Emulex® OneCommand® Manager Application for Windows Release Notes

Versions: Windows Server 2019: 12.0.358.0-2
All other supported systems: 11.4.329.44-1

Systems: Windows Server 2019
Windows Server 2016
Windows Server 2012 and Windows Server 2012 R2 (x64 versions, Enterprise and Server Core installation)
Windows 10
Windows 8 and 8.1

Date: April 17, 2019

Purpose and Contact Information

These release notes describe the new features, resolved issues, known issues, and technical tips associated with this OneCommand® Manager application version for the Emulex®drivers for Windows.

For the latest product documentation, go to www.broadcom.com. If you have questions or require additional information, contact an authorized Broadcom® Technical Support representative at ecd-tech.support@broadcom.com.

New Features

Adds support for Windows Server 2019.

Resolved Issues

There are no resolved issues in this release.

Known Issues

1. **Beginning with software release 11.2, LightPulse® adapters and OneConnect® adapters have independent software kits.**

   Before updating earlier drivers and applications to the software in release 11.4, refer to the *Emulex Software Kit Migration User Guide* for special instructions and considerations for using the 11.2 and later software kits for LightPulse and OneConnect adapters.

2. **For LPe16000-series adapters, remote applications (OneCommand Manager application Graphical User Interface [GUI] or command line interface [CLI]) might not report the latest firmware version immediately after a firmware update. This issue is caused by cache update time intervals in the CIM Provider.**

Workaround

Do one of the following:

- Use the OneCommand Manager plug-in for VMware vCenter Server.
- Refresh the data after a few minutes (maximum of 10 minutes).
- Either restart the CIM model object manager (CIMOM, sfcb) service on the ESXi host, or reboot the server.

Note: This issue is common for all versions of ESXi.

3. **Performing a core dump command might fail if a World Wide Port Name (WWPN) is specified.**

   When performing a core dump operation in the OneCommand Manager CLI and specifying an FC WWPN to indicate which adapter to dump, the command fails if the adapter is in a down state.

   Workaround

   None.

4. **Some management functions are unavailable through the CIM interface with the OneCommand Manager application kits.**

   The following management functions are unavailable through the CIM interface with the OneCommand Manager application kits (OneCommand Manager application GUI and OneCommand Manager CLI):

   - Boot from storage area network (SAN)
   - Get and clear event logs

   Workaround

   None.

5. **When you manage a host using the CIM interface and you initiate a batch download process, all of the adapters of the CIM-managed host are displayed because the required validation logic is not available in the CIM Provider.**

   Workaround

   Manually deselect the adapters that you do not want to include in the batch download before starting the download. If you start the download without deselecting the nonmatching adapters, the firmware download is initiated and results in an error for nonmatching adapters.

6. **When you start the OneCommand Manager application on a Windows Server 2012 R2 system, the following popup message is displayed:**

   ```
   Publisher is unknown
   ```

   This message indicates that the publisher is unknown and you are prompted to allow the program to make changes to the computer.

   Workaround

   Do one of the following:

   - Select **Yes** on the popup message to run the OneCommand Manager application.
   - Disable the popup by setting the User Account Control settings to **Never Notify**.

- Disable the popup by performing the following steps:
  a) Select **Start > Run**, type `secpol.msc`, and click **OK**.
  b) Double-click **Local Policies**.
  c) Double-click **Security Options.**
  d) Double-click **User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode**.
  e) Select **Elevate without prompting**.
  f) Click **OK**.

7. **A set link speed issue occurs after a small form-factor pluggable (SFP) hot swap.**

   The LPe16000-series adapter does not support SFP hot swap if the replacement SFP is not the same model as the original SFP. Two ramifications exist in the OneCommand Manager application:

   - The **Port Attributes** tab in OneCommand Manager application or the OneCommand Manager CLI's `PortAttributes` command might display incorrect data for the Supported Link Speeds attribute. This issue is cosmetic.
   - Boot from SAN management might be unable to set the `Boot Code Link Speed` parameter to 16 Gb/s.

   Workaround

   After changing the SFP, reset the LPe16000 port or reboot the server.

8. **If you are using the OneCommand Manager application to update firmware from a previous version to version 11.x, you must first update the OneCommand Manager application to version 11.x.**

9. **In some cases, the PCI registers in the OneCommand Manager application might display all zeros in the PCI Registers tab when the tab is first opened immediately after a reboot.**

   Workaround

   Perform one of the following tasks:

   - Click on a different tab, and then click back on the **PCI Registers** tab to refresh it.
   - Use the `PciData` command in the CLI to display PCI configuration data.

10. **If the CLI is used to perform a firmware download to a local adapter, and the OneCommand Manager GUI is running while the firmware download is taking place, the OneCommand Manager GUI might not display information on various tabs after the download completes. The value displayed for most of the fields on the affected tabs and dialogs will be N/A.**

    Workaround

    There are three possible workarounds:

    - After having performed a firmware download using the CLI, if **N/A** appears for most of the OneCommand Manager GUI display fields, exit the GUI and restart it. The fields should be displayed correctly.
    - Make sure that the OneCommand Manager GUI is stopped and not running prior to performing a firmware download using the CLI.
    - Perform the firmware download using the OneCommand Manager GUI instead of the CLI.

11. **Disabling ExpressLane™ on all LUNs attached to a vport discovered using the CIM interface fails.**

    Workaround

    Disable ExpressLane on individual LUNs attached to the vport.

12. **The OneCommand Manager application does not show the operating system (OS) Device Name for logical unit numbers (LUNs) attached to virtual ports (vPorts).**

    The **LUN Information** tab, the **Mapping Information** area, and the **OS Device Name** field shows N/A instead of the device name. All other information on the **LUN Information** tab is displayed correctly.

13. **When connecting to an ESXi 6.5 U1 host, the webcli and the Windows OneCommand Manager application using the CIM interface fail with an `ssl_connect` error.**

    Workaround

    Set `sslCipherList` to `HIGH` and `enableSSLv3:true` in the `/etc/sfcb/sfcb.cfg` file, and restart the CIMOM using the following commands:

    ```
    esxcli system wbem set -e 0
    esxcli system wbem set -e
    ```

Technical Tips

1. **FC in-band management is no longer supported.**
2. **The OneCommand Manager application no longer installs OneCommand Vision components.**
3. **If you are running Windows Server 2012 or 2012 R2 with User Account Control (UAC) enabled, you must start a command shell with the Run as Administrator option for OneCommand Manager CLI commands and batch files.**

   If you do not start the command shell with the Run as Administrator option, Windows displays a dialog that prompts you to allow UAC. After you agree to allow UAC, the output from a command is displayed in a separate window, but it vanishes immediately.

4. **Roles-based Secure Management mode is available.**

   Secure Management mode is a management mode available with this release. It is a roles-based security implementation. During the OneCommand Manager application installation, you are prompted as to whether to run in Secure Management mode. When the OneCommand Manager application is installed in this mode, the following changes occur:

   - A non-root or non-administrator user can now run the OneCommand Manager application.
   - The OneCommand Manager application host uses a user's credentials for authentication.
   - A user has OneCommand Manager application configuration privileges according to the OneCommand Manager application group to which the user is assigned.
   - In Secure Management mode, a root or administrator user is provided full privileges on the local machine (the CLI does not require credentials), but no remote privileges.

   Note: Refer to the *OneCommand Manager Application User Guide* for additional information on Secure Management mode.

5. **OneCommand Manager Secure Management mode requires OneCommand Manager user groups to be configured on the domain; or, if the host is not running in a domain, the host machine.**

   OneCommand Manager Secure Management must be able to get the OneCommand Manager application group to which the user belongs from the host's domain (Active Directory or Lightweight Directory Access Protocol [LDAP]) or, if the host is not part of a domain, the host's local user accounts.

   This access is associated with the user groups, not with specific users. An administrator must create these user groups and then set up user accounts such that a user belongs to one of the four OneCommand Manager application user groups listed in the following table.

   Table 1 Secure Management User Privileges

User Group	OneCommand Manager Application Capability
ocmadmin	Allows full active management of local and remote adapters.
ocmlocaladmin	Permits full active management of local adapters only.
ocmuser	Permits read-only access of local and remote adapters.
ocmlocaluser	Permits read-only access of local adapters.

   These four OneCommand Manager application groups must be created and configured on the host machine or domain.

6. **To view online help using the Google Chrome browser, you must disable Chrome's security check using the `--allow-file-access-from-files` option.**
   a) Create a copy of the Chrome shortcut on the desktop and rename it to RH Chrome Local (or something similar).
   b) Right-click the new Chrome icon and select **Properties**.
   c) Add the `--allow-file-access-from-files` text to the end of the path appearing in Target. You must leave a space between the original string and the tag you are adding to the end of it.
   d) Click **OK** to save your settings.
   e) Close any open instances of Chrome.
   f) To open a local copy of the online help, use the new shortcut to open Chrome, then right-click the start page and select **Open With > Google Chrome**.

7. **If you change the port speed by using the Change Port Speed dialog, and the selected speed is supported by the adapter's port but is not supported by the connected hardware, the link does not come up.**

8. **The OneCommand Manager GUI might not appear to display the adapter's next boot configuration for all available ports when a remote management console is being used; for example, integrated Lights Out (iLO), integrated Dell Remote Access Controller (iDRAC), and Interactive Media Manager (IMM).**

   The size of the screen provided by these management modules might not be big enough for the OneCommand Manager window to fully display all of the GUI components and information under the **Adapter Configuration** tab.

   Workaround

   Readjust the size of the OneCommand Manager GUI window for all the GUI scroll bars under the **Adapter Configuration** tab to become visible. You can also decrease the width of the discovery-tree panel.

9. **Enabling and disabling FA-PWWN may cause an adapter port's WWPN to change. The OneCommand Manager application discovery-tree might not display the port's newly assigned WWPN.**

   Workaround

   Stop and restart the OneCommand Manager application services and daemons when prompted by the OneCommand Manager application.

10. **Windows driver parameters do not persist after a reboot if they are set with FA-PWWN enabled.**

    Workaround

    a) Disable FA-PWWN, reset the port, and change the driver parameter, or parameters, using the OneCommand Manager GUI.
    b) Enable FA-PWWN and reboot the system.
    c) Verify that the correct driver parameters are used.