Windows Operating System Settings for OverDrive

Configuring the following Window operating system settings will help ensure the smooth operation of your OverDrive Server computer:

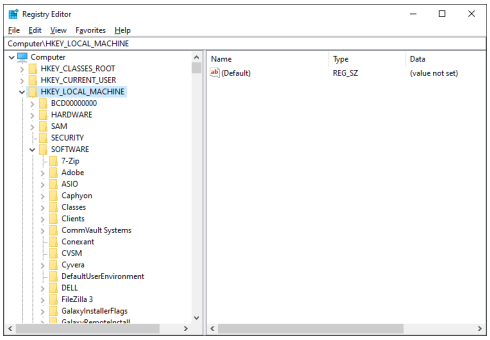
- Registry Entires
- Caprica Hyper-V Installation
- Windows Operating System Vulnerability

Registry Entires

The Windows registry contains entries that you should disable on your OverDrive Server computer.

To disable registry entries

1. Log in to the OverDrive Server computer as a Windows Administrator.
2. In the Windows search bar, enter `regedit` and then press Enter key.
   The Registry Editor opens.



3. Backup the HKEY_LOCAL_MACHINE registry entries as follows:
   a. In the tree view, right-click the HKEY_LOCAL_MACHINE node and select Export from the shortcut menu.
   b. In the Export Registry dialog box, select the folder and file name in which to save the registry entires.
   c. Click Save.
4. Verify that Cortana is disabled as follows:
   a. In the tree view, expand the following path:
   `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Windows Search`
   b. Verify that the Entries list contains the entry "AllowCortana"=dword:00000000.
   Add the entry if it does not exist in the Entries list.
5. Verify that Antispyware in Windows Defender is disabled as follows:
   a. In the tree view, expand the following path:
   `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender`
   b. Verify that the Entries list contains the entry "DisableAntiSpyware"=dword:00000001.
   Add the entry if it does not exist in the Entries list.

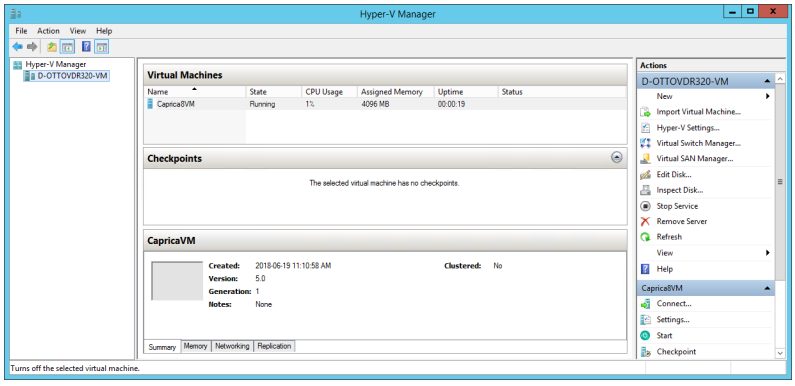
6. Verify that Windows Defender is disabled as follows:
   a. In the tree view, expand the following path:
      `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Policy Manager`
   b. Verify that the Entries list only contains the (Default) the entry.
7. Verify that Windows Firewall is disabled as follows:
   a. In the tree view, expand the following path:
      `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\StandardProfile`
   b. Verify that the Entries list contains the entry "EnableFirewall"=dword:00000000.
      Add the entry if it does not exist in the Entries list.
8. Verify that OneDrive is disabled as follows:
   a. In the tree view, expand the following path:
      `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\OneDrive`
   b. Verify that the Entries list contains the entry "Start"=dword:00000004.
      Add the entry if it does not exist in the Entries list.
9. Verify that Serial Mouse is disabled as follows:
   a. In the tree view, expand the following path:
      `Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\sermouse`
   b. Verify that the Entries list contains the entry "DisableAntiSpyware"=dword:00000001.
      Add the entry if it does not exist in the Entries list.

Caprica Hyper-V Installation

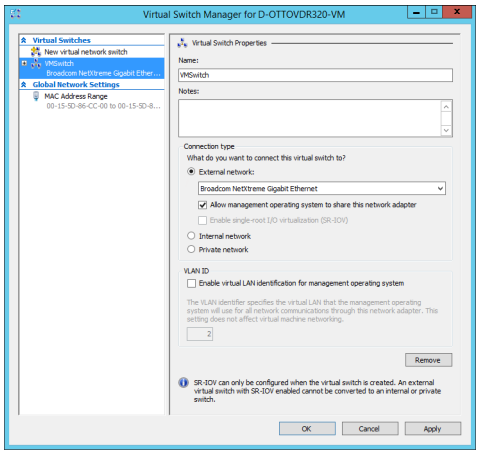
Caprica requires that Hyper-V is installed and running on the OverDrive Server computer.

To verify the Hyper-V installation for Caprica

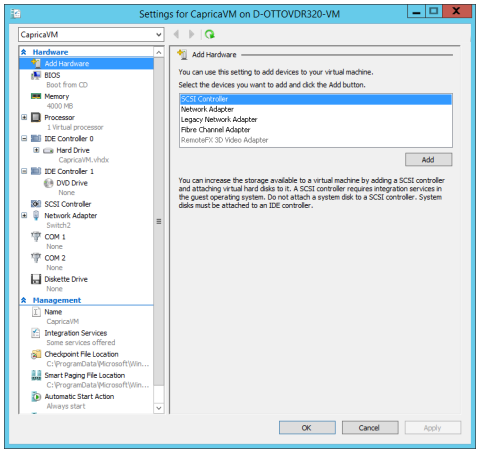
1. Log in to the OverDrive Server computer as a Windows Administrator.
2. Use the Start menu to select Hyper-V Manager.
   The Hyper-V Manager window opens.



3. In the Caprica VM section of the Actions panel, click Virtual Switch Manager.
   The Virtual Switch Manager dialog box opens.

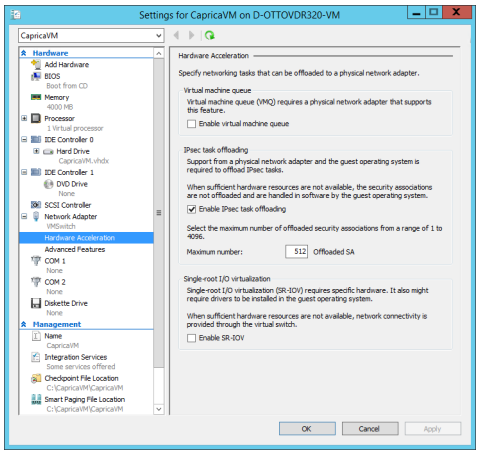


4. In the tree view, select the VMSwitch node.
5. In the Connection Type section, verify that the External network option is selected and configured.
6. Close the Virtual Switch Manager dialog box.
7. In the Hyper-V Manager window Caprica VM section of the Actions panel, select Settings.
   The Settings dialog box opens.

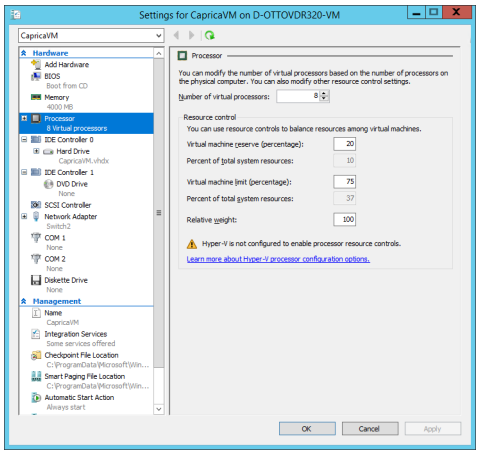


8. In the Hardware section of the tree view, expand the Network Adapter node.

9. the Network Adapter node, click Hardware Acceleration.
   The Hardware Acceleration panel opens.

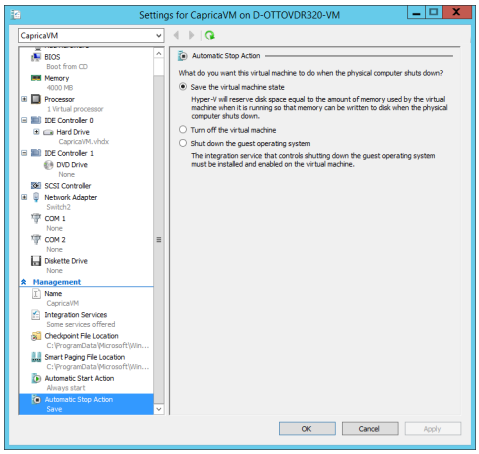


10. In the Virtual machine queue section, verify that the Enable virtual machine queue check box is cleared.
11. In the Hardware section of the tree view, click Processor.
    The Processor panel opens.

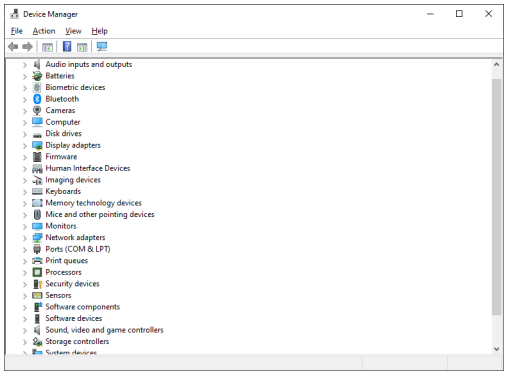


12. In the Resource control section, verify the following setting values:
    - Number of virtual processors — 8
    - Virtual machine reserve — 20
    - Virtual machine limit — 75
    - Relative weight — 100

13. In the Management section of the tree view, click Automatic Stop Action.
    The Automatic Stop Action panel opens.

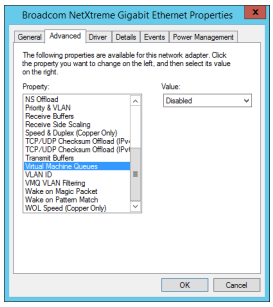


14. In the Automatic Stop Action panel, verify that the **Shutdown the guest operation system** option is selected.
15. Close the Settings dialog box.
16. Verify network interface properties as follows:
    a. In the Windows search bar, enter `device manager` and then press Enter key.
    The Device Manager opens.



    b. Expand the Network adapters node.
    c. Double-click the network adapter used by your OverDrive Server computer.
    The **Properties** dialog box opens for the selected network adapter.

d. Click the Advanced tab.
The Advanced tab opens.



e. Verify that the Virtual Machine Queues property is Disabled.

f. Close the **Properties** dialog box.

g. Close the Device Manager.

17. Verify the network connection for your CapricaVM virtual machine as follows:

a. In the Hyper-V Manager window Virtual Machines list, right-click CapricaVM and select Connect from the shortcut menu.

b. Log in to your Caprica Server.

c. Try browsing the internet and pinging other computers to verify that your Caprica Server has a working network connection.

Windows Operating System Vulnerability

To mitigate CVE-2022-30190 on the OverDrive Server you must delete the MSDT URL Protocol from the registry. For more information, refer to the following Microsoft Security Response Center post:

- https://msrc-blog.microsoft.com/2022/05/30/guidance-for-cve-2022-30190-microsoft-support-diagnostic-tool-vulnerability/

To delete the MSDT URL Protocol from the registry

1. Log in to the OverDrive Server computer as a Windows Administrator.
2. In the Windows search bar, enter `cmd`.
3. In the results list, right-click Command Prompt and select Run as administrator from the shortcut menu.
A Command Prompt window opens.
4. Execute the following command to backup registry keys:
`reg export HKEY_CLASSES_ROOT\ms-msdt <filename>`
Where `<filename>` is the name of the file in which to save registry keys.
5. Execute the following command to delete the MSDT URL Protocol from the registry:
`reg delete HKEY_CLASSES_ROOT\ms-msdt /f`
6. Close the Command Prompt window.

Microsoft Defender Antivirus

Microsoft Defender Antivirus provides detections and protections for possible vulnerability exploitation under the following signatures using detection build 1.367.851.0 or higher:

- Trojan:Win32/Mesdetty.A — blocks msdt command line
- Trojan:Win32/Mesdetty.B — blocks msdt command line
- Behavior:Win32/MesdettyLaunch.A!blk — terminates the process that launched msdt command line
- Trojan:Win32/MesdettyScript.A — detects HTML files that contain msdt suspicious command being dropped
- Trojan:Win32/MesdettyScript.B — detects HTML files that contain msdt suspicious command being dropped

Microsoft Reference Information

- Windows 10, version 1809 and Windows Server 2019
  https://docs.microsoft.com/en-us/windows/release-health/status-windows-10-1809-and-windows-server-2019/
- Diagnostic Tool - Vulnerability
  https://msrc-blog.microsoft.com/2022/05/30/guidance-for-cve-2022-30190-microsoft-support-diagnostic-tool-vulnerability/

Contacting Technical Support

Technical Support is staffed by a team of experienced specialists ready to assist you with any question or technical issue.

Ross Video has technical support specialists strategically located around the globe to ensure a prompt response to technical inquiries. Our primary technical support center is located in Ottawa, Ontario, Canada. In addition, we have offices in The United Kingdom (London), Australia (Sydney), and Singapore with satellite locations in New York City, The Netherlands, and China. As we expand our presence globally, we are constantly evaluating other key locations to have a local technical support specialist in order to better service our customers.

North America

Our North America center located in Ottawa, Ontario, Canada and is open Monday to Friday 8:30 a.m. to 6:00 p.m. EST, with 24/7/365 on-call service after hours.

Our telephone number is: +1-613-686-1557

Toll free within North America: +1 844-652-0645

EMEA

Our EMEA center is open Monday to Friday 8:30 a.m. to 5:00 p.m. GMT. After hours support is provided by our North America location.

Our telephone number is: +44 (0)1189502446

International toll free: +800 3540 3545

If the local support specialist is not available, your call will be transferred automatically to our North America center.

Australia

Our Sydney, Australia office is located in Alexandria, NSW.

Our local support telephone number is: 1300 007 677

If the local support specialist is not available, your call will be transferred automatically to our North America center.

Online

E-mail: techsupport@rossvideo.com

Website: open a support request using the link http://www.rossvideo.com/support/tech-support.html to open a support request.

Copyright