



Intel® vPro Out of Band Management with HP ZBOOK G6

System Configuration

Intel AMT Firmware 12.0.64-build1551

BIOS R92 Ver 01.05.04

Operating System Windows 10 Pro 64bit

Configuring the Management Engine

Power on system and press Shift F6 during boot up

Enable Management Engine

Configure AMT ME5enable the following

- SOL / Storage Redirection / KVM
- Opt-in configurable from Remote IT
- Network Name / Domain (If on a domain)
- Wired LAN IPV4 DHCP
- Active Network - Provisioning Mode PKI
- Sleep States – Mobile ON in S0, ME Wake in S3, S4-5 (AC only)

Configure Wireless Network for AMT

Boot to Windows

Browse to the local AMT user interface

<https://zbook-g6:16992>

Select wireless settings

Select Enabled in S0, Sx/AC

Click on the New button to create a profile

Enter a Profile name, SSID and select the network security type and enter the password used to join the wireless network selected



Wired Ethernet AMT Out of Band Management Functions

- Power Off
- Power On
- Power Reset
- KVM

Wireless Ethernet AMT Out of Band Management

The laptop must be plugged into the AC Power before shutting down or it will not activate the AMT communication while shutdown

Must be in a domain

Wi-Fi designated in AMT must be on

- Power Off
- Power On
- Power Reset
- KVM



Remote out of Band Management

****Please Note - You must use Internet Explorer and Java 8u221 or above 32bit plugin for accessing KVM Console.**

Configure the KVM Password and start the KVM

Remote Management : ZBOOK-G6 (192.168.200.154)

AMT Configuration | AMT Remote Control | **AMT KVM**

AMT KVM

Local user approval required

Timeout (seconds) 60

KVM Password Monitor 0 Monitor 1

KVM Inactivity Timeout (minutes) 5

KVM Status: Running

KVM configured successfully.

Launch the KVM

Java will prompt you for approval to run the plugin, approve and Don't Block

Security Warning

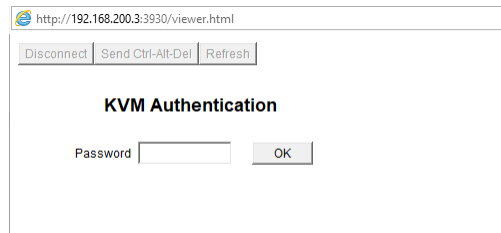
Block potentially unsafe components from being run?

Application: Remote Console

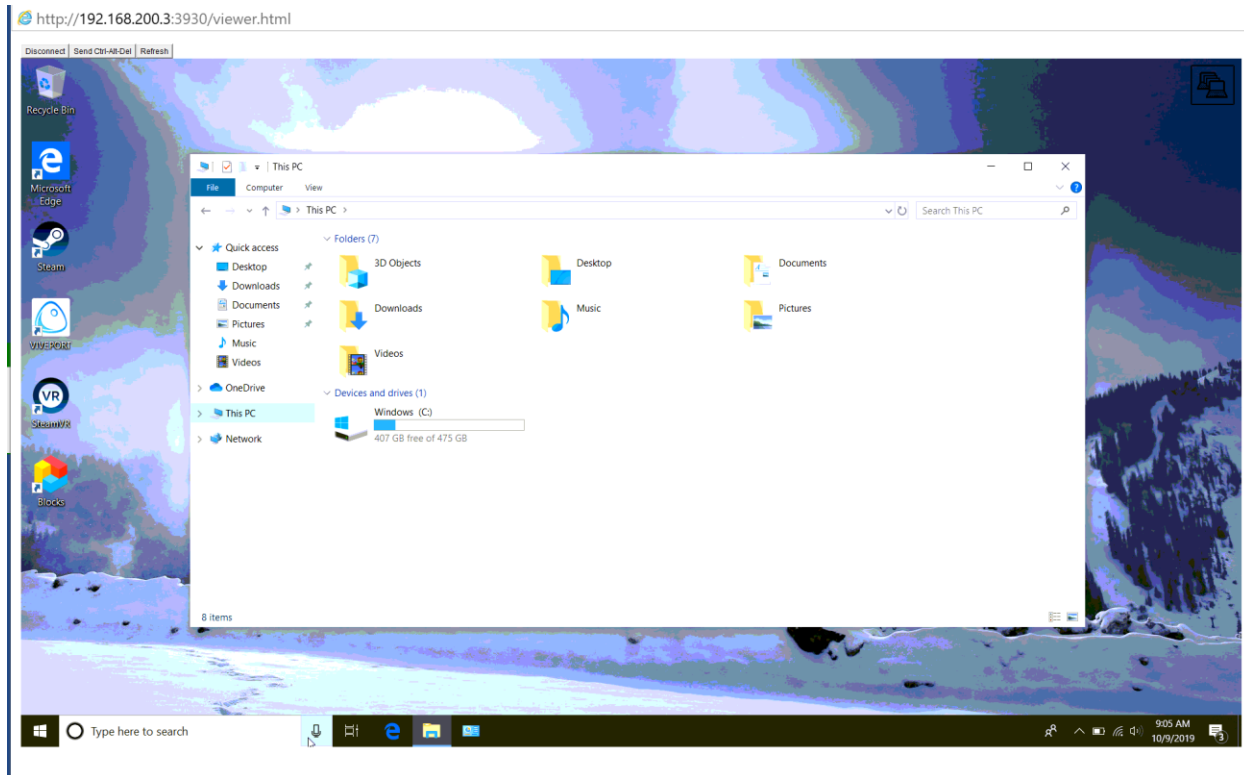
Java has discovered application components that could indicate a security concern. Contact the application vendor to ensure that it has not been tampered with.

The application contains both signed and unsigned code.
[More information](#)

Enter the password to login



You now have control of the target system and interacting with the user through your browser



Click Disconnect to close the session