

ZENworks Endpoint Security Management v4.0 Demo Script

Bhogilal Hirani

August 2009

Demo Script - ZESM v4.0

Demo Script.....	3
USB Device Access	3
Data Encryption.....	3

Demo Script – ZENworks End Point Security Management (ZESM) v4.0

DEMO SCRIPT

USB Device Access

For the User policy show the following:

1. Policy Settings: The Update message
 - 1.1. Change the update message, Publish the policy and on the XP workstation right click the ZESM agent and click “Check for Updates”
 - 1.2. If the Agent is communicating with the ZESM server, the pop up message will show up
2. Wireless Control: disable Wi-fi when Wired
3. Comms hardware
4. Storage Device Control; All device access control allowed
5. USB Connectivity: Mass Storage Control = Default Access Control
 - 5.1. this will allow access to all usb devices (Hard drive + Flash Drive)
 - 5.2. *Plug in a USB Hard Drive, the Kingston flash drive and another flash drive*
6. Now lets block Access to all Mass storage and ONLY allow access to a Kingston flash Drive
 - 6.1. Click on USB Connectivity | Advanced and show that Access is “Always allow” to “Kingston” model of flash drive
 - 6.2. Click on USB Connectivity and change the access for Mass Storage to **Block**
 - 6.3. Notice that only the Kingston Flash drive is allowed access
7. Disable the cd/dvd for location “London Office”
 - 7.1. Click on the Locations tab and show the following
 - a) Icon for London Office
 - b) User Permission Check boxes
 - 7.2. Set the Storage device control for cd /dvd = Disable all Access
 - 7.3. connect to the London Office and make sure that the correct icon shows up in the system tray
 - 7.4. CD / DVD device will be removed
8. **Set the Mass Storage Class back to Default Access**

Data Encryption

let's configure Encryption of data on our only allowed Kingston flash drive and a Non -System Drive. Remember that encryption is at machine level and not at a user level

1. Add a second hard drive of 1Gb to the XP vm and initialize it assigning a volume name of DATA
- 1. Give the Users group full access to the drive**
2. login to the vm as user bob
2. Plug in the Kingston flash Drive
3. Enable Encryption, Safe Harbor (encryption to non system drives, Usb drives and Reboot option
4. publish the policy and at the prompt reboot the client when prompted
5. Right click on the ZESM Agent icon in the system tray and select “encryption” to view the encryption activity
6. On the Non-System drive, create a text file in the Encrypted Files folder with some text in it
7. On the kingston Flash drive create a text file with some text on it
8. Take the Flash drive to another vm (zesm server) and try to access the text file