** tab, click the device in the **Devices** list, then click **Settings** > **Endpoint Security Management** > **Zone Policy Settings** > **Override** settings.

2 In the list, select the policy you want to remove, and then click **Remove**.

3 Click **OK** to save your changes.

Deleting Policies

When you delete a policy, all assignments of the policy to devices and users are removed.

1 In ZENworks Control Center, click the **Policies** tab.

2 Select the check box next to the policy (or policies) that you want to delete.

3 Click **Delete**.

   If the policy is assigned as a Zone policy, deleting it from the **Policies** list does not remove it from the Zone policies list. To remove it as a Zone policy, you must also delete it from the Zone policies list. For information, see Removing Policy Assignments From the Management Zone.

Deleting Versions of a Policy

When you make changes to a policy and publish the changes, the policy version is incremented (for example, from version 1 to version 2). The old version is retained in case you want to use it as the basis for a new version of the policy.

If you don't want to keep older versions of a policy, you can delete them. Doing so does not delete the currently published policy and does not affect the policy's assignments.

To delete a version of a policy:

1. In ZENworks Control Center, click the **Policies** tab.
2. Double-click the policy to display its property pages.
3. In the **Displayed Version** field, select the version you want to delete.
4. After the page refreshes, click **Delete Selected Version**.

   The selected version is deleted and the published version is displayed.

5 Policy Settings

These sections provide information about configuring settings for most of the security policies. Due to the scale of the Antimalware component in Endpoint Security, Antimalware has a separate reference, which contains configuration information about the four security policies below:

- Antimalware Enforcement
- Antimalware Custom Scan
- Antimalware Network Scan
- Antimalware Scan Exclusions

For information about configuring or modifying any of the Antimalware policies, see the *ZENworks Endpoint Security Antimalware Reference*.

- "Application Control Policy" on page 51
- "Communication Hardware Policy" on page 58
- "Firewall Policy" on page 60
- "Location Assignment Policy" on page 67
- "Microsoft Data Encryption Policy" on page 70
- "Scripting Policy" on page 75
- "Security Settings Policy" on page 78
- "Storage Device Control Policy" on page 80
- "USB Connectivity Policy" on page 85
- "VPN Enforcement Policy" on page 90
- "Wi-Fi Policy" on page 99

Application Control Policy

The following instructions assume that you are on the **Configure Application Control Settings** page in the Create New Application Control Policy Wizard (see Creating Security Policies) or that you are on the **Details** page for an existing Application Control policy (see Editing a Policy's Details).

The Application Control policy lets you control file execution and Internet access for applications. Control extends beyond standard executable files (`.exe`) to include other file types such as `.bat`, `.txt`, `.pdf`, `.mpg`, and so forth.

Configure Application Control Settings

Configuration is done through *application controls*. An application control identifies one or more applications and assigns a behavior to the applications. The supported behaviors are: 1) block file execution, 2) block Internet access, and 3) no restrictions (allow execution and Internet access). The behavior controls all instances of the listed applications, regardless of location (fixed disk, removable storage device, CD/DVD, or network drive).

For example, assume that `App1.exe`, `App2.exe`, and `App3.exe` are instant message applications that you don't want users to run. You could create an application control called Messaging Applications, assign the three applications to the control, and set the behavior to block execution of the applications.

Or, assume that `App4.exe` and `App5.exe` are media applications that access music and video from the Internet. You don't want bandwidth consumed by these types of activities, so you create an application control called Internet Media Applications, assign the two applications to the control, and set the behavior to block Internet access.

NOTE: Application controls are not enforced on files in the %WINDIR% and %ZENSERVER_HOME% directories.

Wildcard usage: The wildcard option provides the capability to implement a control on multiple applications or files with a single entry in the Application Control List or to implement a control on a single application or file without providing the full file name. The asterisk * is the only wildcard option supported in the Application Control policy. A few examples of using the asterisk wildcard for application or file names are provided below. In these examples, the Application Control List is configured for **No Execution**.

CAUTION: Careful consideration should be used when implementing the wildcard for applications in a way that could impede critical system files and processes from running. For example, using the "No Execution" control with a *.exe wildcard or wildcards with dll, bin, or lib file extensions could put a device in non-functional state.

Wildcard Example	Enforced Policy Outcome
*.bat	Blocks execution and opening of all files according to the configured enforcement behavior that have `.bat` as the file extension.
setup.exe	Blocks execution and opening of programs and files according to the configured enforcement behavior that have `setup` as part or all of the file name when using the `.exe` file extension.
notepad.*	Blocks execution of the Notepad program or any files named `notepad` regardless of the file extension, according to the configured enforcement behavior.
iexplore.*	Blocks execution of the Internet Explorer program or any files named `iexplore` regardless of the file extension, according to the configured enforcement behavior.
calc	Blocks execution and opening of programs and files with `calc` in the file name according to the configured enforcement behavior.

Before applying any policy that blocks file execution or Internet access for an application, you should test the policy on a single workstation or server to ensure that no adverse or unexpected results occur. For example, blocking a Microsoft Office application could result in repeated attempts to reinstall the application, which could affect system operation or performance.

The following table provides instructions for managing the policy's application controls:

Task	Steps	Additional Details
Create a new application control	1. Click **Add** > **Create New**. 2. Fill in the following fields: **Name:** Specify a unique name for the control. The name must be different than any other application control. For information about valid characters, see Naming Conventions in ZENworks Control Center. **Description:** This information is optional. You can provide text that helps identify the purpose, creator, or owner of the control. **Default Behavior:** Select one of the following behaviors: ◆ **No Execution:** Blocks the application from executing. Blocks a non-executable file from opening. ◆ **No Internet Access:** Blocks the application from accessing Internet content. ◆ **No Restrictions:** Removes any restrictions (No Execution or No Internet Access) from the application. This enables you to override any restrictions for the application that might be inherited from another Application Control policy. **Applications:** Specify the applications or files to control. To do so, click **New**, type the name of the application or file, then click **OK** to add it to the list. You must specify the full name of the application or file. Partial names and wildcards are not supported. For example, to specify Notepad, you must enter `notepad.exe`, not just `notepad`. Do not specify a path. The control behavior is applied to all instances of the application regardless of location. **Define Another Application Control:** Select this option to create another application control after you finish with this one. 3. Click **OK** to save the control. By default, the application control is enabled. If you do not want it enabled at this time, deselect the **Enabled** box. Disabling the application control leaves it in the policy but excludes it from being enforced when the policy is applied to a device.	The following applications cannot be blocked: ◆ `winlogon.exe` ◆ `svchost.exe` ◆ `taskmgr.exe` ◆ `lsass.exe` ◆ `wmiprvse.exe` ◆ `services.exe` ◆ `explorer.exe` ◆ `smss.exe` ◆ `dllhost.exe` ◆ `csrss.exe`

Task	Steps	Additional Details
Copy an existing application control list from another policy	1. Click **Add** > **Copy Existing**. 2. Select the Application Control policies whose lists you want to copy. 3. Click **OK**.	All application controls included in the selected policies are copied. If necessary, you can edit the copied controls after they are added to the list.
Import an application control from a policy export file	1. Click **Add** > **Import**. 2. Click the button. 3. Click the **Browse** button to display the **File Upload** dialog box. 4. Select the export file containing the application controls you want to import, then click **Open**. 5. In the Select File dialog box, click **OK**. 6. In the Import File dialog box, click **OK** to import the application controls to the list.	All application controls included in the export file are imported. If necessary, you can edit the imported controls after they are added to the list. For information about exporting controls, see Export an application control.
Edit an application control	1. Click the application control name. 2. Modify the fields as desired. 3. Click **OK**.	
Rename an application control	1. Select the check box next to the application control name, then click **Edit** > **Rename**. 2. Modify the name as desired. 3. Click **OK**.	
Export an application control	1. Select the check box next to the application control name. You can select multiple controls to export. 2. Click **Edit** > **Export**. 3. Save the file. The default name given to the file is `sharedComponents.xml`. You can change the name if desired. Do not change the `.xml` extension.	
Delete an application control	1. Select the check box next to the application control name, then click **Delete**. 2. Click **OK** to confirm deletion of the control.	

Configure Enforcement Behavior on Running Processes

The enforcement behavior determines when enforcement occurs for applications that are already running when the policy is applied. Choose from the following options:

- **Ignore:** Do not enforce the application control behavior. For example, if the application is not allowed to execute (**No Execution** setting), allow the application to continue to run. Or, if the application is not allowed to access the Internet (**No Internet Access** setting), allow the application to continue to access the Internet.
- **Enforce immediately:** Enforce the application control behavior immediately. For example, if the application is not allowed to execute (**No Execution** setting), terminate the application immediately.

  With immediate enforcement, the user does not receive any warning. If you want the user to know why the application was terminated, you can use the Display message when enforcing behavior option.
- **Enforce after *XX* minutes:** Enforce the application control behavior after the specified number of minutes. For example, is you set this option to 5 minutes (the default) and the application is not allowed to execute (**No Execution** setting), terminate the application after 5 minutes.

  If the application is running when the policy is applied, a Policy Violations dialog box is displayed to inform the user that the application will be terminated after the specified number of minutes. The dialog box includes the application executable name and a countdown of the time remaining until the application is terminated. If multiple applications violate the policy, all applications are listed.

  - **Allow the user to delay enforcement for an additional XX minutes:** Select this option if you want to allow the user to delay the enforcement beyond the time specified by the **Enforce after XX minutes** option. The additional time is applied only if the user clicks the **Delay All** button in the Policy Violations dialog box.

    For example, assume that you set the **Enforce after XX minutes** option to 5 minutes and this option to 10 minutes. At any time before the first 5 minutes expires, the user can click the **Delay All** button to delay the enforcement for an additional 10 minutes.
- **Display message when enforcing behavior:** You can also display a message when enforcing the application control behavior. For example, if you select the **Enforce immediately** option, you can display a message informing the user why the application was terminated.

  To use a display message, select the **Display message when enforcing behavior** option, then fill in the following fields:

  - **Title of Message Window:** Specify the Message Window's title. For example, "Application Shutdown Alert."
  - **Body:** Provide the text for the message body.
  - **Message Hyperlink:** If you want to include a hyperlink in the message, select **Include message hyperlink**, then fill in the following:

    - **Display Text:** The text to display as the hyperlink in the message.
    - **Link:** The Web URL to be executed when the display text is clicked. Any link that starts with http, https, or www is treated as a Web URL and launches a Web browser.

      For example, when linking to a URL, you might include `www.acme.com/appusage` to a open a Web page that provides your corporate policy on authorized application usage.

Communication Hardware Policy

The following instructions assume that you are on the **Configure Communication Hardware Settings** page in the Create New Communication Hardware Policy Wizard (see Creating Security Policies) or that you are on the **Details** page for an existing Communication Hardware policy (see Editing a Policy's Details).

The Communication Hardware policy controls access for communication hardware, including being able to completely disable a hardware type (Bluetooth, wired, wireless, and so forth) or limit a hardware type to specific adapters.

Configure Communication Hardware Settings

This panel lets you control which communication hardware is enabled on a device.

General Settings

The General Settings let you configure the access for the following communication hardware:

- **1394 (FireWire):** Controls the IEEE 1394 bus.
- **IrDA:** Controls the infrared access port.
- **Bluetooth:** Controls Bluetooth access if the device is using the Widcomm Bluetooth Stack software driver to provide the access. Other Bluetooth drivers are not supported.
- **Serial:** Controls the serial communication ports.
- **Parallel:** Controls the parallel communication ports.
- **Dialup/Cellular:** Controls the dialup and cellular adapters.
- **Wired:** Controls the wired network adapters.
- **Wi-Fi:** Controls the Wi-Fi network adapters.
- **Virtual:** Controls the virtual network adapters. Virtual network adapters are programs (rather than actual physical adapters) that allow devices to connect to a network. Virtual private network (VPN) software uses virtual network adapters.

Choose from the following options to configure the communication hardware access. Not all of the options are available for each hardware type.

- **Enable:** Enable access for the hardware. If you select this option for dialup/cellular, wired, or Wi-Fi hardware in a location-based policy, you can use the Approved Adapters list to restrict access to specific adapters.
- **Disable:** Disable access for the hardware.
- **Inherit:** If the policy's **Inherit from Policy Hierarchy** setting is enabled, inherit this setting from other Communication Hardware policies assigned higher in the policy hierarchy. For example, if you assign this policy to a user, the setting is inherited from any Communication Hardware policies assigned to the user's groups, folders, or zone.
- **Disable Dialup/Cellular When Wired:** Disable dialup and cellular access if a wired connection is enabled.
- **Disable Wi-Fi When Wired:** Disable Wi-Fi access if a wired connection is enabled.

Approved Adapters

By default, if you allow access for dialup, wired, or wireless hardware, all adapters are allowed. If you want to allow only specific adapters, you can add the adapters to the appropriate Approved Adapters lists (wired, Wi-Fi, or dialup).

When you add an adapter to a list (**Wired**, **Wi-Fi**, or **Dialup**), only the adapters in the approved list are allowed. For example, if you add Adapter1 and Adapter2 to the Approved Wi-Fi Adapters list, those two adapters are the only Wi-fi adapters that are allowed communication access.

The following table provides instructions for managing the approved adapter lists:

Task	Steps
Add an adapter	1. Click the tab (**Approved Wired Adapters**, **Approved Wi-Fi Adapters**, or **Approved Dialup/Cellular Adapters**) where you want to add the adapter. 2. Click **Add**. 3. Fill in the following fields to define the adapter: **Name:** Specify the adapter name. Names are not case sensitive. The Name field is a partial match field, meaning that the name only needs to match any part of an adapters name for that adapter to be approved. For example, *Adapter1* not only matches *Adapter1* but also matches *Adapter10* and *Acme Adapter100*. The more complete the name, the more limited the matches. **MAC Address:** This field applies only to Wi-Fi and wired adapters; it does not apply to dialup/cellular adapters. The MAC address, which is a unique identifier assigned by the manufacturer of the network adapter, is optional. You can use it to more narrowly identify the adapter you want to approve. Specify the MAC address using the following format: xx:xx:xx:xx:xx:xx. For example, 01:C0:23:45:67:89. 4. Click **OK** to add the adapter to the approved list.
Modify an adapter's settings	1. Click the tab (**Approved Wired Adapters**, **Approved Wi-Fi Adapters**, or **Approved Dialup/Cellular Adapters**) with the adapter you want to modify. 2. Click the adapter name. 3. Modify the settings as desired. 4. Click **OK** to save the changes.
Remove an adapter	1. Click the tab (**Approved Wired Adapters**, **Approved Wi-Fi Adapters**, or **Approved Dialup/Cellular Adapters**) with the adapter you want to remove. 2. Select the check box next to the adapter name, then click **Delete**. 3. Click **OK** to confirm removal of the adapter.

Disable Adapter Bridging Control Settings

This panel lets you prevent a device's network adapters from being bridged. Bridging, which enables the device to act as a hub for access to multiple network segments, can create a significant breach in your network security.

Adapter Bridging

Select one of the following options:

- **Enable:** Enables adapter bridging.
- **Disable:** Disables adapter bridging.
- **Inherit:** If the policy's **Inherit from Policy Hierarchy** setting is enabled, inherit this setting from other Communication Hardware policies assigned higher in the policy hierarchy. For example, if you assign this policy to a user, the setting is inherited from any Communication Hardware policies assigned to the user's groups, folders, or zone.

Use Disable Adapter Bridging Message

This setting is available only if adapter bridging is disabled.

Select this option to display a message dialog box when adapter bridging is disabled and a user attempts to create a bridge. Use the **Title of Message Window**, **Body**, and **Message Hyperlink** fields to create the message you want displayed.

Firewall Policy

The following instructions assume that you are on the **Configure Firewall Settings** page in the Create New Firewall Policy Wizard or (see Creating Security Policies) or that you are on the **Details** page for an existing Firewall policy (see Editing a Policy's Details).

The Firewall policy lets you determine the firewall settings applied to a device.The firewall settings control a device's network connectivity by allowing or blocking ports, protocols, and network addresses (IP and MAC).

- "Configure the Default Behavior" on page 60
- "Disable Windows Firewall and Register Endpoint Security Management Firewall in Windows Security Center" on page 61
- "Configure Port/Protocol Rules" on page 61
- "Configure Standard Access Control Lists" on page 63
- "Create Custom Access Control Lists" on page 64

Configure the Default Behavior

Specify the default behavior for ports and protocols. The default behavior is applied to all ports and protocols unless it is overridden by a port/protocol rule or an Access Control List.

Select one of the following behaviors:

- **Stateful:** Blocks all unsolicited inbound network traffic. Allows all solicited inbound network traffic and all outbound network traffic.
- **Open:** Allows all inbound and outbound network traffic. Because all network traffic is allowed, a device's identity is visible on all ports.

- **Closed:** Blocks all inbound and outbound network traffic. Because all network identification requests are blocked, a device's identity is concealed on all ports.

  If you select this option, you should enable the ZENworks Server ACL and ARP ACL (see Configure Standard Access Control Lists) to ensure that the device can communicate with ZENworks Servers to receive content (policies, bundles, and so forth) and upload report data.
- **Inherit:** If the policy's **Inherit from Policy Hierarchy** setting is enabled, inherits this setting value from other Firewall policies assigned higher in the policy hierarchy. For example, if you assign this policy to a user, the setting value is inherited from any Firewall policies assigned to the user's groups, folders, or zone.

Disable Windows Firewall and Register Endpoint Security Management Firewall in Windows Security Center

Select **Yes** to turn off the Windows Firewall and register the Endpoint Security Agent as the firewall provider in the Windows Security Center. This ensures that the Firewall policy's settings and the Windows Firewall settings do not conflict and generate unexpected results.

Select **Inherit** to inherit this setting value from other Firewall policies assigned higher in the policy hierarchy. For example, if you assign this policy to a user, the setting value is inherited from any Firewall policies assigned to the user's groups, folders, or zone.

Please be aware of the following when using this option:

- On Windows devices that are members of a domain, the GPO setting **Turn On Security Center (Domain PC's Only)** must be enabled. If the setting is not enabled and you apply a Firewall policy that disables the Windows Firewall, the Endpoint Security Agent is unable to turn off the Windows Firewall; the result is that both the Windows and Endpoint Security firewalls are active.
- This setting disables only the Windows Firewall. If the device has other (third-party) firewalls active, those firewalls are not disabled and could conflict with the Endpoint Security firewall. We recommend that you disable any other firewalls.

Configure Port/Protocol Rules

The port/protocol rules let you override the default behavior assigned to ports and protocols. A rule identifies one or more ports or protocols and the behavior to be applied to the ports and protocols.

For example, assume that you want to block streaming media. You would create a Streaming Media rule and close ports 554, 1755, 7070, and 8000 (the common Microsoft and RealMedia streaming media ports) to TCP communication.

The following table provides instructions for managing the policy's port/protocol rules:

Task	Steps	Additional Details
Create a new rule	1. Click **Add** > **Create New**. 2. Fill in the following fields: **Name:** Specify a unique name for the rule. The name must be different than any other rule. For information about valid characters, see Naming Conventions in ZENworks Control Center. **Description:** This information is optional. You can provide text that helps identify the purpose, membership, creator, or owner of the rule. **Default Behavior:** Select one of the following behaviors: ◆ **Stateful:** All unsolicited inbound network traffic is blocked. All outbound network traffic is allowed. ◆ **Open:** All inbound and outbound network traffic is allowed ◆ **Closed:** All inbound and outbound network traffic is blocked **Port/Protocol Types:** Specify the ports and protocols to add to the rule. To do so, click **New**, select the port type (TCP, UDP, or TCP/UDP) or the protocol type (Ether or IP). For TCP, UDP, and TCP/UDP, specify the starting and ending ports, then click **OK** to add the port to the rule. For Ether and IP, specify the starting and ending ether type or protocol type, then click **OK** to add the protocol to the rule. If you want to define a single port or protocol rather than a range, enter only a starting number. **Define Another Rule:** Select this option to create another port/protocol rule after you finish with this one. 3. Click **OK** to save the rule.	
Copy an existing rule from another policy	1. Click **Add** > **Copy Existing**. 2. Select the Firewall policies whose lists you want to copy. 3. Click **OK**.	All rules included in the other Firewall policies are copied. If necessary, you can edit the copied rules after they are added to the list.

Task	Steps	Additional Details
Import a rule from a policy export file	1. Click **Add** > **Import**. 2. Click 🔍 to display the Select File dialog box. 3. Click **Browse**, select the export file, then click **OK**. 4. Click **OK** to add the rules to the list.	All rules included in the export file are imported. If necessary, you can edit the imported rules after they are added to the list. For information about exporting rules, see Export a rule.
Enable or disable a rule	1. Locate the rule in the list 2. In the **Enabled** column, select the check box to enable the rule. or Deselect the check box to disable the rule.	When you add a rule it is enabled by default. You can disable a rule to save it in the policy but no longer apply it.
Edit a rule	1. Click the rule name. 2. Modify the fields as desired. 3. Click **OK**.	
Rename a rule	1. Select the check box next to the rule name, then click **Edit** > **Rename**. 2. Modify the name as desired. 3. Click **OK**.	
Export a rule	1. Select the check box next to the rule name. You can select multiple rules to export. 2. Click **Edit** > **Export**. 3. Save the file. The default name given to the file is `sharedComponents.xml`. You can change the name if desired. Do not change the `.xml` extension.	
Delete a rule	1. Select the check box next to the rule name, then click **Delete**. 2. Click **OK** to confirm deletion of the rule.	

Configure Standard Access Control Lists

The standard Access Control Lists (ACLs) represent predefined protocol packet types. For each ACL, select one of the following settings. The ACL setting overrides the default behavior and any port/protocol rules.

- **Allow:** Allows the ACL's protocol packets.
- **Inherit:** If the policy's **Inherit from Policy Hierarchy** setting is enabled, inherits this setting from other Firewall policies assigned higher in the policy hierarchy. For example, if you assign this policy to a user, the setting is inherited from any Firewall policies assigned to the user's groups, folders, or zone.

The following list provides a brief descriptions of each ACL:

- **802.1x:** Allows 802.1x packets. To overcome deficiencies in Wired Equivalent Privacy (WEP) keys, Microsoft and other companies are utilizing 802.1x as an alternative authentication method. 802.1x is a port-based network access control that uses the Extensible Authentication Protocol (EAP) or certificates. Currently, most major wireless card vendors and many access point vendors support 802.1x. This setting also allows Light Extensible Authentication Protocol (LEAP) and Wi-Fi Protected Access (WPA) authentication packets.
- **ARP:** Allows Address Resolution Protocol (ARP) packets. Address resolution refers to the process of finding an address of a computer in a network. The address is resolved by using a protocol in which a piece of information is sent by a client process executing on the local computer to a server process executing on a remote computer. The information received by the server allows the server to uniquely identify the network system for which the address was required and therefore to provide the required address. The address resolution procedure is completed when the client receives a response from the server containing the required address.
- **Ethernet Multicast:** Allows Ethernet Multicast packets. Multicast is a bandwidth-conserving technology that reduces traffic by simultaneously delivering a single stream of information to thousands of corporate recipients and homes. Applications that take advantage of multicast include video conferencing, corporate communications, distance learning, and distribution of software, stock quotes, and news. Multicast packets can be distributed by using either IP or Ethernet addresses.
- **ICMP:** Allows Internet Control Message Protocol (ICMP) packets. ICMP packets are used by routers, intermediary devices, or hosts to communicate updates or error information to other routers, intermediary devices, or hosts. ICMP messages are sent in several situations; for example, when a datagram cannot reach its destination, when the gateway does not have the buffering capacity to forward a datagram, and when the gateway can direct the host to send traffic on a shorter route.
- **IP Multicast:** Allows IP Multicast packets. Multicast is a bandwidth-conserving technology that reduces traffic by simultaneously delivering a single stream of information to thousands of corporate recipients and homes. Applications that take advantage of multicast include video conferencing, corporate communications, distance learning, and distribution of software, stock quotes, and news. Multicast packets can be distributed by using either IP or Ethernet addresses.
- **IP Subnet Broadcast:** Allows Subnet Broadcast packets. Subnet broadcasts are used to send packets to all hosts of a subnetted, supernetted, or otherwise nonclassful network. All hosts of a nonclassful network listen for and process packets addressed to the subnet broadcast address.
- **Logical Link Layer Control:** Allows LLC-encoded packets.
- **SNAP:** Allows SNAP-encoded packets. Subnetwork Access Protocol (SNAP) is an extension of the Logic Link Control (LLC IEEE 802.2) header and is used for encapsulating IP datagrams and ARP requests and replies on IEEE 802 networks.
- **ZENworks Server:** Allows packets sent to and received from the ZENworks Server.

Create Custom Access Control Lists

You can create custom Access Control Lists (ACLs) to define specific IP or MAC addresses from which unsolicited traffic should always be blocked or should always be allowed. An ACL setting overrides port rules and the default port behavior.

The following table provides instructions for managing the ACLs:

Task	Steps	Additional Details
Create a new ACL	1. Click **Add** > **Create New**. 2. Fill in the following fields: **Name:** Specify a unique name for the Access Control List. For information about valid characters, see Naming Conventions in ZENworks Control Center. **Description:** Provide optional text that helps identify the purpose, membership, creator, or owner. **ACL Behavior:** Select **Trusted** to specify that membership in this ACL allows access. Select **Non-Trusted** to specify that membership in this ACL denies access. **Configure Optional Ports:** By default, the ACL behavior is applied to all ports. For example, if the ACL behavior is trusted, all ports trust the addresses included in the ACL. If you want the ACL to apply to only specific ports, select this option then specify the ports and the behavior for the ports (**Open**, **Closed**, or **Stateful**). This causes the ACL Behavior setting to be ignored in favor of the individual port behavior settings. **Address Types:** Specify the IP and MAC addresses that are members of the ACL. To do so, click **New**, select the type (**IP Address or DNS Name**, **MAC Address**, or **Macro**), specify the appropriate address or select the desired macro, then click **OK**. The macros are predefined IP address groups. For example, **All DHCP** applies the ACL behavior to a device's current DHCP server IP addresses while Default DHCP applies it to the current Default DHCP server IP address. **Define Another Access Control List:** Select this option to create another Access Control List after you finish with this one. 3. Click **OK** to save the Access Control List. By default, the ACL is enabled. If you do not want it enabled at this time, deselect the **Enabled** box.	Use one of the following formats: ◆ xxx.xxx.xxx.xxx: Standard dotted-decimal notation for a single address. For example, 123.45.167.100. ◆ xxx.xxx.xxx.xxx/n: Standard CIDR (Classless Inter-Domain Routing) notation. For example, 123.45.167.100/24 matches all IP addresses that start with 123.45.167. ◆ www.domain_name: Standard domain name notation. For example, www.novell.com. ◆ www.domain_name/n: Standard CIDR (Classless Inter-Domain Routing) notation for a domain name. For example, www.novell.com/16. **IMPORTANT:** To enforce the ACL, an IP address range is expanded to individual IP addresses. A large range can consume significant resources on the device and impact performance. To minimize this impact, define ranges that include only the IP addresses you want to control. Use the following format when specifying a MAC address: xx:xx:xx:xx:xx:xx. For example, 01:23:45:67:89:ab.

Task	Steps	Additional Details
Copy an existing ACL from another policy	1. Click **Add** > **Copy Existing**. 2. Select the Firewall policies whose ACL you want to copy. 3. Click **OK**. **NOTE:** An identifier (GUID) from the policy being copied is appended to each ACL rule name to distinguish it from the original. Each ACL rule must have a unique name.	All ACLs included in the other Firewall policies are copied. If necessary, you can edit the copied ACLs after they are added to the list.
Import an ACL from a policy export file	1. Click **Add** > **Import**. 2. Click to display the Select File dialog box. 3. Click **Browse**, select the export file, then click **OK**. 4. Click **OK** to add the ACLs to the list.	All ACLs included in the export file are imported. If necessary, you can edit the imported ACLs after they are added to the list. For information about exporting ACLs, see Export an ACL.
Enable or disable an ACL	1. Locate the ACL in the list 2. In the **Enabled** column, select the check box to enable the ACL. or Deselect the check box to disable the ACL.	When you add an ACL it is enabled by default. You can disable an ACL to save it in the policy but no longer apply it.
Edit an ACL	1. Click the ACL name. 2. Modify the fields as desired. 3. Click **OK**.	
Rename an ACL	1. Select the check box next to the ACL name, then click **Edit** > **Rename**. 2. Modify the name as desired. 3. Click **OK**.	
Export an ACL	1. Select the check box next to the ACL name. You can select multiple ACLs to export. 2. Click **Edit** > **Export**. 3. Save the file. The default name given to the file is `sharedComponents.xml`. You can change the name if desired. Do not change the `.xml` extension.	
Delete an ACL	1. Select the check box next to the ACL name, then click **Delete**. 2. Click **OK** to confirm deletion of the ACL.	

Location Assignment Policy

The following instructions assume that you are on the **Configure Allowed Locations** page in the Create New Location Assignment Policy Wizard (see Creating Security Policies) or that you are on the **Details** page for an existing Location Assignment policy (see Editing a Policy's Details).

The Location Assignment policy lets you specify the locations against which the Endpoint Security Agent compares its network environment to determine its location. Only the locations included in the Allowed Locations list are considered.

For example, assume that you have defined four locations (**Configuration** tab > **Locations**). Locations 1 through 3 are common locations you want available to all devices, but Location 4 is required by only a few devices. You include the first three locations in this policy and exclude the fourth location. When applying this policy, the ZENworks Agent evaluates the device's current network environment against the three defined locations to determine the location.

Inherit from Policy Hierarchy

ZENworks utilizes a management hierarchy, or structure, that is ordered as follows:

1. Management Zone
2. Folder/Group
3. Device/User

Polices can be assigned at each level. Assignments flow down, which means that policy assignments made at the Management Zone apply to all devices or users in the zone. Likewise, policy assignments made to a folder or group apply to all members of the folder or group. As a result of hierarchical assignments, it is possible for a device or user to be assigned multiple policies of the same type.

The **Inherit from Policy Hierarchy** option determines whether or not this policy can inherit settings from other policies (of the same type) that are above it in the hierarchy. Consider the following table:

Hierarchy Level	Policy (same type)	Inherit from Policy Hierarchy	Policy Setting 1 (Single-Value)	Policy Setting 2 (Single Value)	Policy Setting 3 (Multi-Value)
Zone	Policy_3	Yes	10	False	Device4,Device5
User Group 1	Policy_2	Yes	Inherit	Inherit	Device2;Device3
User A	Policy_1	Yes	Inherit	True	Device1;Device2

User A is directly assigned Policy_1. Because User A is a member of User Group 1 and the Zone, User A is indirectly assigned Policy_2 and Policy_3.

All three of the policies allow for inheritance. As a result, the final policy settings are determined by using the following method:

1. Evaluation of policy settings begins with the lowest policy in the hierarchy (the policy closest to the user). In this case, Policy_1 is the lowest policy (because it is assigned directly to User A) and is evaluated first.

2. If one of the Policy_1 settings is configured as **Inherit**, then the setting is inherited from Policy_2; if the Policy_2 setting is configured as **Inherit**, then the setting is inherited from the next policy in the hierarchy, which is Policy_3.
3. Multi-value policy settings, such as tables, do not have an **Inherit** setting. With multi-value settings, all values from the assigned policies are combined.

Applying the inheritance methodology to the example in the above table, the resulting Policy_1 settings for User A are:

Hierarchy Level	Policy (same type)	Inherit from Policy Hierarchy	Policy Setting 1 (Single-Value)	Policy Setting 2 (Single Value)	Policy Setting 3 (Multi-Value)
User A	Policy_1	Yes	10 (inherited from Policy_3)	True	Device1;Device2 Device3 (inherited from Policy_2) Device4;Device5 (inherited from Policy_3)

Inheritance hierarchy also applies to the precedence of user and device assigned policies in the same hierarchy level. For example, if there are multiple same-type user-assigned policies in the same hierarchy level, policy settings will only flow down to policies lower in the policy list if the **Inherit from Policy Hierarchy** option is applied to the policy higher in the list. In the case of both user and device assigned policies, the conflict resolution rules will also apply. Consider the following table:

Hierarchy Level	Policy (same type)	Inherit from Policy Hierarchy	Policy Setting 1	Policy Setting 2 (Multi-Value)
User A	Policy 1	Yes	10	Device1;Device2
User A	Policy 2	No	5	Device3;Device4
User A	Policy 3	Yes	0	Device3;Device5

In the example above, three policies are assigned to User A in the precedence order shown in the table. Because **Inherit for Policy Hierarchy** is disabled in Policy 2, Policy 3 settings are blocked. The table below shows how the settings are applied.

1. Policy Setting 1 is set to 10, because Policy 2 inherits from Policy 1, overriding 5.
2. Policy Setting 2 includes Device1-4, applying settings from both Policy 1 and Policy 2, but ignoring Device5 from Policy 3, because inherit is disabled in Policy 2.

Hierarchy Level	Policy (same type)	Inherit from Policy Hierarchy	Policy Setting 1	Policy Setting 2 (Multi-Value)
User A	Policy 1, Policy 2	Yes	10	Device1;Device2; Device3;Device4

Manage Allowed Locations

You use the **Allowed Locations** list to add the locations that are allowed by this policy. By default, the Unknown location is automatically added to the policy. This enables the device to fail over to the Unknown location if the current network environment does not match any of the policy's locations.

The following table provides instructions for managing the allowed locations:

Task	Steps
Add a location	1. Click **Add** to display the Select Locations dialog box. 2. Click the locations you want to add to the list. You can add only existing locations. Locations are created on the Locations page (**Configuration** tab > **Locations**) 3. Click **OK** to add the locations.
Modify a location's settings	1. Select the check box next to the location > click **Edit**. 2. Modify the settings as desired: **Allow Manual Change:** Select **Yes** to let the user change to the location and change from the location. For example, assume the policy includes three locations. This setting is enabled for Location1 and Location2, but not for Location3. If the agent determines the current location to be Location1, the user can manually change to Location2 but not to Location3. This is because Location1 and Location2 both allow manual changes, but Location3 does not. If the agent determines that the location is Location3, the user cannot change the location. Select **Inherit** to inherit this setting value from other Location Assignment policies assigned higher in the policy hierarchy. **Show Location in Agent List:** Select **Yes** to include the location in the list of locations displayed when the user right-clicks the agent's ZENworks icon. Select **Inherit** to inherit this setting value from other Location Assignment policies assigned higher in the policy hierarchy. **Use Location Message:** Display a custom message when the agent switches to this location. This message can provide instructions for the user, give details about policy restrictions under this location, or include a hyperlink to more information. 3. Click **OK**.
Remove a location	1. Select the check box next to the location name, then click **Remove**. 2. Click **OK** to confirm removal of the location.

Microsoft Data Encryption Policy

The following instructions assume that you are on the **Configure BitLocker Encryption for Removable Data Drives** page in the Create New Microsoft Data Encryption Policy Wizard (see Creating Security Policies) or that you are on the **Details** page for an existing Microsoft Data Encryption policy (see Editing a Policy's Details).

The Microsoft Data Encryption policy manages Microsoft's BitLocker and Encrypting File System (EFS) tools to encrypt removable drives and fixed disk folders, respectively.

Refer to the sections below for policy details:

- "General Information" on page 70
- "Removable Data Drives" on page 71
- "Fixed Disk Folders" on page 73

General Information

As you configure Microsoft Data Encryption policies and apply them to devices, be aware of the following:

- The Microsoft Data Encryption policy is a device-only policy. It cannot be assigned to users.
- The Microsoft Data Encryption policy does not support inheritance. The Microsoft Data Encryption policy that is assigned closest to the device becomes the effective policy for the device. For example, if a Microsoft Data Encryption policy is assigned to a device and to a group in which the device is a member, the device-assigned policy becomes the effective policy and the policy assigned to the device group is ignored.

When the policy is applied to a managed device, users are automatically notified upon drive insertion of the policy's enforcement. The notification can take several forms depending upon the state of the removable drive and the settings in the policy.

Operating System Requirements

Microsoft BitLocker is native to the operating systems listed below:

- Windows 7 Ultimate and Enterprise (cannot encrypt used sectors only)
- Windows 8 and 8.1 Professional and Enterprise
- Windows 10 Professional, Enterprise, and Education

Removable Data Drives

You can use ZENworks to control Microsoft BitLocker encryption of removable data drives (RDD) on managed devices when the Microsoft Data Encryption Policy is applied to those devices. Removable Data Drives encryption can be enabled or disabled, giving you the ability to apply the policy to devices for one or both policy options, (1) Removable Data Drives encryption and (2) Fixed Disk Folder encryption.

The policy enables you to configure locking and unlocking of encrypted data drives using either a user password or auto-unlock feature when drives are used on managed devices. Depending on the configuration options you choose, you can also enable RDDs that are encrypted via this policy to support unlocking the drives on non-managed devices.

Removable data drives include, but are not limited to, USB thumb drives and externally attached hard drives.

Continuing reading for information about each of the configurable options for encrypting removable data drives.

Enable Removable Data Drive encryption

This box must be checked for encryption of removable data drives to be enabled on devices with the Microsoft Data Encryption Policy enforced. With the capability to disable encryption of removable data drives, you can still have Fixed Disk Folder encryption enabled when a Microsoft Data Encryption policy is enforced.

Encryption Algorithm

Both the AES-CBC and the XTS-AES algorithms use AES (Advance Encryption Standard) with 256-bit encryption. **Compatible mode** encryption provides the greatest compatibility on Windows 7 and newer operating systems. **New encryption mode** is a newer encryption algorithm that works only on Windows 10 version 1511 and newer operating systems.

If you use the policy on devices with both Windows 10 v1511 and earlier operating systems, you can choose the **XTS-AES if supported** option, and the policy will automatically apply XTS-AES encryption to Windows 10 v1511 and AES-CBC encryption to earlier OS versions.

Initial Encryption

You can set the encryption for **used drive space only** or the **entire drive**. The former is the fastest means of encryption, but the latter provides the greatest security, because it ensures that any deleted files are not recoverable.

Unlock Method

The options for unlocking removable data drives include both managed and non-managed devices. You can enable the user to provide an unlock password to unlock the drive on any device. Or, you can use the zone encryption key for the drive with no user unlock password, so only managed devices in your zone will be unlocked.

- **Always prompt for the unlock password:** This option requires a password every time the user inserts the drive into a device, whether the device is a managed or non-managed device. It enables the user to unlock the drive on any Windows device.
- **Prompt for the unlock password on first use:** This option uses the BitLocker Auto-Unlock feature. The first time the user inserts a drive into the device the unlock password is required. Subsequent uses on the same device do not require the password. This option also enables the user to unlock the drive on any Windows device.

- **No unlock password:** This option uses the zone encryption key to unlock the drive on managed devices only. Select this option to automatically unlock BitLocker encrypted drives in the management zone. The drive is automatically unlocked without a user password when inserting the drive into a managed device, but it cannot be unlocked on non-managed devices.

  To unlock a removable drive that uses this setting on a device in a different zone, you need to export the encryption key from the zone managing the encryption and import it into the alternate zone. The Microsoft Data Encryption policy must also be enforced on the device in the alternate zone. For more information, see Data Encryption Key Management.

- **Require a strong unlock password:** Select this option to force users to define an unlock password that meets the following requirements when using a password option:
  - Eight or more characters
  - At least one of each of the four types of characters:
    - uppercase letters from A to Z
    - lowercase letters from a to z
    - numbers from 0 to 9
    - at least one special character ~ ! @ # $ % ^ & * ( ) + { } [ ] : ; < > ? ,. / - = | \ ”

  For example: y9G@wb?

Encrypted Drives

If you have a drive that is already BitLocker encrypted, you can enable the drive to retain its current BitLocker settings to be used on managed devices, or you can apply the policy settings to the encrypted drive.

If the drive was BitLocker encrypted via ZENworks, you can also enable the policy to override the existing encryption settings if they are different than this policy’s settings.

NOTE: Changing an encrypted drive's BitLocker settings might require the drive to be decrypted and then re-encrypted. This will be done automatically if required.

Excluded Drives

All removable data drives are encrypted by default. Use the Excluded Drives option to add removable drives that you do not want encrypted.

You can add drives for exclusion, copy existing exclusions to use as a template for adding drive exclusions, and import or export exclusions to be used from or in a different policy, respectively.

- **Create New:** Click **Add** > **Create New** to manually define the drive to be excluded. When the Add Drive to Exclude from Encryption dialog box is displayed, click the Help icon in the upper-right corner of the dialog box for details about defining a drive.
- **Copy Existing:** Click **Add** > **Copy Existing** to copy drives that are already defined in other Microsoft Data Encryption policies. When you copy excluded drives from another policy, all drives are copied; after the copy is complete, you can remove any unwanted drives from the list.
- **Import:** You can import drives from a policy export file or from a Device Scanner file. Only class 8 (Mass Storage) drives are imported; all other drive classes are ignored.

To import drives from a policy export file, click **Add** > **Import**, make sure that **Existing Policy/Component** is selected in the **Select Source of Data** list, then browse for and select the policy export file.

To import drives from a Device Scanner file, click **Add** > **Import**, then select **ZESM Device Scanner Tool** in the **Select Source of Data** list. Browse for and select the Device Scanner file to import, then select the data fields you want imported. The recommended data fields are selected by default. You can deselect any recommended data fields and select any additional fields. The more data fields that you import, the more you limit the number of matches for a drive. If you include all of the data fields for a scanned device, you can literally isolate a drive definition to the specific USB port on the computer where the drive was scanned.

- **Export:** You can export one or more drive entries to an XML file, which can then be imported at a later time or in another zone for use in another Microsoft Data Encryption Policy.

  To export one or more drives, select them in the Drives to Exclude from Encryption list, and click **Export**. The XML file is automatically downloaded based on your browser download settings.

Fixed Disk Folders

In addition to Microsoft BitLocker, the Microsoft Data Encryption policy can also manage the Microsoft Encrypting File System (EFS) for file and folder encryption on fixed disks. Fixed Disk Folder encryption can be enabled or disabled, giving you the ability to apply the policy to devices for one or both policy options, (1) Removable Data Drives encryption and (2) Fixed Disk Folder encryption.

With this feature enabled, end users will be able to encrypt personal folders once the policy is applied to their devices. Additionally, you can add folders to the policy that are encrypted by default upon policy enforcement.

Fixed disk folder encryption cannot be enforced on the following program folders:

- `C:\Program Files`
- `C:\Program Files (x86)`
- `C:\Windows\System`
- `C:\Windows\System32 "RECYCLE.BIN"`
- `C:\ProgramData`

NOTE: Fast user switching is not supported in the policy and may prohibit users from accessing encrypted folders on devices the policy is deployed to. Fast user switching in the context of the Microsoft Data Encryption policy is defined as multiple users having access to a device and switching users without closing programs or fully logging out.

Continuing reading for information about each of the configurable options for encrypting fixed disk folders.

Enable folder encryption

This box must be checked for encryption of fixed disk folders to be enabled on devices with the Microsoft Data Encryption Policy enforced. With the capability to disable encryption of fixed disk folders, you can still have Removable Data Drive encryption enabled when a Microsoft Data Encryption policy is enforced.

Administrator Recovery

An administrator decryption password is required to use folder encryption in the Microsoft Encryption policy. Once the policy is enforced, you can use the password to decrypt folders on any device to which the policy is applied.

To define the password that the policy will use, click **Set** in the Administrator Recovery panel and provide a password.

To get recovery information for encrypted folders on a specific device, click the device link in the ZENworks Control Center and go to **Encryption** > **Folder Encryption Certificates**. In combination with the encryption password, these certificates can be used via the ZENworks Folder Decryption Tool to decrypt folders encrypted by the policy.

For more information, see Recovering Data in Folders Encrypted by the Microsoft Data Encryption Policy in the *Troubleshooting Endpoint Security* section.

Default Encrypted Folders

You can specify folders that you want encrypted by default, which will include their files and subfolders. These may also be referred to as policy-encrypted folders. If the folder path that you provide does not exist on assigned devices, a new folder will be created on each device when the policy is applied. You can use an environment variable or full folder path to create or add a default encrypted folder to the policy. For example:

- `%userprofile%\Documents`
- `%SYSTEMROOT%\BB_Sys_Root`
- `C:\Windows`
- `C:\Users\username\Documents\EncryptedContent`

IMPORTANT: Multi-user folders are not currently supported. This means if you add a default folder to the policy that is outside of the user profile or home path that multiple users can access when logged into a device, the user logged in at the time of policy enforcement will be the only user that will have access to the folder and its contents.

In the event that one of these folders gets created and another user requires access to the folder who cannot access it, a recovery process is available to copy and decrypt the data. For more information see Recovering Data in Folders Encrypted by the Microsoft Data Encryption Policy.

To add one or more default folders:

1. Click **Add** in the Encrypted Folders section.
2. Type the folder path. For example:

   `C:\%USERPROFILE%\Documents`
3. Click **OK**.
4. Add additional folders if required.

Secondary Authentication

Primary authentication to access encrypted folders happens when a user logs in to a Windows device that has the Microsoft Data Encryption policy applied. You can apply secondary authentication to the policy to require a user to enter another password after the Windows login.

When Secondary Authentication is enabled, the user is initially prompted to create a password during the following conditions:

- You have one or more default folders added to the policy:

  The user is prompted to provide a password for encrypted folders when the policy is applied.

- There are no default folders added to the policy:

  The user is prompted to provide a password when attempting to encrypt a folder via the right-click menu.

Once the initial password is in place, the user will be required to enter that password once for each Windows session, either after login if there are default folders, or when first accessing an encrypted folder when there are no default folders.

If the user cancels a password prompt for encrypted folders after login, encrypted folders will be inaccessible during that Windows session. The user can override this issue by providing the password via **About > Encryption Management** in the ZENworks Endpoint Security Agent.

To require secondary authentication for encrypted folders, select **After Windows login, require user to enter a secondary password to unlock folders**.

Require a strong secondary password: Select this option to force users to define a decryption password that meets the following requirements when using a Secondary Authentication:

- Eight or more characters
- At least one of each of the four types of characters:
  - uppercase letters from A to Z
  - lowercase letters from a to z
  - numbers from 0 to 9
  - at least one special character ~ ! @ # $ % ^ & * ( ) + { } [ ] : ; < > ? ,. / - = | \ ”

  For example: y9G@wb?

Scripting Policy

The following instructions assume that you are on the **Configure Security Settings** page in the Create New Security Settings Policy Wizard (see Creating Security Policies) or that you are on the **Details** page for an existing Security Settings policy (see Editing a Policy’s Details).

The Scripting policy lets you run a script (JScript or VBScript) on a device. You can specify the triggers that cause the script to run. Triggers can be based on Endpoint Security Agent actions, location changes, or time intervals.

Define Script Settings

The Script Settings panel lets you define the language, content, and execution space for the script.

Run As

Select whether you want the script to run in the system context or the user context:

- **System:** The script runs with the same rights as a Windows service.
- **User:** The script runs with the rights provided by the current user session.

Language

Select **JScript** or **VBScript** as the scripting language.

Script Content

Click **Edit** to add the script content.

ZENworks supports standard JScript and VBScript coding methods, with the following exceptions.

1. WScript.Echo is not supported because return values can't be sent back to a parent window that is unavailable. Use the Action.Message ZENworks Endpoint Security Management API instead.
2. Access to Shell Objects. Use the following modified nomenclature/call:

```
[JScript]
   Use:
   var WshShell = new ActiveXObject("WScript.Shell");
   Instead of:
   var WshShell = WScript.CreateObject ("WScript.Shell");

[VBScript]
   Use:
   Dim WshShell
   Set WshShell = CreateObject("WScript.Shell")
   Instead of:
   Dim WshShell
   Set WshShell = WScript.CreateObject("WScript.Shell")
```

ZENworks also provides a scripting interface that lets you create advanced scripts. Using the scripting interface, you can determine current state of the Endpoint Security Agent, run actions that change the behavior of the agent or interact with the user, and store variables for use by the script during the current session or across sessions.

For more details about the scripting interface, see the *ZENworks Endpoint Security Scripting Reference*.

Define Trigger Settings

The Trigger Settings panel lets you determine when the script runs. There are three types of triggers that initiate execution of the script:

- **Agent Triggers:** Executes the script based on one or more Endpoint Security Agent actions, such as the enforcement of the Scripting policy or the change from one network environment to another.

- **Location Trigger:** Executes the script when changing from one location to another.
- **Time Trigger:** Executes the script according to a specified time interval.

You can use one or more of the trigger types to ensure that the script runs at the appropriate times.

Agent Triggers

The Agent Triggers settings executes the script based on one or more Endpoint Security Agent actions, such as the enforcement of the Scripting policy or the change from one network environment to another. Select one or more of the following actions:

- **Enforcement of this policy:** Executes the script any time this policy is enforced. Enforcement occurs on device startup (zone-assigned and device-assigned policies), user-login (user-assigned policies), and policy updates.
- **Any security policy change:** Executes the script any time the agent receives a change to any of the security policies (Firewall, Communication Hardware, and so forth).
- **Network change:** Executes the script any time the agent detects a network change that could affect the location assignment. This involves changes to the device's actual network environment (IP addresses, access points, and so forth) and the network environment definitions used to determine location.
- **Network connect:** Executes the script any time a network connection occurs. This could be a wired network that is detected after plugging in a network cable, a wireless network detected through an access point, a network detected through a modem, or more.
- **Network disconnect:** Executes the script any time a network disconnection occurs.

Location Trigger

The Location Trigger setting executes the script based on a location change. The trigger consists of two conditions that are evaluated to determine if the script should run:

- The location from which the device is switching. This is referred to as the "from" location.
- The location to which the device is switching. This is referred to as the "to" location.

The script is run only if the "from" and "to" locations are different.

Enable Location Trigger

Select this option to enable the location trigger.

Run When Switching From

This setting lets you define the first of the two conditions, the "from" locations:

- **Any location:** Select this option if you want all locations to qualify as valid "from" locations.
- **Selected locations:** Select this option if you want to designate one or more specific locations as valid "from" locations.

  The "from" location and "to" location lists can include the same location. For example, assume that you want the script to be triggered when the location changes from A to B or from B to A. You can add both A and B to the "from" location list and the "to" location list.

And When Switching To

This setting lets you define the second of the two conditions, the “to” locations:

- **Any location:** Select this option if you want all locations to qualify as valid “to” locations.
- **Selected locations:** Select this option if you want to designate one or more specific locations as valid “to” locations.

  The “from” location and “to” location lists can include the same location. For example, assume that you want the script to be triggered when the location changes from A to B or from B to A. You can add both A and B to the “from” location list and the “to” location list.

Must Be a Manual Change

A location change can be automatic or manual. An automatic location change occurs when the Endpoint Security Agent detects a change in the network environment that results in a new location assignment. A manual change occurs when a device’s user manually selects a new location from the agent’s Locations list.

Select this option if you only want the script to run when the user manually changes the location. Any automatic changes will not trigger execution of the script.

Time Trigger

The Time Trigger setting executes the script at a designated interval. The interval begins upon initial enforcement of the policy. If the policy is changed and republished, the interval is restarted.

The interval includes a one-minute boundary, meaning that the script is run within a minute (plus or minus) of the end of the interval.

Select the option to enable it, then enter the interval between each running of the script.

Security Settings Policy

The following instructions assume that you are on the **Configure Security Settings** page in the Create New Security Settings Policy Wizard (see Creating Security Policies) or that you are on the **Details** page for an existing Security Settings policy (see Editing a Policy’s Details).

The ZENworks Endpoint Security Agent (referred to as the Endpoint Security Agent) is the ZENworks Agent module that manages and enforces security policies on a device. This panel lets you configure the security settings for the Endpoint Security Agent.

IMPORTANT: This policy is not used with the current Endpoint Security Agent. The Endpoint Security Agent’s security settings are no longer applied as a policy; instead, they are applied as ZENworks Agent settings (ZENworks Control Center > Configuration > Management Zone Settings > Device Management > ZENworks Agent).

This policy is retained to provide support for devices that are still running the ZENworks 11 or ZENworks 11 SP1 Endpoint Security Agent. Those versions of the agent continue to use the Security Settings policy.

Enable Client Self Defense for Endpoint Security Agent

Client Self Defense protects the Endpoint Security Agent from being shut down, disabled, or tampered with in any way. If a user performs any of the following activities, the device is automatically rebooted to restore the correct system configuration:

- Using Windows Task Manager to terminate any Endpoint Security Agent processes.
- Stopping or pausing any Endpoint Security Agent services.
- Removing critical files and registry entries. If a change is made to any registry keys or values associated with the Endpoint Security Agent, the registry keys or values are immediately reset.
- Disabling NDIS filter driver binding to adapters.

Select one of the following options:

- **Yes:** Enables Client Self Defense.
- **No:** Disables Client Self Defense.
- **Inherit:** If the policy's **Inherit from Policy Hierarchy** setting is enabled, inherits this setting value from other Security Setting policies assigned higher in the policy hierarchy. For example, if you assign this policy to a user, the setting value is inherited from any Security Setting policies assigned to the user's groups, folders, or zone.

Enable Uninstall Password for Endpoint Security Agent

Client Self Defense does not prevent the Endpoint Security Agent from being uninstalled by the agent installation program. If you want to prevent users from removing the Endpoint Security Agent without permission, you must enable an uninstall password.

The uninstall password applies only when a user tries to uninstall the agent at the device. If you use the ZENworks Agent features (**Configuration** tab > **Management Zone Settings** > **Device Management** > **ZENworks Agent**) to uninstall the Endpoint Security Agent, the uninstall password is not used.

Select one of the following options:

- **Yes:** Enables an uninstall password. To specify the password, click **Change**, specify and confirm the password, then click **OK** to save it.
- **No:** Disables an uninstall password.
- **Inherit:** If the policy's **Inherit from Policy Hierarchy** setting is enabled, inherits this setting value from other Security Setting policies assigned higher in the policy hierarchy. For example, if you assign this policy to a user, the setting value is inherited from any Security Setting policies assigned to the user's groups, folders, or zone.

Enable Password Override for Endpoint Security Agent

Password Override lets you specify a password that overrides the device's currently applied security policies. All policies revert to the Endpoint Security Agent's default policies.

You should not distribute the password to users. Instead, you should use the Override Password Key Generator utility to generate a temporary password key (based on the override password) for a user who needs to override security policies. The password key functions the same as the override password with the added benefit that you can specify when the key expires.

Select one of the following options:

- **Yes:** Enables an override password. To specify the password, click **Change**, enter and confirm the password, then click **OK** to save it.
- **No:** Disables the override password.
- **Inherit:** If the policy's **Inherit from Policy Hierarchy** setting is enabled, inherits this setting value from other Security Setting policies assigned higher in the policy hierarchy. For example, if you assign this policy to a user, the setting value is inherited from any Security Setting policies assigned to the user's groups, folders, or zone.

Storage Device Control Policy

The following instructions assume that you are on the **Configure Storage Device Control Settings** page in the Create New Storage Device Control Policy Wizard (see Creating Security Policies) or that you are on the **Details** page for an existing Storage Device Control policy (see Editing a Policy's Details).

The Storage Device Control policy enables control of the Windows AutoPlay feature and access to removable storage devices. You can define the default access control for all removable storage devices and, if required, override that setting with different access controls for the device types indicated below:

- **CD/DVD:** Controls access to any devices listed under **DVD/CD-ROM drives** in Windows Device Manager.
- **Floppy Drive:** Controls access to any devices listed under **Floppy drives** in Windows Device Manager.
- **Removable Storage:** Controls access to any devices reporting as removable storage under **Disk drives** in Windows Device Manager.
- **Portable Device:** Controls access to any devices reporting as Windows Portable Devices under **Disk drives** in Windows Device Manager.

Configure AutoPlay/AutoRun

The AutoPlay/AutoRun setting can only be configured on a global Storage Device Control policy. It is not available on location-based policies. This means that it is always applied regardless of the device's location.

This setting controls the Windows AutoPlay feature. AutoPlay performs two processes. First, it launches the AutoRun process, which looks for an `autorun.inf` in the root directory and executes the instructions in the file. Second, it looks for specific content (music, video, and pictures) and launches the appropriate application to display or play the content. Select one of the following options:

- **Enable:** Enables both AutoPlay and AutoRun.
- **Disable AutoRun:** Disables the AutoRun feature so that `autorun.inf` instructions are not executed. AutoPlay is not disabled so music, video, and picture applications are still launched.
- **Disable AutoPlay/AutoRun:** Disables both the AutoPlay and AutoRun features.

- **Inherit:** If the policy's **Inherit from Policy Hierarchy** setting is enabled, inherits this setting from other Storage Device Control policies assigned higher in the policy hierarchy. For example, if you assign this policy to a user, the setting is inherited from any Storage Device Control policies assigned to the user's groups, folders, or zone.

Configure Removable Storage Device Access

You control access to storage devices by selecting a default access control for all device types and then enabling or disabling an override access control for individual device types. The access control options are defined below:

- **Read/Write:** Enables the user to have full access to the device on the client computer.
- **Disable:** Prevents read and write access. When users attempt to access files on the device, they receive an error message from the operating system, or the application attempting to access the local storage device, that the action has failed.
- **Read Only:** Enables read access and disable write access. When users attempt to write to the device, they receive an error message from the operating system, or the application attempting to access the local storage device, that the action has failed.
- **Inherit:** If the policy's **Inherit from Policy Hierarchy** setting is enabled, inherits this setting from other Storage Device Control policies assigned higher in the policy hierarchy. For example, if you assign this policy to a user, the setting is inherited from any Storage Device Control policies assigned to the user's groups, folders, or zone.

Default Access

The Default Access setting enables you to have one control for all removable storage devices when you want them to have the same access control. This includes FireWire, Windows Portable devices, storage cards, USB devices, and any other devices reported as removable storage under **Disk drives** in Windows Device Manager. If you want to have a different control for device types that use access overrides, you can use the Default Access Overrides configuration to implement those controls.

Default Access Overrides

Use the options in the Default Access Overrides configuration to select an individual access control for any of the three storage device types CD/DVD, Floppy Drive, or USB Device. Select the applicable check box to enable access control selection or deselect a check box to disable an override and reset that device type to the Default Access setting.

Exception Lists

The access controls for USB and WPD devices can include an exception list when the Default Access override option is enabled for these device types. This feature provides the capability to define access controls by device makes, models, or even individual devices if required. For example. Your Default Access control could be set to Disable, your Portable Device Access control could be set to Read Only, and devices in the Exception List could be set to Read/Write.

Each device that you add to an Exception List must include an access assignment. The Default Access setting is used as the default access assignment for (1) any device you import that does not have an access assignment and (2) any device you create whose access you set to Default Access.

Select from the following options:

- **Default Access:** Use the control that is defined in the Default Access setting.
- **Read/Write:** Enables read and write access.
- **Read Only:** Enables read access and disables write access. When users attempt to write to the device, they receive an error message that the action has failed.
- **Disable:** Prevents read and write access. When users attempt to access files on the device, they receive an error message that the action has failed.

The following table provides instructions for managing an **Exception List**:

Task	Steps	Additional Details
Create a new device	1. Click **Add** > **Create New**. 2. Select the access you want assigned to the device: ◆ **Default Access:** Give the device the access specified by the **Default Access** setting. ◆ **Read/Write:** Enable read and write access. ◆ **Read Only:** Enable read access and disable write access. When users attempt to write to the device, they receive an error message from the operating system, or the application attempting to access the local storage device, that the action has failed. ◆ **Disable:** Disable access. 3. (Optional) Add a comment to further identify the device. The **Comment** field is not a match field. It is used only in ZENworks Control Center to identify the device. 4. On the **Recommended** tab, fill in the fields you want to use as match criteria for the device. 5. On the **Advanced** tab, fill in the fields you want to use as match criteria for the device. 6. Click **OK** to add the device to the list.	The fields on the Recommended tab are typically sufficient to use for the match criteria. As a best practice, we recommend that you use the fewest number of fields needed to accurately match the device. The more fields you use, the more restrictive the definition becomes. The **Manufacturer** and **Product** fields are substring match. For example, “San”, and “SanDisk” both match all SanDisk devices while “SanDisk Cruzer” and “Cruzer” match all SanDisk Cruzer devices but excludes all other SanDisk devices. The **Serial Number**, **Vendor ID**, and **Product ID** fields are exact match. Be aware that not all devices have unique serial numbers. To guarantee a unique match based on a serial number, use the **Vendor ID** and **Product ID** fields as well. The Recommended fields are not case sensitive. The fields on the **Advanced** tab can be used to refine the match criteria in order to isolate very specific devices. Use of these fields can literally restrict a device definition so that it only matches a single device on a specific port on a specific computer. All of the Advanced fields are exact match. They are not case sensitive.

Task	Steps	Additional Details
Copy an existing device from another policy	1. Click **Add** > **Copy Existing**. 2. Select the USB Connectivity policies whose devices you want to copy. 3. Click **OK**.	All devices included in the other Storage Device Control policies are copied. If necessary, you can edit the copied devices after they are added to the list.
Import a device from a policy export file	1. Click **Add** > **Import**. 2. In the **Select Source of Data** list, make sure that **Existing Policy/Component** is selected. 3. In the **Select the Exported File** field, click to display the Select File dialog box. 4. Click **Browse**, select the export file, then click **Open**. 5. Click **OK** to add the devices to the list.	All devices included in the export file are imported. If necessary, you can edit the imported devices after they are added to the list. For information about exporting devices, see Export a device.
Import a device from a Device Scanner file	1. Click **Add** > **Import**. 2. In the **Select Source of Data** list, select **ZESM Device Scanner Tool**. 3. In the **Select the Data File** field, click to display the Select File dialog box. 4. Click **Browse**, select the export file, then click **Open**. 5. Click **OK**. 6. Select the fields you want to import for each device in the data file.* The recommended fields are selected by default. As a best practice, we recommend that you import the fewest number of fields needed to accurately match the device. The more fields you use, the more restrictive the definition becomes. 7. Click **OK** to import the devices.	* The Access field must be selected on import if you want the access setting that is defined in the Device Scanner file to map to the Preferred Device List Access setting. Read Only has no Device Scanner mapping and must be selected manually. For information on how Access settings map, see Control Access Import Mapping (Exception List). For information about using the Device Scanner to collect data about USB devices, see Device Scanner in the *ZENworks Endpoint Security Utilities Reference*.
Enable or disable a device	1. Locate the device in the list 2. In the Enabled column, select the check box to enable the device. or Deselect the check box to disable the device.	When you add a device, it is enabled by default. You can disable a device to save it in the policy but no longer have it applied.
Edit a device	1. Click the device name. 2. Modify the fields as desired. 3. Click **OK**.	

Task	Steps	Additional Details
Rename an device	1. Select the check box next to the device name, then click **Edit** > **Rename**. 2. Modify the name as desired. 3. Click **OK**.	
Export a device	1. Select the check box next to the device name. You can select multiple devices to export. 2. Click **Edit** > **Export**. 3. Save the file. The default name given to the file is `sharedComponents.xml`. You can change the name if desired. Do not change the `.xml` extension.	
Delete a device	1. Select the check box next to the device name, then click **Delete**. 2. Click **OK** to confirm deletion of the device.	

Control Access Import Mapping (Exception List)

Device Scanner Access Setting	Exception List Setting
Allow	Read/Write
Block	Disable
Always Allow	Read/Write
Always Block	Disable
Default Access	Default Access
No mapping	Read Only

USB Connectivity Policy

The following instructions assume that you are on the **Configure USB Connectivity Settings** page in the Create New USB Connectivity Policy Wizard (see Creating Security Policies) or that you are on the **Details** page for an existing USB Connectivity policy (see Editing a Policy's Details).

The USB Connectivity policy lets you control whether or not a device supports USB devices. You can allow all USB devices, block all USB devices, or control access for groups or individual USB devices based on attributes such as Device Class, Manufacturer, Product, and Serial Number.

Configure USB Devices

Select whether or not USB connections are supported:

- **Enable:** Enables support for USB connections by keeping a device's USB bus active. You can then enable or disable access for groups of USB devices or individual devices.
- **Disable:** Disables support for USB connections by deactivating a device's USB bus. All USB devices (keyboards, mice, storage devices, and so forth) are disabled. If you select this option, the remaining options (**Default Device Access**, **Device Group Access Settings**, and **USB Device Access Settings**) do not apply and are disabled.
- **Inherit:** If the policy's **Inherit from Policy Hierarchy** setting is enabled, inherits this setting from other USB Connectivity policies assigned higher in the policy hierarchy. For example, if you assign this policy to a user, the setting is inherited from any USB Connectivity policies assigned to the user's groups, folders, or zone.

Choose the Default Device Access

Some USB devices might not match any of the device groups or individual devices you define in this policy. Select the default access (**Enable**, **Disable**, or **Inherit**) to assign to those USB devices.

Configure Device Group Access Settings

You can specify access settings for each of the device groups listed in the following table. Each group is defined by a specific base class code. When a device's base class matches a group, the device receives the group's access setting.

Device Group	Base Class Code	Examples
Human Interface Device (HID)	03h	Mice, keyboards, game controllers
Mass Storage Class	08h	Flash drives, external hard drives, personal digital assistants (PDAs), mobile phones, cameras, Windows portable devices (WPDs)
Printing Class	07h	Printers
Scanning/Imaging (PTP)	06h	Scanners, any device that uses the Picture Transfer Protocol

Select one of the following access settings for each group:

- **Disable:** Disable access for all devices that are members of the device group.

  If there are individual devices in the group for which you want to enable access, you can enable them in the Configure USB Device Access Settings. A device's individual access setting overrides its group access setting.

For example, assume that your organization only supports SanDisk USB devices. You could disable the Mass Storage Class so that all removable storage devices are blocked and then use the **USB Device Access Settings** list to enable all SanDisk devices.

- **Enable:** Enable access for all devices that are members of the device group.

  If there are individual devices in the group for which you want to disable access, you can disable them in the Configure USB Device Access Settings. A device's individual access setting overrides its group access setting.

- **Default Device Access:** Give the device group the access specified by the **Default Device Access** setting.
- **Inherit:** If the policy's **Inherit from Policy Hierarchy** setting is enabled, inherit this setting from other USB Connectivity policies assigned higher in the policy hierarchy. For example, if you assign this policy to a user, the setting is inherited from any USB Connectivity policies assigned to the user's groups, folders, or zone.

Configure USB Device Access Settings

The device groups use one attribute (Device Class) as the match criterion. If you have devices whose access you want to control based on matching different or additional attributes, you can use the **USB Device Access Settings** list.

The individual device access settings override the device group access settings. For example, assume that the only mass storage device you want to allow is the Acme USB2 drive. In the **Device Group Access Settings**, you set **Mass Storage Class** to **Disable**. You then add the Acme USB2 to the **USB Device Access Settings** list and set the access to **Enable**. The individual setting for the Acme USB2 overrides its group setting, so the device is allowed.

Devices are evaluated against the **USB Device Access Settings** list from top to bottom. A device is assigned the access setting for the first device definition it matches, even if it matches another definition lower in the list. For example, assume that you want to disable all SanDisk devices except for the SanDisk Ultra. You add the SanDisk Ultra to the list and set the access to **Enable**. You then add a general SanDisk definition to the list and set the access to **Disable**. As long as the SanDisk Ultra definition is listed before the SanDisk definition in the list, the SanDisk Ultra is allowed.

The following table provides instructions for managing the **USB Device Access Settings** list:

Task	Steps	Additional Details
Create a new device	1. Click **Add** > **Create New**. 2. Select the access you want assigned to the device: ◆ **Disable:** Disable access. ◆ **Enable:** Enable access. ◆ **Default Device Access:** Give the device the access specified by the **Default Device Access** setting. 3. (Optional) Add a comment to further identify the device. The **Comment** field is not a match field. It is used only in ZENworks Control Center to identify the device. 4. On the **Recommended** tab, fill in the fields you want to use as match criteria for the device. 5. On the **Advanced** tab, fill in the fields you want to use as match criteria for the device. 6. Click **OK** to add the device to the list.	The fields on the Recommended tab are typically sufficient to use for the match criteria. As a best practice, we recommend that you use the fewest number of fields needed to accurately match the device. The more fields you use, the more restrictive the definition becomes. The **Manufacturer**, **Product**, and **Friendly Name** fields are substring match. For example, “San”, and “SanDisk” both match all SanDisk devices while “SanDisk Cruzer” and “Cruzer” match all SanDisk Cruzer devices but excludes all other SanDisk devices. The **Serial Number**, **Vendor ID**, and **Product ID** fields are exact match. Be aware that not all devices have unique serial numbers. To guarantee a unique match based on a serial number, use the **Vendor ID** and **Product ID** fields as well. The Recommended fields are not case sensitive. The fields on the **Advanced** tab can be used to refine the match criteria in order to isolate very specific devices. Use of these fields can literally restrict a device definition so that it only matches a single device on a specific USB port on a specific computer. All of the Advanced fields are exact match. They are not case sensitive.
Copy an existing device from another policy	1. Click **Add** > **Copy Existing**. 2. Select the USB Connectivity policies whose devices you want to copy. 3. Click **OK**.	All devices included in the other USB Connectivity policies are copied. If necessary, you can edit the copied devices after they are added to the list.

Task	Steps	Additional Details
Import a device from a policy export file	1. Click **Add** > **Import**. 2. In the **Select Source of Data** list, make sure that **Existing Policy/Component** is selected. 3. In the **Select the Exported File** field, click to display the Select File dialog box. 4. Click **Browse**, select the export file, then click **Open**. 5. Click **OK** to add the devices to the list.	All devices included in the export file are imported. If necessary, you can edit the imported devices after they are added to the list. For information about exporting devices, see Export a device.
Import a device from a Device Scanner file	1. Click **Add** > **Import**. 2. In the **Select Source of Data** list, select **ZESM Device Scanner Tool**. 3. In the **Select the Data File** field, click to display the Select File dialog box. 4. Click **Browse**, select the export file, then click **Open**. 5. Click **OK**. 6. Select the fields you want to import for each device in the data file.* The recommended fields are selected by default. As a best practice, we recommend that you import the fewest number of fields needed to accurately match the device. The more fields you use, the more restrictive the definition becomes. 7. Click **OK** to import the devices.	* The Access field must be selected on import if you want the access setting that is defined in the Device Scanner file to map to the USB Device Access Setting. For information on how Access settings map, see Access Import Mapping. . For information about using the Device Scanner to collect data about USB devices, see "Device Scanner" in the *ZENworks Endpoint Security Utilities Reference*.
Enable or disable a device	1. Locate the device in the list 2. In the Enabled column, select the check box to enable the device. or Deselect the check box to disable the device.	When you add a device, it is enabled by default. You can disable a device to save it in the policy but no longer have it applied.
Edit a device	1. Click the device name. 2. Modify the fields as desired. 3. Click **OK**.	
Rename an device	1. Select the check box next to the device name, then click **Edit** > **Rename**. 2. Modify the name as desired. 3. Click **OK**.	

Task	Steps	Additional Details
Export a device	1. Select the check box next to the device name. You can select multiple devices to export. 2. Click **Edit** > **Export**. 3. Save the file. The default name given to the file is `sharedComponents.xml`. You can change the name if desired. Do not change the `.xml` extension.	
Delete a device	1. Select the check box next to the device name, then click **Delete**. 2. Click **OK** to confirm deletion of the device.	

Access Import Mapping

Device Scanner Access Setting	USB Device Access Setting
Allow	Enable
Block	Disable
Always Allow	Enable
Always Block	Disable
Default Access	Default Device Access

VPN Enforcement Policy

The following instructions assume that you are using the Create New VPN Enforcement Policy Wizard (see Creating Security Policies) or that you are on the **Details** page for an existing VPN Enforcement policy (see Editing a Policy's Details).

Typically, the VPN Enforcement policy is used to provide greater security at locations such as public wireless hotspots and hotel access points. When a device enters one of these locations, referred to as a *Trigger location*, it attempts to detect the Internet. If the Internet is detected, the VPN Enforcement policy settings are applied. You can configure the settings to create a basic policy or an advanced policy. We recommend that you review Understanding the VPN Enforcement Policy to decide what kind of policy best meets your needs.

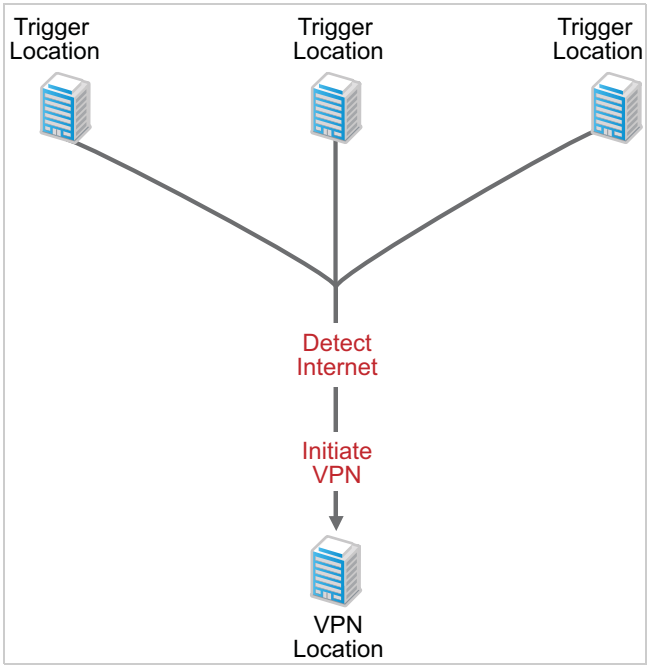
- "Understanding the VPN Enforcement Policy" on page 91
- "Configure Trigger Locations" on page 95
- "Configure VPN Traffic" on page 97
- "Configure Pre-VPN Location" on page 98
- "Configure VPN Location" on page 99

Understanding the VPN Enforcement Policy

You can configure the policy as a basic policy or an advanced policy. Both are described below.

Basic Policy

A basic VPN Enforcement policy consists of one or more *Trigger locations*, a method for detecting the Internet, a method for initiating a VPN connection, and a *VPN location*, as shown in the following figure.



With a basic policy, the following process occurs:

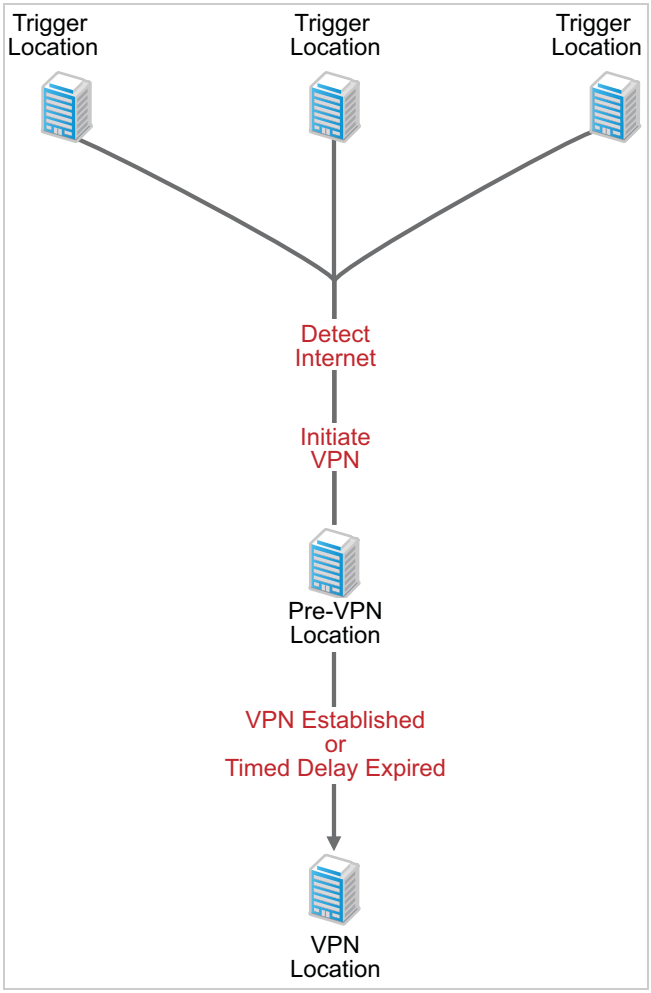
1. When a device enters a Trigger location, it attempts to detect the Internet. There are two methods you can choose from to detect the Internet: 1) Web page retrieval or 2) network traffic monitoring.
2. If the Internet is detected, the rest of the process takes place; otherwise, the device remains in the Trigger location.
3. (Optional) A VPN connection is initiated. There are two methods you can choose from to initiate the connection: 1) execute a command to launch a VPN client or 2) display a message with a link that allows the user to launch a VPN client or informs the user that he or she needs to launch the VPN client some other way.
4. The location switches from the Trigger location to the VPN location and the VPN location's security policies are enforced. This occurs whether or not the VPN connection has been established.
5. The VPN location is exited when the device changes to a non-Trigger location or all network connections are dropped.

Advanced Policy

An advanced VPN Enforcement policy includes the same elements as a basic policy, but also provides the option of using a *Pre-VPN location*.

In some situations, going directly to the VPN location might enforce security policies that prevent the device from establishing a VPN connection. For example, many businesses, such as hotels and motels, use semi-public networks that provide minimal Internet access until the user logs in or accepts a usage agreement. Immediately switching to the VPN location might enforce security policies that prevent the user from completing the login or agreement. To resolve this issue, you can use a Pre-VPN location with security policies that allow the user to perform the required activities and gain the full Internet access required to establish the VPN connection.

The following figure shows an advanced VPN Enforcement policy:

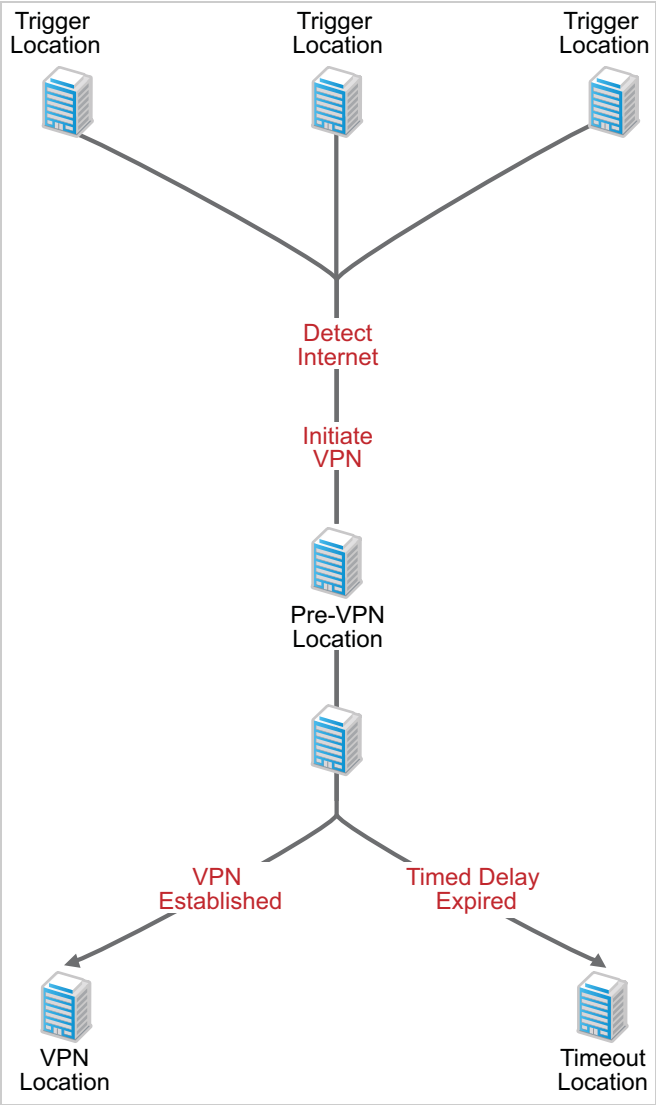


With an advanced policy, the following process occurs:

1. When a device enters a Trigger location, it attempts to detect the Internet. There are two methods you can choose from to detect the Internet: 1) Web page retrieval or 2) network traffic monitoring.
2. If the Internet is detected, the rest of the process takes place; otherwise, the device remains in the Trigger location.

3. (Optional) A VPN connection is initiated. There are two methods you can choose from to initiate the connection: 1) execute a command to launch a VPN client or 2) display a message with a link that allows the user to launch a VPN client or informs the user that he or she needs to launch the VPN client some other way.
4. The location switches from the Trigger location to the Pre-VPN location and the Pre-VPN location's security policies are enforced.
5. The location switches from the Pre-VPN location to the VPN location based on one or both of the following methods (that you choose from):
   - A VPN connection is detected. To use this method, you must enable and configure the VPN detection option in the policy.
   - The delay period expires. You determine the delay period.
6. The VPN location is exited when one of the following events occurs:
   - The device changes to a non-Trigger location.
   - All network connections are dropped.
   - No VPN traffic is detected for a specified amount of time (the default is 2 minutes). To use this exit method, you must enable and configure the VPN detection option in the policy.

The advanced policy can also be configured with an optional *Timeout location*, as shown in the following figure:



With an advanced policy that includes a Timeout location, the following process occurs:

1. When a device enters a Trigger location, it attempts to detect the Internet. There are two methods you can choose from to detect the Internet: 1) Web page retrieval or 2) network traffic monitoring.
2. If the Internet is detected, the rest of the process takes place; otherwise, the device remains in the Trigger location.
3. (Optional) A VPN connection is initiated. There are two methods you can choose from to initiate the connection: 1) execute a command to launch a VPN client or 2) display a message with a link that allows the user to launch a VPN client or informs the user that he or she needs to launch the VPN client some other way.
4. The location switches from the Trigger location to the Pre-VPN location and the Pre-VPN location's security policies are enforced.
5. The location switches from the Pre-VPN location to the VPN location if a VPN connection is detected. This requires that you have enabled and configured the VPN detection option in the policy.

or

The location switches from the Pre-VPN location to the Timeout location if the delay expires before a VPN connection is detected.

6. The VPN or Timeout location is exited when one of the following events occurs:
   - The device changes to a non-Trigger location.
   - All network connections are dropped.
   - (VPN location only) No VPN traffic is detected for a specified amount of time (the default is 2 minutes). To use this exit method, you must enable and configure the VPN detection option in the policy.

Configure Trigger Locations

The **Trigger Location** tab lets you define the policy's Trigger locations, Internet detection method, and VPN client launch commands.

Trigger Locations

A Trigger location is a location in which you want the VPN Enforcement policy settings applied. You can specify one or more locations. To specify a location, click **Add**, select the location, then click **OK** to add it to the list.

Internet Detection Method

This setting is only for the Advanced Version.

When a device enters a Trigger location, it attempts to detect the Internet. If the Internet is detected, the VPN Enforcement policy settings are applied.

To detect the Internet, the device can use one of two methods. It can attempt to retrieve a Web page, or it can monitor the network adapters for traffic from specific addresses. Both methods cannot be used at the same time. You must select one method and then provide the appropriate configuration information for the method.

Retrieve Web Pages

Select this option to use Web page retrieval as the Internet detection method. With this method, the device tries to retrieve specific Web pages to verify Internet access. You can use the default Web pages, custom Web pages, or both:

- **Use the default Web pages:** Select this option to have the device try to retrieve one of the internally-defined Web pages.
- **Use the Web pages included in the list:** Select this option to define custom Web pages to retrieve, then click **New** to add a Web page. If you select **Validate** while adding the Web page, the header information from the retrieved Web page (HTML file) must contain the domain name specified in the URL; if it does not, the Web page is considered invalid and Internet access remains unverified. Only use the **Validate** option with URLs that include a domain name; the option does not support URLs with IP addresses.

Monitor Network Traffic

Select this option to use network traffic monitoring to determine whether or not the Internet is present. You determine which network adapters to monitor and define the network traffic that indicates the presence of the Internet.

- **Adapters to monitor:** Specify the adapter types and specific adapters to monitor:
  - **Adapter Type:** Select whether you want to monitor **All** adapter types, **Wired** adapters only, or **Wireless** adapters only.
  - **Adapter Names:** To monitor all adapters of the selected **Adapter Type**, leave the adapter list empty. To monitor specific adapters only, type an adapter name and then click **Add** to add it to the list. Adapter names are not case sensitive. In addition, partial matching is used. For example, *Adapter1* not only matches *Adapter1* but also matches *adapter10* and *acme adapter100*. The more complete the name, the more limited the matches.
- **Network Traffic:** Add the network addresses you want to use to determine if the device can access the Internet. The Internet is active if the ZENworks Endpoint Security Agent receives a ping reply from any of the addresses or detects continuous packet streams from any of the addresses.

  Click **New** to display the Add Network Traffic Address dialog box, select the address type (IP address or DNS), then enter the address using one of the following formats:
  - xxx.xxx.xxx.xxx: Standard dotted-decimal notation for a single IP address. For example, 123.45.167.100.
  - xxx.xxx.xxx.xxx-xxx.xxx.xxx.xxx: Standard dotted-decimal notation for a range of IP addresses. For example, 123.45.167.100-123.45.167.125.
  - xxx.xxx.xxx.xxx/n: Standard CIDR (Classless Inter-Domain Routing) notation for IP addresses. For example, 123.45.167.100/24 matches all IP addresses that start with 123.45.167.
  - www.domain_name: Standard domain name notation. For example, www.novell.com.
  - www.domain_name/n: Standard CIDR (Classless Inter-Domain Routing) notation for a domain name. For example, www.novell.com/16.

  The addresses are tested in the order they are listed, from top to bottom. Use the **Move Up** and **Move Down** options to reorder the list.

Connect Settings

You can use the Connect Settings to initiate a VPN connection after the Internet is detected. The Connect Command lets you automatically launch a VPN client while the VPN Message lets you create a message that prompts the user to launch the client.

- **Use Connect Command:** This option lets you automatically launch the VPN client after the Internet is detected. If you don't want the VPN client automatically launched, you can use the **Use VPN Message option** instead.
  - **Link:** Specify the executable path for the VPN client.
  - **Parameters:** Specify any parameters you want used when launching the client. Enter the parameters in the format required by the client.
- **Use VPN Message:** This option lets you display a message to the user. Additionally, you can include a hyperlink that enables the user to launch the VPN client.

For example, if you selected the **Use Connect Command** option, you might provide a message informing the user that his or her current location requires a VPN connection to maintain security. The Endpoint Security Agent displays the message before launching the VPN client.

Or, you can use this option without the **Use Connect Command** option. In this case, you would provide a message and a link to the VPN client. The user would then click the link to launch the client.

Select the option, then fill in the following fields:

- **Title of Message Window:** Specify the Message Window's title. For example, "Launch VPN Client."
- **Body:** Provide the text for the message body.
- **Message Hyperlink:** If you want to include a hyperlink in the message, select **Include message hyperlink**, then fill in the following:
  - **Display Text:** The text to display as the hyperlink in the message.
  - **Link:** The command or Web URL to be executed when the display text is clicked. Any link that starts with http, https, or www is treated as a Web URL and launches a Web browser. Any other link is treated as an executable command. For example, you might include `www.acme.com/vpn` to a open a Web page that provides the VPN login.
  - **Parameters:** Applies only to executable commands, not to Web URLs. Specify any parameters that you want appended to the executable command. A space is automatically added between the executable command and the first parameter.

Configure VPN Traffic

This setting is only for the Advanced Version.

VPN traffic detection enables the device to detect when a VPN connection is established and active. VPN traffic detection serves two purposes:

- If the policy includes a Pre-VPN location, VPN detection allows the device to initiate a switch from the Pre-VPN location to the VPN location after the VPN connection is established. If VPN detection is not enabled, you must configure the switch to occur after a specific period of time. For more information about the Pre-VPN location, see "Understanding the VPN Enforcement Policy" on page 91.
- To exit the VPN location after a period of VPN traffic inactivity. If VPN detection is not enabled, the VPN location is not exited until 1) the device changes location or 2) all network connections are dropped.

To use VPN traffic detection, select **Enable VPN Traffic Detection**, then fill in the following fields:

- **Adapters to monitor:** Specify the adapter types and specific adapters to monitor:
  - **Adapter Type:** Select whether you want to monitor **All** adapter types, **Wired** adapters only, or **Wireless** adapters only.
  - **Adapter Names:** To monitor all adapters of the selected **Adapter Type**, leave the adapter list empty. To monitor specific adapters only, type an adapter name and then click **Add** to add it to the list. Adapter names are not case sensitive. In addition, partial matching is used. For example, *Adapter1* not only matches *Adapter1* but also matches *adapter10* and *acme adapter100*. The more complete the name, the more limited the matches.

- **Network Traffic:** Add the network addresses you want to use to determine if the device has an active VPN connection. The connection is active if the ZENworks Endpoint Security Agent receives a ping reply from any of the addresses or detects continuous packet streams from any of the addresses.

  Click **New** to display the Add Network Traffic Address dialog box, select the address type (IP address or DNS), then enter the address using one of the following formats:

  - xxx.xxx.xxx.xxx: Standard dotted-decimal notation for a single IP address. For example, 123.45.167.100.
  - xxx.xxx.xxx.xxx-xxx.xxx.xxx.xxx: Standard dotted-decimal notation for a range of IP addresses. For example, 123.45.167.100-123.45.167.125.
  - xxx.xxx.xxx.xxx/n: Standard CIDR (Classless Inter-Domain Routing) notation for IP addresses. For example, 123.45.167.100/24 matches all IP addresses that start with 123.45.167.
  - www.domain_name: Standard domain name notation. For example, www.novell.com.
  - www.domain_name/n: Standard CIDR (Classless Inter-Domain Routing) notation for a domain name. For example, www.novell.com/16.

  The addresses are tested in the order they are listed, from top to bottom. Use the **Move Up** and **Move Down** options to reorder the list.

Configure Pre-VPN Location

This setting is only for the Advanced Version.

As soon as the Internet is detected, the location switches from the Trigger location to the VPN location. In some situations, going directly to the VPN location might enforce security policies that prevent the device from establishing a VPN connection.

For example, many businesses, such as hotels and motels, use semi-public networks that provide minimal Internet access until the user logs in or accepts a usage agreement. Immediately switching to the VPN location might enforce security policies that prevent the user from completing the login or agreement. To resolve this issue, you can use a Pre-VPN location with security policies that allow the user to perform the required activities and gain the full Internet access required to establish the VPN connection.

Using a Pre-VPN location is optional. To use a Pre-VPN location, select **Use a Pre-VPN location**, then fill in the following fields:

- **Pre-VPN Location:** Select the location you want to use for the Pre-VPN location. This can be any location other than the one you plan to use as the VPN location.
- **Exit Criteria:** The exit criteria determines when the Pre-VPN location switches to the VPN location. You can use one or both of the following options:
  - **Switch from the Pre-VPN location to the VPN location when VPN traffic is detected:** This option applies only if you've enabled VPN detection. Select this option to switch as soon as a VPN traffic is detected.
  - **Switch from the Pre-VPN location after XX minutes:** Select this option to switch after a specific amount of time, then specify the time in minutes (the default is 5 minutes).

Configure VPN Location

This setting is only for the Advanced Version.

The VPN location is a location that provides the security policies you want enforced while using the VPN connection. It cannot be the same location as a Trigger location or the Pre-VPN location.

- **VPN Location:** Select the location whose security policies you want to use during the VPN connection.
- **Exit the VPN location if no VPN traffic has been detected for *XX* minutes:** This option applies only if you have enabled VPN traffic detection. By default, the VPN location is exited only if 1) a network environment change causes a switch to a new location or 2) all network connection is lost. Select this option to also enable the device to exit the VPN location if no VPN traffic is detected, then specify the inactivity time (the default is 2 minutes).
- **Use Disconnect Command:** Select this option if you want to execute a command when leaving the VPN location, the fill in the following fields:
  - **Link:** Specify the command to execute.
  - **Parameters:** Specify any parameters associated with the command. A space is automatically added between the executable command and the first parameter.

Wi-Fi Policy

The following instructions assume that you are on the **Configure Wi-Fi Settings** page in the Create New Wi-Fi Policy Wizard (see Creating Security Policies) or that you are on the **Details** page for an existing Wi-Fi policy (see Editing a Policy's Details).

The Wi-Fi policy lets you control wireless access.

Configure General Settings

The General Settings let you control access for ad hoc network connections and Wi-Fi connections.

Ad Hoc Connections

Ad hoc network connections provide direct wireless access between devices without using a physical wireless access point such as router or mobile phone hotspot. These connections are temporary but can be used for transferring files, playing multi-player computer games, and sharing Internet connection. If you allow connections, you can define the minimum security level for connections in this policy.

Select one of the following options to control ad hoc connections:

- **Enable:** Allows ad hoc network connections.
- **Disable:** Prevents ad hoc network connections.
- **Inherit:** If the policy's **Inherit from Policy Hierarchy** setting is enabled, inherits this setting from other Wi-Fi policies assigned higher in the policy hierarchy. For example, if you assign this policy to a user, the setting is inherited from any Wi-Fi policies assigned to the user's groups, folders, or zone.

Wi-Fi Connections

This setting lets you control Wi-Fi connectivity, which includes mobile phone hotspots, but does not include Bluetooth and infrared wireless connections. To control Bluetooth and infrared connections, use the Communication Hardware policy. For information about setting minimum security levels when connections are enabled, see Configure Minimum Security.

Select one of the following options:

- **Enable:** Allows Wi-Fi connections.
- **Disable:** Prevents Wi-Fi connections. Connections are blocked but the wireless adapter remains active in case you want to use wireless access points to determine location. To completely disable Wi-Fi adapters, use the Communication Hardware policy.
- **Inherit:** If the policy's **Inherit from Policy Hierarchy** setting is enabled, inherits this setting from other Wi-Fi policies assigned higher in the policy hierarchy. For example, if you assign this policy to a user, the setting is inherited from any Wi-Fi policies assigned to the user's groups, folders, or zone.

Define Access Points

You can use the **Access Points** list to control connections to wireless access points, such as routers and mobile phone hotspots. The list works as follows:

- When you add an access point, you designate it as prohibited or approved. Prohibited access points are filtered out of a device's wireless network connection display. If a user manually connects to a prohibited access point, the connection is blocked. You can also define further controls by configuring the Minimum Security settings in the policy.
- All access points are approved (default approval) until you add one approved access point to the list (explicit approval). At that point, the default approval is ignored and only explicitly approved access points are allowed.
- Prohibited access overrides approved access. For example, assume that you have multiple access points that share *Novell* as the SSID. You create an approved access point definition using Novell as the SSID, which results in all access points that share the Novell SSID being allowed. However, there is one Novell access point you want to prohibit, so you create a prohibited access point definition using the access point's MAC address. Based on its SSID and MAC address, the access point matches both definitions (approved and prohibited). Prohibited access overrides approved access, so connection to the access point is prohibited.

The following table provides instructions for managing access points:

Task	Steps	Additional Details
Add a new access point	1. Click **Add** > **Create New**. 2. Fill in the following fields to define the access point: **Name:** Specify a name to identify the access point in the ZENworks system. **SSID and MAC Address:** The **SSID** and the **MAC Address** are the two fields used to determine if a detected access point matches this definition. You must fill in at least one of the fields. Multiple access points can share the same SSID. If you fill in the **SSID** field, any access point that uses that SSID is matched. The SSID is case-sensitive. If you want to identify a specific access point, specify the MAC address. Each access point has a unique MAC address. **Enforcement:** Select whether the access point is prohibited or approved. 3. To define another access point, select **Define another access point**. 4. Click **OK** to add the access point to the list.	
Copy an access point from another policy	1. Click **Add** > **Copy Existing**. 2. Select the Wireless policies whose access points you want to copy. 3. Click **OK**.	All access points included in the selected Wireless policies are copied. If necessary, you can edit the copied access points after they are added to the list.
Import an access point from a policy export file	1. Click **Add** > **Import**. 2. Click to display the Select File dialog box. 3. Click **Browse**, select the export file, then click **Open**. 4. Click **OK** to add the access points to the list.	All access points included in the export file are imported. If necessary, you can edit the imported access points after they are added to the list. For information about exporting access points, see Export an access point.
Edit an access point	1. Click the access point name. 2. Modify the fields as desired. 3. Click **OK**.	

Task	Steps	Additional Details
Export an access point	1. Select the check box next to the access point name. You can select multiple access points to export. 2. Click **Edit** > **Export**. 3. Save the file. The default name given to the file is `sharedComponents.xml`. You can change the name if desired. Do not change the `.xml` extension.	
Delete an access point	1. Select the check box next to the access point name, then click **Delete**. 2. Click **OK** to confirm deletion of the access point.	

Configure Minimum Security

Select the minimum security protocol that an approved access point must provide before a connection is allowed. For example, if you select **WPA**, only approved access points that provide WPA, WPA2, or WPA3 encryption are allowed.

Select **No encryption required** to ignore minimum security. Select **Inherit** to inherit the minimum security from other Wi-Fi policies assigned higher in the policy hierarchy. For example, if you assign this policy to a user, the setting is inherited from any Wi-Fi policies assigned to the user's groups, folders, or zone.

Approved access points that fall below the minimum security level are not displayed in the device's wireless network connections list when detected. If a user tries to manually define a connection to the access point, the connection is blocked.

Define the Minimum Security Message

This option is available only if you selected **WPA**, **WPA2**, or **WPA3** as the minimum security requirement.

You can display a message when a wireless connection is blocked because the access point does not meet the minimum security requirement. Select **Display message when minimum security not met**, then fill in the following fields:

- **Title of Message Window:** Specify the message window's title.
- **Body:** Provide the text for the message body.
- **Message Hyperlink:** If you want to include a hyperlink, select **Include message hyperlink**, then specify the display text for the hyperlink and the link command.

6 Data Encryption Key Management

The Endpoint Security Agent uses encryption keys to encrypt and decrypt removable data drives when a Microsoft Data Encryption policy is applied to a device. These sections explain encryption key concepts and provide instructions for managing encryption keys.

- "About Data Encryption Keys" on page 103
- "Generating a New Encryption Key" on page 104
- "Exporting Encryption Keys" on page 104
- "Importing Encryption Keys" on page 105

About Data Encryption Keys

The following sections explain concepts that can help you better manage the encryption keys for your Management Zone.

Active Key

A Management Zone can have one or more encryption keys. At any one time, however, there is only one active key. The active key is used to encrypt new removable data drives. The non-active keys are retained in order to decrypt removable drives that were encrypted when the non-active keys were the active keys.

For example, assume that Key1 is the active key. All Endpoint Security Agents use Key1 to encrypt removable data drives. You then generate a new key, Key2, which automatically becomes the active key. After Key2 is distributed to devices (during an agent refresh), the Endpoint Security Agent uses it to encrypt new removable data drives. The agent uses Key1 to open any removable drives encrypted with that key.

Multiple Zones

Encryption keys are specific to Management Zones. This means that a removable data drive encrypted in one zone with the **No unlock password** setting enabled in the Microsoft Data Encryption policy cannot be opened on a device registered in another zone because the two zones do not automatically share keys.

If you have multiple zones and want to enable devices in all zones to open encrypted removable drives regardless of the zone in which they were encrypted or the settings configured in the Microsoft Data Encryption policy, you can manually share encryption keys by exporting them from one zone and importing them into another. For instructions, see Exporting Encryption Keys and Importing Encryption Keys.

Key Security

If your organization's policies include a requirement for regularly changing encryption keys, you can generate and activate a new key. After doing so, force an agent refresh to immediately distribute the new key to devices. Note that this key will only be used to encrypt new removable data drives on those devices. Removable drives encrypted using an older key will continue to unlock using the older key. For instructions, see Generating a New Encryption Key.

Generating a New Encryption Key

You can increase data security by regularly generating a new encryption key from the Microsoft Data Encryption policy. The new key becomes the active encryption key, which means that all newly encrypted removable data drives use the key.

1. In ZENworks Control Center, navigate to **Policies** and click the policy link for the Microsoft Data Encryption policy that you are using in your zone, and then select the **Details** tab.
2. Under **Common Tasks** (in the left navigation pane) click **Encryption: Generate Keys**.
3. Click **OK** to confirm creation of the new key.

   The next time a device refreshes its information from the ZENworks Server, the Endpoint Security Agent begins using the new key to encrypt new drives used on the device thereafter.

Exporting Encryption Keys

The Endpoint Security Agent uses encryption keys to encrypt and decrypt removable data drives. You can export the encryption keys from the Management Zone to a key file to:

- Share the encryption keys with another ZENworks Management Zone. This allows users in the second zone to unlock removable drives that were encrypted in the first zone.
- Back up the encryption keys. We recommend that you follow a regular backup schedule in case problems occur with your ZENworks Servers. To back up a key you need to export it.

To export the encryption keys:

1. In ZENworks Control Center, navigate to **Policies** and click the policy link for the Microsoft Data Encryption policy that you are using in your zone, and then select the **Details** tab.
2. Under **Common Tasks** (in the left navigation pane) click **Encryption: Export Keys**.
3. Specify a name for the key file.

   The file requires a `.kbk` extension. If you do not add the `.kbk` extension, it is added automatically.
4. Specify a password for the key file.

   Make sure you remember the password. It is required in order to import the keys into another Management Zone or reimport them into the current zone (as a restored backup).
5. Click **OK**.

   Depending on how your browser is configured to handle saving files, the file might be automatically saved to your browser's download directory or you might be prompted to save it. Follow any prompts to complete the save process.

Importing Encryption Keys

The Endpoint Security Agent uses encryption keys to encrypt and decrypt removable data drives. You can import encryption keys from a key file to:

- Use the encryption keys from another ZENworks Management Zone. This allows users to decrypt removable drives that were encrypted in the other zone.
- Restore a backup of the zone's encryption keys.

To import encryption keys:

1. In ZENworks Control Center, navigate to **Policies** and click the policy link for the Microsoft Data Encryption policy that you are using in your zone, and then select the **Details** tab.
2. Under **Common Tasks** (in the left navigation pane) click **Encryption: Import Keys**.
3. In the **File Name** field, click to browse for and select the encryption key file.
4. In the **Password** field, specify the file's password.

   This password was assigned when the keys were exported to the file.
5. If you want to change your zone's active key to the active key included in the file, select the **Use the active encryption key from the imported file** option.

   A Management Zone can have one or more encryption keys. At any one time, however, there is only one active key. The active key is used to encrypt new removable data drives. The non-active keys are retained in order to decrypt files that were encrypted when the non-active keys were the active keys.
6. Click **OK.**

A Naming Conventions in ZENworks Control Center

When you name an object in ZENworks Control Center (folders, bundles, policies, groups, registration keys, and so forth), ensure that the name adheres to the following conventions:

- The name must be unique in the folder.
- Depending on the database being used for the ZENworks database, uppercase and lowercase letters might not create uniqueness for the same name. The embedded database included with ZENworks is case insensitive, so Folder 1 and FOLDER 1 are the same name and cannot be used in the same folder. If you use an external database that is case-sensitive, Folder 1 and FOLDER 1 are unique.
- If you use spaces, you must enclose the name in quotes when you enter it on the command line. For example, you must enclose reg key 1 in quotes (“reg key 1”) when you enter it in the zman utility.
- The following characters are invalid and cannot be used: / \ * ? : " ' < > | ` % ~

B Troubleshooting Endpoint Security

This document provides troubleshooting guidelines for issues related to ZENworks Endpoint Security. If, after completing troubleshooting steps for an issue described in this section does not resolve your problem, you should contact Technical Support for additional help.

Recovering Data in Folders Encrypted by the Microsoft Data Encryption Policy

This section explains how to copy and decrypt fixed disk folders encrypted by the Microsoft Data Encryption Policy using the standalone ZENworks Folder Decryption Tool to recover encrypted data. It also explains how folder encryption works and the behavior of default encrypted folders for multi-user folders, which are not currently supported. While multi-user folders are not supported, the data can be recovered for a user who is denied access to a multi-user folder using this same decryption procedure.

Understanding how Fixed Disk Folder encryption works

ZENworks Endpoint Security manages the Microsoft Encrypting File System (EFS) feature to encrypt fixed disk folders on managed devices when folder encryption is enabled in the Microsoft Data Encryption Policy. EFS uses certificates as part of the encryption process. When the policy is first enforced, it looks for an existing EFS certificate to encrypt folders. If one is not found on the device, a new EFS certificate is created. These certificates are uploaded to the ZENworks server for recovery purposes and can also be viewed in the Personal folder of Certificate Manager (certmgr) on the managed device.

Understanding multi-user folders encrypted by the Microsoft Data Encryption Policy

Multi-user encrypted folders are not currently supported for default folders encrypted by the Microsoft Data Encryption Policy. Access to encrypted public folders outside of a user's profile directory is only guaranteed for the user logged into the device when the policy is applied. If any users receive the prompt that the file or folder is inaccessible due to permissions, they can use the copy and decrypt procedure below to decrypt the files they are trying to access.

Identifying the user who has access to a multi-encrypted folder

To see who can access a policy encrypted folder that is public or available for more than one user, right-click the encrypted folder or file on the manged device and go to **Properties** > **General** tab > **Advanced** > **Details**. You can use this information to associate the user with the required encryption certificate in ZENworks Control Center, which is required to decrypt folders.

How to copy and decrypt folders encrypted by the Microsoft Data Encryption Policy

Before performing these steps, ensure that you have access to the encrypted folder via portable media or a network share and can identify the user who has access to the folder. You will also need network access to the ZENworks Control Center to access the encryption password and download the EFS certificate.

1. Download and install the ZENworks Folder Encryption Tool via the ZENworks Control Center download page by going to **Administrative Tools** > **Endpoint Security**.
2. Download the applicable folder encryption certificate to a portable media device, a local drive, or a network share by selecting the managed device in ZENworks Control Center and going to the **Encryption** tab.

   You can identify which certificate to download by first discovering the user that has access to the folder. For more information, see Identifying the user who has access to a multi-encrypted folder.
3. Follow the instructions in the ZENworks Folder Encryption Tool to provide the paths for the certificates, the encrypted folder, and the destination for copying and decrypting the folder.

NOTE: If needed, the Options menu at the top of the Encryption Tool provides the means to change the language in the tool.

Other Troubleshooting Scenarios

Network Communication Initially Blocked for Permitted Applications

Source: ZENworks Endpoint Security Management, Application Control Policy

Explanation: Network Communication is initially blocked for applications when an Application Control Policy is assigned to the device. After few seconds, the communication starts to work automatically.

Action: Disable the `ZesNetAccess` service in the registry to use the network communication after the Application Control Policy is assigned to the device.

To disable the `ZesNetAccess` service in the registry, you can add a QueryClient key at the following location in the registry editor:

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ZesNetAccess\Parameters]"QueryClient"=dword:00000000
```