# Emulex® OneCommand® CNA Manager Application for Linux for OneConnect® Adapters Release Notes

**Version:** 11.2.1193.38-1

**Systems:** SLES 12 SP1 and SP2
RHEL 6.7, 6.8, 6.9, 7.1, 7.2, and 7.3

**Date:** May 26, 2017

## Purpose and Contact Information

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

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 ccx-tech.support@broadcom.com or request assistance online at https://oemsupportportal.broadcom.com/web2tech/ccx.html.

## New Features

- Beginning with software release 11.2, OneConnect adapters and LightPulse® adapters have independent software kits. Before updating earlier drivers and applications to the software in release 11.2, refer to the *Emulex Software Kit Migration User Guide* for special instructions and considerations for using the 11.2 software kits for OneConnect and LightPulse adapters.
- Support was added for the following operating systems:
  - RHEL 7.3 (out of box)
  - SLES 12 SP2 (out of box)
- RHEL 6.6 is no longer supported.

## Resolved Issues

There are no resolved issues in this release.

## Known Issues

1. **Known issues regarding updating firmware.**

   The following notes apply to updating firmware on OCe14000-series adapters for this release.

   **Caution:** After an adapter has been flashed to firmware version 11.x.xxx.xx or later, do not attempt to flash down to an older version without first contacting Lenovo System x support. Lenovo System x support provides a special required downgrade flash procedure. If this procedure is not followed, there is a risk in making the adapter permanently unusable.

- If the adapter in use is currently running firmware 10.0.803.2202 or earlier and iSCSI boot firmware table (iBFT) functionality is required, special steps must be followed when upgrading to this release. The recommended flash method is to use the Emulex OneConnect Offline Flash International Standards Organization (ISO), which allows flashing in a single step.
- To upgrade and enable iBFT functionality with online tools, the most recent version of the network interface card (NIC) driver, the OneCommand CNA Manager application, and the Emulex Common Interface Module (CIM) Provider must first be installed. Additionally, the firmware must be flashed twice with a reboot after each flash.

  Some online flash utilities, such as the OneCommand CNA Manager application, may instruct you to reboot and flash the firmware a second time. If iBFT functionality is not required, this message can be safely ignored. No additional procedures are necessary when iBFT functionality is not required.

2. **On the Channel Management tab, the OneCommand CNA Manager application always shows the permanent Media Access Control (MAC) address for each channel.**

   **Workaround**

   View the **Port Information** tab, which always shows the current (user-settable) MAC address and the permanent MAC address.

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

   **Workaround**

   None.

4. **Creating OneCommand CNA Manager Secure Management users and groups after the OneCommand CNA Manager application is installed in Secure Management mode causes the graphical user interface (GUI) to fail.**

   If the OneCommand CNA Manager Secure Management users and groups are created after the OneCommand CNA Manager application has been installed in Secure Management mode, when you attempt to start the OneCommand CNA Manager application GUI as a member of this group, the GUI does not run. The operating system displays the following error message:

   ```
   -Bash: /usr/sbin/ocmanager/ocmanager: Permission denied
   ```

   **Workaround**

   Do one of the following:

   - Create the users and groups before you install the OneCommand CNA Manager application in Secure Management mode.
   - Uninstall and reinstall the OneCommand CNA Manager application.

5. **OneCommand CNA Manager Secure Management mode on Linux systems requires Pluggable Authentication Modules (PAM) authentication configuration on the host machine.**

   In OneCommand CNA Manager Secure Management mode, a user is authenticated on the machine at OneCommand CNA Manager application GUI startup. The PAM interface handles this authentication. The `/etc/pam.d/passwd` file auth section or its earlier equivalent must be configured.

   **Note:** Refer to the *OneCommand CNA Manager Application User Guide* for more information about Secure Management mode.

6. **Installing the OneCommand CNA Manager application on a guest operating system prompts for a management mode.**

   When installing the OneCommand CNA Manager application on a guest operating system running on a virtual machine, the installer prompts you for a management mode (such as local-only, full-remote, Secure Management, and so on) and read-only mode. However, when the OneCommand CNA Manager application runs on a guest operating system, it runs in local-only and read-only modes, so it does not matter how these modes are specified during installation.

   **Workaround**

   None.

7. **Some Red Hat Enterprise Linux (RHEL) 6.x versions are not configured by default to return Lightweight Directory Access Protocol (LDAP) group user membership.**

   By default, some versions of RHEL 6.x do not return the LDAP group user membership along with the LDAP group information for LDAP client machines, as can be evidenced by inspecting the output of the `getent group` Linux command.

   **Workaround**

   To work with OneCommand CNA Manager Secure Management, these machines must be configured such that the `getent group` command returns not only the groups configured on the machine or domain but also each group's users. Otherwise, OneCommand CNA Manager Secure Management requires the OneCommand CNA Manager group to be the user's primary group to provide the OneCommand CNA Manager Secure Management function.

8. **Single root-I/O virtualization (SR-IOV): Running the OneCommand CNA Manager application on a guest operating system with more than one virtual function causes all NIC ports to appear under a single adapter.**

   If you assign NIC virtual functions from adapters to a virtual machine and run the OneCommand CNA Manager application in the virtual machine’s guest operating system, the NIC functions appear under a single adapter node in the OneCommand CNA Manager application discovery–tree. In this situation, the guest operating system in a virtual machine reports the same Peripheral Component Interconnect (PCI) bus number for all virtual functions, and the OneCommand CNA Manager application incorrectly determines that each of the discovered NICs are from the same adapter.

   **Workaround**

   None.

9. **On OCe11100-series adapters, if the Mode is set to Force and the Speed is set to 1 Gb/s, do not perform a MAC loopback test in the OneCommand CNA Manager application.**

   If you perform a MAC loopback test, the link does not come back up after the test is performed.

   **Workaround**

   None.

10. **If you enable DHCP for iSCSI ports from the Modify TCP/IP Configuration dialog (under the Port Information tab) and if virtual local area networking (VLAN) is already enabled, a Transmission Control Protocol/Internet Protocol (TCP/IP) address might not be obtained from the DHCP server (remaining 0.0.0.0): IP address, subnet mask, and gateway address.**

    You might encounter this known issue if your DHCP server is not VLAN-aware or is not configured for VLAN.

    **Workaround**

    Use one of the following workarounds:

    - Use a DHCP server that is VLAN-aware and properly configured.
    - Follow these steps to disable and enable DHCP and VLAN:
      a) On the **Port Information** tab, click **Modify**. The **Modify TCP/IP Configuration** dialog is displayed.
      b) Clear the **VLAN Enabled** and **DHCP Enabled** options.
      c) Click **OK**. The **Port Information** tab is displayed.
      d) On the **Port Information** tab, click **Modify**. The **Modify TCP/IP Configuration** dialog is displayed.
      e) On the **Modify TCP/IP Configuration** dialog, select the **VLAN Enabled** and **DHCP Enabled** options and click **OK**.

11. **The NIC driver must be installed to run the OneCommand CNA Manager application on OneConnect adapters.**

    If the OneConnect adapter is run without the NIC driver installed and enabled, many of the management functions are unavailable, and the OneCommand CNA Manager application can display erroneous information.

    The following management functions are unavailable:

    - Firmware
      - Core dump
      - Download
      - All diagnostics, including beaconing and diagnostic dumps
      - Disabling or enabling a port
    - Erroneous display information includes the following:
      - **Fibre Channel over Ethernet (FCoE)** storage ports are incorrectly grouped under the physical port
      - NIC, FCoE, and iSCSI ports do not appear under the correct adapter
      - Active and flash firmware versions
      - Firmware status
      - Basic input/output system (BIOS) version

- Boot code version
- Transceiver data display
- Physical port link status
- All Converged Enhanced Ethernet (CEE) settings
- Event log display (OneCommand CNA Manager CLI only)
- Adapter temperature

**Workaround**

The NIC driver must always be installed on OneConnect adapters.

12. **The following is a requirement for unloading or loading Emulex FCoE, NIC, or iSCSI device drivers.**

    If you load or unload an Emulex FCoE, NIC, or iSCSI device driver for Linux after the machine is rebooted, you must perform the following steps:

    a) Close any open OneCommand CNA Manager applications.

    b) Restart the OneCommand CNA Manager application daemons. To restart OneCommand CNA Manager application daemons, the daemons must be stopped and started.

       i) Run the `/usr/sbin/ocmanager/stop_ocmanager` script.

       ii) Run the `/usr/sbin/ocmanager/start_ocmanager` script.

    c) Run the OneCommand CNA Manager application GUI or the OneCommand CNA Manager CLI client application.

13. **If both VLAN and Data Center Bridging Capabilities Exchange (DCBX) are disabled, the iSCSI priority configured in the DCB tab is not set in the iSCSI packets sent out by the port.**

    **Workaround**

    Enable or disable VLAN from the **iSCSI Port Info** tab in the OneCommand CNA Manager application.

14. **Interference can occur when the OneCommand CNA Manager application attempts to permanently change World Wide Names (WWNs).**

    Some newer adapters (for example, converged network adapters [CNAs]) on some newer systems use techniques in the BIOS code at boot time to configure the adapter, such as the adapter WWN. In such cases, this might interfere with the OneCommand CNA Manager application’s ability to make permanent (nonvolatile) changes to the adapter’s WWN.

    **Workaround**

    None.

15. **Messages appear on the terminal during Web-Launch installation or uninstallation.**

    On Linux SLES 11 SP2 systems, when the OneCommand CNA Manager Web-launch component is installed or uninstalled using the `wsinstall` and `wsuninstall` scripts, respectively, the following messages are displayed:

    ```
    insserv: Script jexec is broken: incomplete LSB comment.
    insserv: missing `Required-Stop:'  entry: please add even if empty.
    ```

These warning messages do not affect the operation or installation of the Web-launch component. They appear on SLES 11 SP1-specific versions of the relevant software (insserv and jexec). The scripts invoke this software by invocation of the standard Linux chkconfig utility typically used for daemon installations.

**Workaround**

None.

16. **On SLES 11 systems, the Open-FCoE Resource Package Manager (RPM) package (open-fcoe-1.0.4-10.2) is incompatible with the OneCommand CNA Manager application package and must be removed from the target host machine.**

    The host bus adapter (HBA) application programming interface (API) library that the Open FCoE package installs (libhbalinux.so.1) causes all OneCommand CNA Manager application processes to crash with a segmentation violation.

    **Workaround**

    To recover, you must reinstall the OneCommand CNA Manager application without loading the Open-FCoE package.

17. **On SLES 11 systems, installing or uninstalling the Open-FCoE RPM package after the OneCommand CNA Manager application is installed, removes OneCommand CNA Manager application entries in the system file in the `/etc/hba.conf` file.**

    This issue breaks the Linux system HBA API functionality, and, as a result, the OneCommand CNA Manager application client applications no longer run.

    **Workaround**

    Reinstall the OneCommand CNA Manager application.

18. **On RHEL host systems and on Citrix 5.6 and later host systems, the OneCommand iSCSI Simple Network Management Protocol (SNMP) daemon does not start if the libsensors shared object library is not found (for example, if the libsensors RPM package is not installed).**

    **Workaround**

    Install the libsensors RPM package from the appropriate RHEL or Citrix distribution, and restart the OneCommand iSCSI SNMP daemon.

19. **On some RHEL x86_64 and Power PC (PPC) 64 systems, uninstalling the Red Hat 32-bit or 64-bit libhbaapi RPM deletes entries in the `/etc/hba.conf hbaapi` configuration file, thereby disabling the OneCommand CNA Manager hbaapi layer.**

    **Workaround**

    Reinstall the OneCommand CNA Manager application.

20. **Unloading the NIC driver from a Linux machine causes the OneCommand CNA Manager application to lose connectivity.**

    If you unload the NIC driver from a Linux machine, any OneCommand CNA Manager application (GUI or OneCommand CNA Manager CLI client) running on the machine loses connectivity with the NIC and related configuration data.

**Workaround**

To recover, you must perform the following steps:

a) Stop the OneCommand CNA Manager applications and daemons using the stop_ocmanager script.

b) Reload the NIC driver using modprobe.

c) Restart the OneCommand CNA Manager application daemons using the start_ocmanager script.

d) Restart the OneCommand CNA Manager application GUI or OneCommand CNA Manager CLI client).

21. **When the SNMP daemon starts, it triggers warning messages within SELinux for certain operations.**

**Workaround**

To avoid SELinux warning messages, disable SELinux.

a) To disable SELinux, open a terminal, and enter the following command at the prompt:

```
echo 0 > /selinux/enforce
```

b) To enable SELinux, open a terminal, and enter the following command at the prompt:

```
echo 1 > /selinux/enforce
```

22. **A permanent driver parameter change fails if the system is rebooted too soon.**

When you make permanent driver parameter changes with the OneCommand CNA Manager application, the application automatically makes the required entry in the `/etc/modprobe.conf` or equivalent file. Because the LightPulse Fibre Channel (LPFC) driver loads so early in the Linux machine boot sequence, the new contents of the `/etc/modprobe.conf` file must be reinserted into the Linux system initrd file (using the mkinitrd utility) for the driver to pick up the new driver parameter value on the next boot. Failure to generate the new initrd file causes the driver to fail to get the new driver parameter value on subsequent driver loads (machine boots). The OneCommand CNA Manager application automatically does this function for you (re-creates initrd with the mkinit function); however, it can take as long as 45 to 60 seconds after the driver parameter is changed for a complete initrd rebuild. If you reboot the machine immediately after the driver parameter change is made, the auto-recreation of the initrd file by the OneCommand CNA Manager application might fail to complete. In these cases, this failure causes the driver to not obtain the new driver parameter value upon subsequent reboots.

**Workaround**

Wait a minimum of 45 to 60 seconds after making the driver parameter change before rebooting the machine.

23. **Newly added LUNs on a storage array might not appear on the host machine Linux operating system or the OneCommand CNA Manager application.**

**Workaround**

Do one of the following:

- Run the following script from the command shell:

```
/usr/sbin/lpfc/lun_scan all
```

- Reboot the host machine after the LUN has been added at the target array.

24. **When using iSCSI Enterprise Target (IET) software, target portals with more than 60 iSCSI targets might not be discovered.**

    When using the open source IET software package to present targets to the iSCSI initiator, adding target portals that contain greater than 60 targets fails the resulting target discovery operation. This is the result of an error in the IET target implementation.

    **Workaround**

    None.

25. **Logged-in iSCSI targets retain login options through reboots.**

    When an iSCSI target is discovered by adding a target portal, that target takes the target portal's login options. The target portal's login options are taken from the initiator login options. However, you can modify them when adding a target portal. If the Internet storage name service (iSNS) discovers a target, it gets its default login options from the initiator login options.

    After a target is discovered, its login properties are not changed when the initiator login options are changed. When you log into a target, the login properties used at the time of login are remembered. If you reboot, the logged-in targets are logged in again with the remembered login options (initiator login options are not used).

    When you remove the targets (and the target portal, if that is how they were discovered) and then cause the targets to be rediscovered, the target's login properties are defined again by how they are discovered as described at the beginning of this known issue.

    **Workaround**

    None.

26. **The Web Launch browser client must be run with administrator or root privileges.**

    When running the OneCommand CNA Manager Web Launch GUI, you must have administrator privileges when logged into the Web Launch client user. On a Linux browser client, you must be logged in as the root user. Unusual behavior might occur if this requirement is not met.

    **Workaround**

    None.

27. **The dump command on a boot-from-SAN adapter causes a system panic.**

    When the OneCommand CNA Manager application performs a dump of an adapter that is booting from SAN and has no failover support, the operating system halts when the adapter is taken offline to perform the boot and writes the dump file to the host file system. The file system is unavailable because the adapter was taken offline.

    **Workaround**

    Before performing a dump of an adapter, make sure that the adapter is not a boot-from-SAN adapter. Alternatively, provide failover support so when the adapter is taken offline to perform the dump, the boot-from-SAN connection is maintained by the failover.

28. **The OneCommand CNA Manager application elxhbamgrd daemon can take up to 30 seconds to stop.**

    The OneCommand CNA Manager application elxhbamgrd daemon process might take up to 30 seconds to stop when attempting to terminate it. This condition applies to SLES 11 SP1 and RHEL 6.0 and all subsequent Linux distributions corresponding to the 8.3.x LPFC driver versions.

    **Workaround**

    None. The behavior of the elxhbmgrd daemon is linked with the MAX timeout that the Linux kernel associates with small computer system interface (SCSI) block SCSI generic driver (BSG) interface commands and the OneCommand CNA Manager application register for events function.

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

30. **The Linux operating system with Security Enhanced Linux (SELinux) enabled receives numerous benign warning messages in `/var/log/messages` when starting the OneCommand CNA Manager application.**

    When the OneCommand CNA Manager application is installed and SELinux is enabled, numerous messages similar to the one that follows will appear in the `/var/log/messages`:

    ```
    SELinux is preventing /usr/sbin/ethtool from write access on the file.
    For complete SELinux messages. run sealert -l
    a5c4abd9-5279-4621-8976-52ed71bd8c13 Oct 16 19:12:07 localhost python:
    SELinux is preventing /usr/sbin/ethtool from write access on the file.
    ```

    **Workaround**

    To suppress these messages, run the following two commands:

    ```
    grep ethtool /var/log/audit/audit.log | audit2allow -M mypol
    ```

    ```
    semodule -i mypol.pp
    ```

31. **For multichannel configuration, if you attempt to switch from SIMode to vNIC1 in the OneCommand CNA Manager application when more than eight functions have been configured in SIMode, the operation fails, and an error message is displayed.**

    **Workaround**

    To configure vNIC1, use the OneCommand CNA Manager CLI `SetAdapterPortConfig <MAC|WWPN>` command.

    For example:

    ```
    HbaCmd SetAdapterPortConfig <MAC|WWPN> p0=nic,fcoe,nic,nic
    p1=nic,fcoe,nic,nic mctype=VNIC1
    ```

32. **If you enable Custom mode, the personality might revert to NIC, iSCSI, or FCoE if an actual Custom configuration is not defined.**

    If Custom mode is enabled, the following conditions apply:

    - If you leave all functions set to NIC, the configured personality is automatically switched from Custom to NIC.
    - If you leave the functions configured the same as they would be for iSCSI, the configured personality is automatically switched from Custom to iSCSI.

- If you leave the functions configured the same as they would be for FCoE, the configured personality is automatically switched from Custom to FCoE.

33. **The OneCommand CNA Manager application does not display adapter-specific information (such as model, serial number, and firmware state) for OCe10100-series adapters on Oracle Linux operating systems.**

    **Workaround**

    None.

34. **For OCe14000-series adapters, on the Adapter Configuration tab, the third function does not allow the selection of any storage protocol.**

    For example:

    On the **Adapter configuration** tab with the **Custom** button selected, if you select **FCoE** from the list of the second function, the third function does not display other protocols (such as iSCSI) in the list.

    **Workaround**

    a) Switch the protocols from FCoE to iSCSI for the second function. The third function now displays FCoE.
    b) Switch back to the original option for the second function (FCoE). This action now displays iSCSI for the third function.

    This workaround can be repeated for the remaining ports if needed.

35. **LUNs are not displayed when the target connection is refreshed after port flap.**

    **Workaround**

    Restart the OneCommand CNA Manager application.

36. **If the CLI (HBACMD) is used to perform a firmware download to a local adapter, and the OneCommand CNA Manager GUI is up and running while that firmware download is taking place, the OneCommand CNA Manager GUI might experience problems displaying information on various display tabs after the download completes. The value displayed for most of the fields on the affected tabs and dialogs is N/A.**

    **Workaround**

    There are three possible workarounds:

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

## Technical Tips

1. **The OneCommand CNA Manager application no longer installs OneCommand Vision components.**

2. **If Data Center Bridging (DCB) settings are required when connected to a non-Data Center Bridging Exchange Protocol (DCBX) switch (or a switch with DCBX disabled), DCBX must be disabled on the OneConnect adapter to use the adapter's configured parameters.**

   If DCBX is enabled, DCB priority flow control (PFC) and Priority Groups are ignored (the adapter assumes the switch does not support these parameters) and for FCoE adapters, the FCoE priority (COS) is 3.

3. **The `HbaCmd UmcEnableChanLink` command has been removed.**

   To enable the logical link status of a channel, use the `CMSetBW` command to set the minimum bandwidth to a value greater than 0. To disable the logical link status, set the minimum and maximum bandwidths to 0.

4. **Emulex SR–IOV features are available on SLES 11 distributions beginning with the SP2 release.**

   The OneCommand CNA Manager application support for displaying the SR–IOV virtual functions on the base operating system is provided on SLES 11 distributions beginning with the SP2 release.

5. **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 CNA Manager application installation, a user is prompted as to whether to run in Secure Management mode. When the OneCommand CNA Manager application is installed in this mode, the following changes occur:

   - A non-root or non-administrator user can now run the OneCommand CNA Manager application.
   - The OneCommand CNA Manager application host uses a user's credentials for authentication.
   - A user has OneCommand CNA Manager application configuration privileges according to the OneCommand CNA 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 CNA Manager Application User Manual* for additional information on Secure Management mode.

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

   OneCommand CNA Manager Secure Management must be able to get the OneCommand CNA Manager application group to which the user belongs from the host's domain (Active Directory or LDAP) or, if the host is not part of a domain, the host's local user accounts. This access is associated with user groups, not with specific users. Administrators set up user accounts, such that a user belongs to one of the four OneCommand CNA Manager application user groups listed in the following table.

**Table 1** Secure Management User Privileges

| User Group | OneCommand CNA 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 CNA Manager application groups must be created and configured on the host machine or network domain. OneCommand CNA Manager Secure Management uses the C-library API calls `getgrnam` and `getgrid` to retrieve the OneCommand CNA Manager Secure Management group information. The equivalent to these calls can be obtained on the shell command line by typing the `getent group` command. If the four OneCommand CNA Manager application groups are listed, along with their member users, this is an indication that the host machine is sufficiently configured to work with OneCommand CNA Manager Secure Management.

7. **An end-to-end (ECHO) diagnostic test fails if the corresponding targets are not supported.**

   Make sure that the connected targets are supported.

8. **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 L.

   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 that appears 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 press **Ctrl + Open** and browse to the start page; or open Chrome with the new shortcut, then right-click the start page and select **Open With > Google Chrome**.

9. **On OneConnect adapters, if you change the port speed in 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.**

10. **The OneCommand CNA 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 CNA Manager window to fully display all the GUI components and information under the **Adapter Configuration** tab. Readjust the size of the OneCommand

CNA 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.

11. **When installing new OCe11102 adapter driver and firmware versions, it is best to install both the driver and the firmware without rebooting between installations to minimize the possibility of operating with mismatched versions of driver and firmware.**