ZENworks Endpoint Security Use Cases

December 2016

This document provides information and resources to help you use ZENworks Endpoint Security Management to solve common security issues faced by organizations today.

1 Controlling USB Device Access

USB mass storage devices, or removable storage devices, are commonplace in the business and consumer world today. One of the driving forces behind their widespread use is their ultra-portable form factor and universal recognition across all operating systems.

However, this *ease of use* and *universal recognition* introduces several security threat vectors by these same devices. For example, USB mass storage devices can contain viruses that readily propagate upon the devices insertion into any computer. Additionally, users can easily copy large volumes of data containing protected personal information or corporate intellectual property.

So while users demand ease of use, IT administrators have to balance this demand with concerns regarding data confidentiality and enterprise security. In short, USB mass storage devices need to be allowed, but in a controlled manner based on enterprise, regulatory, and other requirements of a business.

So while users demand ease of use, IT administrators have to balance this demand with concerns regarding data confidentiality and enterprise security. In short, USB mass storage devices need to be allowed, but in a controlled manner based on enterprise, regulatory, and other requirements of a business.

Example Use Cases

The following list provides common use cases related to controlling USB devices. ZENworks Endpoint Security Management provides a solution for each case.

- An administrator wants to be able to specify USB device criteria to determine an “approved USB mass storage device” list.
- When connected to an enterprise managed computer, an administrator wants only “approved USB mass storage devices” to have full access while access to all other USB mass storage devices is prohibited.
- An administrator wants to encrypt all Removable Storage Devices (RSD) connected to an enterprise managed computer.
- An administrator wants to be able to specify USB device criteria to determine an “approved USB mass storage device” list.
- An administrator wants to encrypt all Removable Storage Devices (RSD) connected to an enterprise managed computer, except those on an “approved USB mass storage device” list.
- An administrator wants computer based policy to block USB Mass Storage Devices on all enterprise managed computers.
- An administrator wants to allow specific users to have full access to USB Mass Storage Devices, regardless of computer based policies, when using enterprise managed computers.

Test Scenarios

1. Implement a device-assigned policy that disables all USB mass storage devices. For instructions, see Disabling Access to USB Mass Storage Devices.
2. Implement a user-assigned policy that overrides the device-assigned policy (scenario 1) and allows ZENworks administrators to access specific USB devices. For instructions, see Enabling Users to Access Specific USB Mass Storage Devices.

2 Enforcing VPN Usage

Most enterprises and companies have “road warrior” employees that have notebook computers containing some level of confidential data, personal data, or intellectual property. When these mobile users travel or work from home, they often connect to the internet. Their internet connection exposes them to numerous security threat vectors that would not be threats if they were using corporate network connections.

One of the main concerns for IT administrators is ensuring that mobile users are using the Virtual Private Network (VPN) to securely transmit data over their network connections. So an administrator wants to go beyond just recommending to users that they launch and use the VPN connection by actually enforcing VPN use for these mobile users. Ensuring that all network traffic passes through a dedicated VPN tunnel means the data is transmitted in an encrypted and protected format.

Example Use Cases

The following list provides common use cases related to enforcing VPN use for mobile users. ZENworks Endpoint Security Management provides a solution for each case.

- An administrator wants to be able to specify a VPN is required when detecting internet connectivity in a location that is NOT the corporate network.
- An administrator wants to restrict the firewall in the VPN “switch-to” location to ensure all network traffic is passed over the full tunnel VPN ports through a trusted IP address ACL.
- An administrator wants to combine the two use cases above and launch the VPN software automatically for the end user. If the end-user fails to establish or maintain a VPN connection then the computer will switch to a quarantined location.

Test Scenarios

1. Implement a device-assigned policy that forces a change to a VPN “switch-to” location when internet connectivity is detected. A warning message will appear to tell the user to launch their VPN software. For instructions, see Prompting a User to Initiate a VPN Session When in an Unknown Location.
2. Building on test scenario 1, assign a restrictive firewall to the VPN “switch-to” location. This firewall ensures that all traffic is passed to a specified, trusted ACL of the VPN concentrator. All other network traffic is blocked. For instructions, see Enforcing a Restrictive Firewall During the VPN Session.
3. Building on test scenario 2, modify the device-based policy to automatically launch the VPN software for the user to log in to. For instructions, see Launching a VPN Client to Initiate a VPN Session When in an Unknown Location.

3 Using Scripting to Enhance 3rd Party Solutions

Most enterprises and companies have internally created applications or point solutions that help their particular business needs. However, a common problem is that these internally developed applications or 3rd party point solutions do not share the advantages of ZENworks solutions. Specifically, they are not centrally managed from one console, do not have location awareness, are not controlled by both user-assigned and device-assigned policies, do not have reporting or auditing, and do not have agent self defense mechanisms. ZENworks Endpoint Security Management scripting allows an administrator to extend these inherent ZENworks features to other applications and solutions.

Example Use Cases

The following list provides common use cases that can be solved by ZENworks Endpoint Security Management scripting.

- An administrator wants to be able to monitor a process or application and, if it is shut down, warn the user that it's a required application and restart it.
- An administrator wants to be able to use location awareness to launch a 3rd party application or solution in specific locations.

Test Scenarios

1. Implement a device-based policy that monitors a process or application. If the process or application isn't running, displays a message to the user and starts the process or application. For instructions, see Enforcing the Running of a Required Application.

4 Controlling Access to Wireless Networks

Administrators with mobile users often have to try to control which wireless (802.11) networks the users can connect to. When within the corporate infrastructure, in terms of a geophysical location, administrators can control the SSIDs of their Access Points. Additionally, the corporation may also have contracts with Internet Service Providers (ISPs) that support world-wide travelers with static SSIDs.

In order to ensure that data transmitted over wireless connections is protected, an administrator needs to require that their end users either 1) use a VPN tunnel when wireless connections have no security or 2) connect to wireless networks that meet a minimal level of security such as WPA2. Using VPN enforcement is covered in Enforcing VPN Usage. This section covers how to filter wireless networks based on minimum security levels.

Example Use Cases

The following list provides common use cases related controlling access to wireless networks. ZENworks Endpoint Security Management provides a solution for each case.

- An administrator wants to ensure that users can connect to approved SSID values only.
- An administrator wants to ensure that users can only connect to wireless networks that meet a specified minimum level of security (for example, WPA).
- An administrator wants to ensure that users can only connect to AdHoc wireless connections that meet the minimum level of security specified (for example, WPA2).

Test Scenarios

1. Implement a set of location-based Wi-Fi policies that use the security level to filter which wireless networks are allowed in different locations. For instructions, see Preventing Devices from Connecting to Unsecure Wireless Networks.
2. Implement a Wi-Fi policy for a “Work” location that only allows connection to two approved SSIDs. For instructions, see Allowing Access to Approved Wireless Network Access Points (SSIDs) Only.

5 Additional Information and Resources

We frequently add to our list of use cases, test scenarios, and sample policies and scripts. For the most up-to-date ZENworks Endpoint Security Management resources, visit the ZENworks Endpoint Security Management Resource Kit website.

6 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.novell.com/company/legal/.