ioSphere®

ioSphere Management Solution 3.7.0

User Guide

January 29, 2014

FUSION-IO

Copyright Notice

Fusion-io, Inc.
2855 E. Cottonwood Parkway
Suite 100
Salt Lake City, UT 84121
USA

(801) 424.5500

Part Number: D0005267-005_4

Published: January 29, 2014

Table of Contents

Introduction

Welcome to the ioSphere Management Solution, where you can easily manage ioMemory device across multiple servers throughout a data center. This manual describes ioSphere Management Solution's controls and functionality.

ioSphere Management Solution runs on both Windows and Linux platforms. ioSphere Management Solution can manage hosts running Windows, Linux, and Mac OS X. Visit http://support.fusionio.com for the latest list of supported systems.

> All operating systems must be 64-bit architecture to support ioMemory devices.

Getting Started

For detailed instructions to install ioSphere Management Solution, see the *ioSphere Management Solution 3.7.0 Installation Guide.*

First Time Setup, New Install

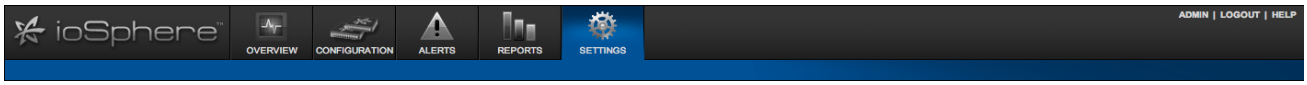
To return to the New Install screen at any point during the setup, refresh the browser window.

1. Select **New Install.**
2. Enter the Administrator password.
3. Enter the **ioMemory Push Frequency**. The default setting is 15 second increments. Increasing this number will make updates less frequent and the history/report information less detailed. Decreasing this number makes updates more frequent, but could affect performance if you are using many clients (for example, more than 20 or 30 clients).
4. Enable **Remote Access** (optional).This setting is unchecked by default. Check this box to allow remote access to this ioSphere Management Solution server.
5. Advertise Using Zeroconf (optional). This allows Agents to automatically discover and connect to ioSphere Management Solution (requires Avahi on Linux or Bonjour on Windows).
6. Enter the remote host name in ***Host Name*** field.
7. The ***Port*** field is set to 9051 by default; You have the option of entering a different port here.
8. Use the pre-configured SSL certificate (optional).

The ioSphere Management Solution includes a pre-configured SSL certificate, but it is recommended that you create and use a custom certificate.

Top-Level Tabs

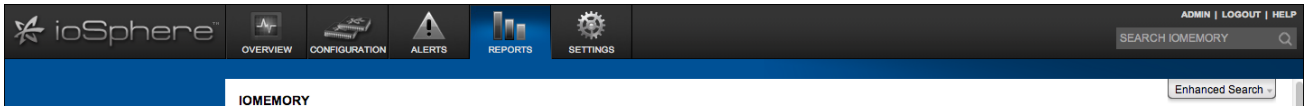
The ioSphere Management Solution application is divided into five top-level tabs: ***Overview, Configuration, Alerts, Reports,*** and ***Settings.*** These tabs are static and appear at the top of the window regardless of the page you are viewing.



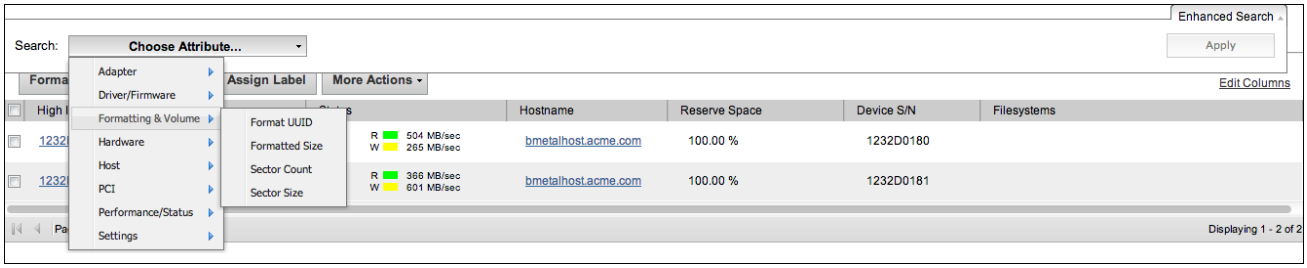
To the right of the top-level tabs are the following title bar links:

- ***Admin***--This is only visible when logged in as an administrator.
- ***Logout***
- ***Help***--This will provide links to Fusion-io support and the online Knowledge Base.

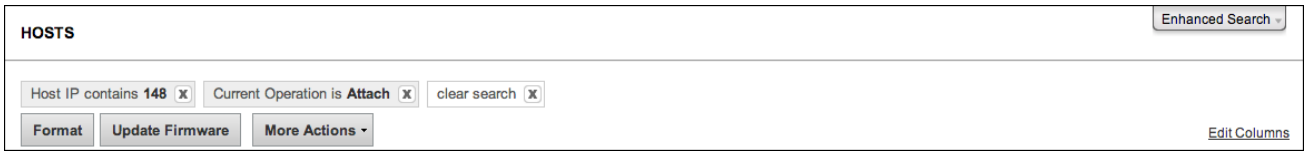
A search box is available below the title bar links when using the ***Configuration, Alerts,*** and ***Reports*** top-level tabs. Search is a quick method of filtering items based on a keyword from within the screen you are viewing. It does not give you as much of a refined searching ability as ***Enhanced Search*****,** which is located below the search box.



Enhanced Search is more detailed than the default search. ***Enhanced Search*** allows you to search for devices using a variety of attributes. These attributes are based on the columns (categories) available on each page. The following is an example of some of the attributes you can search for with ***Enhanced Search*****:**



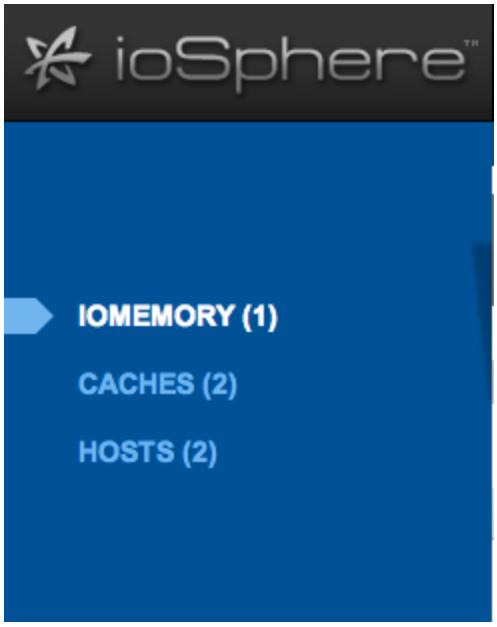
If a current search criteria is applied on any of the pages where the ***Search*** box is active, you will see that criteria displayed above the grid. Use ***Enhanced Search*** to add additional search criteria to the search. (Additional search criteria are evaluated as a logical AND, where all search criteria must be satisfied for results to display.)



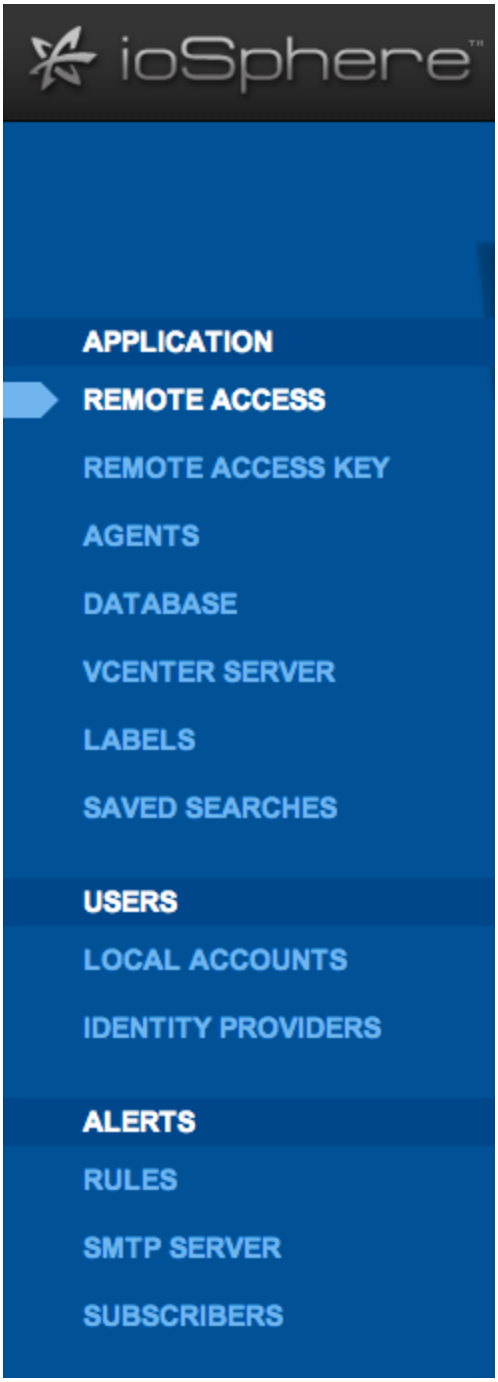
Click on the criteria itself to remove an item from the search criteria, or click on **Clear Search** to clear all search filters.

Sidebar

Each of the main tabs, except ***Overview***, has a navigation sidebar on the left side of the screen that provides selection options for the active tab.

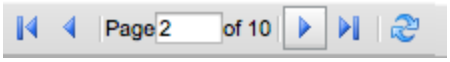


For the ***Settings*** tab, the following options are provided:


ioSphere
APPLICATION
REMOTE ACCESS
REMOTE ACCESS KEY
AGENTS
DATABASE
VCENTER SERVER
LABELS
SAVED SEARCHES
USERS
LOCAL ACCOUNTS
IDENTITY PROVIDERS
ALERTS
RULES
SMTP SERVER
SUBSCRIBERS

Paging and Refresh

On the ***Configuration*** and ***Alerts*** tabs, data is presented as grids. These grids display 10 items per page, and you can use controls at the bottom of the grid to navigate through the pages. The following paging controls are available:



- ***Last Page***
- ***Previous Page***
- ***Page Number*** – where you can enter the number of the page you want to view
- ***Next Page***
- ***First Page***

At the bottom of these grids there is also a ***Refresh*** icon that will force the data in the grid to be updated. If you do not click **Refresh**, data currently displayed in the grid is automatically updated every 10 seconds.

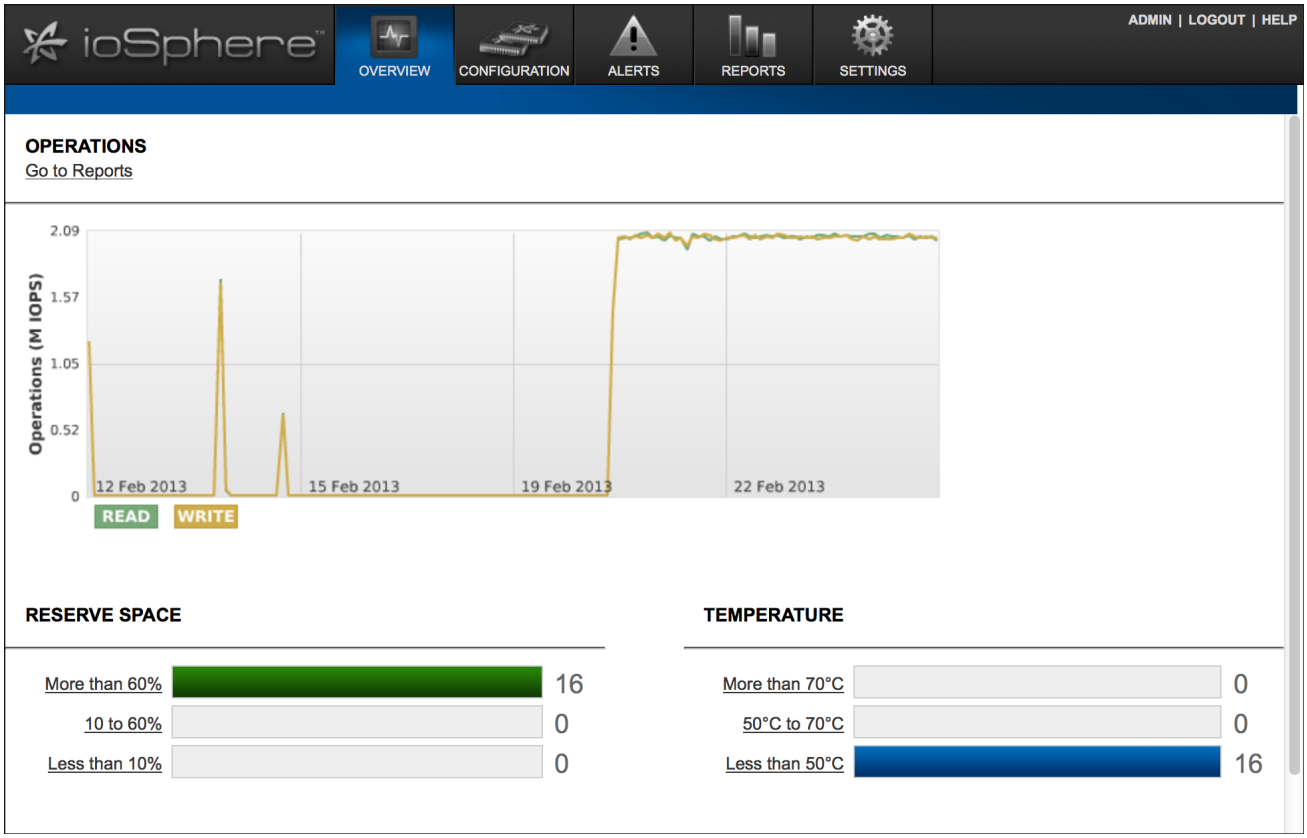
> In some cases, clicking the **Refresh** icon does not refresh the grid completely. In these cases, refreshing or reloading the browser content can reformat the screen and update the grid correctly.

The ioSphere Management Solution Feature Set

This section describes the controls and features of the ioSphere Management Solution.

Overview Tab

The **Overview** tab summarizes key information gathered from all ioMemory devices, including **IOPS, Reserve Space,** and **Temperature.**



Operations

Operations shows a historical trend of **IOPS** for all devices being managed by the ioSphere Management Solution Management Solution.

Read READ and ***Write*** WRITE buttons at the bottom of the graph allow you to toggle between the display of Read and Write data of the Operations report.

Go To Reports

Click the ***Go to Reports*** link to take you to the information contained on the Reports Tab. For more information, see the Reports Tab on page 33.

Reserve Space

Reserve Space (as shown on the **Overview** tab) displays helpful information regarding the health of the devices being monitored as determined by the percentage of reserve space available. The reserve space decreases as NAND blocks are retired, with write operations tending to wear out blocks faster than reads do.

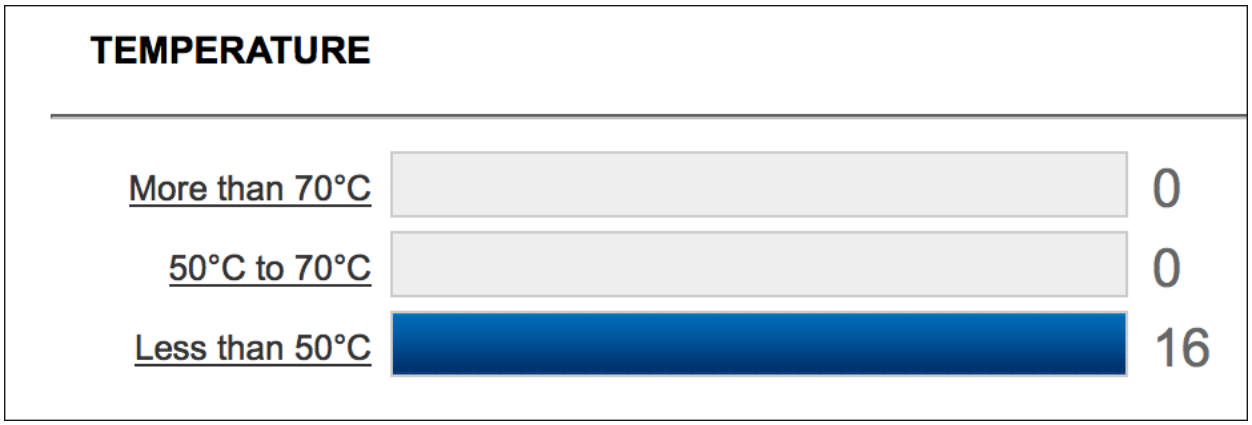
An early warning message is sent by the driver when the amount of reserve is close to reaching the 10%-available threshold. If the reserve space decreases to 0% of its original size, the device enters write-reduced mode (degraded) in order to prolong the lifespan of the device. Sometime after the reserve space is depleted, the device enters read-only mode and no further writes to the device can be done. If crossed, these thresholds and their accompanying messages should provide ample time for you to back up and migrate data on the device.

The links on the left of the reports will take you to the Configuration tab with an Enhanced Search filter set that matches the link. For example, clicking on the "More than 60%" link will take you to the Configuration tab where an "Reserved Space is greater than 60" filter only shows ioMemory device that have at least 60% reserve space remaining.

The number to the right of the report is the number of devices being monitored. In the example shown, 16 devices are at More than 60%.

Temperature

The temperature report shows how many of the ioMemory devices are within preset temperature ranges.



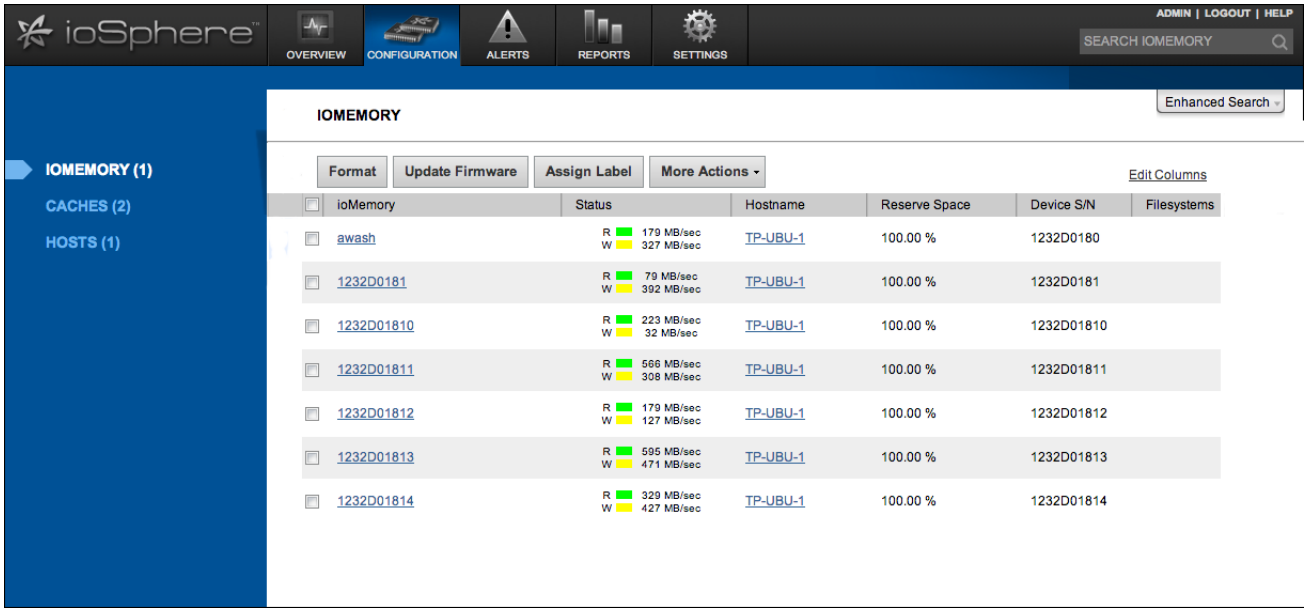
The links on the left of the reports are links that will take you to the **Configuration** tab with an Enhanced Search filter set that matches the label. For example, clicking on the "Less than 50°C" link will take you to the **Configuration** tab where an "FPGA Temperature is less than 50" filter only shows devices whose temperature is less than 50 degrees centigrade.

Normal operating temperatures for devices vary. However, as device temperatures rise the following alerts may be generated:

- **Warning** – the temperature of the device is high enough to take note of, but can still operate normally.
- **Error** – the temperature of the device is too high to continue normal operation, and it is removed from the bus. However, the device can still be queried.
- **Shut Down** – the temperature has reached or exceeded the maximum allowable temperature, and the FPGA shuts the device down completely.

Configuration Tab

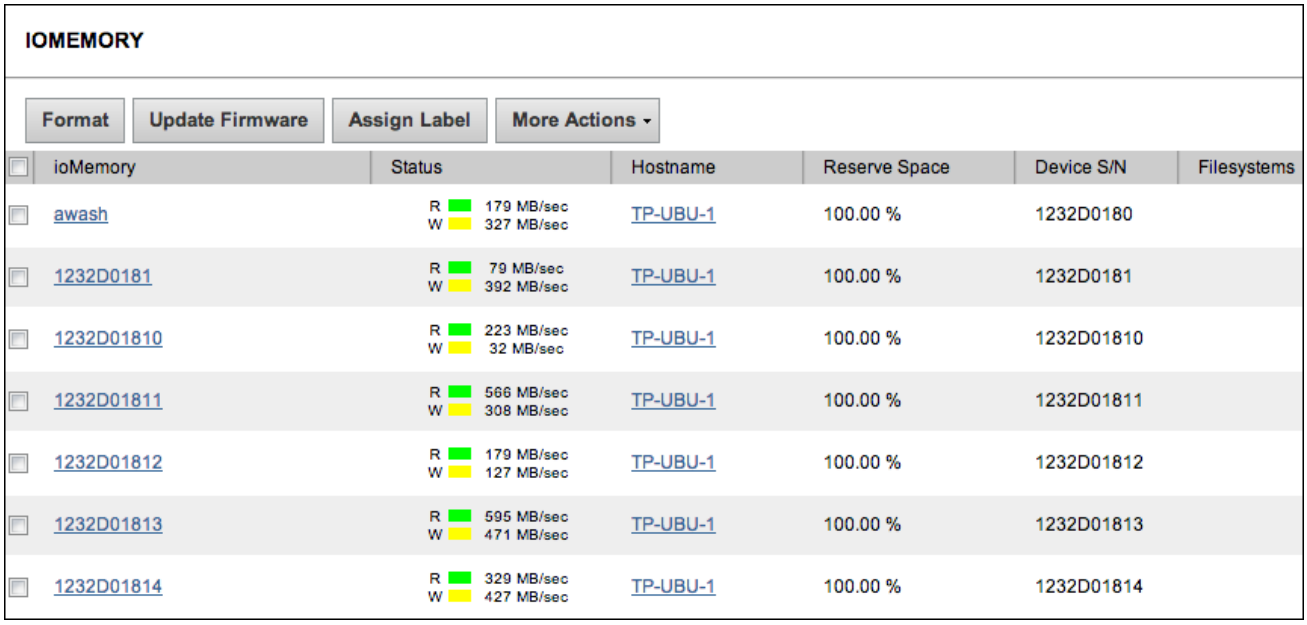
This page provides a central location where you can configure and manage your devices.



Click the ***More Actions*** button to access the **Attach Device** and**Detach Device** options. See More Actions on page 23 for more information.

Device List

To the right of the sidebar is the main content area where a grid is displayed that contains all items that match the currently-selected sidebar item (in this case, **ioMemory**).



Click the checkbox next to each device on which you want to perform an action, or click the device's name to open its Device Page (see the Device Page on page 59 for more information).The actions that can be performed are:

- **Format**
- **Update Firmware**
- **Assign Label**
- **Attach device**
- **Detach device**

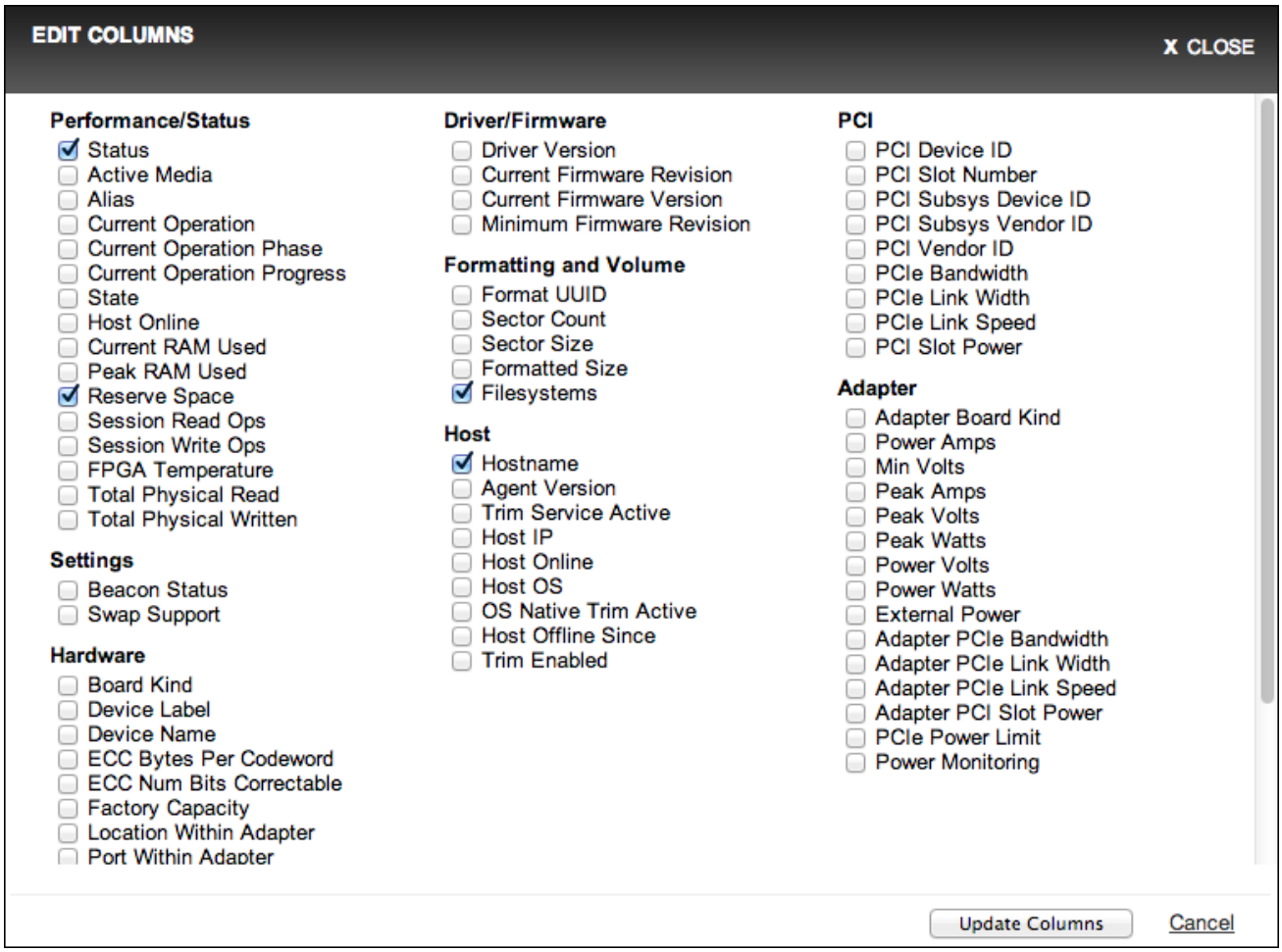
You can select multiple checkboxes to perform an action across multiple devices.

Do not Update Firmware across multiple devices simultaneously. Update firmware on one device at a time. A Duo card should be treated as two logical devices and each half should be updated separately.

In the image above, the **ioMemory** filter has been selected in the sidebar. ioSphere Management Solution is displaying the information selected by the user. In this case, it displays each device's **Status, Hostname,** amount of **Reserve Space, Device Serial Number, and Filesystems.** The information displayed is different when **Caches, Hosts,** or **Clusters** are selected.

Columns

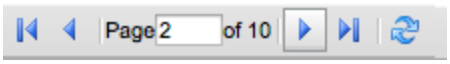
Click the **Edit Columns** link to specify what device data you want displayed in the device grid.



Select the columns you want to display, then click ***Update Columns***.

Pagination

The main pages under the configuration tab display up to 10 devices on a page. If a search results in more than 10 devices, the results will be paged, and you can use the controls at the bottom of the list to move between result pages.



ioMemory

The ioMemory device screen displays a list of ioMemory devices that are being managed. The devices are listed by alias, which, by default, is the serial number of the device. (However, the alias can be changed on the Configure Device Tab. For more information, see Configure Device Tab on page 61)

On the ioMemory device screen, the alias is an active link that will take you to the Device Page, where device tabs provide additional information and configuration options for the device. For more information, see Device Page on page 59

Click the checkbox next to each device on which you want to perform an action, or click the device's name to open its Device Page.The actions that can be performed are:

- **Format**
- **Update Firmware**
- **Assign Label**
- **Attach device**
- **Detach device**

You can select multiple checkboxes to perform an action across multiple devices.

> Do not Update Firmware across multiple devices simultaneously. Update firmware on one device at a time. A Duo card should be treated as two logical devices and each half should be updated separately.

Format

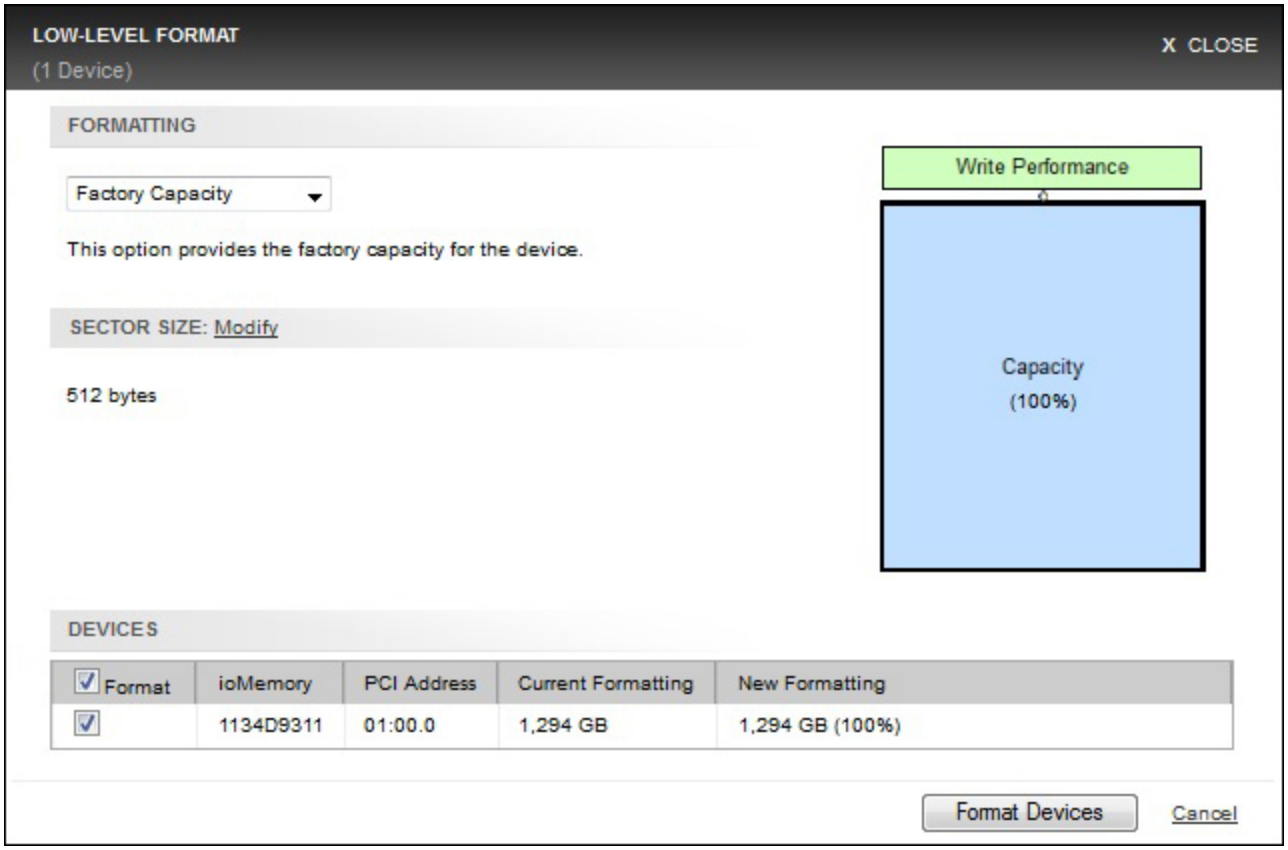
> Formatting a device will destroy any data still remaining on it. Please be sure to back up your data before proceeding.

Your ioMemory device comes pre-formatted to factory capacity.Generally, it is not necessary to use this option. However, you would use it if any of these situations arise:

- You need to re-format the drive to change its logical size or modify write performance.
- Your application supports sector sizes larger than 512 bytes (the default), and you want to tune your device accordingly. Larger sector sizes allow for more optimal CPU/memory use, and the Maximum Capacity format option provides a larger format size when the sector size is increased.
- You are instructed to do so by Fusion-io Customer Support.

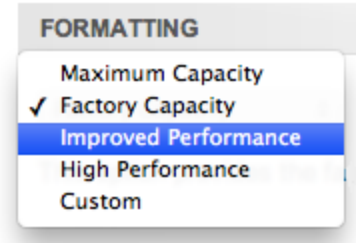
ioSphere Management Solution performs a low-level format that is different from a format performed by an operating system using standard disk management utilities. You do not need to perform a low-level format to create an operating system-specific volume on the device. You can select one or more ioMemory device on the ioSphere Management Solution page to format simultaneously.

When you click the **Format** button, the **Low-Level Format** dialog appears.



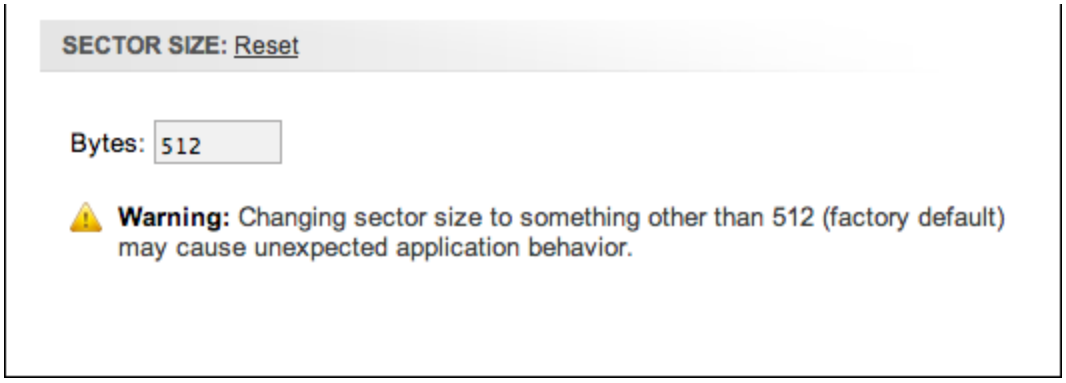
> In some configurations, the sector size will not be able to be modified from this screen. If that is the case, the Modify link will not be displayed.

Here you can set the ratio of **Write Performance to Capacity.** You can increase Write Performance by decreasing the ioMemory device's capacity--the reverse is also true. You can select from a drop-down list of preset ratios (**Maximum Capacity, Factory Capacity, Improved Performance, High Performance).**

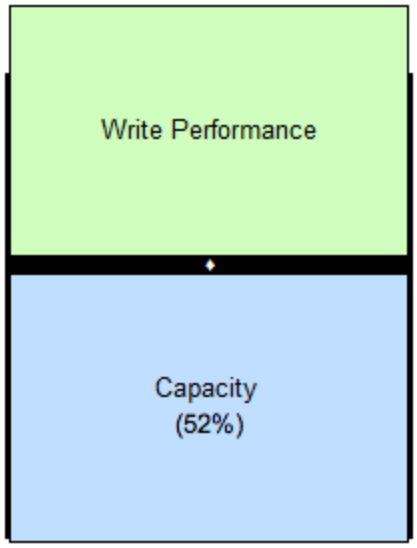


You can customize the Write ratio with the **Custom** selection (from the drop-down menu) or by dragging the line between **Write Performance and Capacity** in the graphic.

You can modify the sector size here. Click the **Modify** link and enter a new sector size in bytes.



You can also change the sector size by dragging the sizing bar in the **Write Performance** box.



> Changing sector size to something other than 512 (factory default) may cause unexpected application behavior.

The selected ioMemory device(s) appear below the Write Performance/Capacity graphic. Check the corresponding checkbox to perofrm the desired action on the selected device or devices.

> If an ioMemory device is unable to format (that is, it is busy or the formatting is not valid for that particular device), you will not be able to select it for formatting.

When you are ready to format the selected ioMemory device(s), click the **Format Devices** button.

To exit the Low-Level Format dialog without formatting any devices, click, the **Cancel** link.

When the format process begins, the **Config History** bar appears at the bottom of the screen. For more information, refer to the Config History section of Appendix B - Software Updates on page 99.

Update Firmware

Updating ioMemory device involves two procedures: updating the ioMemory VSL (driver) on the host machine, and updating the firmware on the ioMemory device. Refer to Appendix B - Software Updates on page 99 for more information.

> Before using the GUI to update firmware, you must place the new firmware packages on the machines that contain the device you want to upgrade. In some cases, you may need to create the folder or directory where the GUI will look for the firmware packages.
>
> For Linux, verify that the following directory exists:
>
> **/usr/share/fio/firmware**
>
> If the directory does not exist, create it. After the directory is created, copy the firmware package to the directory.
>
> For Windows, verify that the following folder exists:
>
> **C:\Program Files\Fusion-io ioMemory VSL\Firmware**
>
> If the folder does not exist, create it. After the folder is created, copy the firmware package to the directory.

The **Update Firmware** operation lets you upgrade the ioMemory device's firmware. You should upgrade the firmware if:

- ioSphere Management Solution presents a warning icon stating that the firmware is out of date.
- The Windows System Event Log or Linux system log (typically in **/var/log/messages**) reports a problem due to out-of-date firmware.
- The ioMemory device stops working.
- You are instructed to do so by Fusion-io Customer Support.

> In most cases, if you upgrade the ioMemory device firmware, you must also upgrade the ioMemory device driver. Most support issues arise from mismatched firmware and drivers.

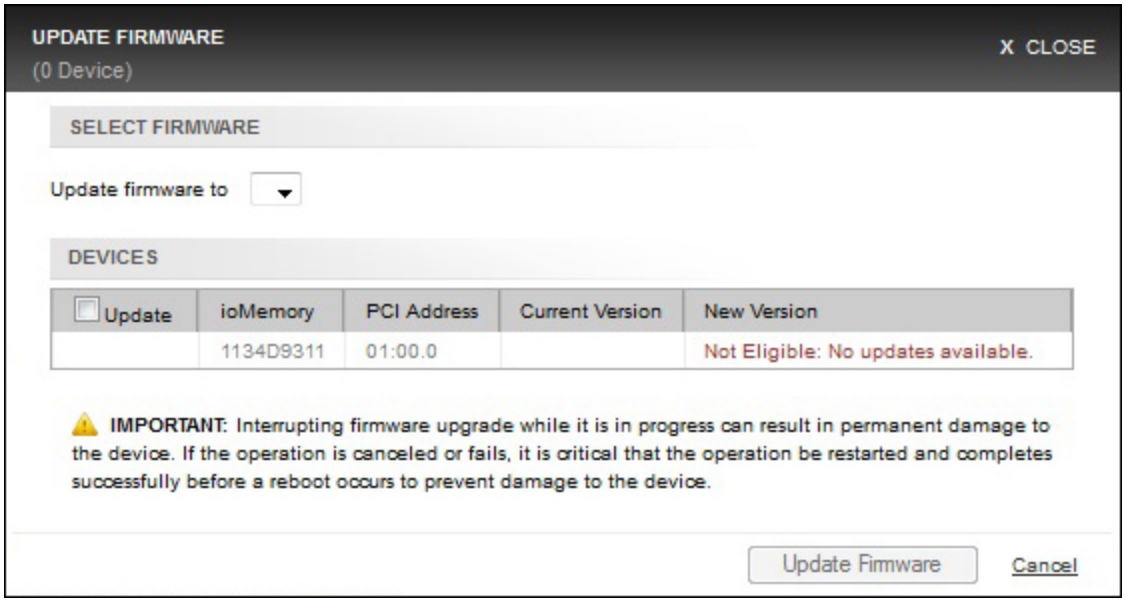
Upgrading the firmware may take some time. Monitor the progress using ioSphere Management Solution.

> Back up the data on your ioMemory device(s) prior to performing the upgrade.

It is extremely important that the power not be turned off during a firmware upgrade, as this could cause device failure. If a UPS is not already in place, consider adding one to the system prior to performing a firmware upgrade.

Interrupting an update while it is in progress can result in permanent damage to the device. Never use the Windows Task Manager to stop the update or kill the process in Linux. (For this same reason, the Agent process ignores all termination requests.) If the operation fails, it is critical that you restart this operation and complete it successfully before restarting the computer to prevent damage to the device.

When you click the **Update Firmware** button, the **Update Firmware** dialog appears. Here you can select from the drop-down menu the version of the firmware you would like to install.



The selected ioMemory device(s) appear below the Update firmware drop-down menu. Check the corresponding checkbox to perofrm the desired action on the selected device or devices.

If an ioMemory device is unable to update (that is, it is busy or updates are not available for that particular device), it will display in a separate section titled Unable to Update at the bottom.

When you are ready to upgrade the selected ioMemory device's firmware, click the **Update Firmware** button. Or, to exit the **Update Firmware** dialog without updating any devices, click the **Cancel** link.

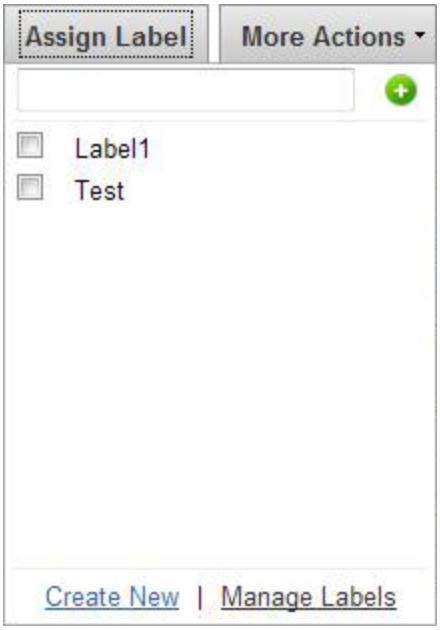
When the firmware update process begins, the **Config History** bar appears at the bottom of the screen. For more information, refer to the Config History section of Appendix B - Software Updates on page 99.

Assign Label

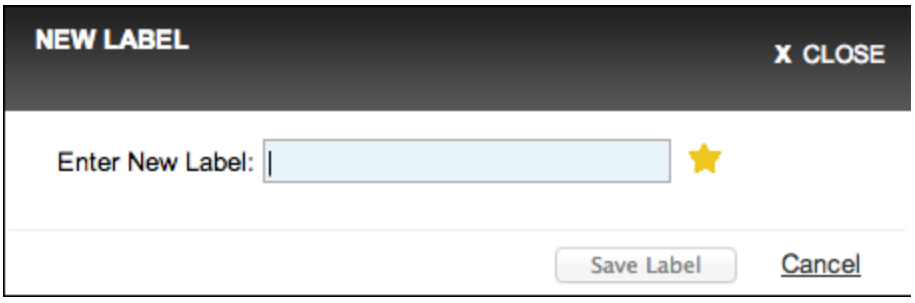
Assign Label lets you organize your ioMemory devices into categories or groups.Clicking on the label will quickly display all ioMemory devices belonging to that group.

> When you create a new label, you can mark it as a **Favorite** by selecting the star icon. For more information about Labels, see Labels on page 39.

> You can also create new labels on the **Settings** tab.



To create a new label, select one or more ioMemory devices on the ioSphere Management Solution page and click the **Assign Label** button, then click the **plus** button. The **New Label** drop-down appears.



Type in the label's name and click **Save Label.**

The New Label dialog will close after you save the label. Alternately, you can close the window with the Cancel link or the x in the upper right corner.

Label Favorites

The **Favorites** feature lets you tag a label as a **Favorite** by clicking the gold star next to the label name. You can mark any label as a favorite, including your own labels and those created by other users.

More Actions

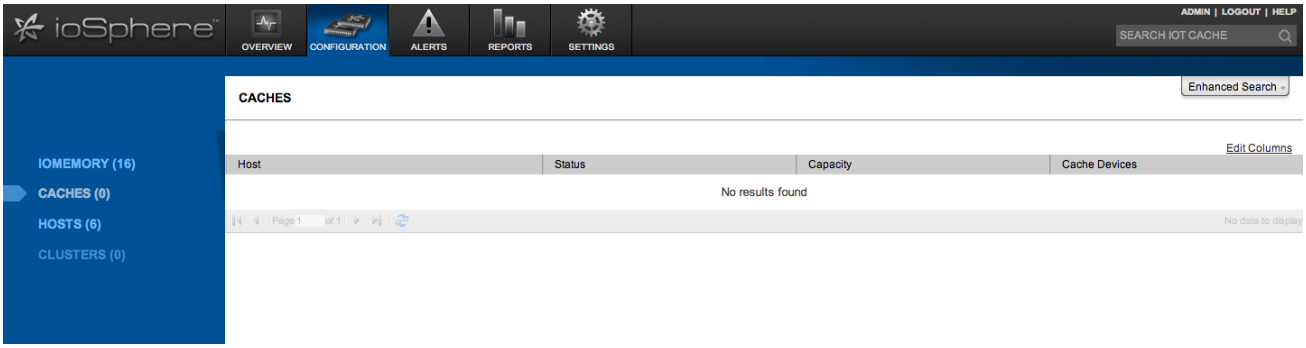
Here you can attach or detach the selected ioMemory devices.

The **Attach Device**operation creates a link, so the ioMemory device interacts with the operating system. In most cases, the operating system driver automatically attaches the installed device at boot time, so you only need to use **Attach Device** when you manually detach an ioMemory device (that is, to perform a low-level format).

Detach Device disconnects your ioMemory device from the operating system. Once detached, the device is not accessible to users or applications. (You need to use **Attach Device** to make it accessible.) You will not need to use this action because ioSphere Management Solution automatically detaches when performing an update or format from the UI.

Caches

The Caches table displays the name of the cache, its status (**Enabled** or **Disabled**), the ioMemory device in use, the **Hostname,** the **Cluster Name,** and the **Backing Store Device Name** (the backing store device is the name of the device being cached). All these links take you to the Device page, except the **Cluster Name** that takes you to a table showing all the hosts that are part of the cluster.

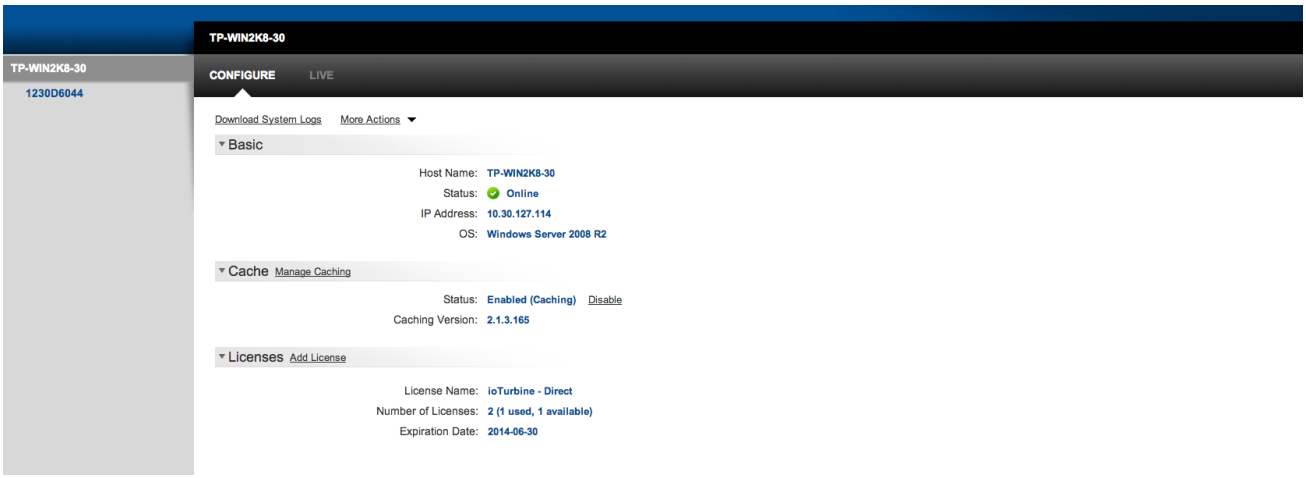


For information on caching concepts and administration, see the *ioTurbine 2.0.3.0 Administrators Guide* and the *ioTurbine 2.0.3.0 Concepts Guide*.

Manage Caching

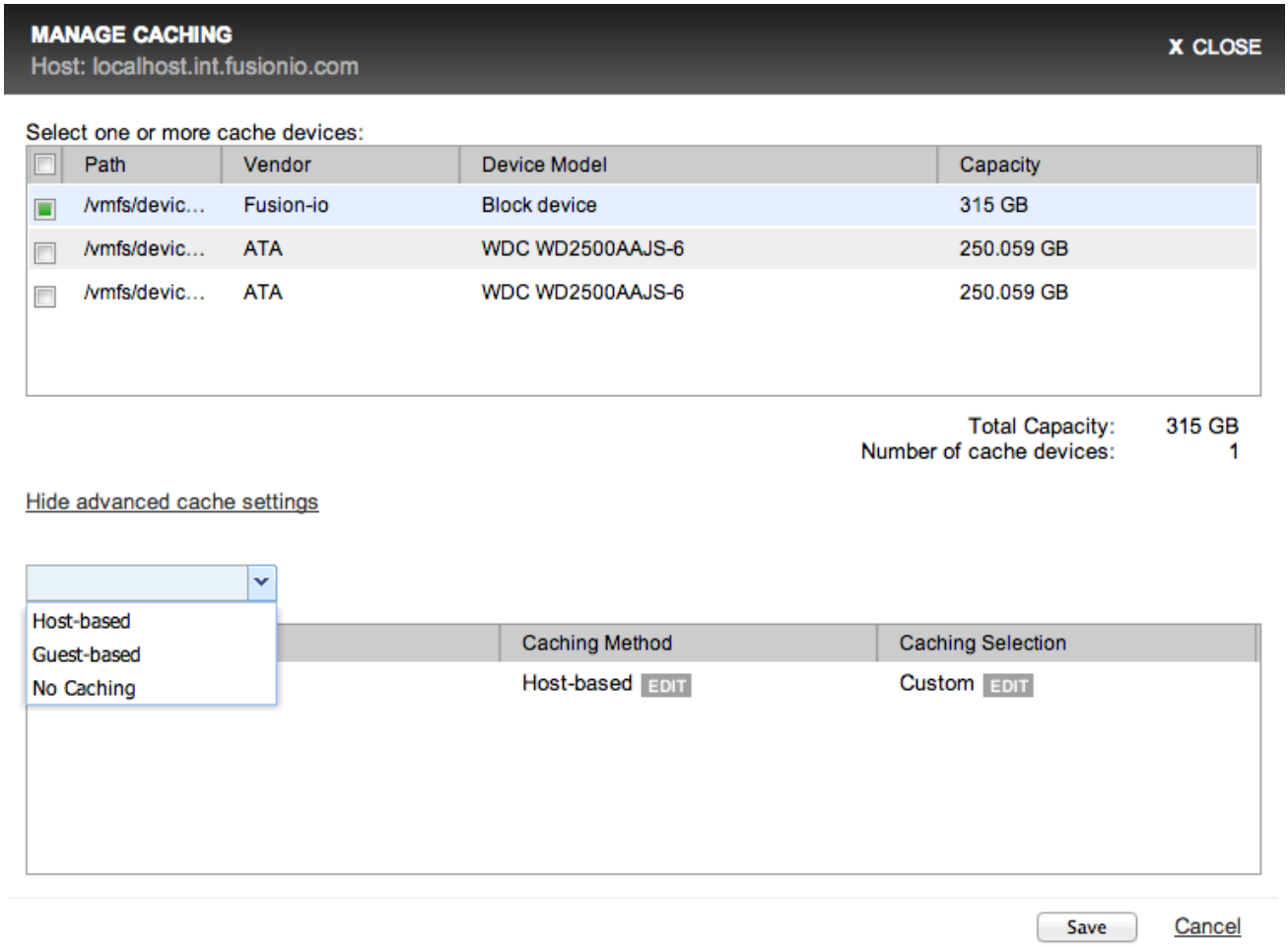
The Manage Caching dialog is launched from the **Cache** section of the Host Configure Tab when the host is selected.

The Manage Caching screen allows the user to manage the caching settings for the host. The user may use this dialog to set up caching for the first time or to edit the existing cache settings. Selecting one or more cache devices is the minimum necessary user action to enable caching on the host. However, more granular caching options are available by clicking Show advanced cache settings.



Rows in the cache devices table can be sorted by clicking on column headings. Scroll through this table to view all available cache devices for the host.

Change Cache Selection

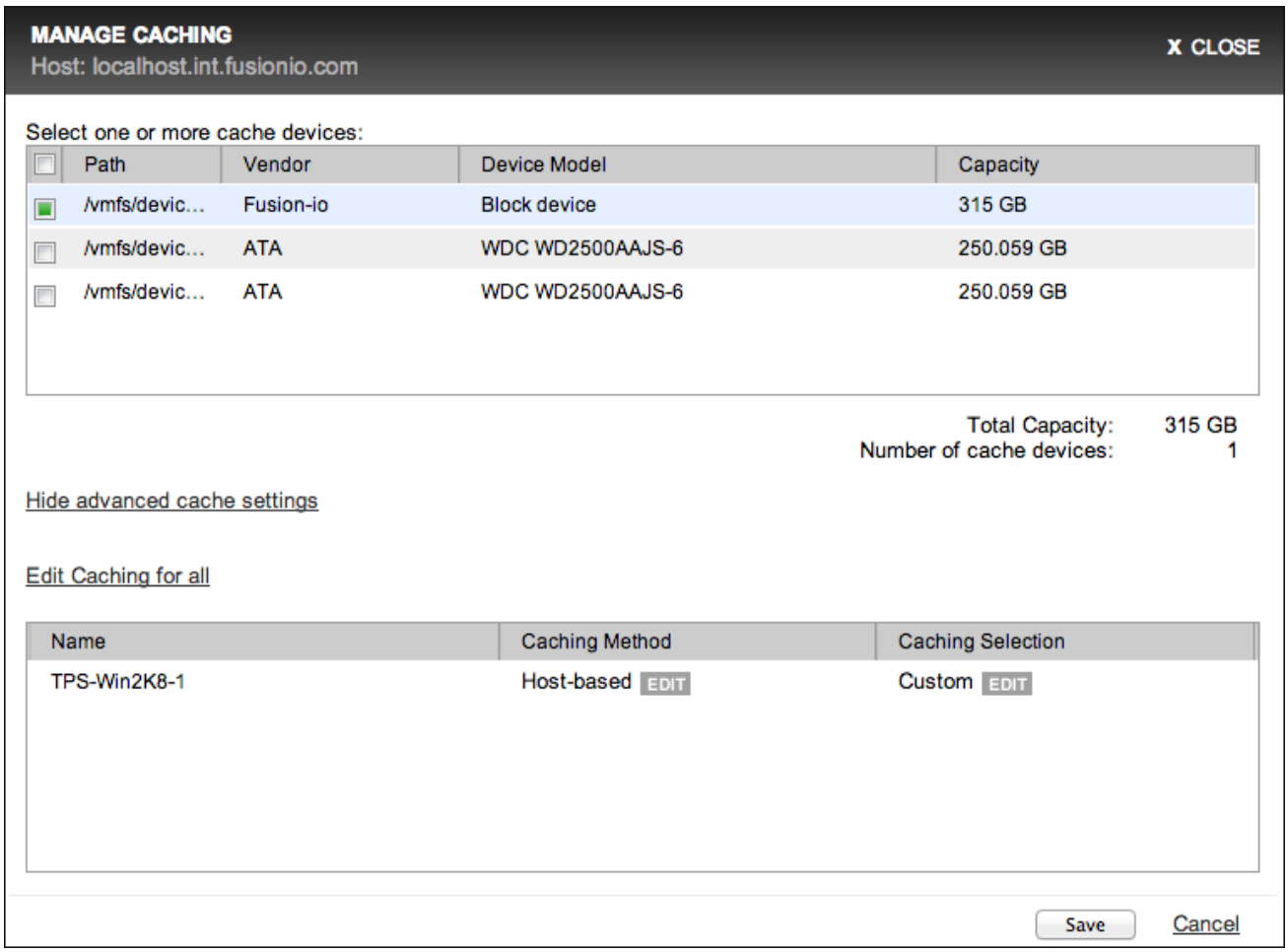


Advanced Cache Settings

The advanced caching section of the Manage Caching Dialog displays when the user clicks the ***Show advanced cache settings*** link. The Manage Caching dialog's advanced section presents the user with a drop-down menu containing two choices: Cache All (default) and Custom.

This section will differ between the physical caching and virtual caching

Choosing the ***Edit Caching for all*** option causes all disks, partitions, and files on the on the host to be cached. This is the default setting.



Choosing the **Custom** selection from the drop down displays additional options to choose what to cache. The options differ between Windows and Linux.

For Windows hosts, the user has the option to cache specific disks, partitions, or files.These three options can be reached by three tabs displayed in the custom caching section labeled: Volumes, Disks, Files.

For Linux, all the block devices on the host are listed in a single table of "Volumes". This can include disks, extents, raids, and LVM volumes. All checkboxes are checked by default.

Advanced Cache Dialog--Physical Caching

The physical version of the Manage Caching dialog's advanced section presents the user with a drop-down menu containing two choices: **Cache All** (default) and **Custom**.

Cache All

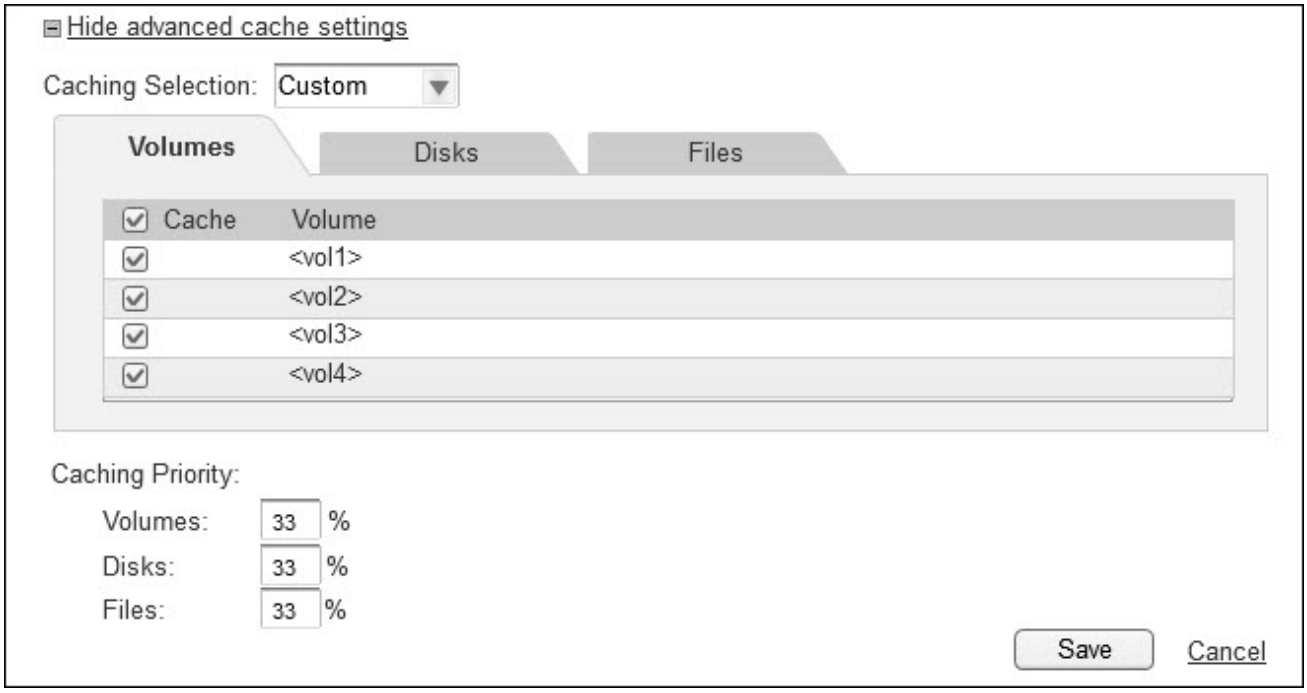
Choosing the **Cache All** option causes all disks, partitions, and files on the on the host to be cached. This is the default setting.

⚠ Caching is only enabled on volumes that currently exist. If a volume is added afterwards, caching will need to enabled manually on that volume.

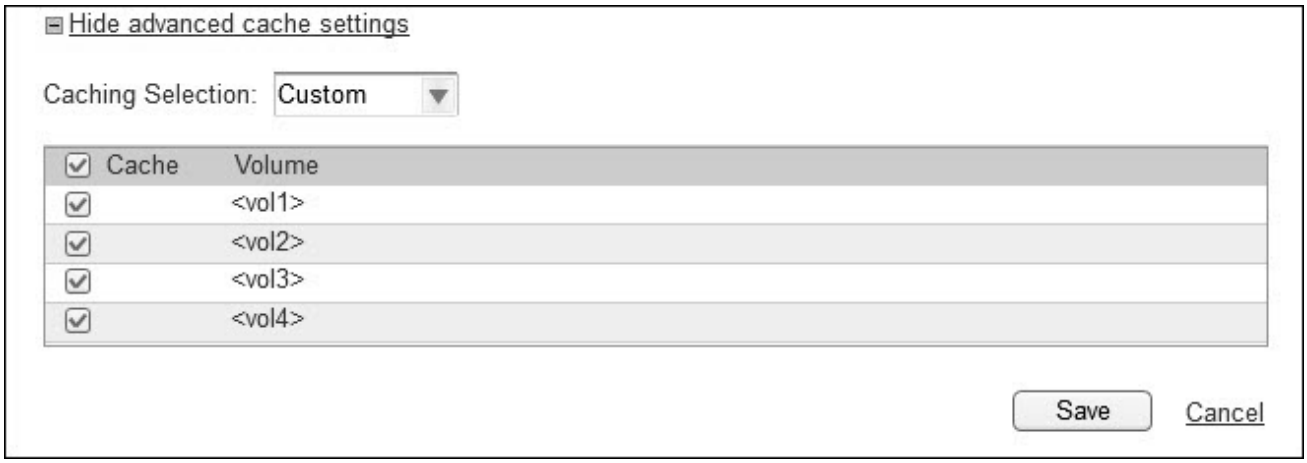
Custom

Choosing the **Custom** selection from the drop down displays additional options to choose what to cache. The options differ between Windows and Linux.

For Windows hosts, the user has the option to cache specific disks, partitions, or files.These three options can be reached by three tabs displayed in the custom caching section labeled: Volumes, Disks, Files.

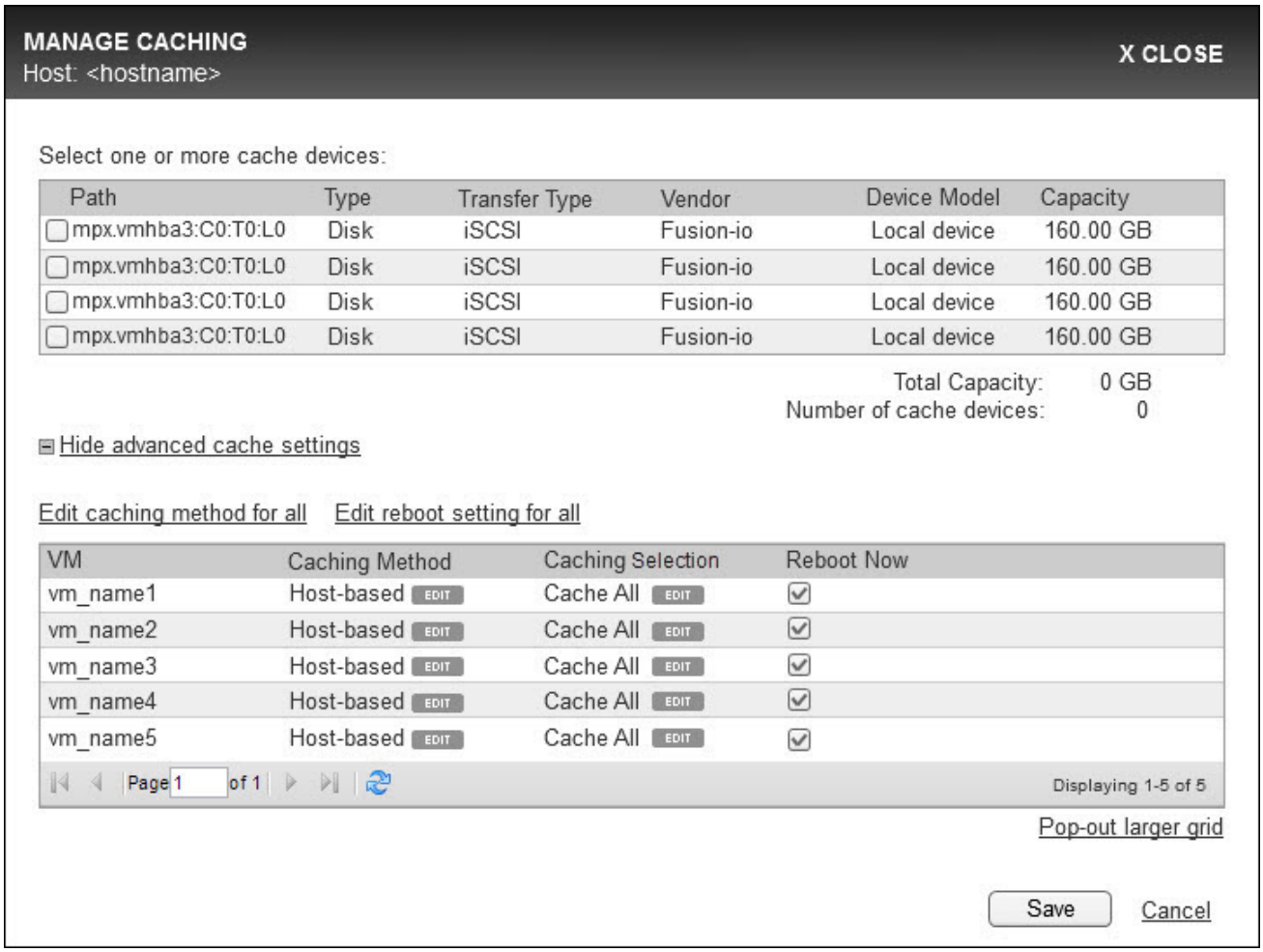


For Linux, all the block devices on the host are listed in a single table of "Volumes". This can include disks, extents, raids, and LVM volumes. All checkboxes are checked by default.



Advanced Cache Dialog--Virtual Caching

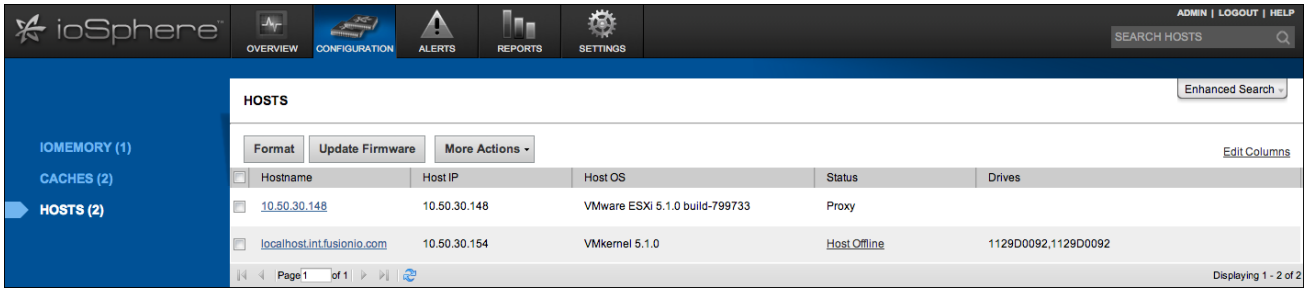
When using ioSphere Management Solution in vCenter, clicking on the Show advanced cache settings link in the Manage Caching Dialog displays the advanced cache settings grid shown below. Clicking Hide advanced cache settings collapses the grid and related links.



Hosts

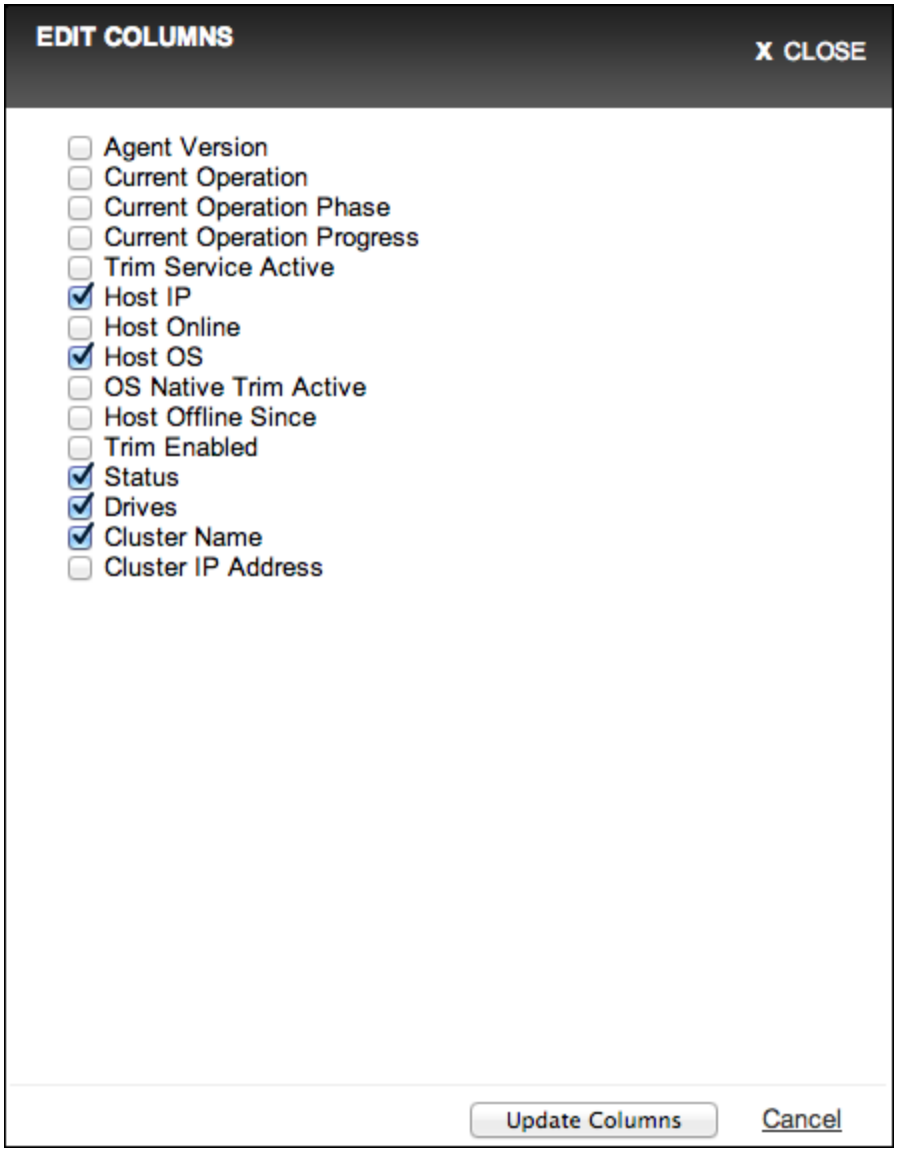
The ioSphere Management Solution Host Screen displays when the user clicks a Host link in the interface.

When you select **Hosts** from the sidebar, the host page displays information about the hosts that contain ioMemory devices. By default, the hosts grid shows **Hostname, Host IP, Host OS, Status, Drives,** and **Cluster Name** (if applicable).



The aliases of the devices (which, by default, are the serial numbers of the devices), and any labels assigned to the devices, display in the **Drives** column.

You can add additional columns to the host page by clicking **Edit Columns.**



Select the columns you want to display, then click ***Update Columns***.

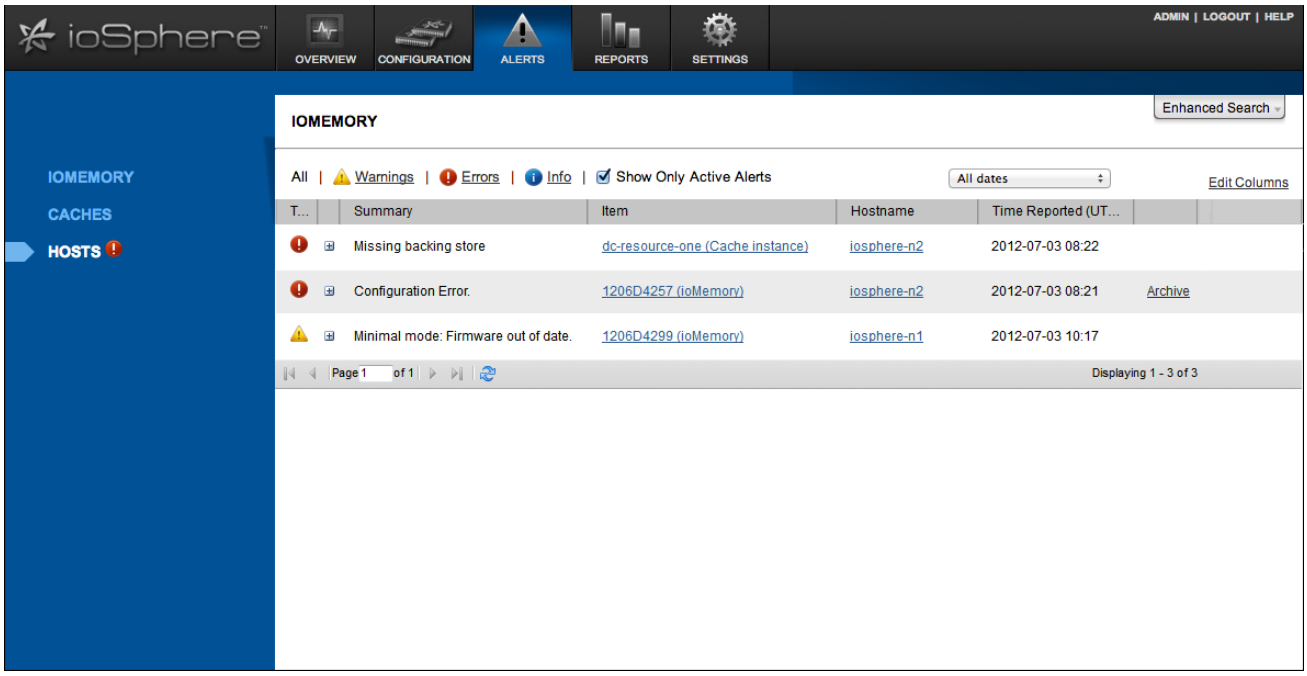
Alerts Tab

This page lists current and historical alerts for ioMemory devices and cache instances. Alerts are for recording or notification purposes.

> If there are current alerts, the Alerts icon will illuminate.

There are three types of alerts that are recorded and displayed in the alerts section.

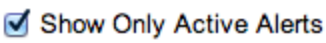
- **Error:** An error or problem has occurred
- **Warning:** A condition has occurred that might cause a problem in the future
- **Info:** Useful information



Active Alerts

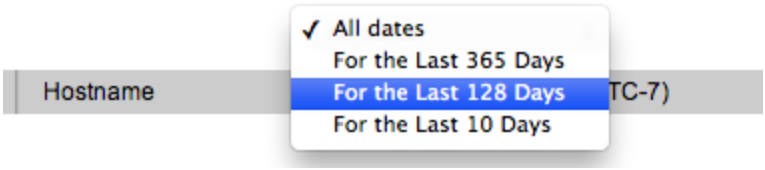
Active alerts are conditions that are persistent and need to be corrected, or that occurred recently and need to be acknowledged and archived. If there are Current Alerts, the Alerts icon will illuminate.

To show only Active alerts, click the **Show Only Active Alerts** box.



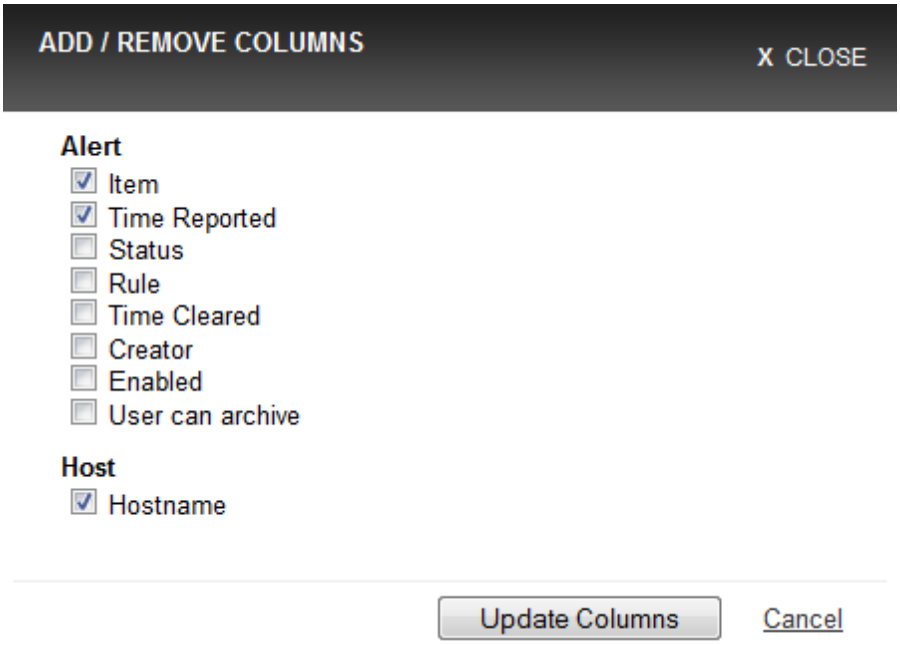
For the Last _____ Days

From the drop-down list, you can choose to show alerts for the selected time span. Select all dates, or 365, 128, or 10 days.



Columns (Alerts Tab)

Click the **Edit Columns** link to select what information is displayed in the list for each device.



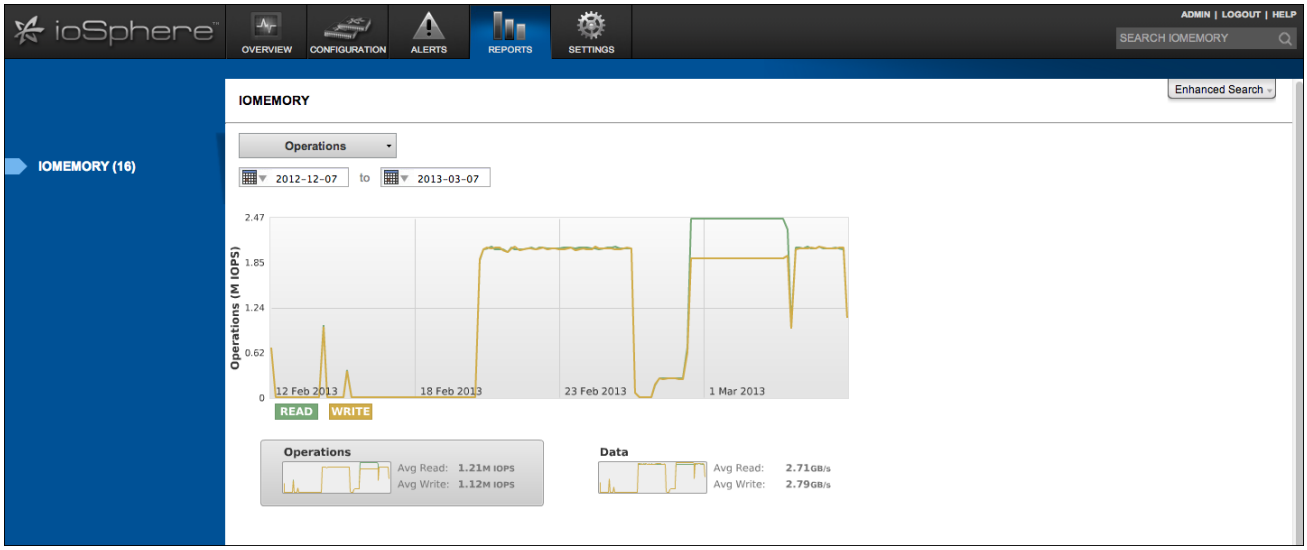
Select the columns you want to display, then click ***Update Columns***.

Archive

Alerts are automatically cleared from the **Active Alerts** grid when the condition that caused them no longer exists. You may manually archive Alerts that are present due to a user-created **Alert Rule**, and those that are a result of a failed configuration operation. Click the **Archive** link to the right of the alert in the list. Archived alerts are still viewable in the **Alert History.**

Reports Tab

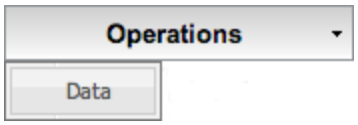
This page reports the Operations and the Data information for ioMemory devices.



For more information on the specific graphs available, see Reports Device Tab on page 63.

Operations - Data Drop-Down

Click to display information about **Operations (IOPS)** or **Data Volume (Data).**



The selected information's corresponding button (at the bottom of the graph) will be highlighted. You can also click on the **Operations** or **Data** boxes to display their information in the graph.

Date Range

Select the start and end dates for the time range you wish to display.

Read and Write Buttons

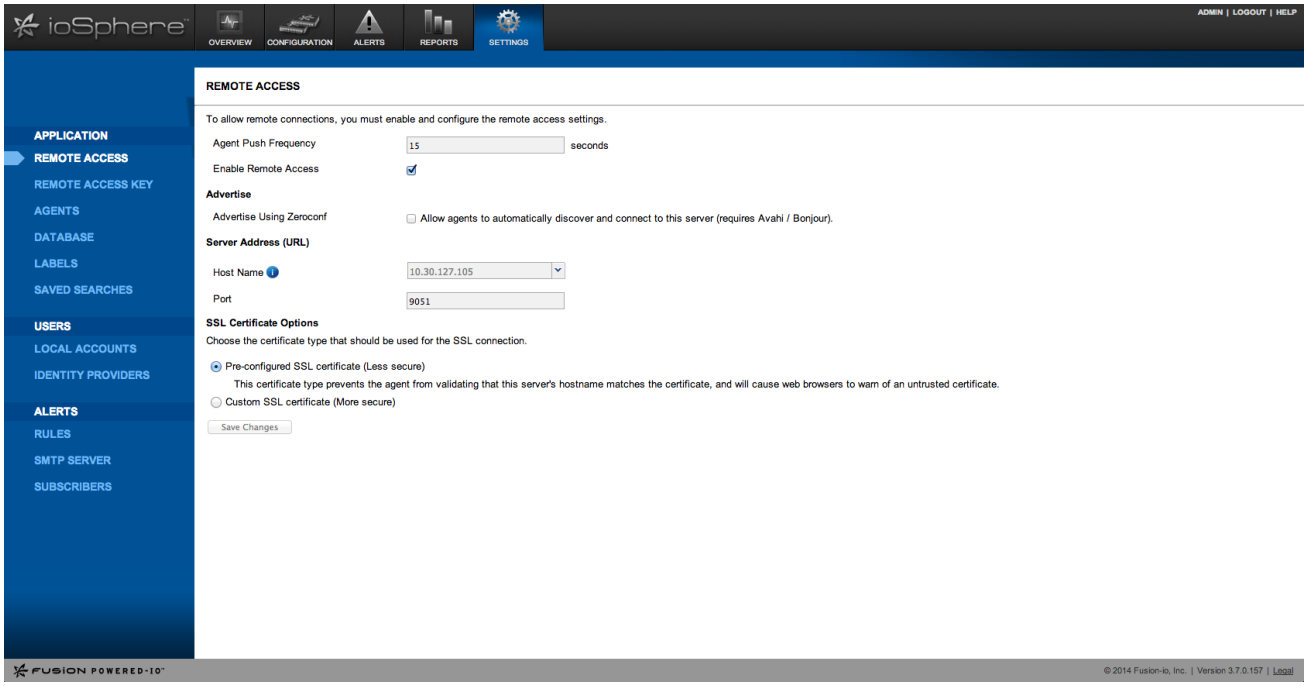
Click **Read** 

or **Write** 

under the graph to show or hide their data.

Settings Tab

Use the **Settings** page to manage remote access options, local accounts and identity providers, alert rules, SMTP server options, subscribers, ioMemory device labels, and saved searches.



> Some features on the Settings page are only available to a Server Admin.

Remote Access

Use the Remote Access screen of the Settings Tab to configure users' and hosts' remote access settings.

Agent Push Frequency

Use this field to enter the **Agent Push Frequency.** The default is 15 seconds. Increasing this number will make updates less frequent (and history/report information less detailed). Decreasing this number makes updates more frequent, but could affect performance if you are using many clients (more than 20 or 30, for example).

> Increasing this number above 600 displays this message:
> "A high push frequency will potentially result in data being out of date in ioSphere."

Enable Remote Access

Check this box to allow remote access to the Management Server from Agent processes not located on the same machine as the Management Server.

Do not disable remote access from within the VMWare VCenter plugin. Doing so will cause vSphere clients to fail to connect to ioSphere Management Solution.

Advertise Using Zeroconf

Check this box to cause the Management Server to advertise its service using the Zeroconf service discovery protocol. This allows remote Agent services to automatically discover and communicate with the Management Server.

The Zeroconf protocol requires that Avahi be installed on Linux operating systems and Bonjour be installed on Windows operating systems.

Host Name

Enter an IP address that will not change in an uncontrolled way (such as a DHCP lease that expires). This address is used by Agent services to communicate to the Management Server.

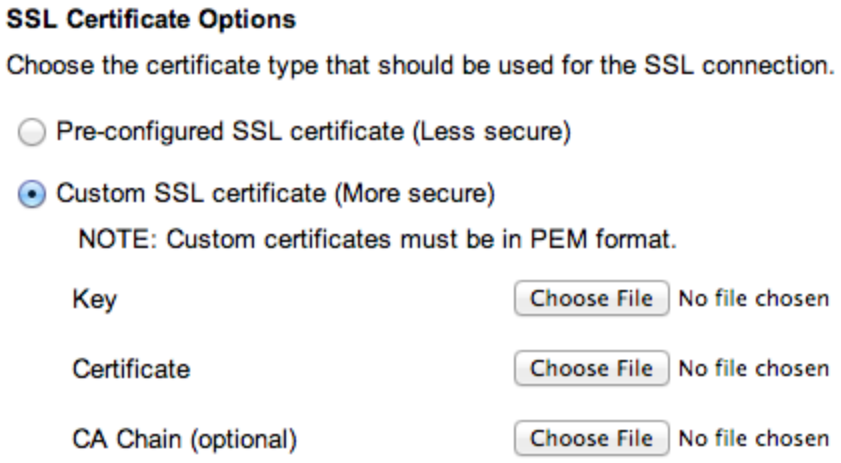
Port

By default, the port is set to 9051, which is reserved for ioSphere Management Solution worldwide and should not conflict with any other applications. You may opt to change the port (to 443, for example) depending on your requirements.

In the vCenter plugin, the port is set by default to 443. It is strongly recommended that you do not change this port. If you do change the port you will need to re-register the plugin. You can re-register the vCenter plugin by connecting to the web browser version of your ioSphere Management Solution plugin, clicking **Settings**, then clicking **VCenter Server.** Click Register to save the changes..

SSL Options

You have two options to set the SSL Certificate you will use while running ioSphere Management Solution: a pre-configured certificate or a custom certificate.



If you chose to set a custom SSL certificate, you will need to select the Key and Certificate PEM files.

The CA Chain is required as well. However this Chain may be appended to the Certificate file or uploaded as its own file. If the Chain is in the Certificate you are uploading, no additional file is necessary.

> ⚠ You must ALWAYS upload a CA chain for your server certificate.

Use pre-configured SSL Certificate

Select this option to use the pre-configured certificate provided. This will result in "untrusted certificate" messages. It is less secure than using a certificate made specifically for your server that is signed by a trusted CA.

Use my own custom SSL Certificate

Select this option to update your own Key, Certificate, and CA Chain.

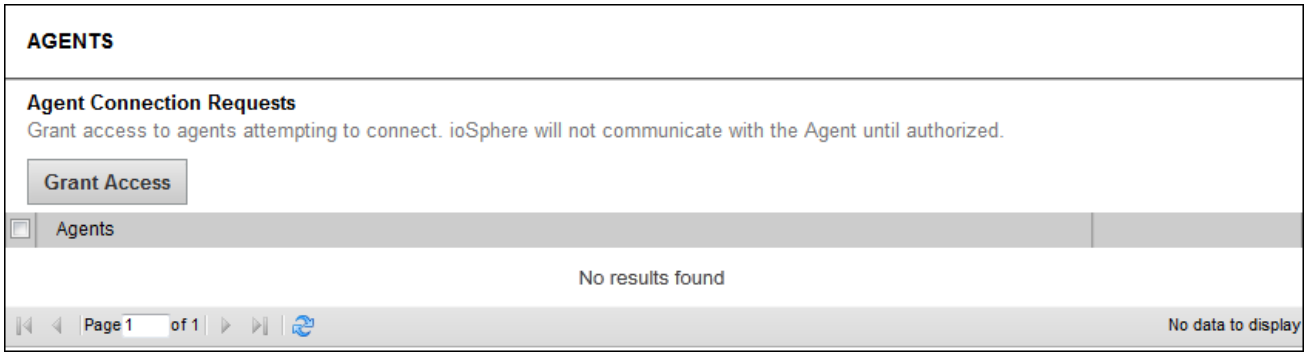
Remote Access Key

To manually configure an Agent to communicate with the Management Server, you can download a remote access key and install it on Agent machines. This may be required in cases where Advertisement has been disabled (either by configuration or due to lack of Zeroconf support), or the network has multiple Management Servers.

Copy the `.key` file to the cache host machine in the following folder:
`C:\ProgramData\fio\agent_keys`

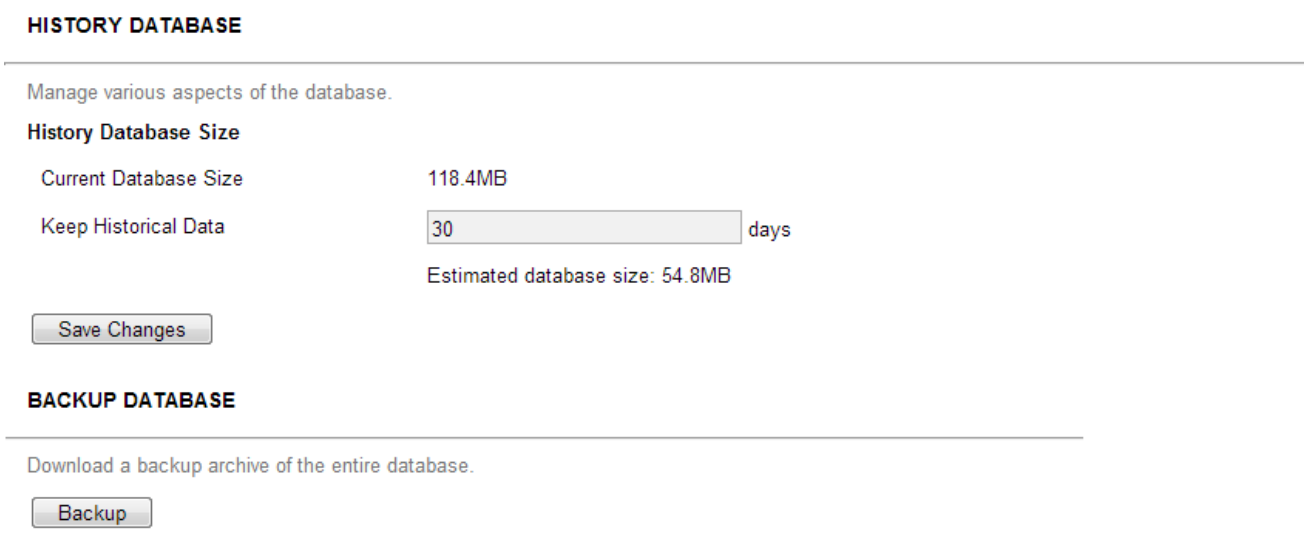
Agents

There are two ways to grant access to Agents: click on the box next the Agent name and then click the Grant Access button, or click the link to the right of each Agent's name. Once an Agent is authorized, it gets its own username and password in the database and has a full access key.



Database

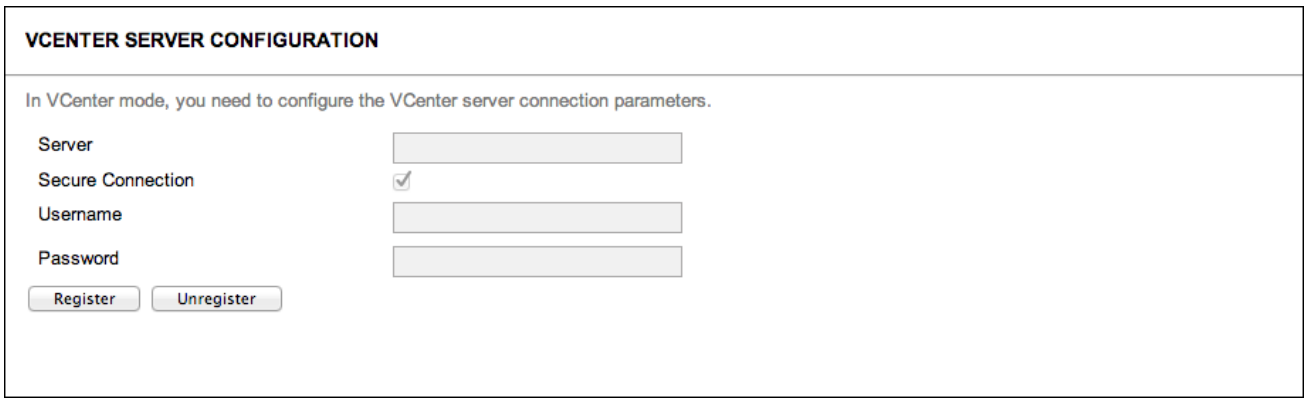
Here you can adjust the size of your history database by specifying how many days to include in the historical data. Click **Save Changes** after you have made any changes.



By default, ioSphere Management Solution keeps the last 30 days of data. This can be modified to store up to two years.

VCenter Server

Use the VCenter screen of the Settings Tab to configure VCenter Server settings.

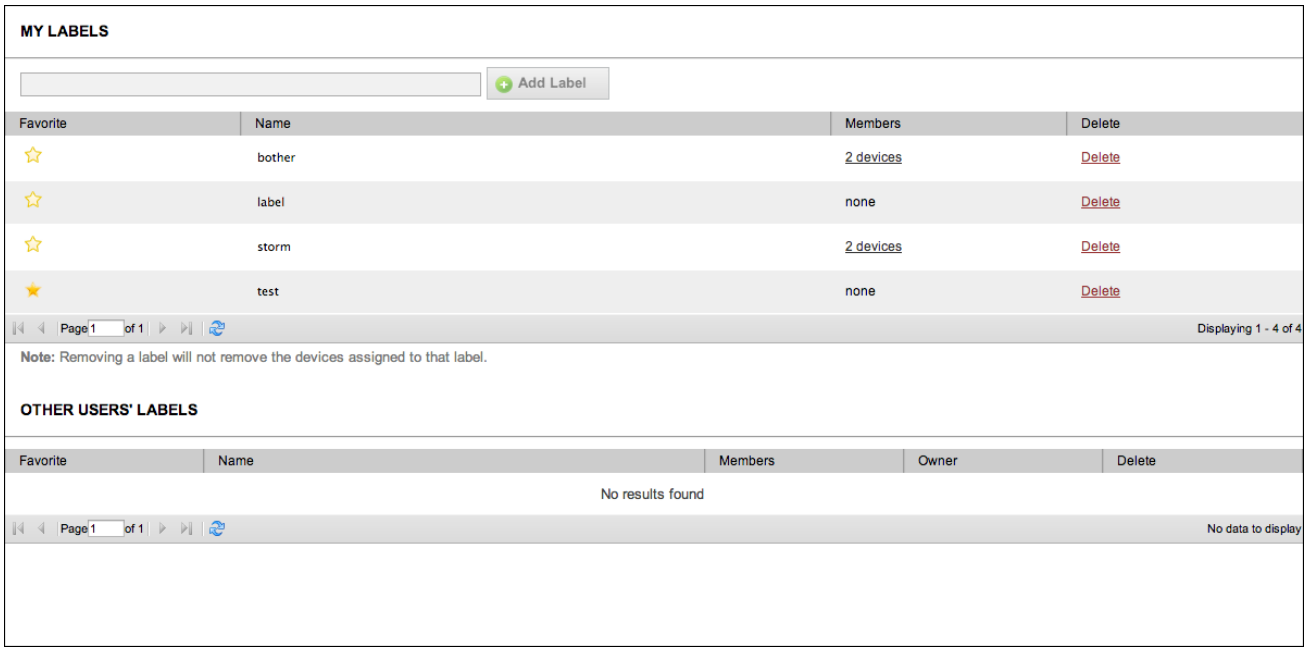


Enter the server information needed to configure the VCenter, then click **Register**.

For more information on using the VMware VCenter Plugin, see VMware vCenter Plugin Installation and Usage on page 66.

Labels

Labels are used to organize your ioMemory devices into categories or groups. Once a label is created on the **Configuration** tab, you can rename it, mark it as a favorite, or delete it on this screen. See Configuration Tab on page 14 for more information about creating labels.



Other Users' Labels: While only an Admin can edit labels created by other users, anyone can add another users' label to their favorites.

Rename

To rename a label, click on the name and enter your changes.

Favorite

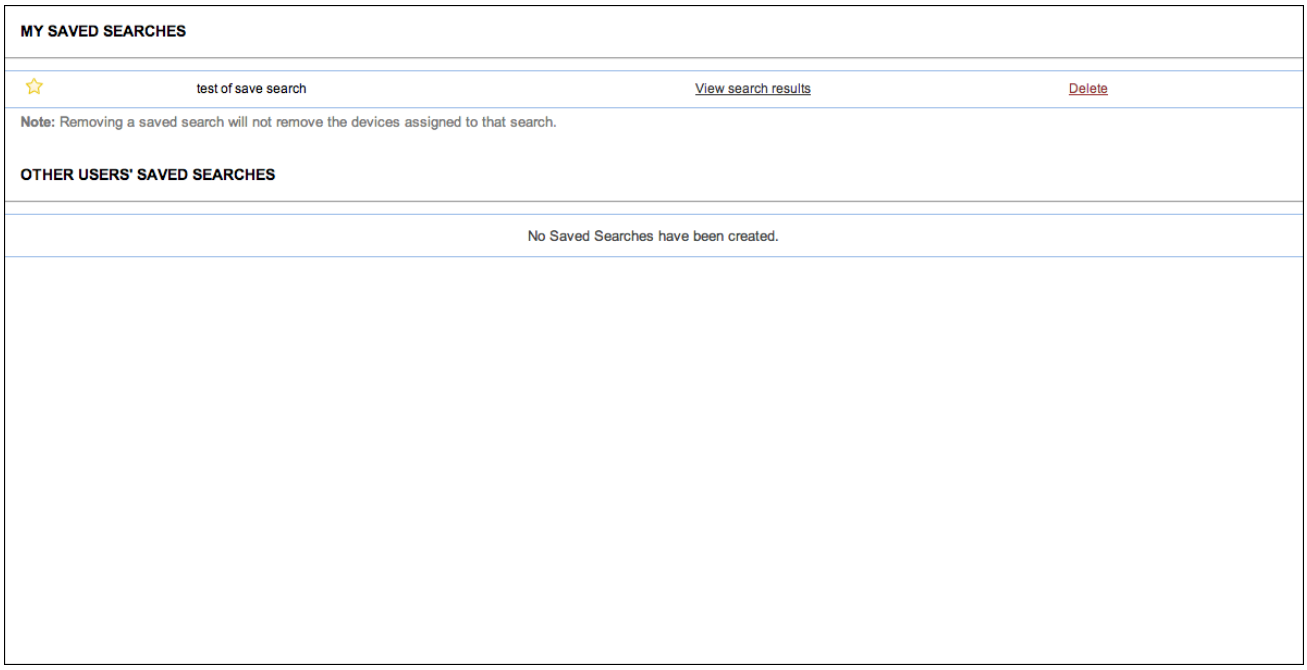
To change the **Favorite** settings of a label, click the star icon next to the label name. A yellow star means it is a favorite, a faded star means it is has not been marked as a favorite.

Delete

To delete a label, click on the **Delete** link next to the name.

Saved Searches

Saved Searches let you easily return to a previous search multiple times. Once a saved search is created on the **Alerts** (see Alerts Tab on page 31)or **Reports** tab (see Reports Tab on page 33), you can come here to rename it, mark it as a favorite, or delete it.



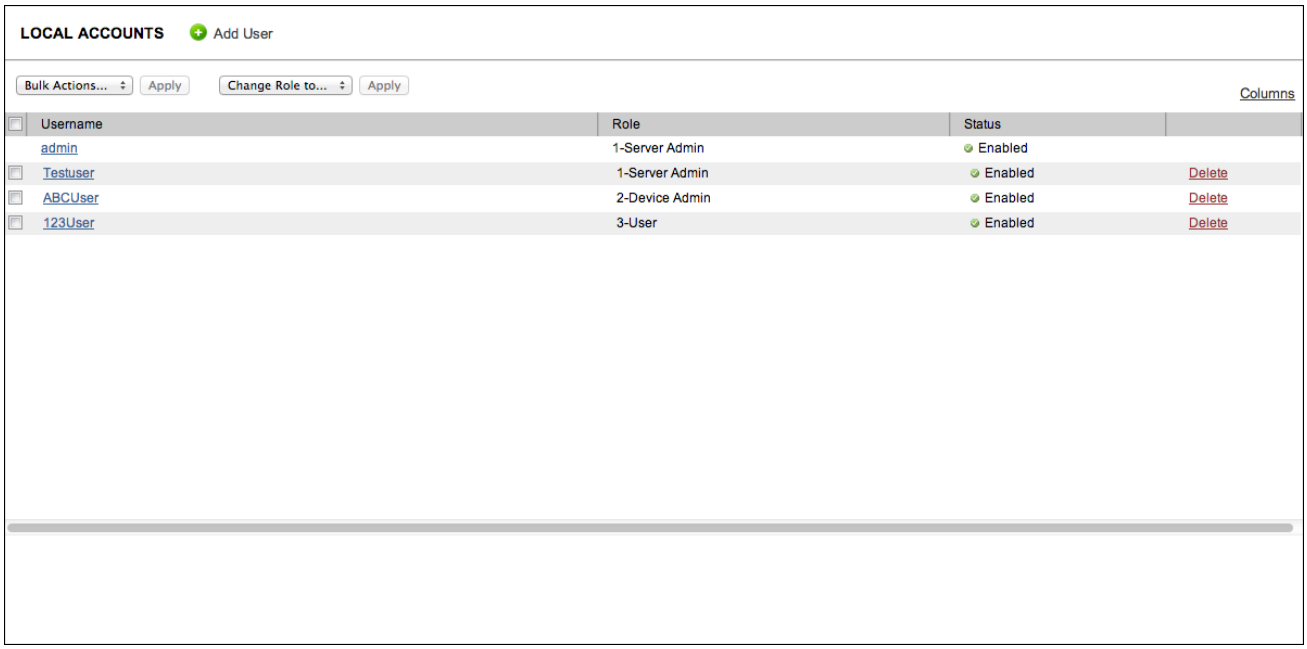
To view the results of a saved search, click the **View Search Results** link. The search results will display in the appropriate tab.

To rename a saved search, click on the name and enter your changes. To change to the Favorite settings of a saved search, click the star icon next to the name. A yellow star means it is a favorite, an empty star means it is not. To delete a saved search, click on the **Delete** link next to the name.

> Other Users' Saved Searches: While only an admin can edit saved searches created by other users, anyone can add another user's saved search to their favorites.

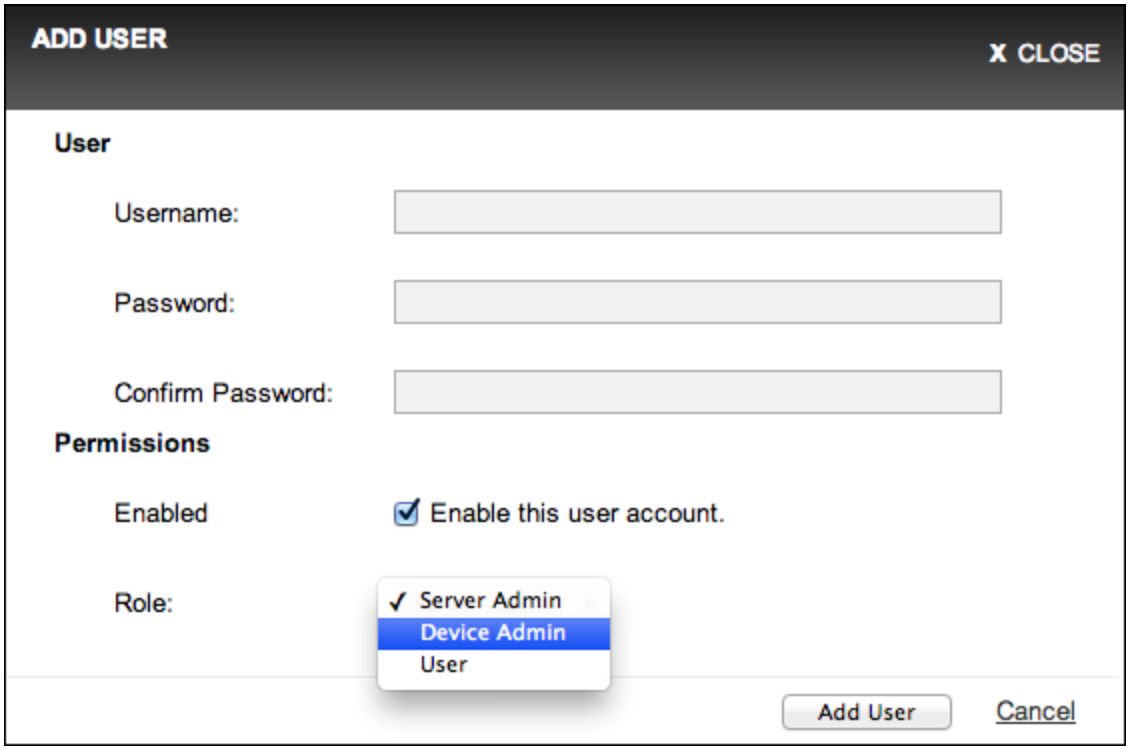
Local Accounts

Here you can create and manage user accounts and user roles.



Add User

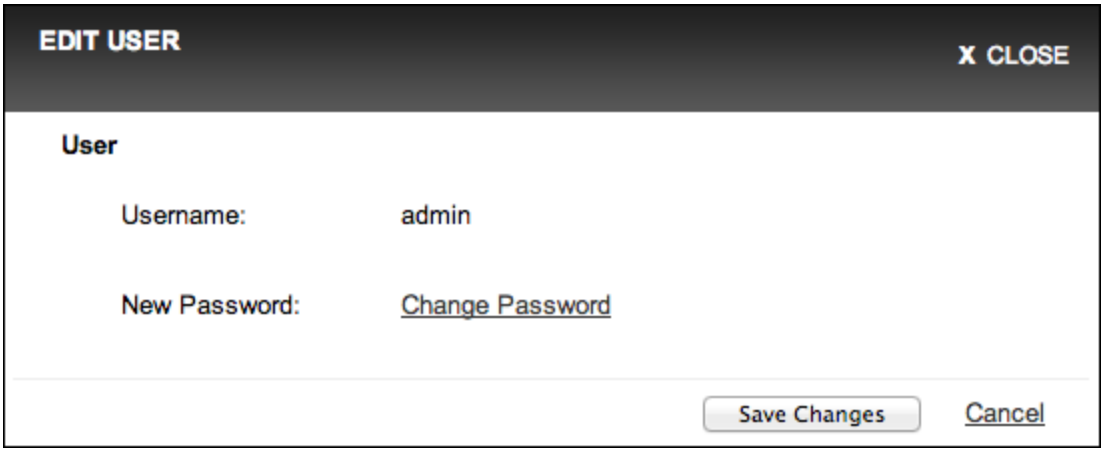
To add a new user, click the **Add User** link. 



Enter a unique username, password, and assign the user's role, which will affect that user's permissions. Click **Add User** to save the user information.

Edit User

To edit a user, click on the username link.



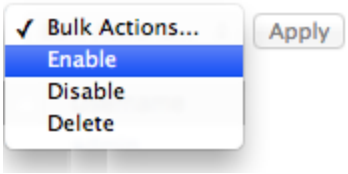
To change a user's password, see Changing Passwords on page 43.

Delete User

To delete a user, click on the **Delete** link given in the **Delete** column.

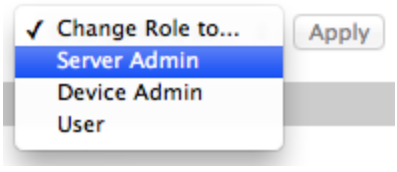
Bulk Actions

Using the checkboxes next to each user, you can select an action to apply to all the selected users. Select **Enable, Disable,** or **Delete.** Then click **Apply.**



Change Role to

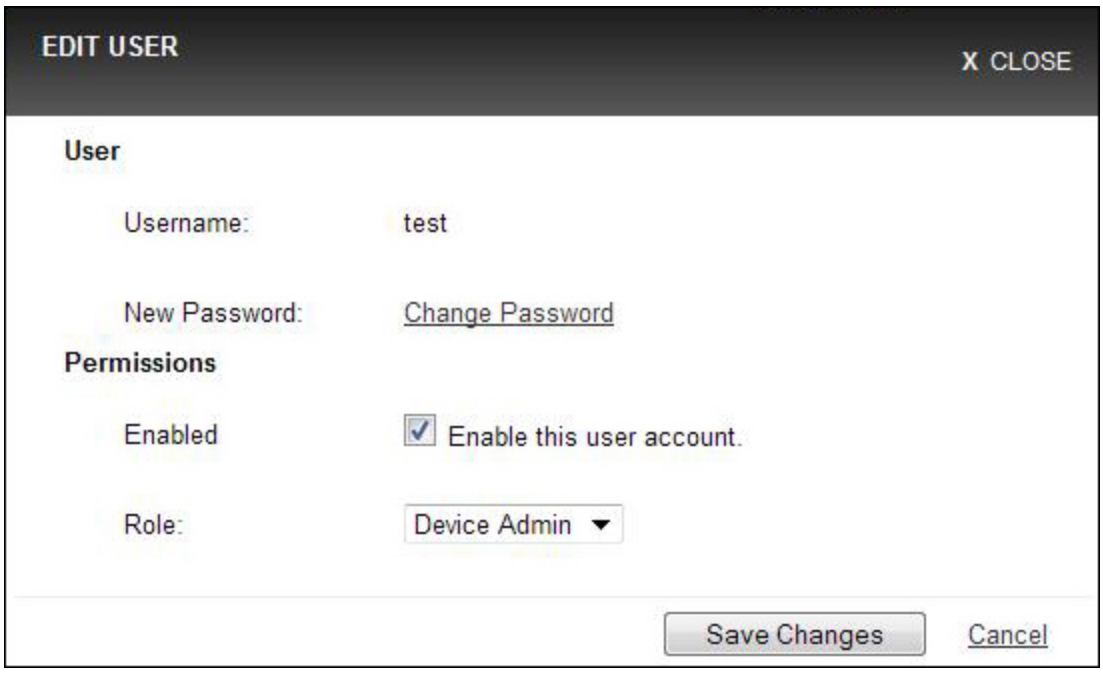
Using the checkboxes next to each user, you can assign a role and grant that role's rights to all selected users. Select the user, then select:



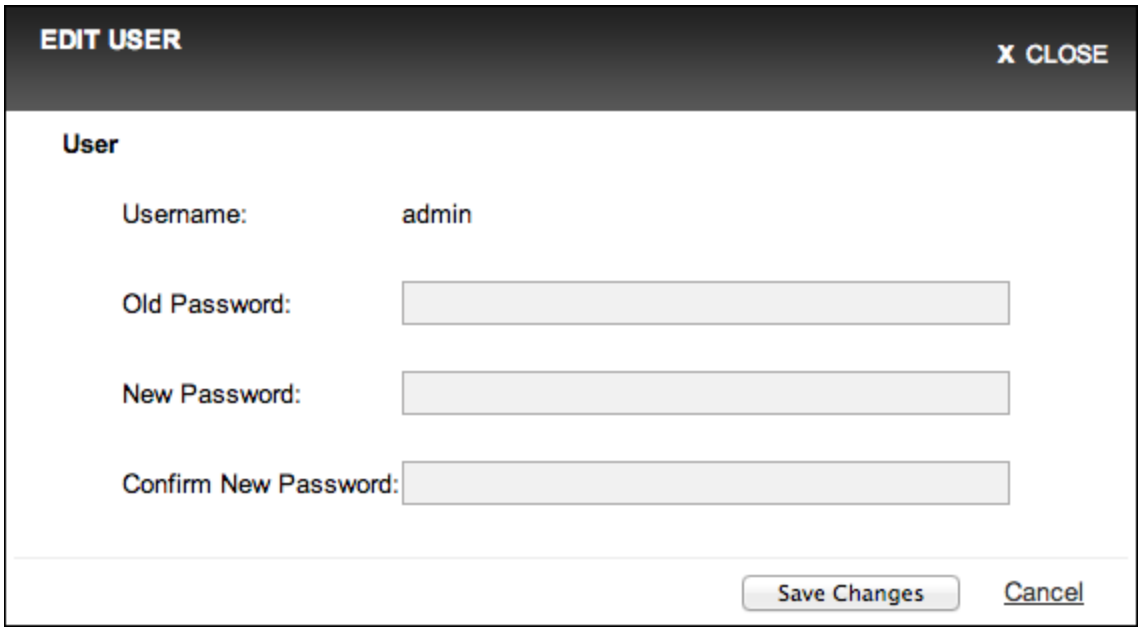
Then click **Apply.**

Changing Passwords

To change a user's password, click a username in the **Local Accounts** screen (located under the **Settings** tab). Either action results in the **Edit User** dialog appearing.



Click **Change Password** to change the user's password.

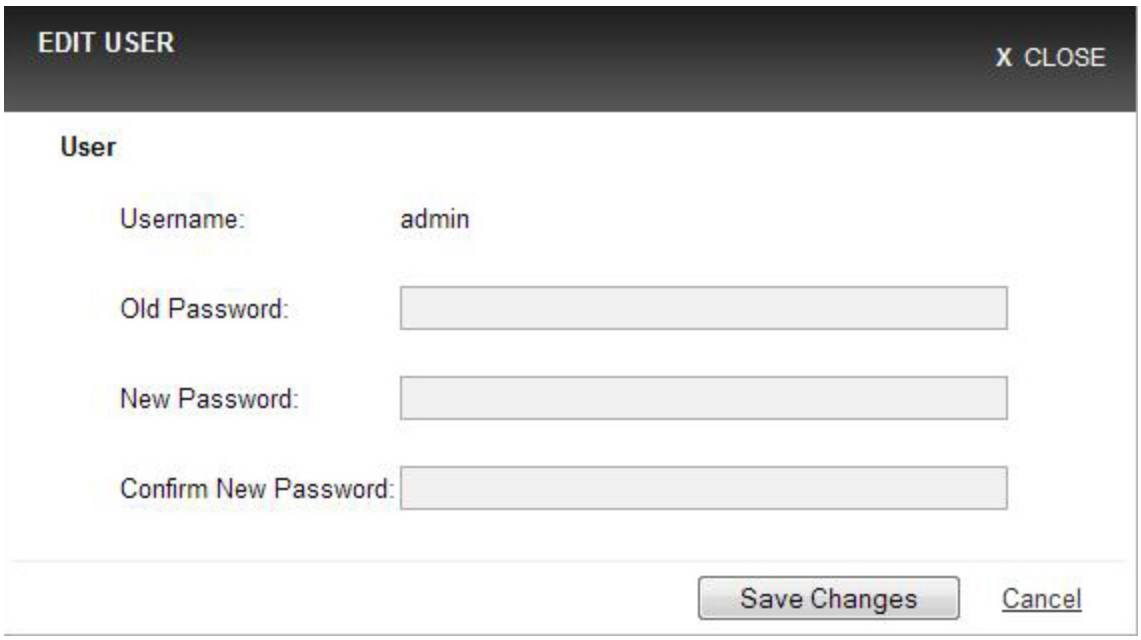


Enter the new password information, then click **Save Changes.**

To change your password while you are logged in, click your user name in the upper right corner of the screen.

Resetting the Admin Password

If you change another user's password, you do not need to enter the old password, and you must be an ioMemory device Admin. However, when you change the admin's account password, you must enter the old password.



If you forget your admin password, you can reset it by running `fio-msrv -w` at the command line.

Example Role Mappings

Here are some examples of role mappings that might be configured for different LDAP directory deployments:

Members of the Administrator group are in role Server Admin

- Set the Search Base DN field to the Administrators group entry. For example: `CN=administrators,OU=groups,DC=example,DC=com`
- Set the Search Filter: `(member=${dn})` " (typical for AD) or `(uniqueMember=${dn})` (typical for non-AD). If you are unsure which attribute holds the members of the group, you can use the search filter `(|(member=${dn})(uniqueMember=${dn}))`
- Set the Scope to Base level
- Set the Role to Server Admin

Members of the Administrator group are in role Server Admin (alternate AD config)
Sometimes in Active Directory, and some other LDAP deployments a user is given group membership by placing an attribute on the user's entry (like `memberOf`). This role mapping will grant the same role as above for these cases:

- Set the Search Base DN field to the user's entry: `${dn}`
- Set the Search Filter: `(memberOf=CN=administrators,OU=groups,DC=example,DC=com)`

- Set the Scope to Base level
- Set the Role to Server Admin

Users who have the title of manager are in the Device Admin role
In this scenario, we use an attribute called title on the user's object to determine whether they are in the Device Admin role.

- Set the Search Base DN field to the user's entry: `${dn}`
- Set the Search Filter: `(title=manager)`
- Set the Scope to Base level
- Set the Role to Device Admin
  Click **Next Step** to test your settings.

Grant a specific user the Server Admin role
You may find situations where a specific user is not in a group, but needs to be in a role. This can be done by creating search criteria which matches true only for that user.

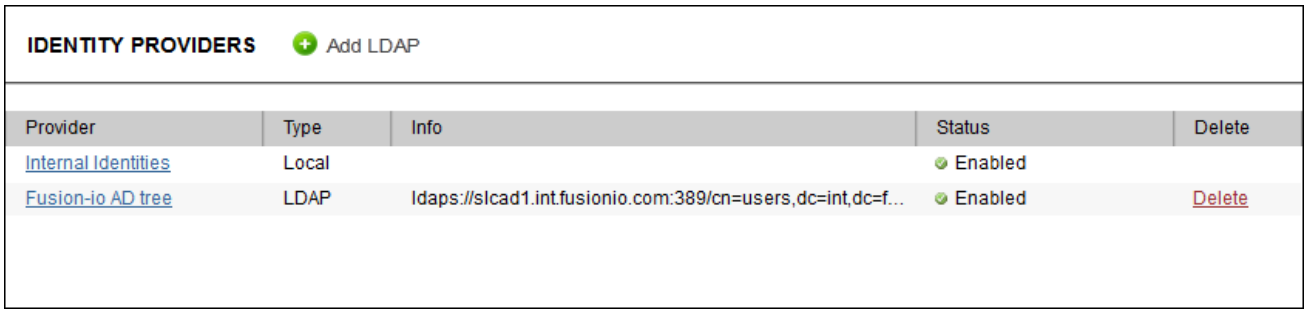
- Set the Search Base DN field to the user's entry: `${dn}`
- Set the Search Filter: `(sAMAccountName=jdoe)`
- Set the Scope to Base level
- Set the Role to Server Admin

Grant the User role to everyone who is able to authenticate
If you want everyone who is able to log in to have at least the User role, you can do this:

- Set the Search Base DN field to the user's entry: `${dn}`
- Set the Search Filter: `(objectclass=*)`
- Set the Scope to Base level
- Set the Role to User

Identity Providers

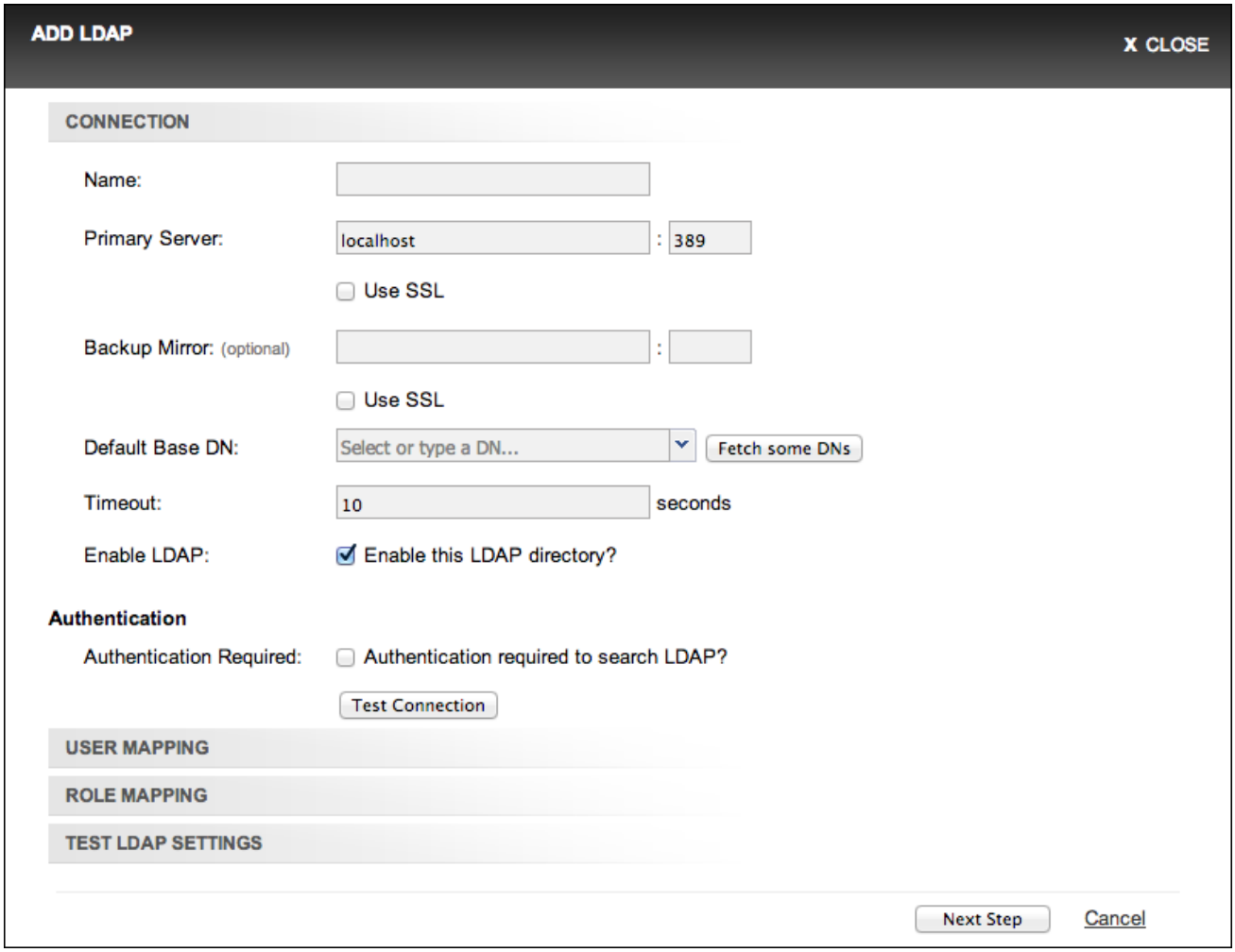
Currently the ioSphere Management Solution only supports LDAP identity providers.



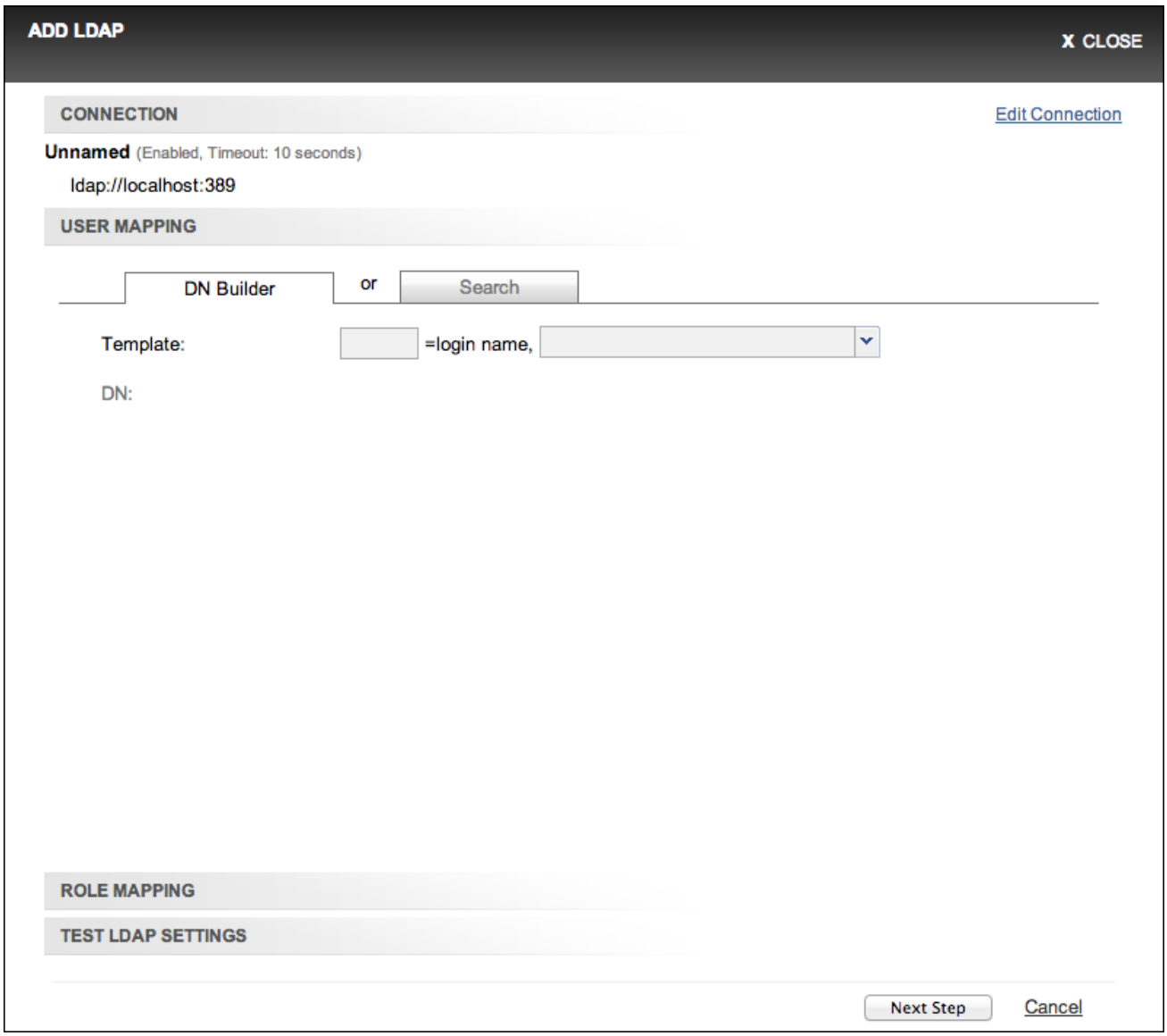
For more information about LDAP settings, refer to Appendix A - Adding and Editing LDAP Providers on page 90

Add LDAP

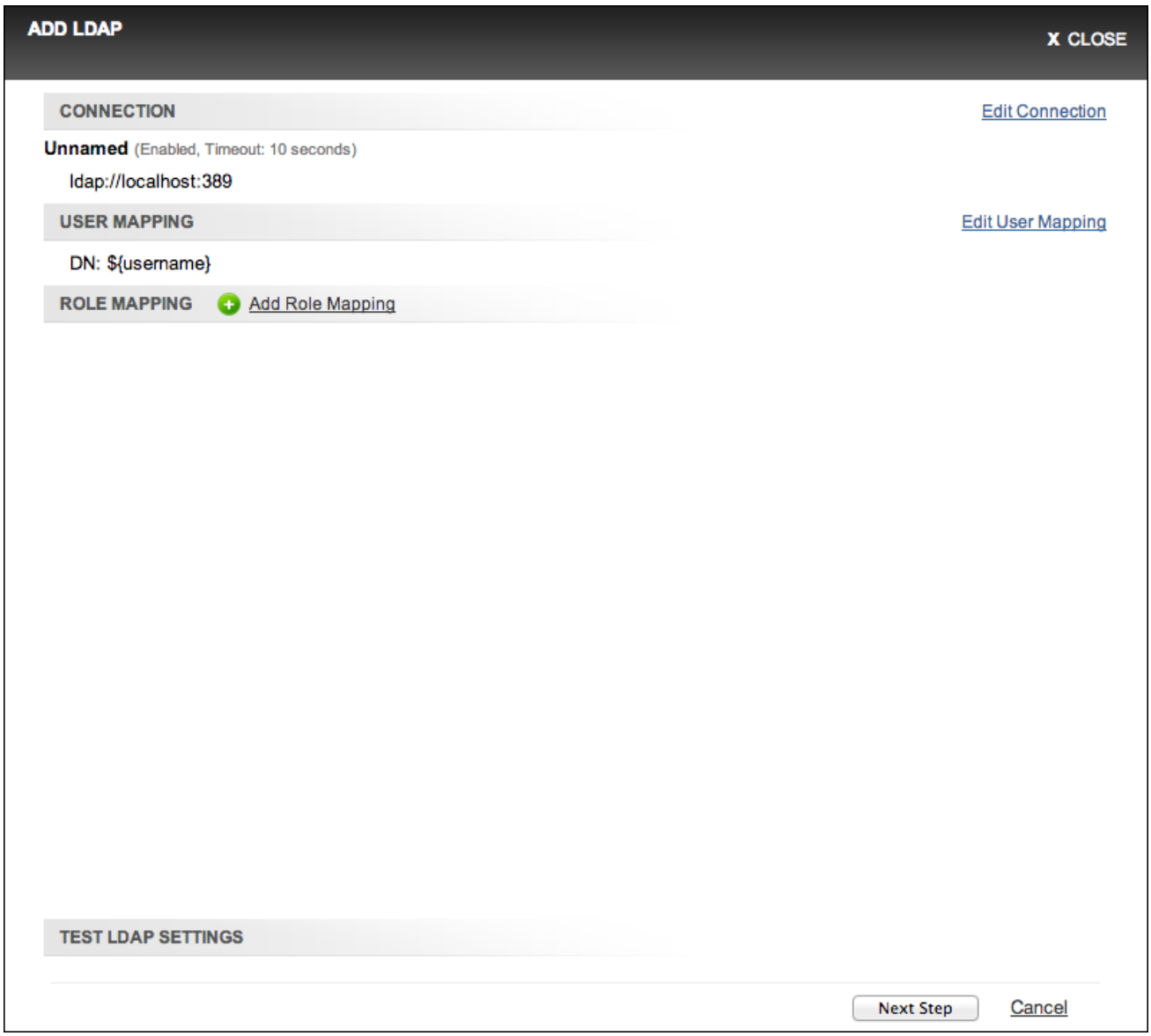
Click the **Add LDAP** Add LDAP link to open the Add **LDAP** wizard, where you can configure the LDAP connection, User **Mapping, Role Mapping**, test LDAP settings, and add additional LDAP configurations.



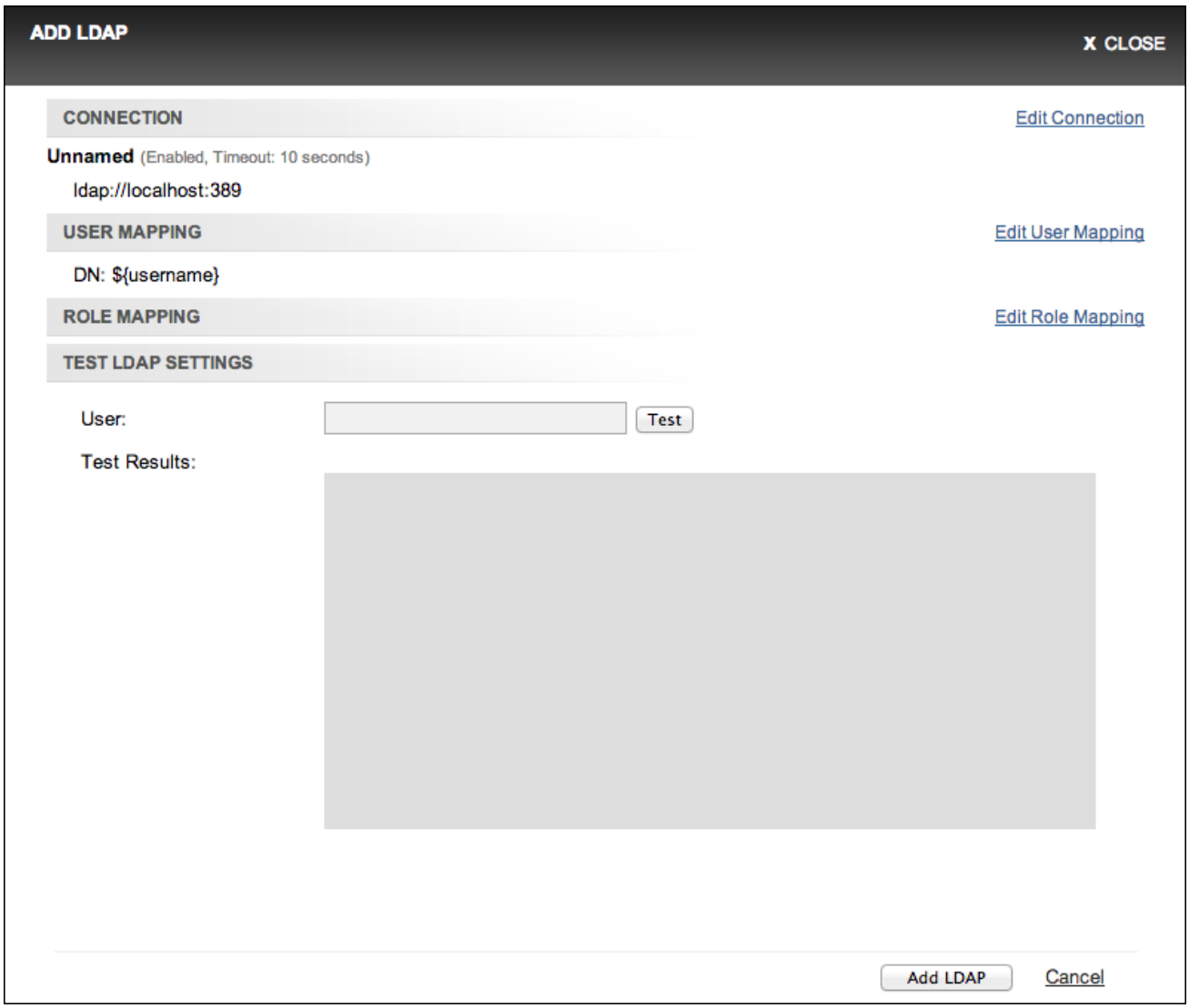
Enter the LDAP connection information, then click **Next Step.**



Enter the LDAP User Mapping information, then click **Next Step.**



Enter the LDAP Role Mapping information, then click **Next Step.**



Enter the Test LDAP Settings information, then click **Test** to test the LDAP setup. When the setup is complete and functional, click **Add LDAP.**

Edit LDAP

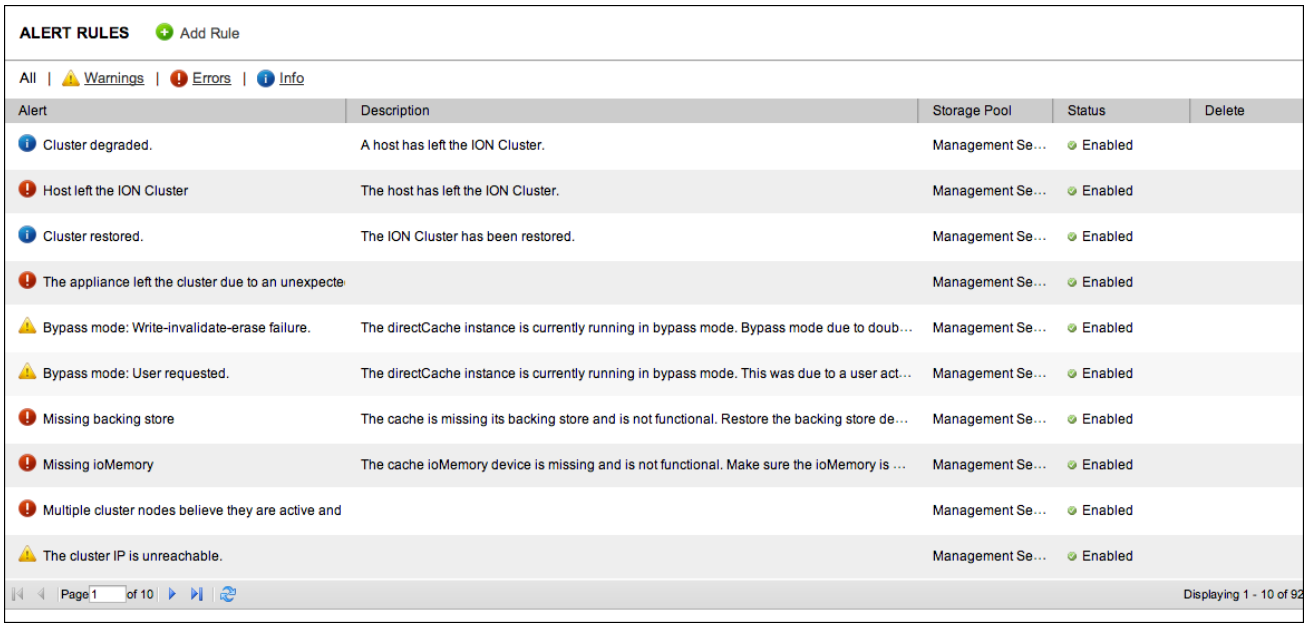
To edit an LDAP entry, click on the **Provider** link.

Delete LDAP

To delete an LDAP entry, click on the **Delete** link next to the provider.

Rules

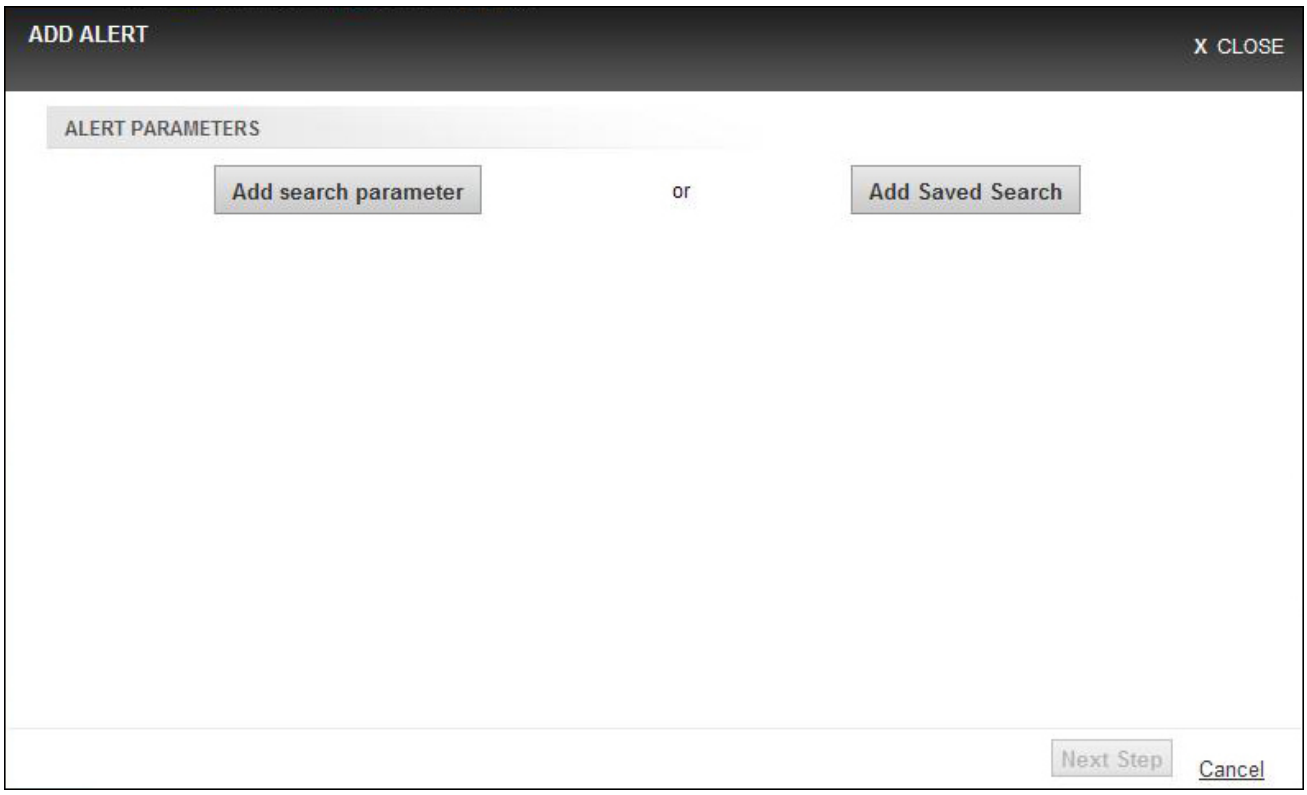
In this screen, you can create, edit, and review rules that generate alerts.



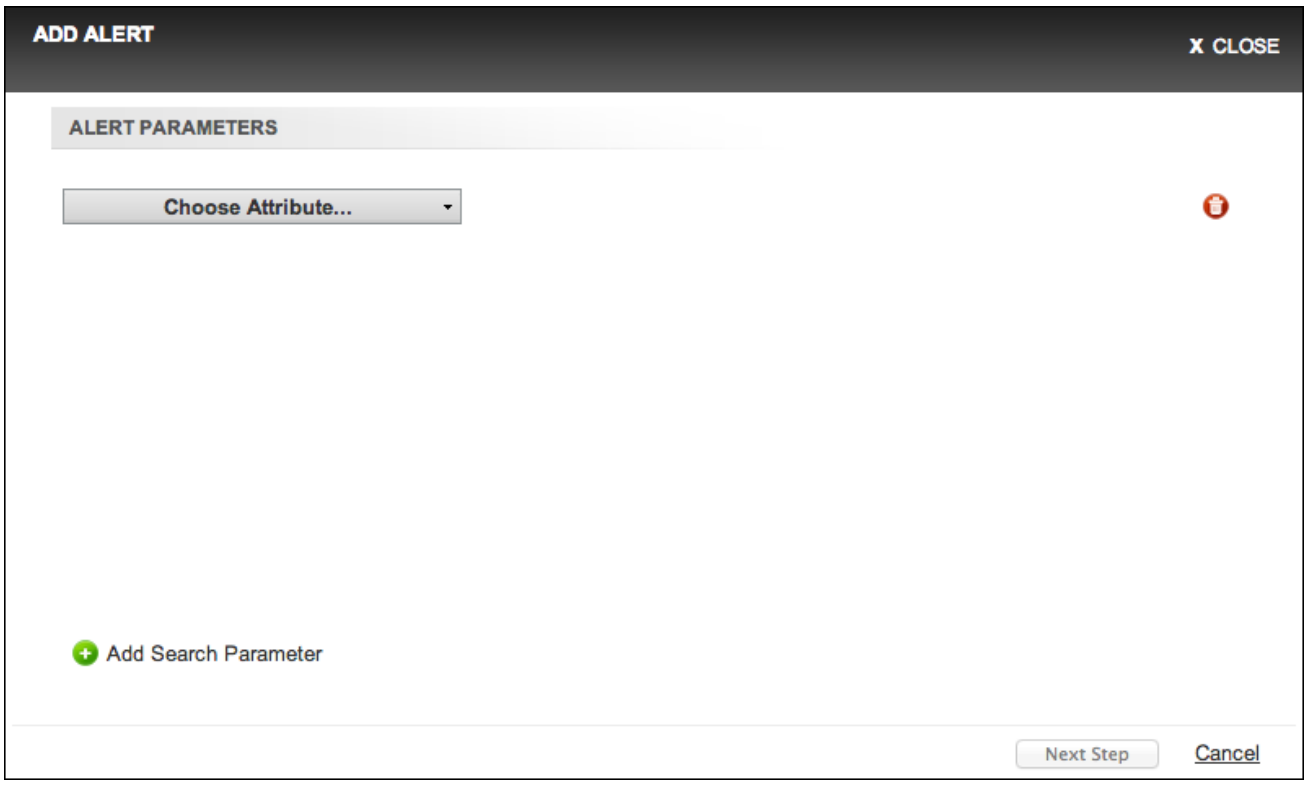
Add Rule

Click the **Add Rule** 

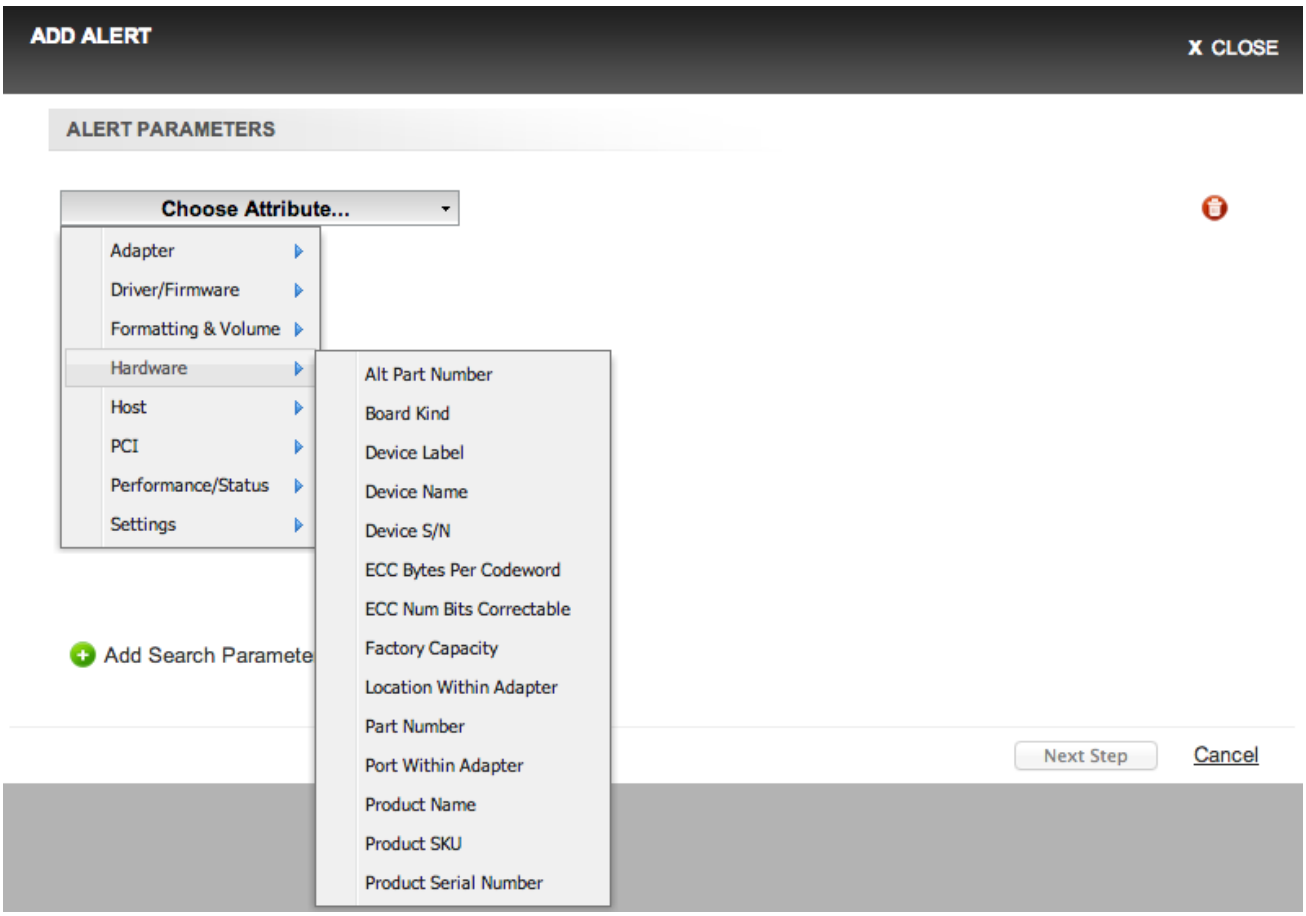
link to open the **Add Alert** dialog, where you can create a custom filter that will trigger an alert.



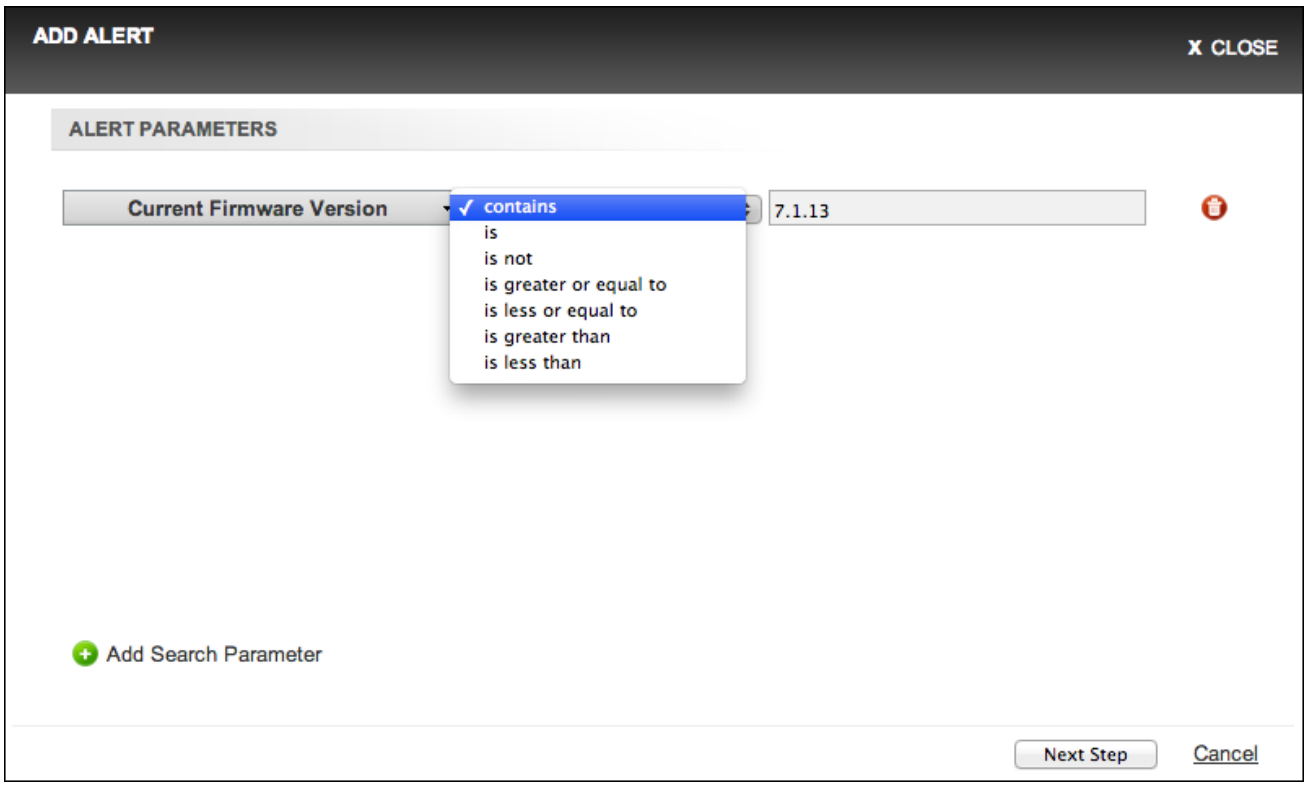
In the **Add Alert** dialog, click the **Add search parameter** button or (if you have one or more saved searches) the **Add Saved Search** button. When you add a saved search, its parameters are automatically added to the new Alert.



From the **Choose Attribute** drop down list, select the attribute you wish to add to the rule.



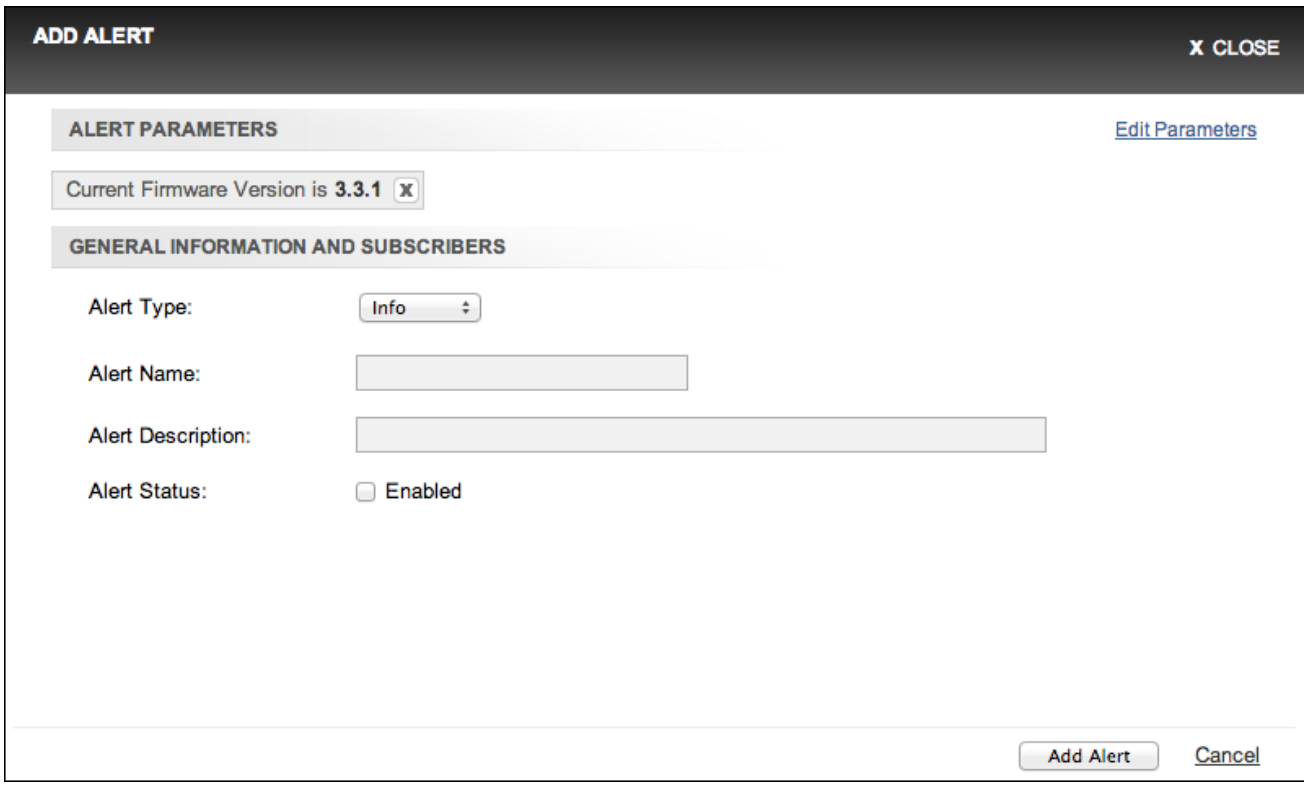
Enter the Rule parameters for the chosen attribute.



To add additional search attributes to the rule, click the **Add Search Parameters** Add Search Parameter link.

To delete an attribute, click the delete icon next to the attribute.

Click the **Next Step** button to continue.



Add additional information about the alert here, including **Alert Type, Alert Name, Alert Description**, and **Alert Status**. You can also click the **Edit Parameters** link to go back and add, remove, or change parameters. Click the **Add Alert** button to add the alert, or the **Cancel** link to discard the alert.

Edit Rule

To edit custom rule entry, click on the **Rule** link.

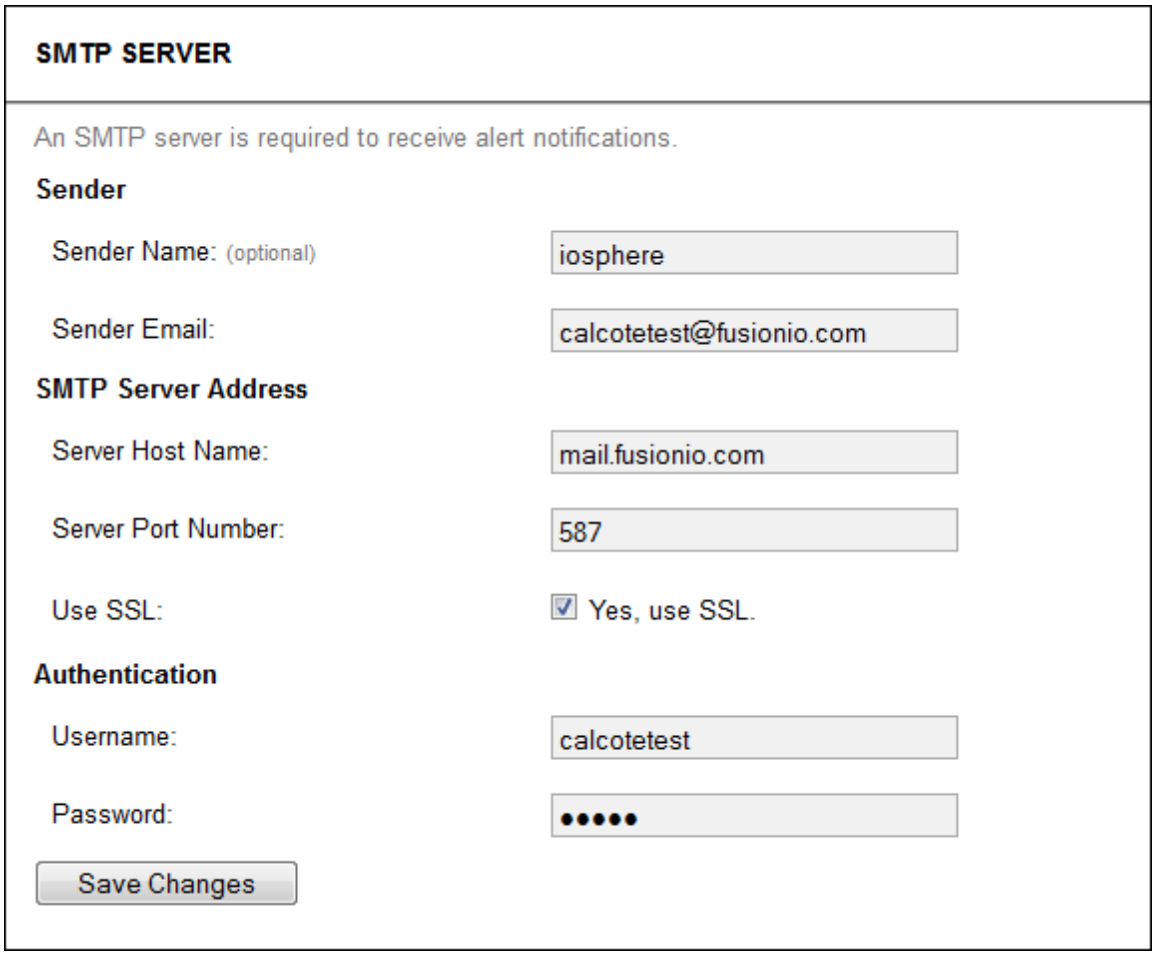
Delete Rule

To delete a custom rule entry, click on the **Delete** link next to the **Rule.**

> Only custom rules can be modified and deleted.

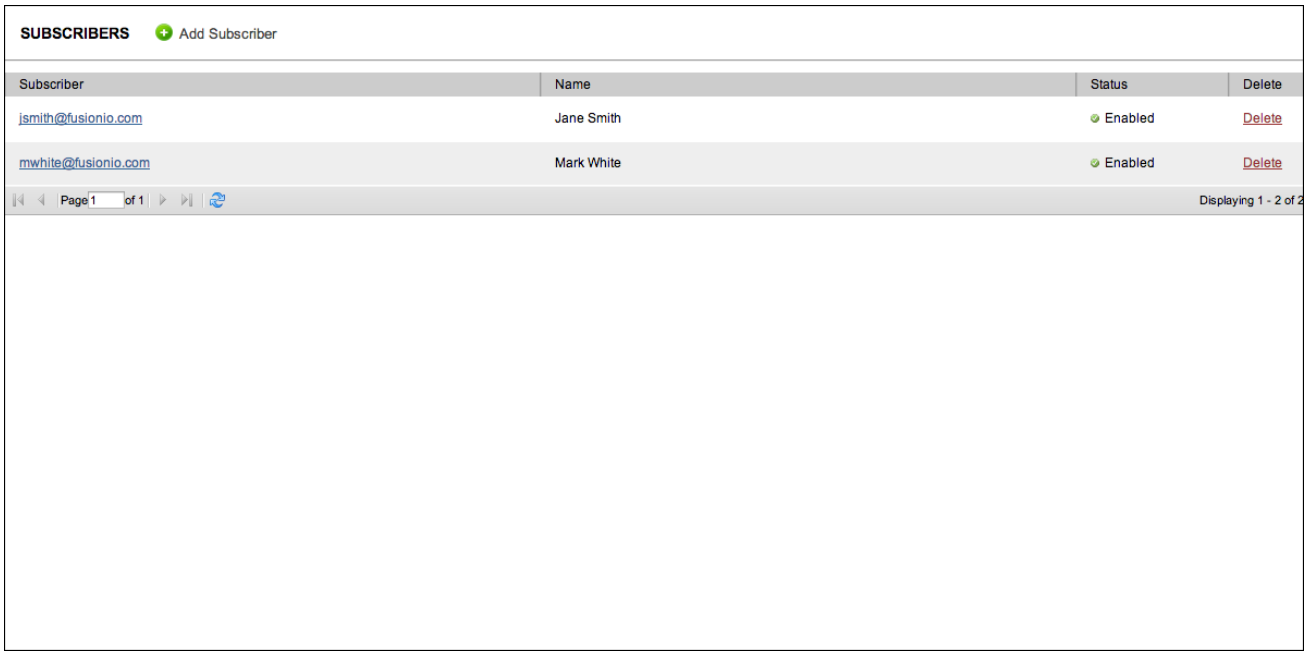
SMTP Server

In order for the ioSphere Management Solution to send alert emails, you must first configure the SMTP server settings here. Once you enter in the correct parameters, click the **Save Changes** button to save the SMTP settings.



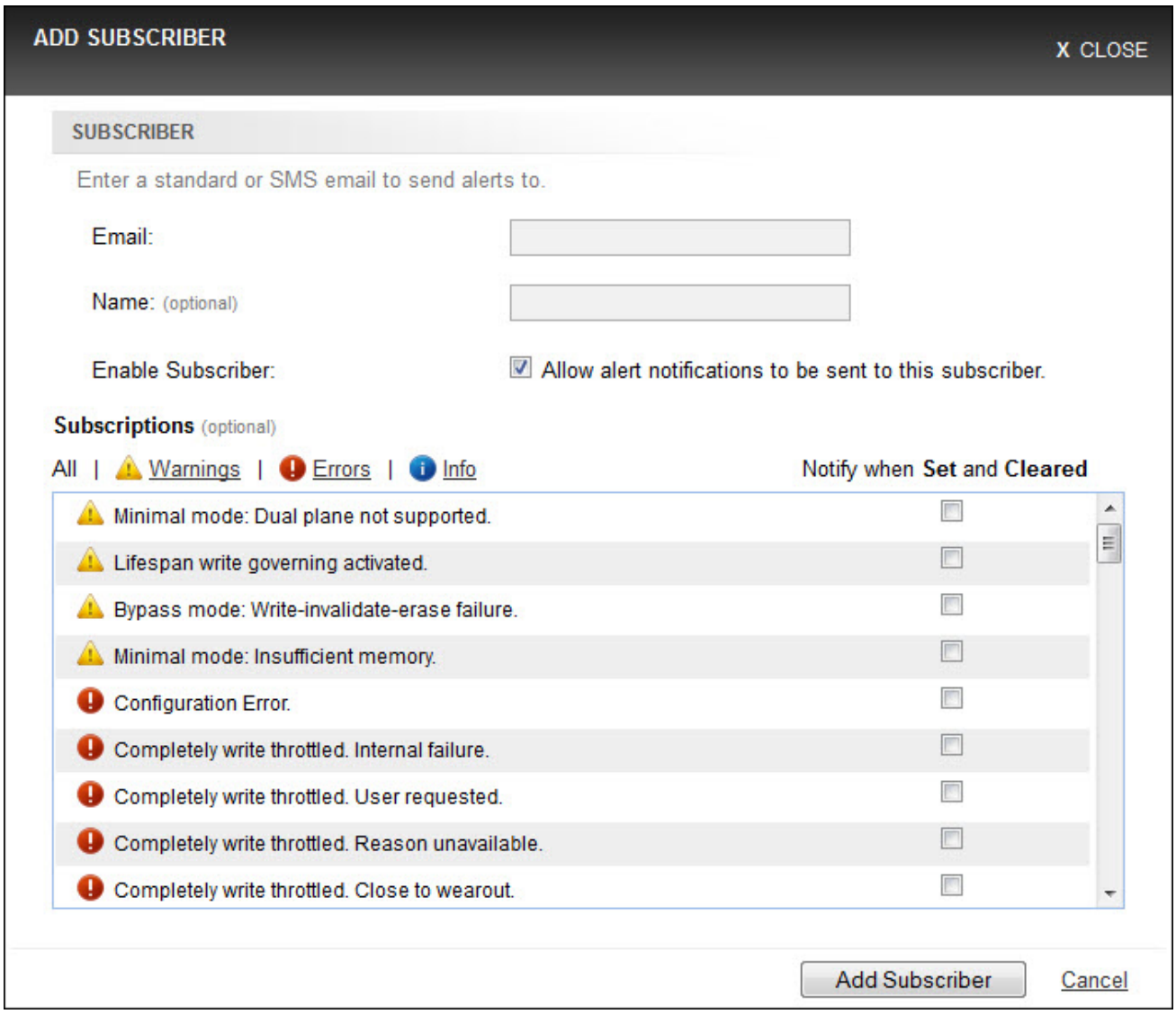
Subscribers

The ioSphere Management Solution Management Solution can send email alerts to standard or SMS email addresses. After configuring the SMTP server settings, you can create subscribers and assign them to receive specific alerts.



Add Subscriber

Click the **Add Subscriber** link to open the **Add Subscriber** dialog, where you can enter a standard or SMS email address and assign the subscriber to be notified when an alert is Set or Cleared.



Edit Subscriber

To edit a subscriber, click on the subscriber email address link.

Delete Subscriber

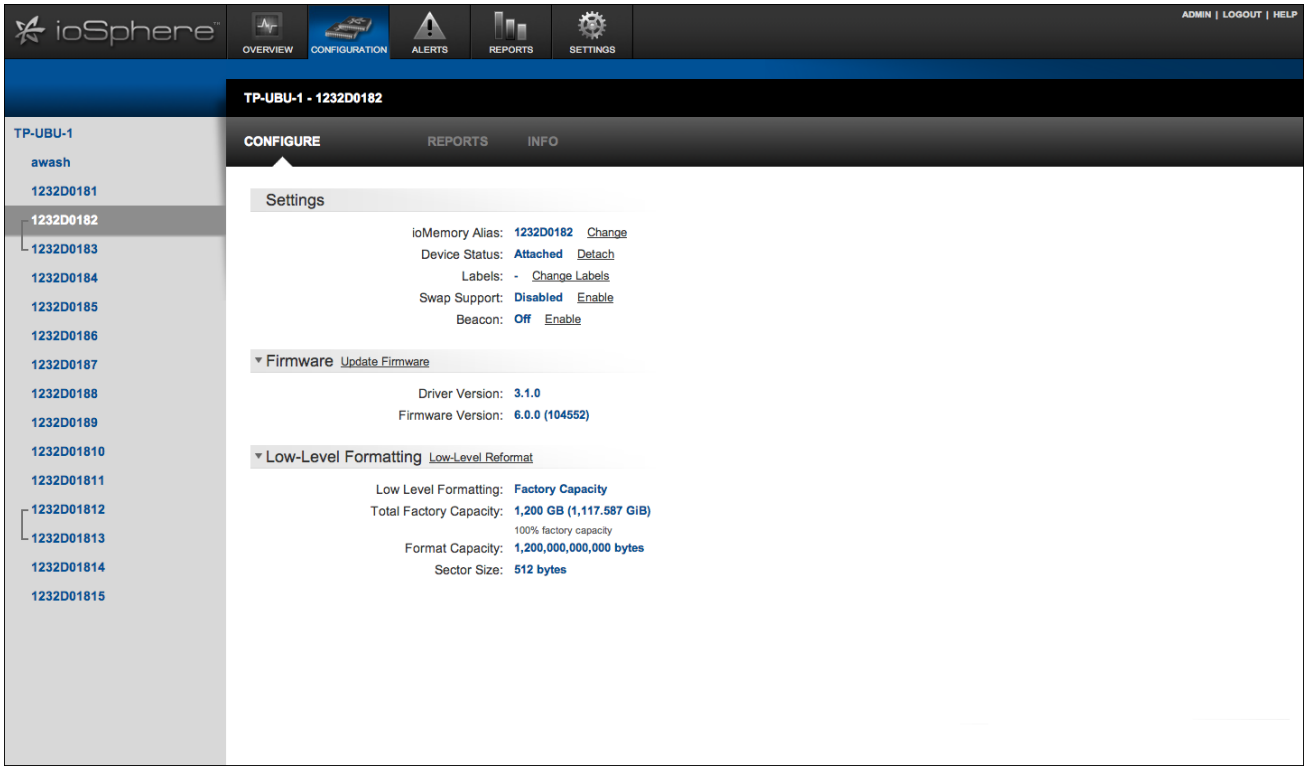
To delete a subscriber, click on the **Delete** link next to the subscriber.

> **Email To SMS:** Most mobile carriers offer free Email To SMS gateways which can be used to forward simple text emails to a mobile phones. Check with your provider to determine your Email to SMS email address.

Device Page

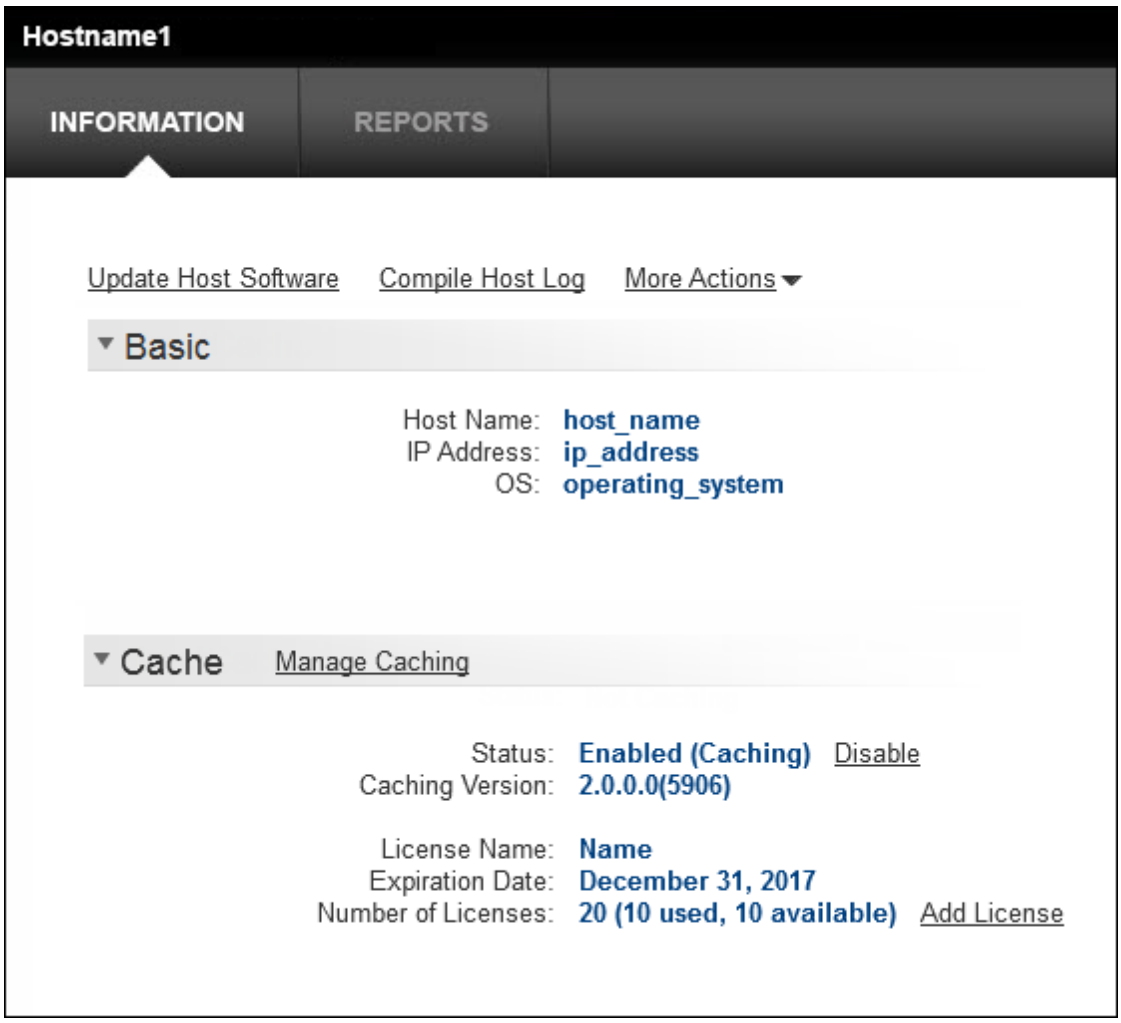
The **Device** page provides a way to monitor and configure devices controlled by a single Agent service. There are several ways to navigate to the **Device** page:

- Click a hostname link from any table in ioSphere Management Solution
- Click an ioMemory device link name link from any table in ioSphere Management Solution.



When the **Device Page** displays, information pertaining to the server running the Agent service appears in the upper left-hand corner. A left sidebar lists each ioMemory device installed in that server, and a tab panel on the right monitors and lets you perform configuration tasks.

The **Configure** and **Info** tabs include Host Log Report link found at the top of the window.



Click this link to compile and download a host log for the selected device, when instructed to do so byFusion-io Customer Support.

Configure Device Tab

Here you can edit the following settings:

- ioMemory device Alias (Name, by default the serial number is used)
- Device Status (Attach/Detach)
  The **Attach Device** operation creates a link so the ioMemory device interacts with the operating system. In most cases, the operating system driver automatically attaches the installed ioMemory device(s) at boot time, so you only need to use Attach Device when you manually detach an ioMemory device (such as to perform a low-level format).

  Detach Device disconnects your ioMemory device from the operating system. Once detached, the device is not accessible to users or applications. (You need to use Attach Device to make it accessible.) You should only need to detach an ioMemory device to perform a low-level format or a firmware upgrade.
- Labels/Change Labels link
- Swap Support (Enable/Disable)
  ioMemory device can be used as swap space. By enabling swap here, you are enabling the device for use as a swap space. This allows the driver to preallocate the memory needed for the device to be used as swap.

> ⚠ When you select Enable here, the device is ready to be used as swap space, but your operating system still needs to be configured to use the device as swap. You will need to configure the system to use the device in that manner.

> ⚠ You must have 400MB of free RAM per 80GB of ioMemory device capacity (formatted to 4KB block size) to enable an ioMemory device for use as swap. Enabling swap without sufficient RAM will result in the loss of user processes and system instability.

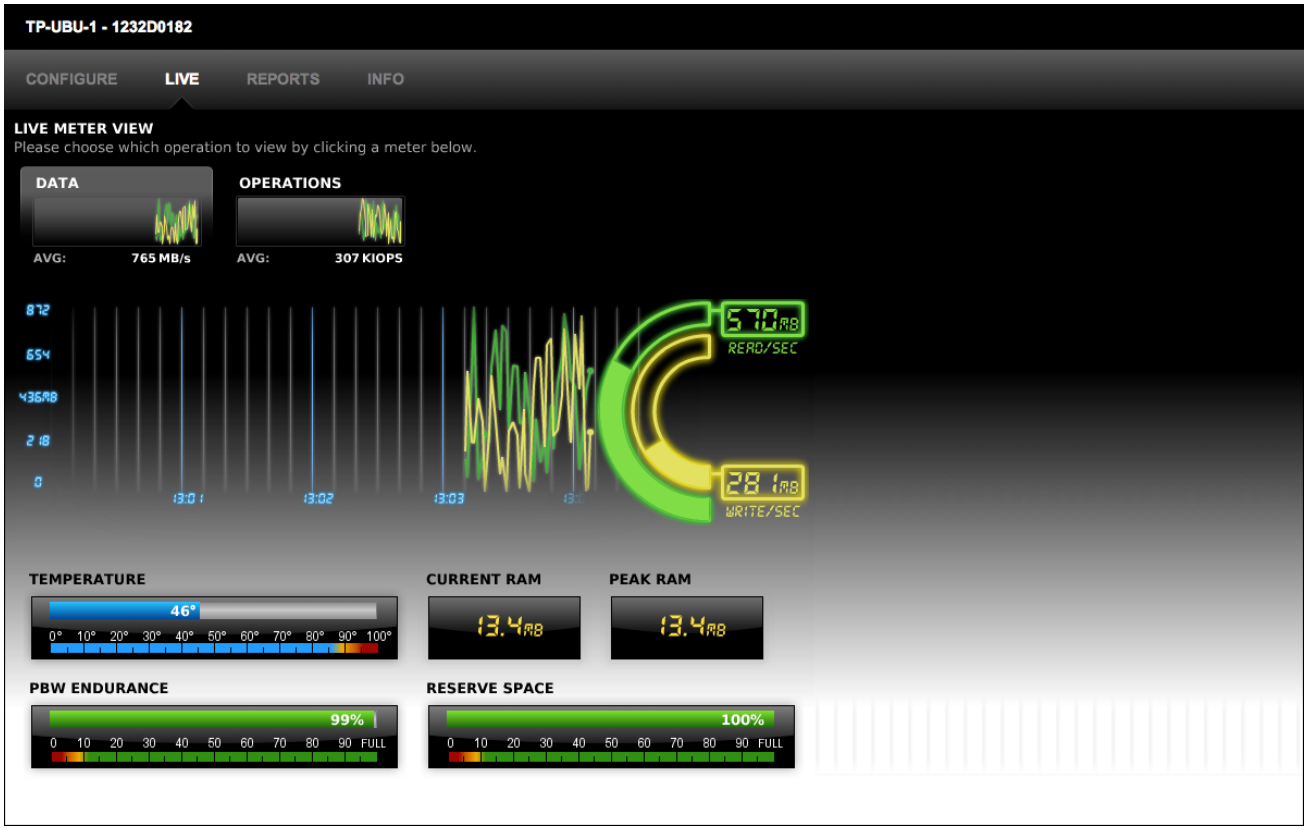
- Beacon (Enable/Disable)
  The **Beacon** feature causes the selected ioMemory device's LEDs to blink, making it easier to find among several devices.

You can also update firmware (see Appendix B - Software Updates on page 99 for more information) and perform a low-level reformat.

Live Device Tab

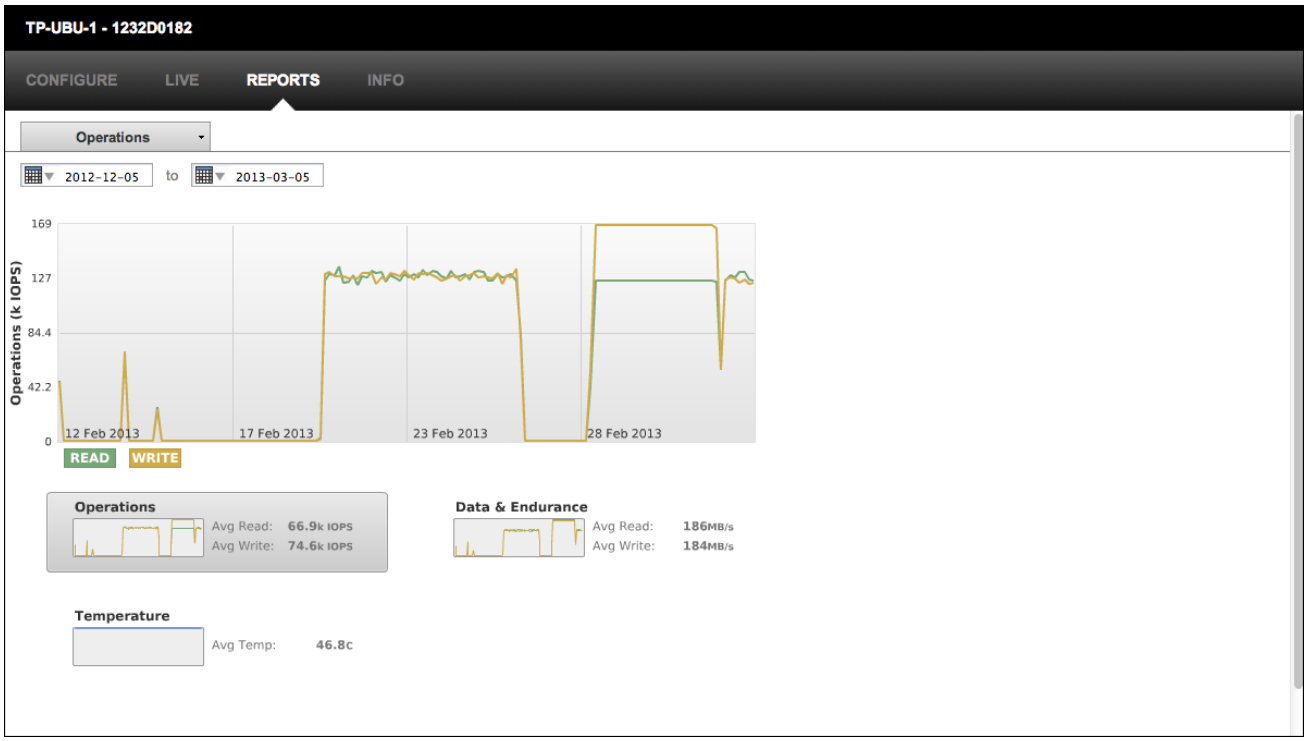
The **Live** tab lets you monitor important information for one or several ioMemory devices in real time. The **Live** tab displays **IOPS Read/Write** when **Operations** is selected, **MB/Second** when **Data** is selected, and **Temperature** and **Reserve Space.** Select **Data** or **Operations** using the large button above the graph.

The **Live** tab also displays information for **PBW Endurance.**



Reports Device Tab

The **Reports** tab shows from three to five history graphs for a single ioMemory device: **Operations, Data & Endurance, Temperature, Cache Hit Requests,** and **Cache Latency** (the later two graphs are available only when the device is being used as a cache).



Enter start and end dates in the drop down menus above the graph to show data for different dates.

To see larger versions of the available graphs, click on the smaller graph of the data you wish to view.

Operations Graph

Click the small Operations graph to display information about **Operations (IOPS).** The selected button will be highlighted. **Operations** displays the average **Read** and **Write** hits as the amount of IOPS.

Data & Endurance Graph

Data & Endurance shows you the **Average Read** and **Write** hits in Bytes per second.

Each ioMemory device has a PBW Rating (Petabytes Written Rating). The device's warranty is based on this PBW Rating.

When **Data & Endurance** is selected, the following message appears above the graph: "Future performance based on this date range suggests this device's X PBW Endurance will last for more than X years."

If the date range selected is not an accurate representation of the anticipated future performance of the ioMemory device, you can modify the date range to include data that better represents future behavior and thereby include a better prediction of the warranty expiration.

Temperature Graph

This data shows you how temperature changes over time (over days or throughout a day).

Cache Hit Requests Graph

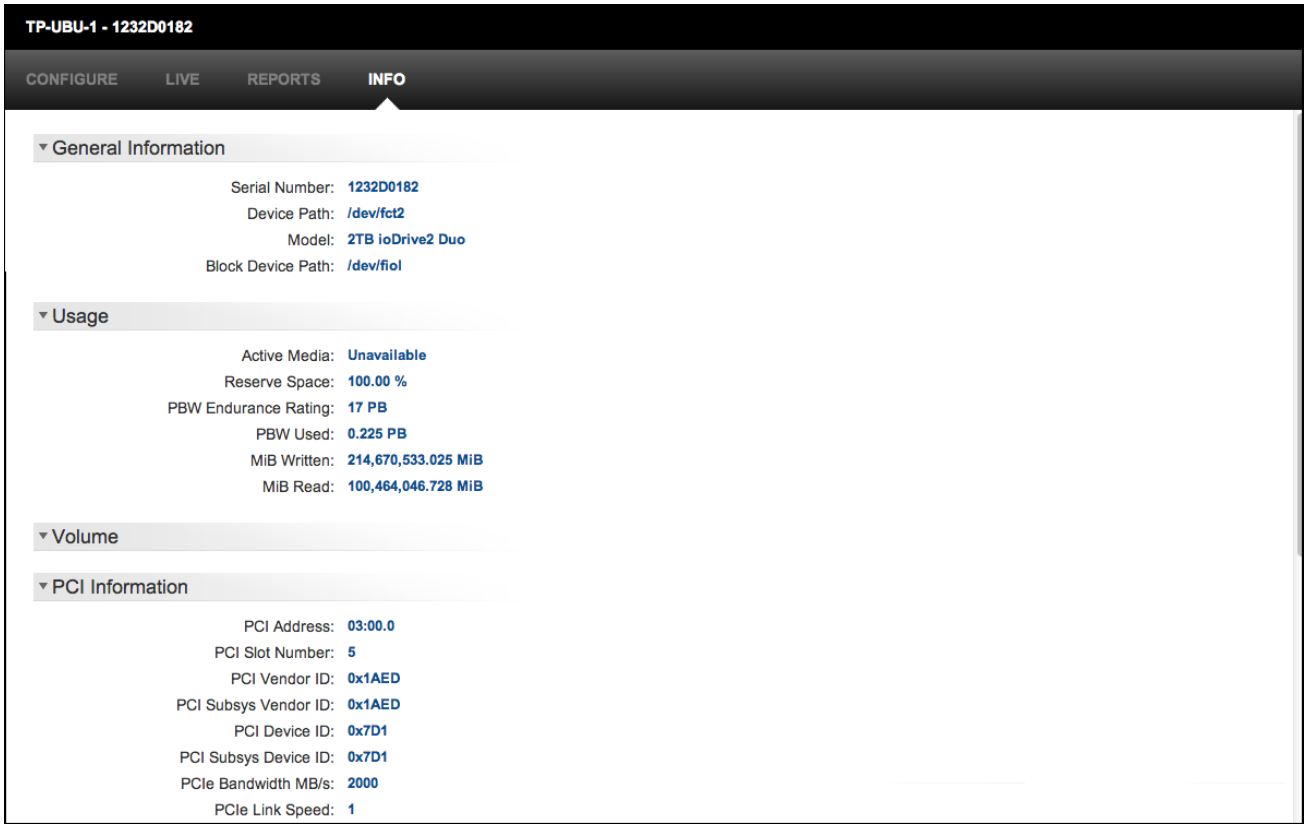
This charts the percent of read requests that were serviced from the cache.

Cache Latency Graph

The graph shows **Cache Latency** for **Read Hits, Read Misses,** and **Read Average.**

Info Device Tab

The **Info** tab provides details about a single ioMemory device.



As shown in the following closeup of the **Info** tab screen, this tab also shows detailed **Adapter Information.**

Adapter Information

Adapter Board Kind:	**Dual**
External Power:	**Not Connected**
Adapter S/N:	**1232D018A1**
Adapter PCI Slot Power:	**25 W**
Location Within Adapter:	**Not calculated - Sim Laziness (0)**
PCIe Bus voltage:	**Avg 12.22 V, Min 12.08 V, Max 12.31 V**
Adapter PCIe Link Width:	**4 lanes**
PCIe Bus current:	**Avg 0.76 A, Max 1.99 A**
Adapter PCIe Link Speed:	**5.0 Gbits/sec/lane**
PCIe Bus power:	**Avg 9.21 W, Max 24 W**
Adapter PCIe Bandwidth:	**2,000 MB/s**
PCIe Power Limit:	**24.75 W**

VMware vCenter Plugin Installation and Usage

The ioSphere Management Solution VMware vCenter plugin can easily manage ioMemory devices located on multiple ESX hosts from within VMware's vSphere client. A vCenter plugin is essentially a web service that runs on a virtual machine in the vCenter environment. This web server communicates with ioMemory devices in the vCenter environment and displays information on a tab in the vSphere Client interface. Fusion-io's ioSphere Management Solution VMware vCenter plugin is a VMware Studio image.

This section describes how to install the ioSphere Management Solution VMware vCenter plugin (hereafter referred to as vCenter plugin), and describes its controls and functionality.

For information on new features or known issues with this release refer to the ioSphere Management Solution 3.7.0 Release Notes.

VMware vCenter Product Overview

The vCenter plugin is a VMware vCenter management plugin, a virtual machine image that helps you to:

- detach or attach ioSphere Management Solution devices
- rename your various devices
- perform a low-level format
- view information about your ioMemory devices
- enable host-based caching/guest-based caching
- assign caching shares

On a regular configurable interval the vCenter plugin polls configured ESX servers' SMI-S services for status updates. This data is stored in the ioSphere Management Solution database for processing and consumption by web service requests made from clients. The vCenter plugin also produces reports on data, endurance, and temperature. For example, clicking on the **Info** tab gives you the following information: general information, such as serial number, device path, the number of MiB's written, and PCI and adapter information. Later sections in this manual address these features and other tabs in greater detail.

VMware vCenter Components

The vCenter plugin relies on four components:

- the Fusion-io VSL driver and CIM provider running on the ESX hosts
- the Fusion-io vCenter plugin Virtual Machine running fio-msrv (the ioSphere Management Solution middle-tier server)
- the vSphere client application
- the vCenter management server

> The Fusion-io management tool, ioSphere Management Solution, is integrated into VMware's existing vSphere client. The vCenter plugin provides many of the same features and capabilities as the browser-based ioSphere Management Solution web application. vCenter plugin reuses much of the ioSphere Management Solution infrastructure, so a standard web browser may also be used to access the vCenter plugin.

> The vCenter plugin does not cover the management of ioMemory devices assigned to virtual machines via the PCI Passthrough feature. Normally, because the ioMemory devices are really resources within a non-virtual environment, this case would fall outside the scope of the ioMemory device management capabilities of the plugin. An ioMemory device driver and management agent (fio-agent) may be loaded within the VM image to manage such virtualized devices.

To make the vCenter plugin fully functional, the Fusion-io SMI-s module is enhanced with an additional generic data bundle function in the root-level FIO_ComputerSystem class. This data bundle provides the same data as fio-agent would normally send to an ioSphere Management Solution server on one of its regular-interval pushes.

VMware vCenter Plugin Assumptions

You are familiar with installing and managing ioMemory devices in an ESX/ESX(i) environment, and are familiar with the VMware vSphere management infrastructure.

VMware vCenter Supported Operating Systems

- ESX Version 4.x
- ESX(i) Version 4.x, 5.1, 5.5
- vCenter Server - 4.x, 5.0, 5.1, 5.5

VMware vCenter Supported Software

If you will be using the vCenter plugin with ESX/ESXi hosts that do not currently have VSL drivers or CIM providers installed on them, you can add the required software to your ESX/ESXi hosts after installing the vCenter plugin using the ***Update Host Software*** link at the top of the **Configure** section of the ioSphere Management Solution tab. For more information, see VMware Update Host Software on page 84.

If you have older versions of VSL drivers and CIM providers running on your ESX/ESXi hosts, you can also use the ***Update Host Software*** link to update the drivers and software to compatible versions with the vCenter plugin.

If you are running versions of the VSL drivers and CIM providers on your ESX/ESXi hosts that are at revision level 3.2.2 or higher, then your drivers are compatible with the 3.7.0 version of the ioSphere Management Solution vCenter plugin. However, it is strongly recommended that you update the VSL driver, VSL SDK, and CIM provider to the level of drivers provided with the vCenter plugin. In the case of the 3.7.0 release of the ioSphere Management Solution vCenter plugin, the following versions are provided and recommended:

- VSL Driver--Version 3.2.3
- VSL SDK--Version 3.2.3
- CIM Provider--Version 3.7.0

User Interface Differences Between ioSphere Management Solution and the VMware vCenter Plugin

If you are familiar with ioSphere Management Solution, you will immediately notice some differences in the standalone ioSphere Management Solution user interface and the vCenter plug-in user interface.

What looks to be different, but is not, is the Host screen as displayed in a web browser and in the vSphere client. It is actually the same screen, but fio-msrv displays it differently in these two environments. The plugin presents a restricted view of what you would normally see in a browser. For instance, the top-level menu bar of ioSphere Management Solution has been removed in vSphere client, so the Overview, ioMemory, Settings, etc., buttons are not available.

Despite the restricted view, the vCenter plugin has significant enhancements in functionality from fio-msrv running in *normal* (non-vCenter) mode. For example:

- the main login page is never seen -- authentication is done transparently using the vCenter server user's credentials
- when an unmanaged (meaning no Fusion-io hardware or CIM provider is installed) host is selected, a new "unmanaged host" screen displays
- when a ***Successful*** or ***Error*** link is selected in the config history bar, a different vCenter-centric view is presented
- the Host Log Report link is missing in vCenter mode because Host Log Report is not currently supported through this interface
- the update host software link is available in the vCenter plugin version of ioSphere Management Solution. (This link shows up where the Host Log Report link would normally be displayed.)

VMware Installation Overview

There are two ways to install the vCenter plugin and its required software:

- Automatic driver installation--which consists of deploying the vCenter Plugin OVA and then using the plugin to install and update ioMemory device drivers.
- Manual driver installation--which consists of manually installing compatible drivers on all the ESX hosts in the virtual center environment that use ioMemory devices, and then deploying the vCenter Plugin OVA.

VMware Automatic Driver Installation

1. Deploy the vCenter Plugin OVA. For detailed instructions, see VMware OVA Deployment on page 72.
2. After OVA deployment, register it to a vCenter.Then login to the vCenter,navigate to the desired ESX host in the inventory tree of the vSphere client.
3. Select the Fusion-io ioSphere Management Solution tab and then on the displayed host page select the **Configure** tab.
4. Click the ***Update Host Software*** link. The **Update Host Software** dialog appears.
    - If the selected host already has Fusion-io software installed, the version information for these packages will be displayed in the **Current Version** column.
    - If the Fusion-io vSphere plugin has newer software available for the selected host, the newer versions will be displayed in the **New Version** column.
    - If the **New Version** column is empty, the button will be grayed out, as the plugin's update repository has nothing newer than the software already installed on the selected host.
5. Click the **Install** button and confirm that you want to update the specified host. ioSphere will automatically install the drivers to the ESX host.

A progress bar displays the status of the update process, which could take as long as five minutes.

> ⚠ At least one reboot of the ESX host will be required by this process.

> ⚠ If an *unexpected* error occurs on software update, you may have to manually reboot the ESX host. When errors occur in the command sequence between the proxy and the ESX host, the command sequence is cancelled, which usually results in the reboot not occurring. Oftentimes the software installs properly, but the reboot doesn't occur. Manually rebooting the host enables the installed software.

VMware Manual Driver Installation

1. Obtain versions of the CIM provider, ioMemory device driver, and VSL SDK that have versions later than 3.2.2.

   For example, download files from the Fusion-io support site with names similar to these:

   > ⚠ Fusion-io files often contain three-digit numbers that represent a build number. In the filenames below, "***" represents the highest available version number for the specified file.

ESX/ESXi 4

Support Site Location	ioSphere > VMware_ESXi-5.0 > 3.7.0-iosphere > Utilities
Filename	fusionio-cimprovider-esxi5-bundle-3.7.0-***.zip
Support Site Location	ioDrive2 > VMware_ESX_and_ESXi_4.x > 3.2.3 > Software Binaries
Filename	cross_vmware-esx-drivers-block-iomemory-vsl_400.3.2.3.950.164009.208167-offline-bundle.zip
Support Site Location	ioDrive2 > VMware_ESX_and_ESXi_4.x > 3.2.3 > Software Binaries
Filename	libvsl-1.0.0-4X-3.2.3.950.zip

ESXi 5

Support Site Location	ioSphere > VMware_ESXi-5.0 > 3.7.0-iosphere > Utilities
Filename	fusionio-cimprovider-esxi5-bundle-3.7.0-***.zip
Support Site Location	ioDrive2 > VMware_ESXi_5.x > 3.2.3 > Software Binaries
Filename	iomemory-vsl-5X-3.2.3.950-offline_bundle-979464.zip
Support Site Location	ioDrive2 > VMware_ESXi_5.x > 3.2.3 > Software Binaries
Filename	libvsl-1.0.0-5X-offline-bundle.3.2.3.950.zip

2. Obtain the Fusion-io vCenter plugin OVA.

Support Site Location	ioSphere > VMware_Virtual_Appliance > 3.7.0-iosphere > ioSphere
Filename	Fusion_vCenter_plugin_OVF10-3.5.0.***.ova

3. Install the host software on each ESX host
    a. Uninstall any previous version of Fusion-io CIM provider.

       If your CIM provider is at a version level earlier than 3.2.2, then you will need to uninstall the CIM provider and associated libvsl. After uninstalling, you will need to reboot the host to completely remove the CIM provider and libvsl.

    b. Install iomemory-vsl and libvsl packages.

    c. Install ioSphere Management Solution CIM provider package.

    d. Reboot the system.

4. Deploy the vCenter plugin OVA as described in the **OVA Deployment** section. For more information, see page VMware OVA Deployment on page 72.

VMware Upgrading or Re-installing the vCenter Plugin

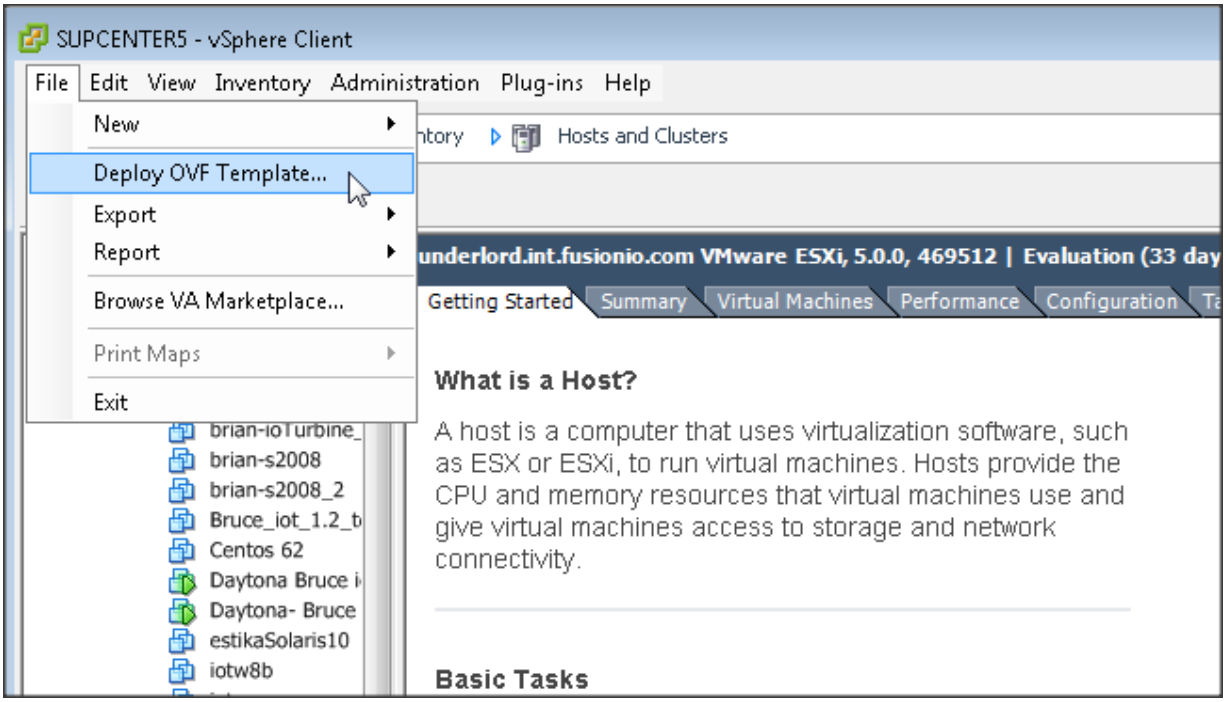
If you are upgrading a previous version of the vCenter plugin or if you are installing over an existing vCenter plugin installation, consider performing the following steps before beginning the installation:

- Export the vCenter plugin database--if you export your current plugin database you will have the opportunity to restore it to your new plugin during the OVA deployment process. Export the database by connecting to the web browser version of your ioSphere Management Solution plugin, click **Settings**. Then on the left-hand side of the screen, click **Database,** and then click **Backup.**
- Unregister your current vCenter plugin--if you do not unregister your current vCenter plugin there may be a registration conflict when deploying the plugin OVA. Unregister your current vCenter plugin by connecting to the web browser version of your ioSphere Management Solution plugin, click **Settings.** Then on the left-hand side of the screen, click **VCenter Server**, and then click **Unregister**.

VMware OVA Deployment

After you have downloaded the correct file from the support center, you can deploy the vCenter plugin OVA template. The vCenter plugin OVA will have a file name similar to this: **Fusion_vCenter_plugin_OVF10-3.7.0.***.ova.**

1. From the vSphere Client, click **File > Deploy OVF Template.**



2. Choose the OVA file to install.

3. Review the plugin details.

4. Accept the license agreement.

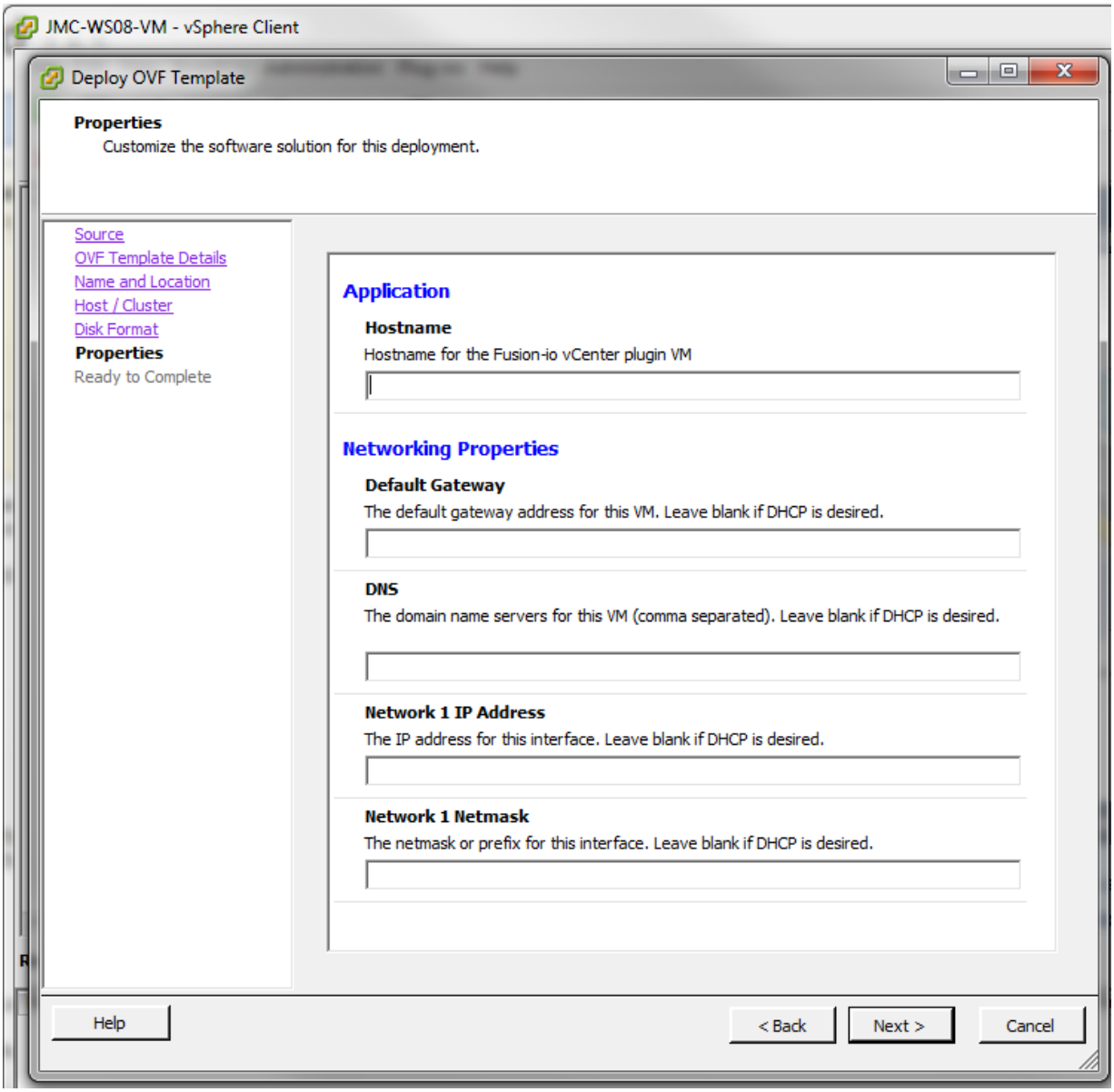
5. Provide a name for the plugin and select and inventory location for it in the vCenter tree. (This is not the hostname of the plugin; rather it is the vCenter name for the plugin.)

6. Choose the host or cluster you want to deploy the plugin on.

7. Choose the datastore the plugin will use.

8. Choose how you want the plugin provisioned. Thick provisioning will theoretically yield better performance, but it will also take longer to initialize the plugin. The plugin should run satisfactorily Thin Provisioned.

9. Set the networking properties for the plugin.



⚠ You must give the ioSphere Management Solution vCenter Plugin VM (in the Hostname box) a fully qualified domain name. Network settings should be configured properly using a static IP address and a properly registered DNS hostname. To ensure proper plugin behavior, make sure you correctly fill in the fields Default Gateway, Network 1 IP Address, and Network 1 Netmask.

⚠ Do not use underscores in the Hostname for the plugin. DNS does not allow hostnames to contain underscores, and if you include one in the Hostname, you may not be able to log in to the plugin.

10. Click Finish to install the vCenter plugin.

> The Password is set during OVF deployment, and no longer set on first boot.

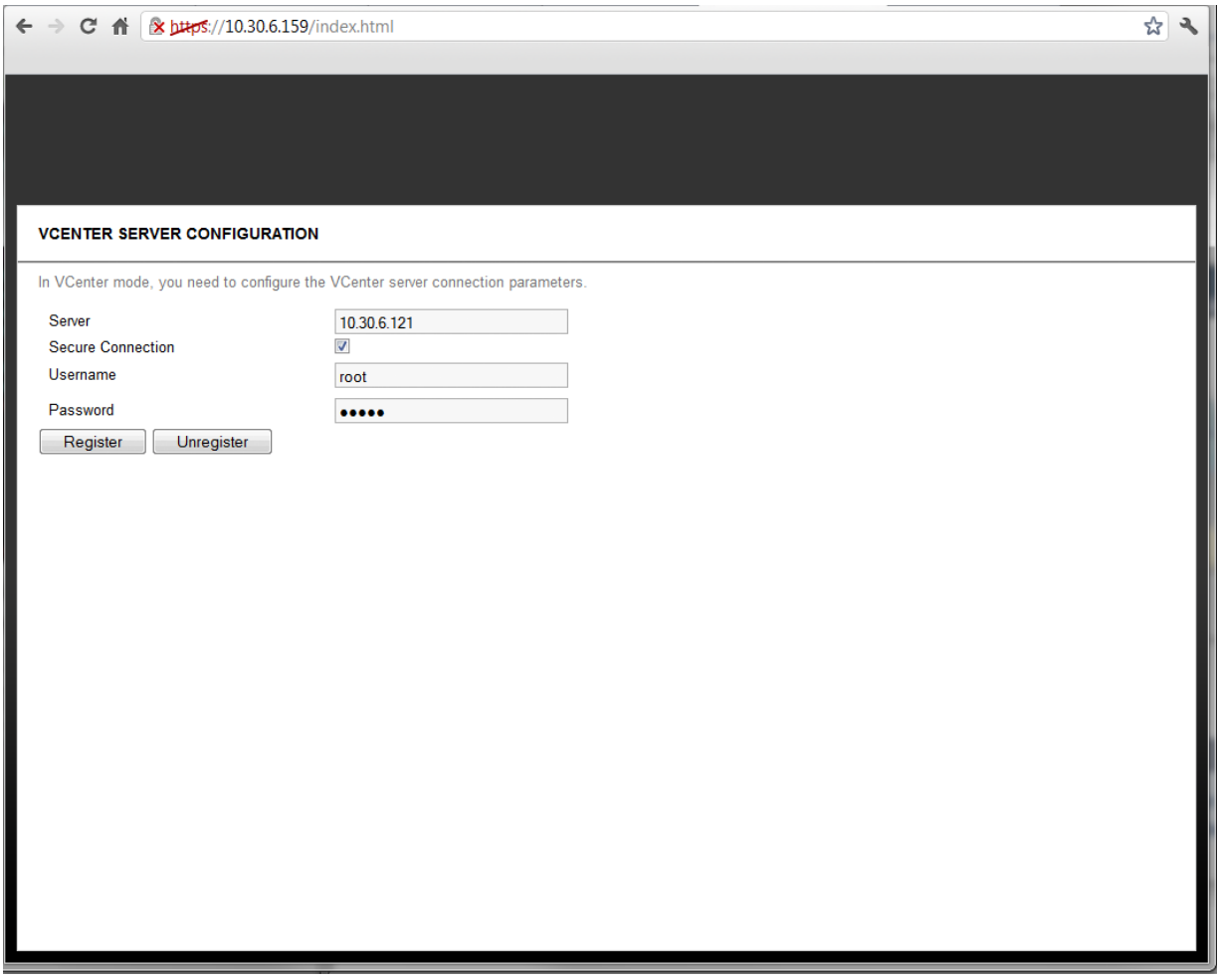
11. Open a web browser and navigate to the plugin's secure (https) root page:

```
https://<ipAddress>/index.html
```

where ipAddress is the IP address of the plug-in.

Login as admin, using the password you specified in step 3. If you were running version 3.7.0 of the vCenter plug-in, and you exported the plug-in's data before installing this instance, you have the option to Restore the data from your previous plugin. Otherwise, click **New Install** on the screen to install a new version of the plugin.

12. Enter the vCenter credentials, and click Register.



After initial set up, changing the Server name on this screen or clicking Unregister can have unrecoverable results. For details on modifying values on this page after initial set up, see VMware Modifying vCenter Server Configuration on page 87.

13. Configure remote access options as desired and then click **Save Changes**. Remote access options are described in greater detail below.

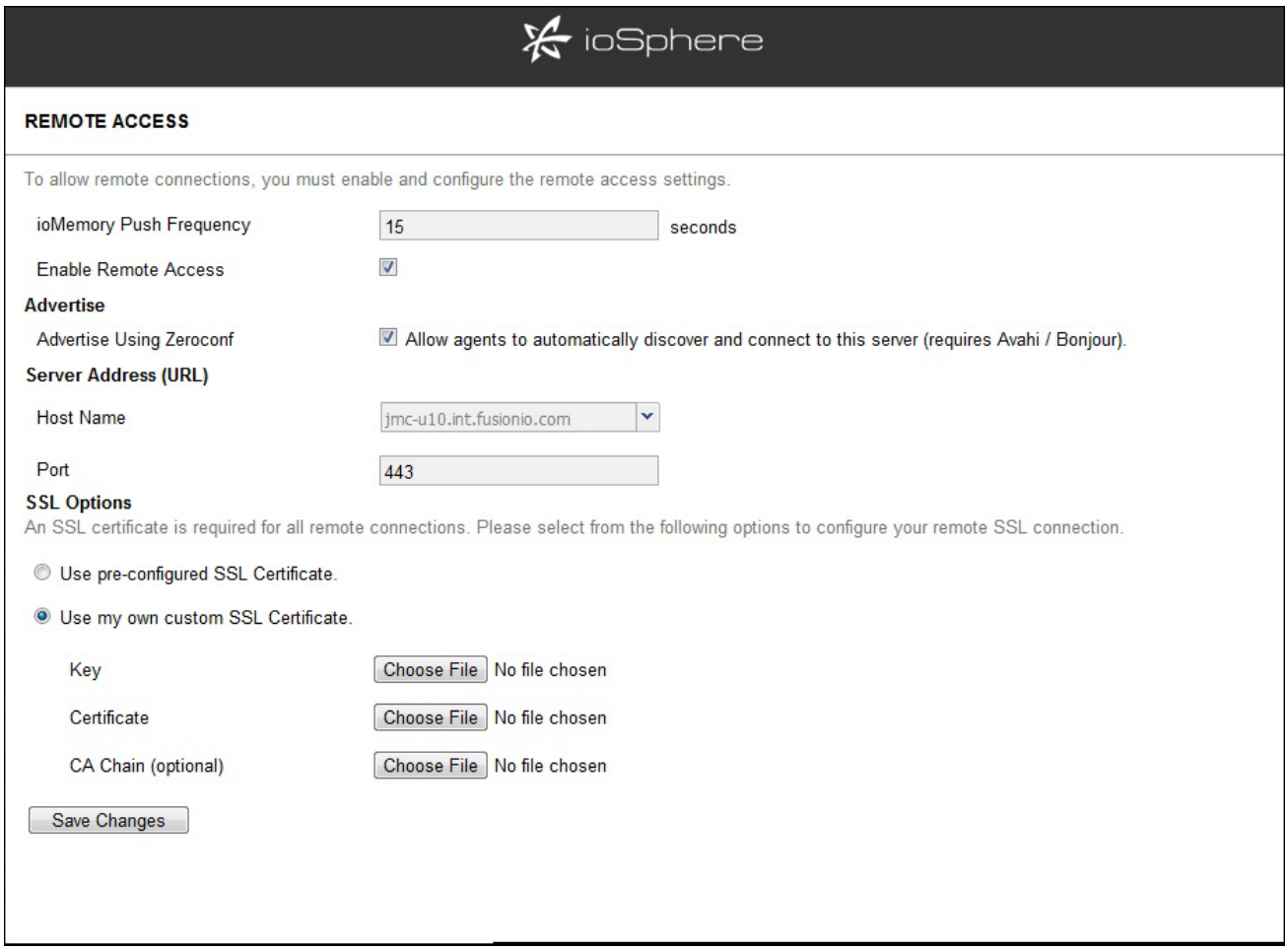
If you do not have a custom certificate, choose the **Use pre-configured SSL Certificate** option.

After clicking **Save Changes,** the vCenter plugin is configured.

It is possible that even if the vCenter plugin starts, the ioSphere Management Solution tab may not display in the vCenter interface. If this occurs go to Plug-ins > Manage Plug-ins in the the vCenter client, and then check to see if the vCenter plugin has a red icon next to it and has a status of *Disabled*. If it does, right click on the plug-in and select **Enable**. This should enable the plug-in, and the ioSphere Management Solution tab should appear.

VMware Remote Access

Configure your remote access settings here.



For more information on configuring the remote access settings, see Remote Access on page 34.

> Do not disable remote access to the plugin. Doing so will cause vSphere clients to fail to connect to ioSphere Management Solution.

> In the vCenter plugin, the port is set by default to 443. It is strongly recommended that you do not change this port.

VMware Getting Started

There are three levels of access in ioSphere Management Solution:

- **anonymous** - synonymous with none -- you cannot see any information about this host
- **read-only** - buttons or links do not work or even appear for this server with this access level -- information about the host and devices is available, but configuration operations are not
- **write-admin** - administrative rights -- with this level of rights, you can do anything you need to do as an administrator (such as attach or detach a device, update the firmware, etc.)

The vCenter plugin assigns one of these three levels of rights to any user authenticated through vSphere client, based on that user's assigned vCenter privileges to each managed ESX server. The vCenter privileges map in this manner:

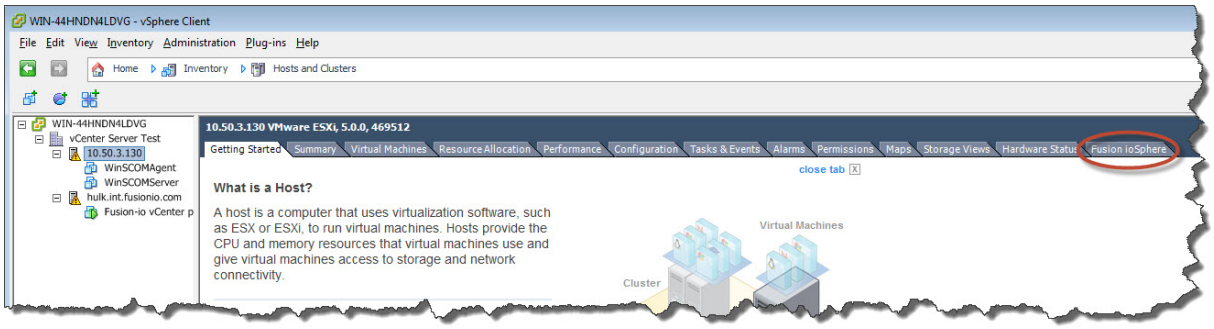
vCenter Privilege	ioSphere Management Solution Rights
Host.Cim.CimInteraction	Write-admin
System.View	Read-only
Anything else	Anonymous

If a user does not have vCenter's System.View privilege on a given ESX server, the server will not show up in the inventory view. Therefore, you will not be able to see the effect of ioSphere Management Solution's Anonymous rights because you will not be able to select such an ESX server.

A user who logs into fio-msrv as **admin** using a web browser has administrator privileges on all associated ESX hosts relative to ioMemory devices. Therefore, the global system administrator should protect the password for the ioSphere Management Solution admin account.

VMware Post Deployment

1. Open the vSphere client. After supplying the appropriate logon credentials, this screen displays:

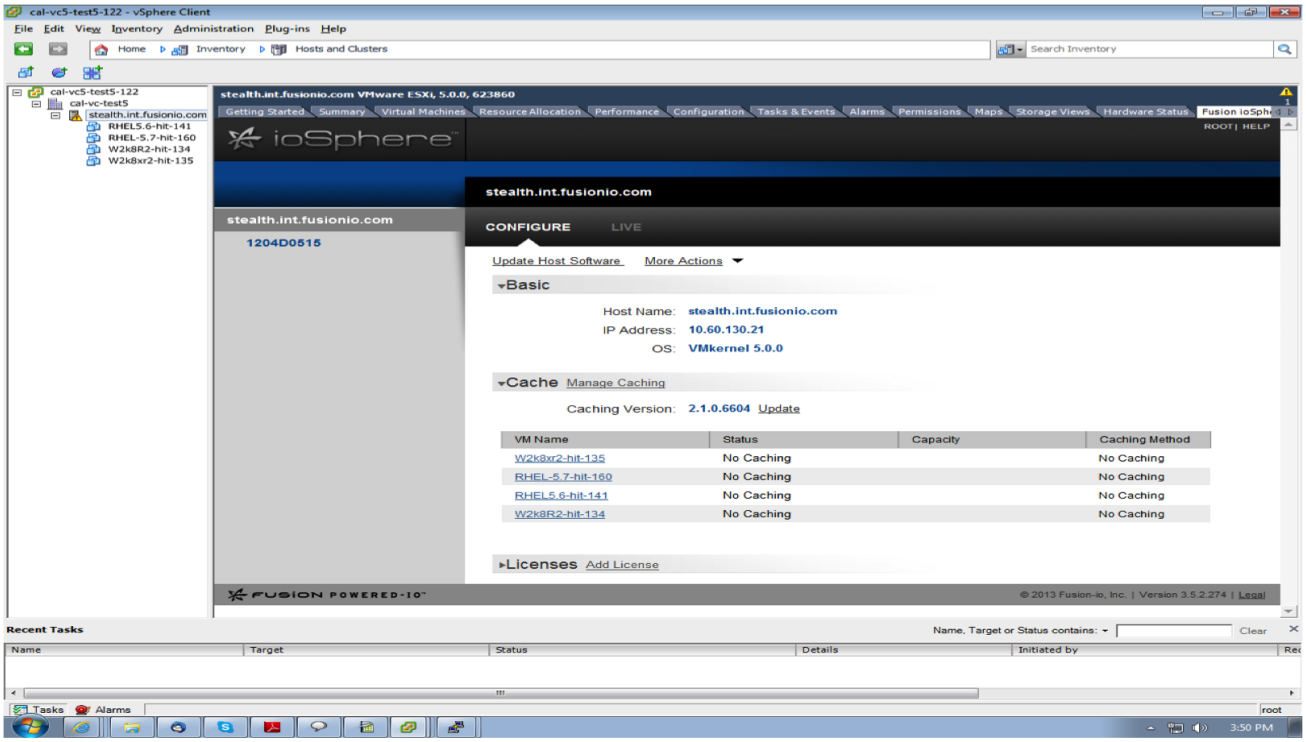


2. What you see looks like a normal vSphere client screen, including the tree on the left-hand side of the screen. The Fusion-io vCenter plugin provides the ioSphere Management Solution tab at the end of the tab bar. Use the tree-view to select the ESX server that you want to configure and monitor using the Fusion-io vCenter plugin.

> ⚠ The ioSphere Management Solution tab is only available if you have selected a Host node in the tree view.

VMware vCenter Plugin Configure Tab

From the tree-view, select your desired server and then select the Fusion-io ioSphere Management Solution tab. You will see this screen, with the Configure tab highlighted.



> If your user account has the Host.Cim.CimInteraction privilege on this ESX host, you can make the changes outlined below.

VMware Sidebar

Notice the sidebar, directly under the ioSphere Management Solution logo.

This shows you the following information:

- Host Name
- The ioMemory device adapters available to the particular host

> For a 3rd party SSD/ioMemory adapter, only the Host name will be displayed.

VMware Settings

The following Settings can be edited from **ioMemory device>Configure>Settings:**

- ioMemory device Alias - By default the serial number is used.
- Device Status - Can be Attach, Detach, or Busy. The status of "Busy (Configuring)" may indicate that operations like format, attach, detach, or firmware upgrade are in process.

  The Attach Device operation creates a link so the ioMemory device interacts with the operating system. In most cases, the operating system driver automatically attaches the installed ioMemory device(s) at boot time, so you only need to use Attach Device when you manually detach an ioMemory device (such as to perform a low-level format). Device Status is continuously updated to reflect the current status of the adapter.

  Detach Device disconnects your ioMemory device from the operating system. Once detached, the device is not accessible to users or applications. (You need to use Attach Device to make it accessible.) You should only need to detach an ioMemory device to perform a low-level format or a firmware upgrade.

  > You must always manually unmount any file systems on the device before detaching it. Attempting to detach a device on ESX while a filesystem is mounted can cause the system to become unstable.

- Labels - Show Labels link.
- Beacon - Can be either On or Disable.

  Turning on the Beacon feature turns on all three LEDs. This feature enables an Administrator to physically locate a given adapter in a host or server. Whenever you make a change to the configuration, you will see a confirmation dialog.

VMware Firmware

You can use the ***Update Firmware*** link to update the firmware on the selected ioMemory devices.

1. Download the latest version of the firmware to a filesystem on the machine where you are running the vSphere client.
2. Click **Update Firmware**.
3. Click **Browse** and navigate to the location of the firmware file that you downloaded.
4. Click **Update Firmware**.

   The vCenter plugin upgrades the firmware on the selected device.

VMware Low-Level Formatting

The third group of information, under the *Low-Level Formatting, Low-Level Reformat* header gives you device capacity information.

Here you can perform the following:

- Low-Level Formatting
- Total Factory Capacity
- Format Capacity
- Sector Size

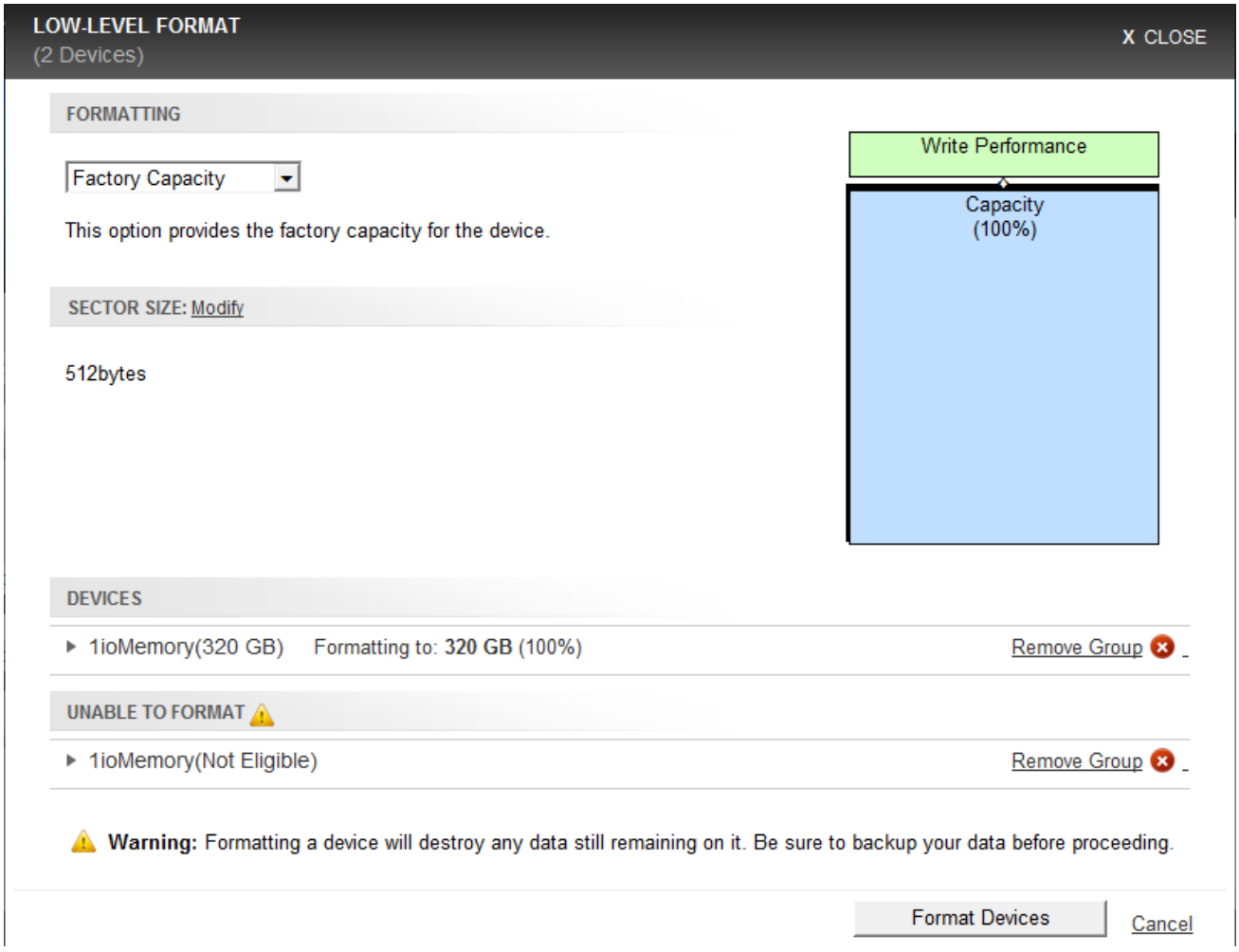
Formatting a device will destroy any data still remaining on it. Please be sure to back up your data before proceeding.

Your ioMemory device comes pre-formatted to factory capacity, so generally it is not necessary to use this option. However, you would use it if any of these situations arise:

- You need to re-format the drive to change its logical size or modify write performance.
- Your application supports sector sizes larger than 512 bytes (the default), and you want to tune your device accordingly. Larger sector sizes allow for more optimal CPU/memory use, and the Maximum Capacity format option provides a larger format size when the sector size is increased.
- You are instructed to do so by Fusion-io Customer Support.

ioSphere performs a low-level format that is different from a format performed by an operating system using standard disk management utilities. You do not need to perform a low-level format to create an operating system-specific volume on the device.

When you click the Low-Level Reformat link, the following dialog appears:



Here you can set the ratio of Write Performance to Capacity. You can increase Write Performance by decreasing the ioMemory device's capacity -- the reverse is also true. You can select from a drop-down list of preset ratios (Maximum Capacity, Factory Capacity, Improved Performance, High Performance), or customize the ratio with

the Custom selection (also in the drop-down menu) or by dragging the line between Write Performance and Capacity in the graphic.

The selected ioMemory device(s) appear as a group below the Write Performance/Capacity graphic. Click the arrow to the left of the group to reveal more details and the option to remove devices from the group, or click Remove Group to remove the device(s) from the Low-Level Format dialog.

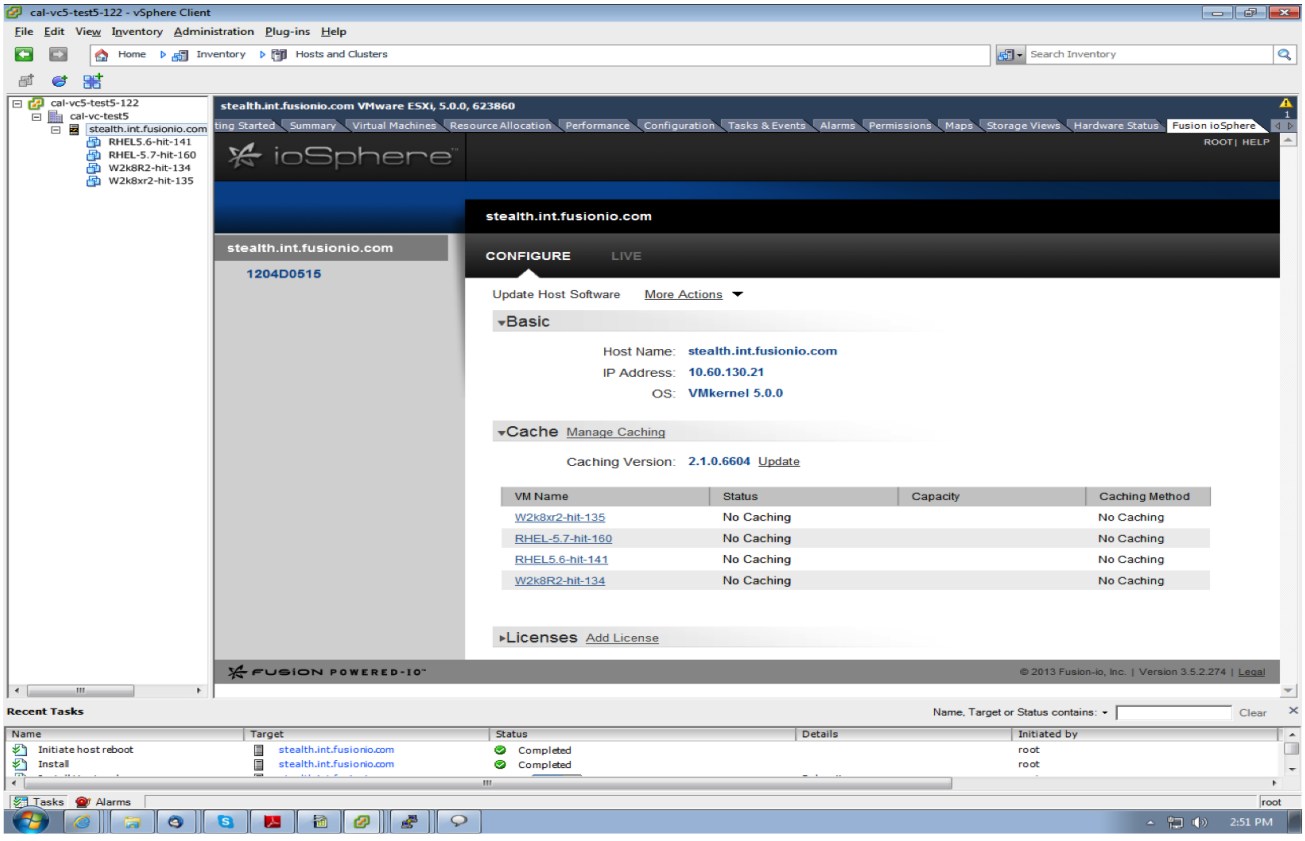
> If an ioMemory device is unable to format (e.g., it is busy, or the formatting is not valid for that particular device), it will display in a separate section titled Unavailable for Formatting at the bottom.

When you are ready to format the selected ioMemory device, click the Format Devices button.

To exit the Low-Level Format dialog without formatting any devices, click the Cancel link.

VMware Update Host Software

At the top left side of the **Configure** page, there is a link to ***Update Host Software***.



Clicking this link displays a dialog that identifies current driver levels on the host.

- If the selected host already has Fusion-io software installed, the version information for these packages will be displayed in the **Current Version** column..
- If the Fusion-io vSphere plugin has newer software available for the selected host, the newer versions will be displayed in the **New Version** column.
- If the **New Version** column is empty, the **Install** button will be grayed out, as the plugin's update repository has nothing newer than the software already installed on the selected host.

Click the **Install** button,then click **Confirm** to update the specified host. ioSphere Management Solution will automatically install the drivers to the ESX host.

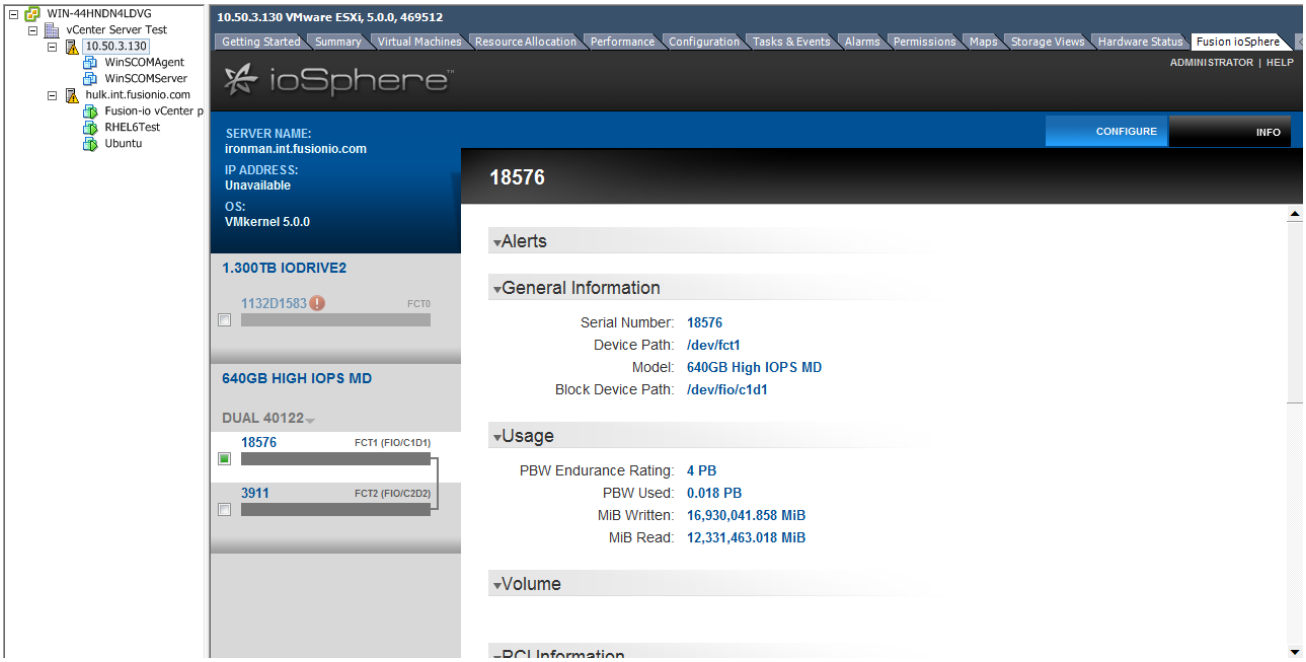
A progress bar displays the status of the update process, which could take as long as five minutes.

> ⚠ At least one reboot of the ESX host will be required by this process.

If you want to update the host drivers to the drivers packaged with the vCenter plug-in, click **Install.**

VMware Info Tab

When you click on the **Info** tab, you will see a scrolling screen similar to this:



The Info tab provides details about a single ioMemory device including recent Alerts and a history of alerts, the device's Serial Number, Model, Device Path, Block Device Path, Volume and PCI Information (such as PCI Address, PCI Device ID, and PCIe Link Speed.) The Info tab also shows such Adapter information as Board Kind (Single or Duo), the Serial Number, and PCIe Bus Voltage, Current, Power, and Bandwidth.

> ⚠ If VMare does not have any alerts, the Alert pane will not be seen.

VMware Modifying vCenter Server Configuration

After initial set up you can use the vCenter Server Configuration screen, accessible from ioSphere **Browser>Settings> vCenter Server** to modify the initial settings.

The following actions can be taken from this screen

- Change vCenter Server
- Change Username and Password
- Unregister the Plug-in from vCenter

> **Change Connection Security** is always set to **Secure** connection. This cannot be changed.

Changing vCenter Server

If you want to register the plug-in with a different vCenter enter the name or the IP address of the new vCenter in the Server field and then click **Register.**

> Changing the vCenter Server name on this screen will delete the previous vCenter's settings from ioSphere Management Solution. Additionally, information about any host that was discovered or managed by the previous vCenter will be deleted.

Changing Username and Password

To change the username that the plug-in uses to connect to vCenter, enter the new name in the **Username** field, enter the password for that username in the **Password** field, and then click **Register.**

To change only the password of the current username, enter the new password in the **Password** field and click **Register.**

Unregistering the Plug-in from vCenter

To unregister the plug-in from the vCenter listed in the Server field, click **Unregister.**

> Clicking **Unregister** will delete the vCenter's settings from ioSphere Management Solution. Additionally, information about any host that was discovered or managed by the vCenter will be deleted.

Maintenance and Troubleshooting

The following items provide information on troubleshooting issues with ioSphere Management Solution.

Location of ioSphere Management Solution Logs

On Linux, ioSphere Management Solution logs can be found in the following directory:

```
/var/log/fusionio
```

On Windows, ioSphere Management Solution logs can be found in the following folder:

```
C:\programData\fio-logs
```

Changing a Management Server's Host Name

If you need to change a Management Server's host name, follow the steps below:

For vCenter Deployments

1. Open a browser to the management server UI (for example: `https://new-host-name`), Login and navigate to the **Settings > REMOTE SETTINGS** screen.
2. Select the host name or IP address you would like the management server to use from the host name drop-down.
3. Update the custom certificate and key files for new host name, if needed.
4. Click **Save**. The management server UI will restart.
5. Re-authenticate and navigate to the **Settings > VCENTER SERVER** screen.
6. Click **Unregister**.

   ⚠ Ignore any errors indicating the server was not registered.

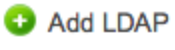
7. Enter the proper vCenter server name, if needed, and enter the user name and password.
8. Click **Register**. vCenter server registration will now be configured properly with the new host name. All newly started vSphere clients will now display the ioSphere Management Solution tab on host and VM inventory items.
9. Download a new copy of the management server key from **Settings > ACCESS KEY** and copy it to each VM host using guest-caching mode and each bare-metal host that is managed by this server. The file should be copied to Linux hosts as `/var/lib/fio/agent_keys/remote.key` and to Windows hosts as `C:\ProgramData\fio\agent_keys\remote.key`. Agents will automatically begin to connect and register themselves with the newly named management server as soon as the new key is copied.

For Non-vCenter Deployments

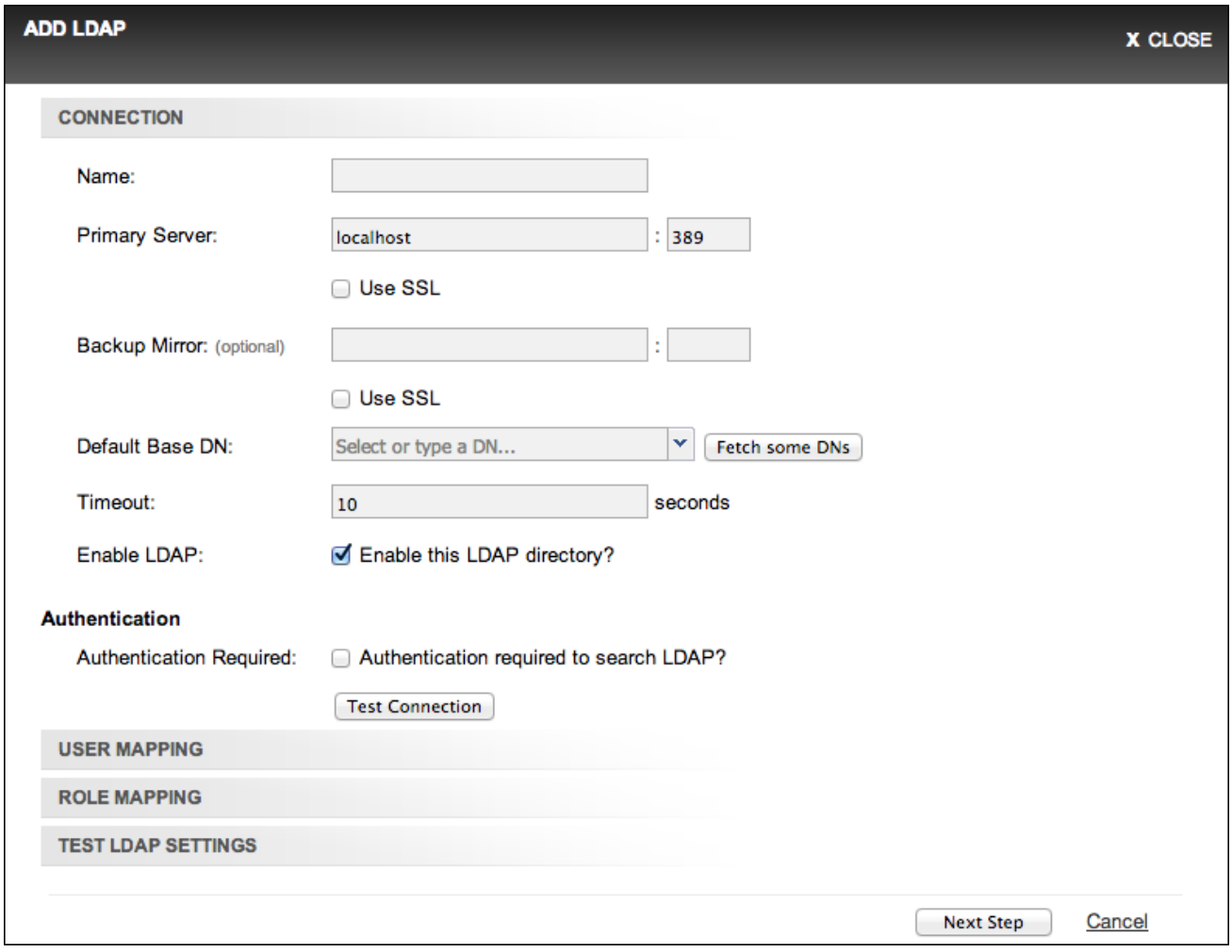
1. Open a browser to the management server UI (for example: `https://new-host-name`), login and navigate to the **Settings > REMOTE SETTINGS** screen.
2. Select the host name or IP address you would like the management server to use from the host name drop-down.
3. Update custom certificate and key files for new host name, if needed.
4. Click **Save**. The management server UI will restart.
5. Download a new copy of the management server key from the **Settings > ACCESS KEY** page and copy it to each host that is managed by this server. The file should be copied to Linux hosts as `/var/lib/fio/agent_keys/remote.key` and to Windows hosts as `C:\ProgramData\fio\agent_keys\remote.key`. Agents will automatically begin to connect and register themselves with the newly named management server as soon as the new key is copied.

Appendix A - Adding and Editing LDAP Providers

Some users create multiple LDAP configurations to coordinate with multiple directories deployed within their organization. This section describes how to add and edit LDAP providers.

To begin, go to the **Settings** tab and click the **Add LDAP** button 

found at the top of the Settings screen. The **Add LDAP** dialog appears.



Add LDAP dialog contains four sections: **Connection, User Mapping, Role Mapping,** and **Test LDAP Settings.** Start with the Connection section.

Connection

Enter a name for the LDAP configuration in the **Name** field. For example: "Corporate Directory."

Enter the hostname (DNS or IP address) and port for the primary LDAP server in the **Primary Server** fields. If multiple LDAP servers are used to access the directory, you may enter a secondary hostname and port in the **Backup Mirror** field.

For security purposes, it is recommended that you mark the **Use SSL** checkbox for your configured LDAP servers.

> The ioSphere Management Solution is not able to import the LDAP server's public key. Instead, it automatically trusts the server's certificate when performing the SSL handshake.

The **Default Base DN** field is optional. If your users and/or groups are located below a common branch in your LDAP tree, enter the DN for that branch here. This field is only used in order to make it easier to configure the user mapping and role mappings later.

The timeout used for making server connections and for searching is specified in the **Timeout** field.

> The ioSphere Management Solution will always use the smaller of the timeout you specify and 20 seconds. This prevents the web application from encountering connection timeout problems.

Oftentimes, LDAP directories are configured to disallow anonymous searching. In other words, one may need to be authenticated in order to search the LDAP directory. If this is the case, mark the **Authentication Required** checkbox, and enter the DN and Password for the identity that will be used to perform searches in the LDAP directory.

> Best security practices call for a "least privileged user" to be created in the LDAP directory and used for this purpose. This user is granted just enough rights to perform LDAP search operations in the portion(s) of the tree where users and groups reside.

> The Auth DN and Password are securely stored in the ioSphere Management Solution, but if the **Use SSL** checkbox is not marked, then these credentials may be seen by others with the use of a network traffic sniffer.

Click the **Test Connection** button to ensure that your configuration steps thus far are correct. The test will:

- Connect to the LDAP Server(s) specified
- Perform a StartTLS operation (if the server(s) have the Use SSL checkbox marked)
- Perform an LDAP Bind with the Auth DN and Password if one is specified

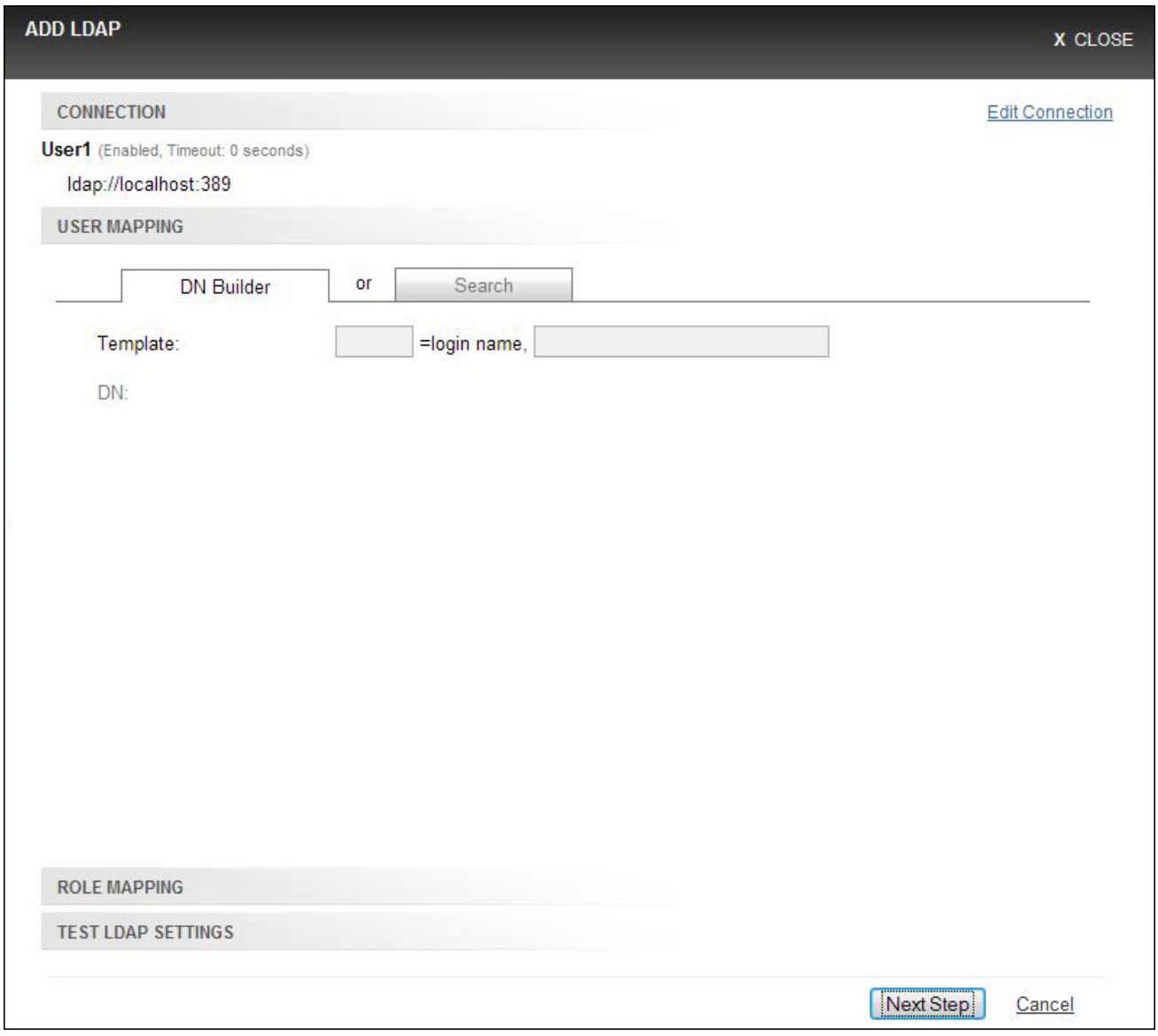
Any errors encountered are displayed at the top of the dialog.

When finished, click **Next Step** to enter the User Mapping section.

User Mapping

A primary function of the LDAP Provider is to verify a username and password. It also verifies that the username maps to an entry in the LDAP server, and that the user's LDAP entry along with their password can be used to authenticate to the LDAP directory.

ioSphere Management Solution gives you two ways to map usernames to LDAP entries: an easy DN Builder (essentially a DN template), and a traditional search-based mapping configuration.



DN Builder

In some LDAP deployments, all users reside in a single, flat container (like `OU=people,DC=example,DC=com`), and all users are named with a common naming attribute (like UID). In this case, it is much easier to use the DN

Builder to configure the User Mapping. In order to map a username like jdoe to an LDAP entry like `UID=jdoe, OU=people,DC=example,DC=com`, type `UID` into the template's left field, and `OU=people,DC=example, DC=com` into the right field.

You will notice that an example DN is shown below the Template fields in the form of `UID=$\{username\}, OU=people,DC=example,DC=com`. This shows you what the resulting username map will be (where the string "`$\{username\}`" will be replaced with the username entered when a user attempts to login.

Search

The traditional method of mapping a username to an LDAP entry is to search for the username as a unique value of the entry that represents that user. For example, ActiveDirectory deployments often populate an attribute called `sAMAccountName` with the username. Other directory deployments may populate the `UID` attribute with the username.

Enter the DN of the tree branch that is hierarchically above your user entries (for example, `OU=people, DC=example,DC=com`). If you previously entered a Default Base DN, you may simply pick that from the drop-down list if you wish.

For the search filter, you can add one or more attributes to the **Search Attribute(s)** field and a search filter will be automatically created for you. For example, if your user entries have a UID attribute that holds their unique username, typing `UID` into the **Search Attribute(s)** field will produce a standard LDAP search filter of `(UID=$\{username\})`

If you need a specialized search filter, you may edit it in the Search Filter field (use the radio buttons to toggle between entering attributes and editing the search filter).

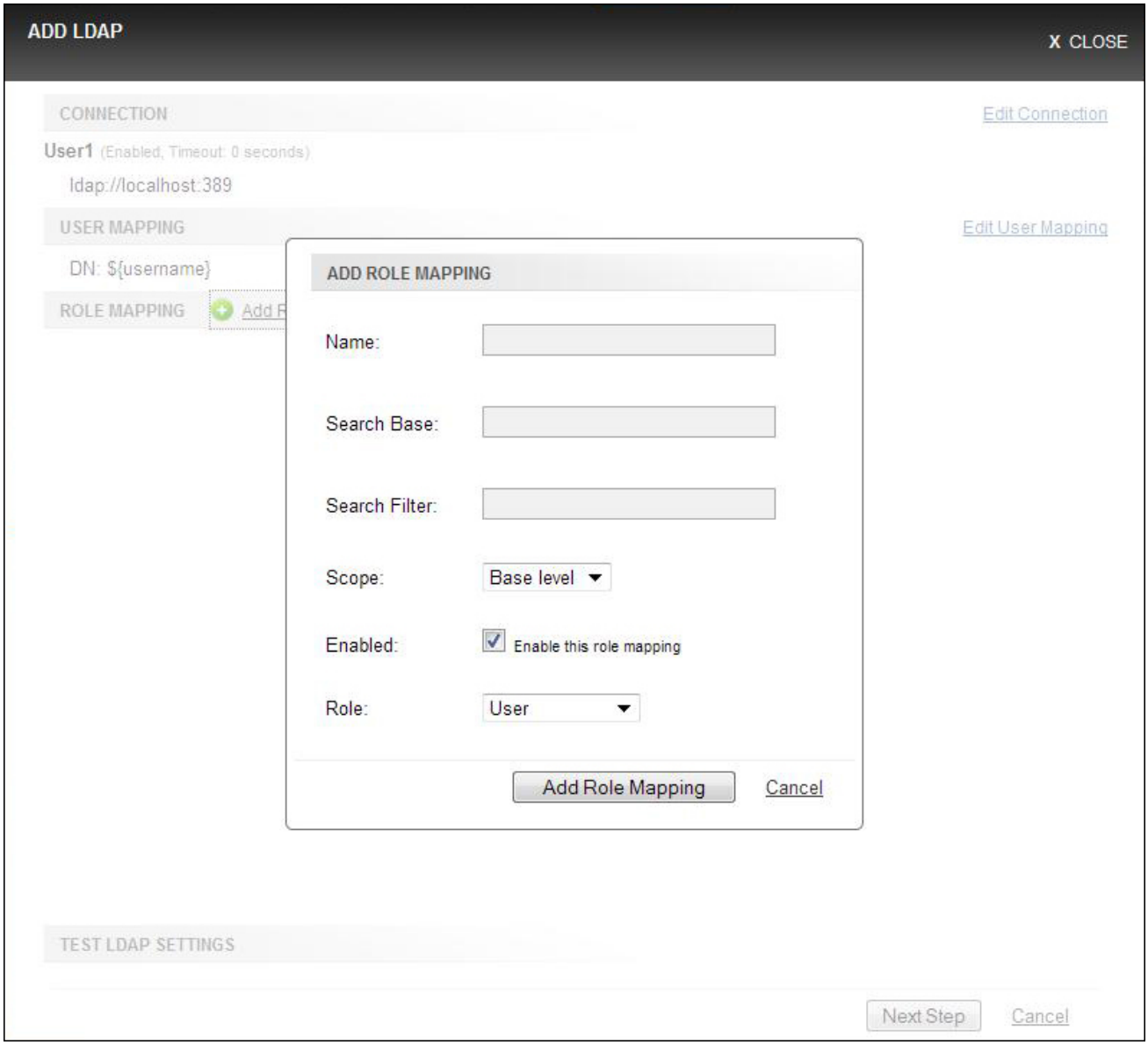
> The special token "$\{username\}" is replaced with the name the user is attempting to log in with when ioSphere Management Solution performs the authentication.

The **Scope** should normally be set to Subtree. It may be set to One Level if the users are all in a single container.

Click **Next Step** to proceed to the Role Mapping section.

Role Mapping

The **Role Mapping** section details how to configure the ways in which users are granted roles.



Role Mapping Rules are used to place a user into one or more roles in ioSphere Management Solution: User, Device Admin, or Server Admin.

Each role mapping is essentially an LDAP search specification along with a Role. When the search specification is true (returns one or more entries) for a user, then that user is granted the Role.

Click **Add Role Mapping** to create a new role mapping.

Enter a name for this mapping in the **Name** field. This lets you identify the role mapping later if you decide to edit it. For example: "Administrators"

Enter a DN in the **Search Base DN** field. This could be the DN of some container, or a specific DN (like that of a group - e.g., `CN=administrators,OU=groups,DC=example,DC=com`. The special value `${dn` may be used here to set the search base DN to the user's LDAP entry. This is useful when creating a role mapping based of the user's attributes (such as memberOf).

Enter an LDAP search filter in the **Search Filter** field. The search filter may contain the special values `${username}` (which is replaced by the name the user logged in with), or `${dn}` (which is replaced by the DN of the logged-in user's LDAP entry). For example, a search filter of (`member=${dn}`) will match true for entries where there is a member attribute that is has the logged-in user's DN as a value (common in group entries).

Set the **Scope** appropriately. If the Search Base DN names a specific entry in the LDAP tree, the scope should be Base level; otherwise it should be either Subtree or One level.

Choose the **Role** to be granted to users meeting the search criteria (for example: if the search criteria matches true for users who are listed in and LDAP group entry full of administrators, set the role to Server Admin).

Click **Add Role Mapping** to finish the Role Mapping section.

Continue to the Test LDAP Settings section.

Example Role Mappings

Here are some examples of role mappings that might be configured for different LDAP directory deployments:

Members of the Administrator group are in role Server Admin

- Set the Search Base DN field to the Administrators group entry. For example: `CN=administrators,OU=groups,DC=example,DC=com`.
- Set the Search Filter: (`member=${dn}`)" (typical for AD) or (`uniqueMember=${dn}`) (typical for non-AD). If you are unsure which attribute holds the members of the group, you can use the search filter (`|(member=${dn})(uniqueMember=${dn})`)
- Set the Scope to Base level
- Set the Role to Server Admin

Members of the Administrator group are in role Server Admin (alternate AD config)

Sometimes in Active Directory, and some other LDAP deployments a user is given group membership by placing an attribute on the user's entry (like memberOf). This role mapping will grant the same role as above for these cases:

- Set the Search Base DN field to the user's entry: `${dn}`
- Set the Search Filter: (`memberOf=CN=administrators,OU=groups,DC=example,DC=com`)
- Set the Scope to Base level
- Set the Role to Server Admin

Users who have the title of manager are in the Device Admin role

In this scenario, we use an attribute called title on the user's object to determine whether they are in the Device Admin role.

- Set the Search Base DN field to the user's entry: `${dn}`
- Set the Search Filter: (`title=manager`)
- Set the Scope to Base level
- Set the Role to Device Admin, then click **Next Step** to test your settings.

Grant a specific user the Server Admin role

You may find situations where a specific user is not in a group, but needs to be in a role. This can be done by creating search criteria that matches true only for that user.

- Set the Search Base DN field to the user's entry: `${dn}`
- Set the Search Filter: (`sAMAccountName=jdoe`)
- Set the Scope to Base level
- Set the Role to Server Admin

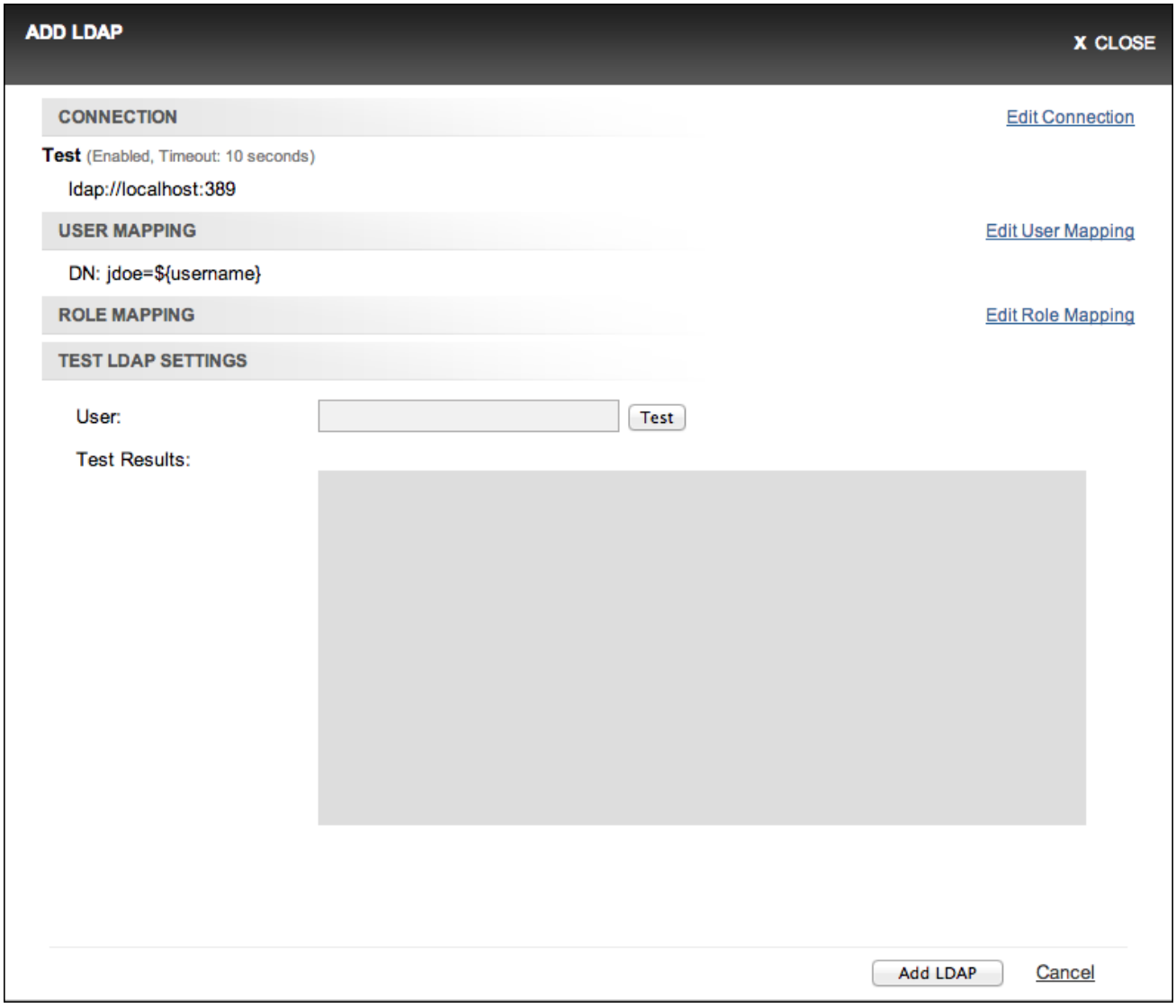
Grant the User role to everyone who is able to authenticate

If you want everyone who is able to log in to have at least the User role, you can do this:

- Set the Search Base DN field to the user's entry: `${dn}`
- Set the Search Filter: (`objectclass=*`)
- Set the Scope to Base level
- Set the Role to User

Test LDAP Settings

This section lets you test your connection, user mapping, and role mappings configuration.



Type the name of a user into the User field (like "jdoe") and click Test.

The results of the test will display as each step is completed. Each step will also contain timing information. This may be helpful in fine-tuning your user mapping and role mappings

Ideally, you will see results that look like this:

```
setup: 0 seconds.

Connection succeeded. Endpoint: ldaps://ldap.example.com:389

bind: 0 seconds.
```

```
Using search to resolve user. Base: ou=people,dc=example,dc=com Scope: subtree
Filter: (samaccountname=jdoe)

resolve: 0 seconds.

Resolved jdoe to CN=John Doe,OU=People,DC=example,DC=com

total resolve time: 0 seconds.

Attempting role map: {base: ${dn}, filter: (objectclass=*), scope: 0} to test
user: jdoe for role(s): (Server Admin, Device Admin, User). ${username} = jdoe.
${dn} = CN=John Doe,OU=People,DC=example,DC=com

resolve roles: 0 seconds.

Found match with role map: {base: ${dn}, filter: (objectclass=*), scope: 0}

In role(s): (User)

total resolve and role calculation time: 0 seconds.
```

Appendix B - Software Updates

Updating ioMemory devices involves two procedures: updating the ioMemory device VSL (driver) on the host machine, and updating the firmware on the ioMemory device.

To update the ioMemory device VSL on the host machine:

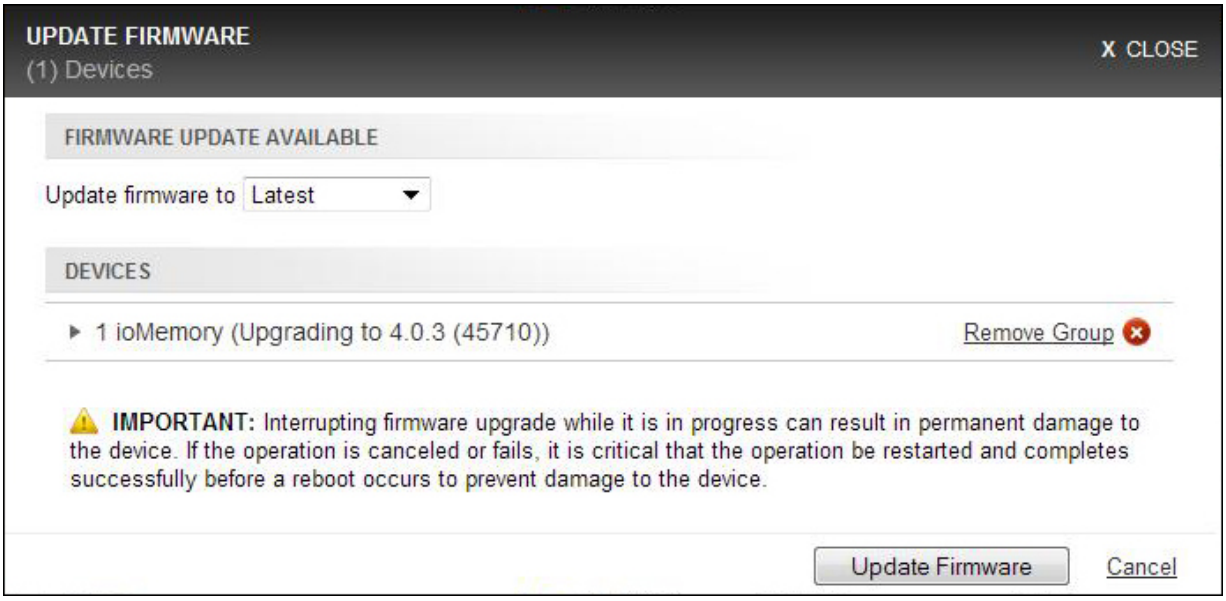
1. Get the latest ioMemory device VSL files and documentation.
2. Follow the instructions in the *ioMemory device VSL User Guide* to install the ioMemory device VSL on the host machine.

> When you install the ioMemory device VSL, the firmware is copied to the host machine (but not installed).

> Before using the GUI to update firmware, you must place the new firmware packages on the machines that contain the cards you want to upgrade. In some cases, you may need to create the folder or directory where the GUI will look for the firmware packages.
>
> For Linux, verify that the following directory exists:
> `/usr/share/fio/firmware`
> If the directory does not exist, you need to create it. After the directory is created, copy the firmware package to the directory.
>
> For Windows, verify that the following folder exists:
> `C:\Program Files\Fusion-io ioMemory VSL\Firmware`
> If the folder does not exist, you need to create it. After the folder is created, copy the firmware package to the directory.

To install the firmware to the ioMemory devices:

1. Open the ioSphere Management Solution.
2. If you are using ioSphere Management Solution, click the Overview tab and click the ***x devices have updates available*** link.
3. Click the **Update Firmware** button. The Update Firmware dialog appears.



4. Click the **Update Firmware** button to begin updating. The Config History bar appears at the bottom of the screen.

Config History - ioSphere Management Solution

Click the **PROCESSING** link to see a list of devices being updated. Click the **Skipped** link to see a list of devices that were selected but are not being updated.

Each device's progress is shown in the sidebar.

When the firmware update process is complete, the Config History bar shows how many ioMemory device were updated, how many failed, and how many devices were skipped or require reboot. Click on the SKIPPED, FAILED or REQUIRES REBOOT link to see a list of those devices.

Click the arrow at the left end of the Config History bar to expand the bar and see previous updates.

Appendix C- SMI-S Interface Guide

The SMI-S interface is based on Web-Based Enterprise Management (WBEM) and provides a Common Information Model (CIM) model that represents the ioDrive device and associated software, in accordance with existing Distributed Management Task Force (DMTF), Storage Networking Industry Association (SNIA), and Storage Management Initiative Specification (SMI-S) standards. This model permits backward-compatible extension, accommodating new hardware and software features developed by Fusion-io.

It is assumed that you are versed in WBEM, SMI-S and DMTF standards. This document and associated model may change at any time as feedback is received.

References

CIM Schema v2.26
http://dmtf.org/standards/cim/cim_schema_v2260

DMTF DSP1011, Physical Asset Profile
http://www.dmtf.org/standards/published_documents/DSP1011_1.0.2.pdf

DMTF DSP1023, Software Inventory Profile
http://www.dmtf.org/standards/published_documents/DSP1023_1.0.1.pdf

DMTF DSP1033, Profile Registration Profile
http://www.dmtf.org/standards/published_documents/DSP1033_1.0.0.pdf

DMTF DSP1075 PCI Device Profile
http://www.dmtf.org/standards/published_documents/DSP1075_1.0.0.pdf

DMTF DSP1002, Diagnostics Profile
http://www.dmtf.org/standards/published_documents/DSP1002_2.0.0.pdf

SMI-S v1.4 Architecture
http://www.snia.org/sites/default/files/SMI-Sv1.4r6_Architecture.book.pdf

SMI-S v1.4 Common Profiles
http://www.snia.org/sites/default/files/SMI-Sv1.4r6_CommonProfiles.book.pdf

SMI-S v1.4 Host Profiles
http://www.snia.org/sites/default/files/SMI-Sv1.4r6_Host.book.pdf

SMI-S v1.4 Common Diagnostic Model
http://www.dmtf.org/standards/mgmt/cdm/

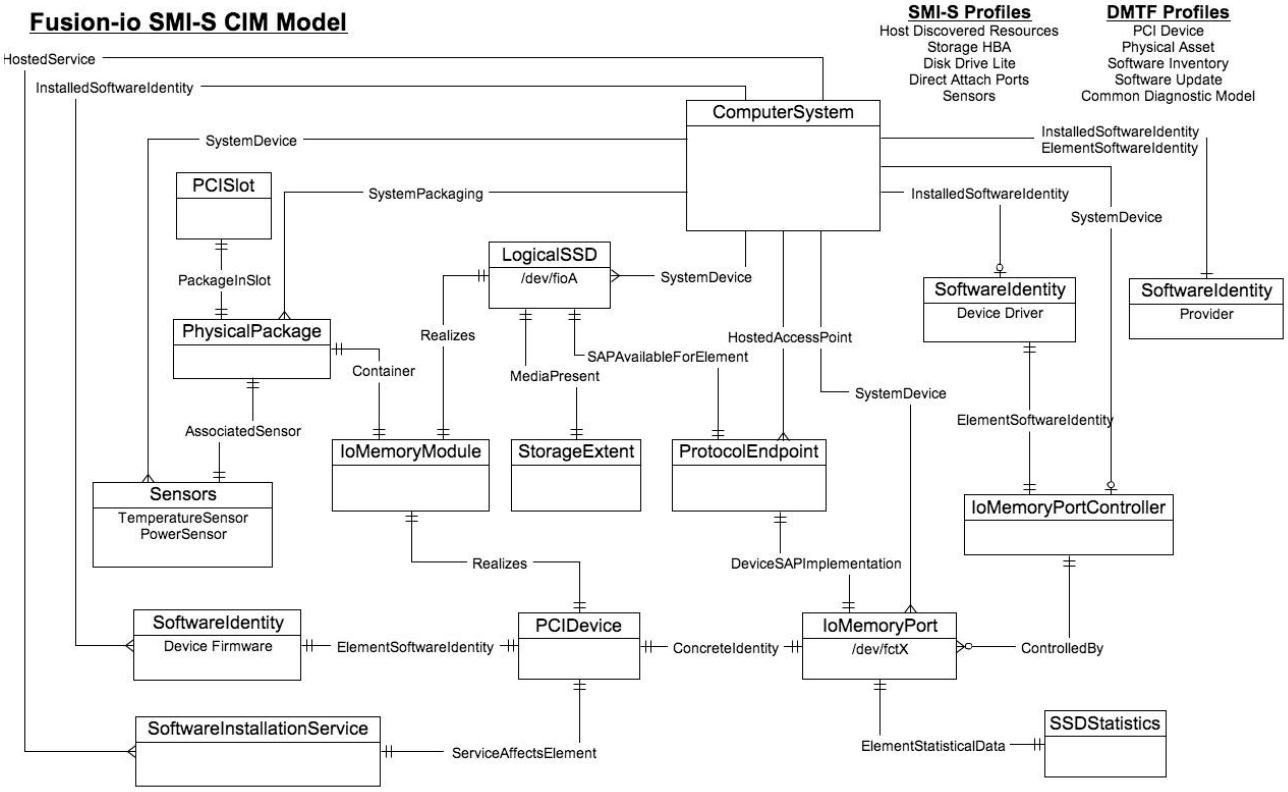
Description

SMI-S is a collection of specifications that traditionally focus on Storage Area Network (SAN) systems based on the SCSI command set, such as Fibre Channel, iSCSI, and SAS. However, the general pattern used to model

these storage systems can be applied to solid state, direct-attached storage systems such as those provided by Fusion-io.

The Fusion-io ioDrive device CIM design is modeled using the SMI-S patterns established in the Storage HBA, Direct Attached (DA) Ports, and Host Discovered Resources Profiles. The physical aspects of the ioDrive device and all firmware and driver software are modeled using published DMTF specifications, including the Physical Asset, Software Inventory, and PCI Device Profiles.

The following figure depicts the instance diagram modeling the ioMemory and its associated firmware/software.



For simplicity, the prefix FIO_ has been removed from the class names.

The central instance of the model is an instance of the IOMemoryPort class, a logical representation of the ioMemory device module and associated PCI adapter. It supports the extrinsic methods necessary to provision the drive. An instance of PCIDevice and IOMemoryPort exists for each Fusion-io ioMemory device module installed in the system and they are associated with an instance of ConcreteIdentity. An instance of SSDStatistics is associated to each IOMemoryPort by an ElementStatisticalData association and contains important performance and capacity data pertaining to the associated drive. IOMemoryPort is scoped by an instance of the ComputerSystem class. The SystemDevice aggregation aggregates ioMemory modules within the containing ComputerSystem.

An instance of IOMemoryPortController represents the functional driver used to control the ioMemory device modules installed in the host system. IOMemoryPortController specializes CIM_PortController. It aggregates

IOMemoryPorts with the ControlledBy aggregation. The driver version and vendor information are represented by the SoftwareIdentity instance associated to IOMemoryPortController via ElementSoftwareIdentity. The SoftwareIdentity that represents the installed driver software is associated to the scoping ComputerSystem using the InstalledSoftwareIdentity association.

An instance of the ProtocolEndpoint class represents both ends of the logical data path between the IOMemoryPort and the solid state storage. This aspect of the model is derived from the pattern in the DA Ports Profile, where the port is both an initiator and target.

ProtocolEndpoint is associated to the IOMemoryPort using the DeviceSAPImplementation association and to the ComputerSystem using the HostedAccessPoint association.

The block device exposed to applications (file systems, database, logical volume manager) is modeled using an instance of LogicalSSD, a subclass of CIM_DiskDrive. It is associated with a StorageExtent using the MediaPresent association but the StorageExtent is always be present. It is also associated to the ProtocolEndpoint representing the IOMemoryPort using SAPAvailableForElement association and to the scoping ComputerSystem using the SystemDevice aggregation.

The ioMemory device module, being a PCI-E device, is also represented by an instance of the PCIDevice class. IOMemoryPort is an alternate representation of the PCIDevice and its associated control device. It is associated to it by the ConcreteIdentity association.

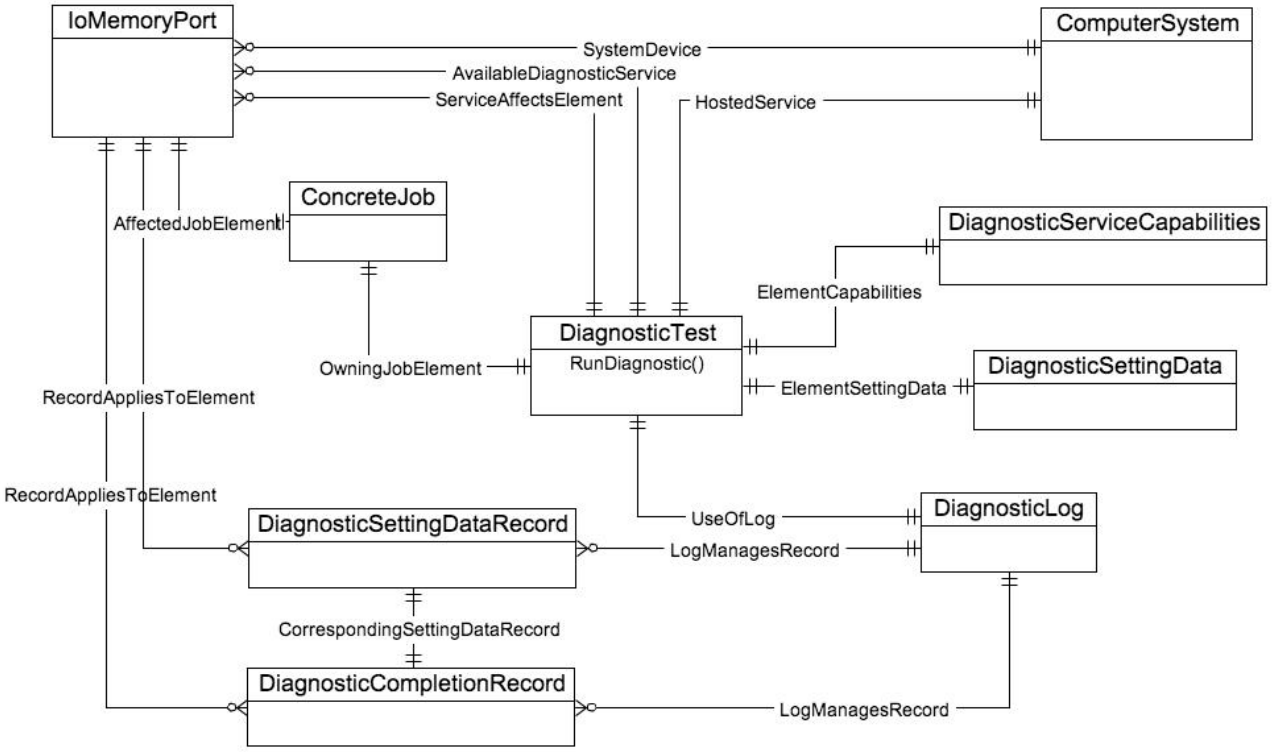
Firmware installed on the ioMemory device is represented by an instance of the SoftwareIdentity class, which is associated to the PCIDevice by the ElementSoftwareIdentity association. The SoftwareIdentity that represents the firmware is associated to the scoping ComputerSystem using the InstalledSoftwareIdentity association. An instance of SoftwareInstallationService is associated with each PCIDevice that can be used to update device firmware.

The physical aspects of the ioMemory device module are represented by an instance of the PhysicalPackage class, which is associated to the PCIDevice and LogicalSSD using the Realizes association and to the scoping ComputerSystem using the SystemPackaging association. The temperature and power sensors on the ioMemory device module are represented by one instance of TemperatureSensor and five instances of PowerSensor, three for PCI bus power usage and two for internal voltages, and are associated to the PhysicalPackage with AssociatedSensor.

The PCI slot into which an ioMemory device is installed is represented by an instance of the Slot class, which is associated to the PhysicalPackage class using the PackageInSlot association.

The following figure shows the details of the Common Diagnostic Model for Fusion-io drives.

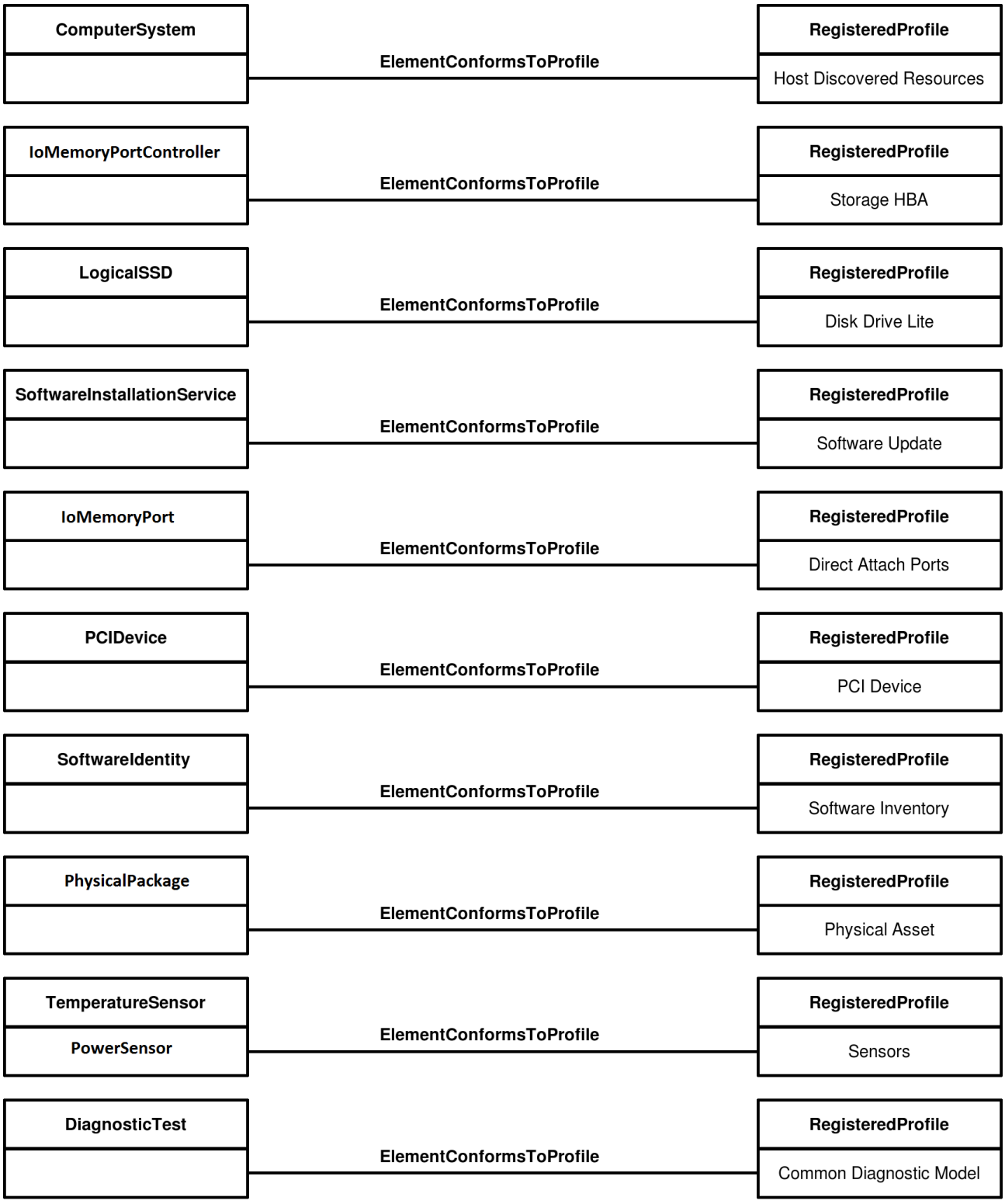
Fusion-io Common Diagnostic Model



The central class is DiagnosticTest. An instance is always be available by associations to ComputerSystem and each IOMemoryPort. After a test is run using the RunDiagnostic method specifying the target IOMemoryPort, the resulting ConcreteJob object provides the status of the operation. DiagnosticSettingDataRecord and DiagnosticCompletionRecord instances are also created for each run and is associated with the DiagnosticLog object using a LogManagesRecord association. These instances are also associated to the respective IoMemoryPort object with a RecordAppliesToElement association. The DiagnosticCompletionRecord records the results of the test and is associated to a default instance of DiagnosticSettingDataRecord via a CorrespondingSettingDataRecord association.

The Fusion-io CIM model implements the Disk Drive Lite, Direct Attach Ports, Storage HBA, Host Discovered Resources, PCI Device, Software Inventory, Software Update, Physical Asset and Sensors Profiles, and the Common Diagnostic Model all of which must be registered in the /root/interop namespace using an instance of the RegisteredProfile, class.

The following figure depicts these relationships.


ComputerSystem
ElementConformsToProfile
RegisteredProfile
Host Discovered Resources
IoMemoryPortController
ElementConformsToProfile
RegisteredProfile
Storage HBA
LogicalSSD
ElementConformsToProfile
RegisteredProfile
Disk Drive Lite
SoftwareInstallationService
ElementConformsToProfile
RegisteredProfile
Software Update
IoMemoryPort
ElementConformsToProfile
RegisteredProfile
Direct Attach Ports
PCIDevice
ElementConformsToProfile
RegisteredProfile
PCI Device
SoftwareIdentity
ElementConformsToProfile
RegisteredProfile
Software Inventory
PhysicalPackage
ElementConformsToProfile
RegisteredProfile
Physical Asset
TemperatureSensor
PowerSensor
ElementConformsToProfile
RegisteredProfile
Sensors
DiagnosticTest
ElementConformsToProfile
RegisteredProfile
Common Diagnostic Model

Implementation

This section describes the arrangement of instances and associations for the Fusion-io device CIM model. Not all class properties are described in detail. Consult the CIM schema for detailed description of all properties.

Data Model Classes

IOMemoryPort

One instance of IOMemoryPort exists for each Fusion-io ioMemory device module installed in the ComputerSystem.

The **LocationIndicator** property reflects the state of the device indicator beacon (e.g., all LEDs on solid). Reading the value gives the current state of the indicator. Invoking the Beacon method with *true* or *false* can be used to enable or disable the indicator to show the device's physical location.

The drive health is indicated by the value of the **HealthLevel** property. Values include: *Healthy, Warning, Reduced Write* and *Read Only.* These values are mapped to standard HealthState values *OK, Degraded/Warning* and *Critical Failure* as appropriate.

Extrinsic methods for drive provisioning includes *Attach*, *Detach*, *Format* and *FormatSize*. The Attach method creates a block device for the drive. Detach disables the block device.

Format formats the device using preconfigured default values, while *FormatSize* allows users to specify the device size in either megabytes or a percentage and block size in bytes.

Drive longevity is indicated by the value of the **HealthPercentage** property.

FlashbackAvailability indicates whether or not this feature of the ioMemory device module is online. This value is deprecated as of the 3.0 driver release with the new Adaptive Flashback feature, but remains in the CIM data model to support use of legacy 2.x drivers.

IOMemoryPorts are aggregated by IOMemoryPortController via the ControlledBy aggregation. IOMemoryPorts are associated to their corresponding PCIDevice with the ConcreteIdentity association. IOMemoryPorts are logical devices of the scoping ComputerSystem, and are indicated as such by the SystemDevice aggregation.

The current operating state of the drive is listed in the State property. If the drive state is shown as *Minimal*, the reason for the minimal state is displayed in the **MinimalModeReason** property.

The write functionality of the drive is displayed in the Writability property. If writability is not normal, the **ReducedWritabilityReason** and **WriteRegulationLevel<Type>** properties displays the cause.

IOMemoryPorts is aggregated by **IOMemoryPortController** via the **ControlledBy** aggregation. **IOMemoryPorts** are associated to their corresponding PCIDevice with the ConcreteIdentity association. **IOMemoryPorts** are logical devices of the scoping **ComputerSystem**, and are indicated as such by the **SystemDevice** aggregation.

The ioDuo is a similar product with connectors for two ioMemory device modules. Logically, it looks just like two ioDrive devices. The **IOMemoryPort** class is extended to include information about the carrier card type, serial number and external power connection. This way, both the ioDrive device and the ioDuo is supported.

SSDStatistics

One instance of SSDStatistics exists for each **IOMemoryPort** instance. Properties of this object provide performance and capacity information, including the current, maximum, and factory default format sizes, the lifetime volume of data read/written by the device, and the device's system memory (RAM) usage. Some of this information is only available when the drive is attached e.g., the state of the associated **IOMemoryPort** is *Attached.*

IOMemoryPortController

Only one instance of **IOMemoryPortContoller** exists, representing the driver software used to control **IOMemoryPorts**. **IOMemoryPortController** specializes **CIM_PortController.**

IOMemoryPortController is aggregated to the scoping **ComputerSystem** using the **SystemDevice** aggregation. **IOMemoryPortController** is associated to a **SoftwareInventory** instance representing the driver software properties via the **ElementSoftwareIdentity** association.

ProtocolEndpoint

One instance of **ProtocolEndpoint** exists for each instance of **IOMemoryPort** and is associated to the **IOMemoryPort** using the **DeviceSAPImplementation** association and **LogicalSSD** using the **SAPAvailableForElement** association. Since an IOMemory**Port** represents both the initiator and target ports, only one **ProtocolEndpoint** per **IOMemoryPort** is needed to model the connection between **IOMemoryPort** and **LogicalSSD.**

LogicalSSD

One instance of **LogicalSSD**, a subclass of **CIM_DiskDrive**, exists for each block device(`/dev/fioX`) exposed by a Fusion-io drive. Correlatable IDs, based on operating system device names, are used, allowing client applications to associate block devices discovered through this model with resources discovered from other SMI-S models instrumented on the host system.These IDs are used in the **Name, ElementName,** and **InstanceID** properties of the **LogicalSSD**, while the **DeviceID** property always uses the same identifier as the associated **IOMemoryPort,** in order to properly preserve the association between the classes when the block device is unavailable.

The **LogicalSSD** also exposes properties of the device related to its format capabilities, including default and allowed values for format sector size.

ComputerSystem aggregates **LogicalSSDs** via the **SystemDevice** aggregation. **LogicalISSDs** are associated to their **ProtocolEndpoints** via **SAPAvailableForElement** association. If the **IOMemoryPort** associated to the endpoint is not attached then the **Availability** property is set to *Off Line* and the **DeviceID** property value is *Unknown*.

StorageExtent

One instance of **StorageExtent** is associated with each **LogicalSSD** and represents the logical storage of the associated device. The **StorageExtent** instance exposes properties of the device's current formatting including sector size and sector count.

SoftwareIdentity

This instance of **SoftwareIdentity** representing the driver software. The firmware is also modeled using **SoftwareIdentity**, but requires an instance for each ioMemory device module installed in the system. The **IsEntity** property has the value of *True,* indicating that the **SoftwareIdentity** instance corresponds to a discrete copy of the driver software or firmware.

The **MajorVersion, MinorVersion, RevisionNumber,** and **BuildNumber/LargeBuildNumber** properties is used to convey the driver/firmware version information. The **Manufacturer** property can be used to identify Fusion-io

SoftwareInstallationService

An instance of **SoftwareInstallationService** exists for each **PCIDevice** and can be utilized to update the associated device's firmware via the **InstallFromURI** method.

Each instance of **SoftwareInstallationService** lists any available firmware updates detected on the system in the **AvailableVersions** property, as well as the currently configured directory where firmware update files are located in the **FirmwareDirectory** property. The search directory can be modified by invoking the **UpdateFirmwareDirector**y method and specifying a new directory.

PCIDevice

An instance of **PCIDevice** is instantiated for each Fusion-io drive (PCI-E card) in the computer system. The **BusNumber** property is set to the bus number where the PCI-E device exists. The **DeviceNumber** property is set to the device number assigned to the PCI device for this bus. The **FunctionNumber** property is set to the function number for the PCI device. The **SubsystemID, SubsystemVendorID, PCIDeviceID, VendorID,** and **RevisionID** properties are optional but can be populated if values can be extracted from the configuration registers of the PCI device. The **PCIDevice** instance also exposes values related to the capabilities of the negotiated PCI-e link, including link speed, link lanes, bandwidth, and available power.

PCIDevice is associated to **IOMemoryPort,** its alternate logical representation, using the **ConcreteIdentity** association. **PCIDevice** is also associated to **PhysicalPackage,** representing the physical aspects of the ioMemory device module, via the **Realizes** association.

PCISlot

One instance of **PCISlot** exists for each ioMemory device. This class represents the PCI-E slot that the device is installed in. The **Number** property can be used to determine the PCI Slot number.

Each **PCISlot** is associated to **PhysicalPackage** via the **PackageInSlot** association.

PhysicalPackage

One instance of **PhysicalPackage** exists for each discrete, physical ioMemory device card installed in the computer system. The **Manufacturer, Model, SKU, SerialNumber, Version,** and **PartNumber** properties can be used to describe these aspects of the physical card.

PhysicalPackage is associated to PCIDevice and LogicalSSD via the **Realizes** association and the scoping **ComputerSystem** via **SystemPackaging** association.

TemperatureSensor / PowerSensor

One instance of **TemperatureSensor** and five instances of **PowerSensor**, three for PCI bus power usage and two for monitoring internal voltages, exist for each **PhysicalPackage.** Temperature and power consumption information for the drive is available in the properties of these objects.

Each sensor instance supports thresholds for determining the **HealthState** of the sensor. The possible threshold types for each individual sensor are listed in the **SupportedThresholds** property, and any whose threshold value can be detected from the device is also listed in the **EnabledThresholds** property. For each enabled threshold, a corresponding property is populated with that threshold's value. When the current reading of the sensor exceeds one of the enabled threshold values, the **HealthState** of the sensor is set appropriately.

Each **TemperatureSensor** and **PowerSensor** instance is associated to **PhysicalPackage** via the **AssociatedSensor** association, and to the **ComputerSystem** via the **SystemDevice** association.

Diagnostic Model Class

Diagnostic Test

One instance of **DiagnosticTest** exists. The **RunDiagnostic()** method triggers a snapshot of device status for the specified **ManagedElement** that must be an instance of **IOMemoryPort.** The diagnostic run is synchronous and runs instantaneously.

The resulting **ConcreteJob** object associates to the originating **DiagnosticTest** instance and the respective **IOMemoryPort** instance that was specified (for more information, see Description on page 101). At this time, **RunDiagnostic()** can only be used with the default **DiagnosticSettingData** provided. Each run adds a single entry of **DiagnosticSettingDataRecord** and associated **DiagnosticCompletionRecord** in the **DiagnosticLog.** The **RecordData** property of the **DiagnosticCompletionRecord** records critical device status at the time of the run. The format of the **RecordData** string can be found in the **RecordFormat** property. The format is a series of status strings, each of which can hold one of the following values delimited by an asterisk * character: *Unknown*, *OK*, *Warning* or *Error*.

Currently, seven status values are recorded: **WearoutStatus, WritabilityStatus, FlashbackStatus, TemperatureStatus, MinimalModeStatus, PciStatus** and **InternalErrorStatus.** All of these should report *OK* under normal operating conditions. Additionally, an **OtherStatus** value indicates any error or warning conditions that do not fall into any of these categories.

WearoutStatus is set to *Warning* when less than 10% reserve space is left on the device. It is set to *Error* when there is no more reserved space.

WritabilityStatus is set to *Error* whenever the device is write throttling or in read-only mode. This can happed due to a variety of conditions including device wearout and insufficient power.

FlashbackStatus reports *Warning* if a catastrophic error causes Flashback protection to be degraded. This condition cannot occur when using a 3.x series ioMemory device VSL driver.

TemperatureStatus reports *Warning* when the device temperature is nearing the maximum safe temperature and *Error* when the maximum safe temperature is reached or surpassed.

MinimalModeStatus reports either *Warning* or *Error* whenever the device is in minimal mode.

PciStatus reports *Warning* or *Error* if there are compatibility problems with the host PCIe bus.

InternalErrorStatus reports *Error* if there are any internal problems with the driver.

The **CompletionState** property summarizes the results and may be set to *Unknown, OK, Warning* or *Failed.* If any status is in error, the state reports as *Failed.* Otherwise, if there is any warning status, the state reports *Warning.*

The **Message** property sets to indicate the appropriate action if there are any warnings or errors.

DiagnosticSettingData

There is an instance of DiagnosticSettingData associated with the DiagnosticTest instance (for more information, see Description on page 101). It records the default settings for each call to RunDiagnostic.

DiagnosticServiceCapabilities

An instance of **DiagnosticServiceCapabilities** associated with the **DiagnosticTest** instance records the capabilities of the DiagnosticTest service.

DiagnosticLog

An instance of **DiagnosticLog** is associated with the **DiagnosticTest** instance and stores the results of each run.

DiagnosticSettingDataRecord

A copy of the default **DiagnosticSettingData** is stored in a **DiagnosticSettingDataRecord** each time a diagnostic is run and is associated with an instance of **DiagnosticCompletionRecord.**

DiagnosticCompletionRecord

An instance of **DiagnosticCompletionRecord** stores the results of each **RunDiagnostic** execution.

Profile Class

RegisteredDiskDriveLiteProfile

Only one instance of this class is needed. It resides in the **Interop** namespace and indicates the implementation of the **Disk Drive Lite Profile.** The **InstanceID** property is set to a value of *SNIA:DiskDriveLiteProfile-1.4.0.* The **RegisteredOrganization** property is set to a value of *11* (SNIA). The **RegisteredName** property is set to a value of *Disk Drive Lite Profile*. The **RegisteredVersion** property is set to a value of *1.4.0.*

RegisteredDAPortsProfile

Only one instance of this class is needed. It resides in the **Interop** namespace and indicate the implementation of the **DA Ports Profile.** The **InstanceID** property is set to a value of *SNIA:DAPortsProfile-1.4.0.* The **RegisteredOrganization** property is set to a value of *11* (SNIA). The **RegisteredName** property is set to a value of *Direct Access Ports Profile*. The **RegisteredVersion** property is set to a value of *1.4.0.*

RegisteredStorageHBAProfile

Only one instance of this class is needed. It resides in the **Interop** namespace and indicate the implementation of the **Storage HBA Profile.** The **InstanceID** property is set to a value of *SNIA:StorageHBAProfile-1.4.0.* The

RegisteredOrganization property is set to a value of *11* (SNIA). The **RegisteredName** property is set to a value of *Storage HBA Profile*. The **RegisteredVersion** property isset to a value of *1.4.0.*

RegisteredHostDiscoveredResourcesProfile

Only one instance of this class is needed. It resides in the **Interop** namespace and indicate the implementation of the **Host Discovered Resources Profile**. The **InstanceID** property is set to a value of *SNIA:HostDiscoveredResourcesProfile-1.2.0.* The **RegisteredOrganization** property is set to a value of *11* (SNIA). The **RegisteredName** property is set to a value of *Host Discovered Resources Profile*. The **RegisteredVersion** property is set to a value of *1.2.0.*

RegisteredPCIDeviceProfile

Only one instance of this class is needed. It resides in the **Interop** namespace and indicate the implementation of the **PCI Device Profile.** The **InstanceID** property is set to a value of *DMTF:DSP1075-PCIDevice-1.0.0a*. The **RegisteredOrganization** property is set to a value of *2* (DMTF). The **RegisteredName** property is set to a value of *PCI Device Profile.* The **RegisteredVersion** property is set to a value of *1.0.0a.*

RegisteredSoftwareInventoryProfile

Only one instance of this class is needed. It resides in the **Interop** namespace and indicate the implementation of the **Software Inventory Profile**. The **InstanceID** property is set to a value of *DMTF:DSP1023-SoftwareInventory-1.0.*1. The **RegisteredOrganization** property is set to a value of *2* (DMTF). The **RegisteredName** property is set to a value of *Software Inventory Profile.* The **RegisteredVersion** property is set to a value of *1.0.1.*

RegisteredSoftwareUpdateProfile

Only one instance of this class is needed. It resides in the **Interop** namespace and indicate the implementation of the **Software Update Profile**. The **InstanceID** property is set to a value of *DMTF:DSP1023-SoftwareUpdate-1.0.0*. The **RegisteredOrganization** property is set to a value of *2* (DMTF). The **RegisteredName** property is set to a value of *Software Update Profile*. The **RegisteredVersion** property is set to a value of *1.0.0.*

RegisteredPhysicalAssetProfile

Only one instance of this class is needed. It resides in the **Interop** namespace and indicate the implementation of the **Physical Asset Profile**. The **InstanceID** property is set to a value of *DMTF:PhysicalAssetProfile-1.0.2.* The **RegisteredOrganization** property is set to a value of *2* (DMTF). The **RegisteredName** property is set to a value of *Physical Asset Profile*. The **RegisteredVersion** property is set to a value of *1.0.2*.

RegisteredSensorsProfile

Only one instance of this class is needed. It resides in the **Interop** namespace and indicate the implementation of the **Sensors Profile**. The **InstanceID** property is set to a value of *SNIA:SensorsProfile-1.0.0*. The **RegisteredOrganization** property is set to a value of *11* (SNIA). The **RegisteredName** property is set to a value of *Sensors Profile*. The **RegisteredVersion** property is set to a value of *1.0.0.*

RegisteredCommonDiagnosticProfile

Only one instance of this class is needed. It resides in the **Interop** namespace and indicate the implementation of the **Common Diagnostic Model Profile**. The **InstanceID** property is set to a value of *DMTF:DiagnosticsProfile-*

2.0.0a. The **RegisteredOrganization** property is set to a value of *2* (DMTF). The **RegisteredName** property isset to a value of *Diagnostics Profile*. The **RegisteredVersion** property isset to a value of *2.0.0a*.

Indications

An indication is generated periodically when a serious condition exists for a particular ioMemory device. The Fusion-io SMI-S CIM provider currently supports twenty different indications. They alert users of the SMI-S provider to conditions, such as imminent wearout, degradation of writability, degradation of the flashback feature, high temperature and internal error states. The indications are instances of the **FIO_AlertIndication** class that specializes the **CIM_AlertIndication** class.

Indication Format

The properties **MessageID, MessageFormatString,** and **MessageArguments** are defined in the **Fusion-io Alert Message Registry**, which is installed with the provider.

Property	Value
IndicationIdentifier	See below for each type
IndicationTime	Timestamp when sent
AlertingManagedElement	root/fio:FIO_IoMemoryPort.DeviceID=…
AlertingElementFormat	CIM Object Path (2)
OtherAlertingElementFormat	Not used
AlertType	Device Alert (5)
PerceivedSeverity	See below for each type
ProbableCause	See below for each type
SystemCreationClassName	“FIO_ComputerSystem”
SystemName	<hostname>
ProviderName	“fiosmis”
CorrelatedIndications	Not used
Description	Alert description
OtherAlertType	Not used
OtherSeverity	Not used
ProbableCauseDescription	Not used
EventID	Not used
OwningEntity	“Fusion-io”

Property	Value
MessageID	See below for each type
MessageFormatString	See below for each type
MessageArguments	<FIO_IoMemoryPort.DeviceID>

The properties **MessageID, MessageFormatString,** and **MessageArguments** are defined in the **Fusion-io Alert Message Registry,** which is installed with the provider.

Indication Values

Failed State indication

If the device is in an internal error state, the error indication is generated.

Property	Value
IndicationIdentifier	<mfr>:<hostname>:failed
PerceivedSeverity	Major (5)
ProbableCause	Other (1)
MessageID	FIO_0001
MessageFormatString	“Device <Device ID> has experienced an internal error”

Minimal Mode indication

If the device is currently running in a minimal state, the minimal mode indication is sent. When the device is in minimal mode, the reason can be found in the **MinimalModeReason** property of the **IOMemoryPort** instance.

Property	Value
IndicationIdentifier	<mfr>:<hostname>:minimal
PerceivedSeverity	Minor (4)
ProbableCause	Other (1)
MessageID	FIO_0002
MessageFormatString	“Device <Device ID> is currently running in a minimal state”

Slot Bandwidth indications

If the device is currently installed in a PCI slot with suboptimal or incompatible bandwidth characteristics, the corresponding indication is generated.

Property	Value
IndicationIdentifier	<mfr>:<hostname>:slot_<suboptimal/incompatible>
PerceivedSeverity	Degraded (3) / Minor (4)
ProbableCause	Bandwidth Reduced (4)
MessageID	FIO_0003/FIO_0004
MessageFormatString	“Device <Device ID> is installed in a PCI-°© -e slot with <suboptimal/incompatible> bandwidth”

Reduced writability indication

The ioMemory device driver can dramatically reduce write throughput to manage device conditions such as excessive wear, high temperature and insufficient power. The reduced writability indication is generated while the drive is in this mode. If the triggering condition is excessive wear, the **IOMemoryPort** health percentage reports 0% health. The reason for reduced writability can be found in the **ReducedWritabilityReason** property of the **IOMemoryPort** instance.

Property	Value
IndicationIdentifier	<mfr>:<hostname>:write_reduced
PerceivedSeverity	Degraded/Warning (3)
ProbableCause	Other(1)
MessageID	FIO_0005
MessageFormatString	“Device <Device ID> has reduced its write performance”

Read-only indication

When the drive has reached the end-of-life, it can no longer be written to and can only be read from. The read-only indication is sent when this occurs. The **IOMemoryPort** health percentage continues to report 0% health when this happens.

Property	Value
IndicationIdentifier	<mfr>:<hostname>:read_only
PerceivedSeverity	Degraded/Warning (3)
ProbableCause	Other(1)
MessageID	FIO_0006
MessageFormatString	“Device <Device ID> is not allowing write operations”

Temperature indications

The ioMemory device reports when an internal temperature threshold has been crossed. Only the highest threshold that has been crossed generates indications.

Property	Value
IndicationIdentifier	<mfr>:<hostname>:temperature_ <warning/critical/shutdown>
PerceivedSeverity	Degraded (3)/Major (6)/Major (6)
ProbableCause	Temperature Unacceptable (51)
MessageID	FIO_0007/FIO_0008/FIO_0009
MessageFormatString	“The temperature of Device <Device ID> has exceeded the <warning/critical/shutdown> threshold.”

Internal voltage indications

If the ioMemory device detects that its internal voltages have exceeded safe limits, the device shuts down to prevent damage or data corruption. An indication is generated if this condition is detected.

Property	Value
IndicationIdentifier	<mfr>:<hostname>:voltage_<core/aux>
PerceivedSeverity	Fatal (7)
ProbableCause	Power Problem (36)
MessageID	FIO_0010/FIO_0011
MessageFormatString	“The internal <core/IO supply> voltage of Device <Device ID> is outside of safe limits. The device has stopped allowing I/O operations”

Flashback indication

If a catastrophic part failure degrades the effectiveness of the flashback feature, this indication is sent. This condition cannot occur in the 3.x or newer series of Fusion-io ioMemory device VSL drivers.

Property	Value
IndicationIdentifier	<mfr>:<hostname>:flashback
PerceivedSeverity	Major (5)
ProbableCause	Protection Mechanism Failure (114)
MessageID	FIO_0012
MessageFormatString	“Device <Device ID> has exhausted its Flashback protection”

PCI -e error indications

If the ioMemory device detects errors on the PCI -e communications channel, an indication is generated, indicating the severity of errors detected.

Property	Value
IndicationIdentifier	<mfr>:<hostname>:pcie_<correctable/uncorrectable>
PerceivedSeverity	Degraded (3)
ProbableCause	Other(1)
MessageID	FIO_0013/FIO_0014
MessageFormatString	“Device <Device ID> has experienced <correctable/uncorrectable> PCI -e errors.”

Powerloss protection indication

The ioMemory device has a powerloss protection feature to reduce the risk of data loss in the event of a power failure. An indication is generated when this feature is available, but disabled.

Property	Value
IndicationIdentifier	<mfr>:<hostname>:powerloss
PerceivedSeverity	Degraded (5)
ProbableCause	Configuration (8)
MessageID	FIO_0015
MessageFormatString	“Powerloss protection has been disabled on device <Device ID>”

Reserve space indications

As the drive wears out, an indication is generated as a warning when drive health percentage drops below 10%, before write throughput is reduced. An indication is also generated when drive health drops to 0 to signal the user that further use results in the device reducing or disabling write operations.

Property	Value
IndicationIdentifier	<mfr>:<hostname>:reserves_<low/depleted>
PerceivedSeverity	Degraded/Warning (3)
ProbableCause	Threshold Crossed (52)
MessageID	FIO_0016/FIO_0017
MessageFormatString	“Device <Device ID> <is approaching/has surpassed> the wearout threshold”

PCI -e power budget indication

An indication is generated if the ioMemory device is drawing excessive power, based on the power rating of the PCI -e slot in which the device is installed.

Property	Value
IndicationIdentifier	<mfr>:<hostname>:overpower
PerceivedSeverity	Degraded/Warning (3)
ProbableCause	Power Problem (36)
MessageID	FIO_0018
MessageFormatString	“Device <Device ID> has exceeded the power budget of the PCI -e slot.”

Missing LEB map indication

An indicationn is generated if the ioMemory device is missing a persistent LEB map, which prevents the device from being attached.

Property	Value
IndicationIdentifier	<mfr>:<hostname>:lebmap
PerceivedSeverity	Minor (4)
ProbableCause	Other (1)
MessageID	FIO_0019
MessageFormatString	“Device <Device ID> is missing a LEB map and cannot be attached.”

Upgrade in Progress indication

An indication is generated if the device is currently in the process of upgrading to a new major version of the Fusion-io ioMemory device VSL driver, and requires a low-level reformat before it can be used.This prevents the device from being attached.

Property	Value
IndicationIdentifier	<mfr>:<hostname>:upgrade
PerceivedSeverity	Minor (4)
ProbableCause	Other (1)
MessageID	FIO_0020
MessageFormatString	“Device <Device ID> is in the process of upgrading to a new major version of the Fusion -io driver. Device must be formatted before use.”

Installing the SMI-S Provider on Linux

The Fusion-io SMI-S provider implements a standard WBEM interface based on DMTF and SNIA standards for remote management of Fusion-io products including the ioDrive, ioDrive Duo and ioOctal. The provider is CMPI-based and should work with popular CIMOMs including SFCB, OpenPegasus, and OpenWBEM.

Software dependencies

The Fusion-io ioMemory device CIM provider requires the following software to be installed and functioning properly:

- Fusion-io ioMemory device VSL driver (2.x or 3.x series driver)
- Fusion-io ioMemory device VSL SDK (version must match driver)
- Package `libfio` for 2.x driver on Linux
- Package `libvsl` for 3.x driver on Linux
- Included in Windows driver installation
- Must match the architecture (32/64-bit) of the Fusion-io CIM provider

In addition, the following open-source libraries must be installed on Linux host systems. No source code from these libraries is included in the Fusion-io CIM provider, but it requires linking dynamically to the libraries at runtime:

• `libuuid`

• `libblkid`

Hardware support

The Fusion-io ioMemory device CIM provider supports all Fusion-io ioMemory devices. The CIM provider works with any 2.x or 3.x series Fusion-io VSL driver, and has no requirement on minimum firmware versions of connected devices. Each version of the Fusion-io VSL driver may require a minimum firmware version in order for connected devices to work properly, but this does not prevent those devices from being displayed in the CIM provider.

Platforms supported

- Redhat Enterprise Server 5
- Redhat Enterprise Server 6
- SUSE Linux Enterprise Server 10
- SUSE Linux Enterprise Server 11

Driver Installation

⚠ For the following instructions, replace * with the specific filename info.

1. Install the driver packages on a RHEL 5 64-bit system with ioMemory device(s):

```
$ rpmbuild --rebuild iomemory-vsl-*.src.rpm
$ rpm -i /usr/src/redhat/RPMS/x86_64/iomemory-vsl-*.x86_64.rpm
```

2. Install the utilities and firmware:

```
$ rpm -i fio-util-*.x86_64.rpm
$ rpm -i fio-firmware-*.noarch.rpm
```

3. Start the driver:

```
$ modprobe iomemory-vsl
```

4. Update firmware if necessary:

```
$ fio-update-iodrive /usr/share/fio/firmware/iodrive_101971.fff
```

5. Check drive status:

```
$ fio-status
```

6. Check CIM Provider Installation:

```
$ rpm -i fio-smis-*.rpm
```

Fusion-io CIM provider updates cached data from Fusion-io VSL SDK on a regular interval. Currently, this interval is configured as once every 15 seconds. Future releases of the CIM provider may expose this value to user configuration to allow for tuning the update interval as desired. This interval is also used to check for the conditions that generate indications.

A README file is distributed with each release and contains information about new features, bug fixes, known issues and specific installation details.

Linux Testing

The `cimcli` utility can be used to test the SMI-S provider.

Query the provider for the driver version and the firmware version for each IoDimm in the system:

```
$ cimcli -n root/fio ei FIO_SoftwareIdentity
```

The output should look similar to this (values may change as development continues):

```
//Instance of FIO_SoftwareIdentity
instance of FIO_SoftwareIdentity
{
Caption = "Software Identity";
Description = "A class derived from SoftwareIdentity representing the FIO driver
```

```
software.";
ElementName = "FIO driver software";
...
InstanceID = "FIO:host:driver";
MajorVersion = 1;
MinorVersion = 3;
RevisionNumber = 0;
BuildNumber = NULL;
...
VersionString = "1.3.0";
...
};
path= FIO_SoftwareIdentity.InstanceID="FIO:fct0:firmware"
//Instance of FIO_SoftwareIdentity
instance of FIO_SoftwareIdentity
{
Caption = "Software Identity";
Description = "A class derived from SoftwareIdentity representing FIO drive
firmware.";
ElementName = "Firmware for FIO drive 10000";
...
InstanceID = "FIO:fct0:firmware";
MajorVersion = 4;
MinorVersion = 0;
RevisionNumber = 1;
BuildNumber = 36897;
...
VersionString = "4.0.1.36897";
...
};
Query the SMI-S provider for each ioDimm's health:
cimcli -n root/fio ei FIO_IoMemoryPort
The output should look something like this (values may change as development
continues):
//Instance of FIO_IoMemoryPort
instance of FIO_IoMemoryPort
{
InstanceID = "FIO:fct0:drive";
Caption = "ioDimm";
Description = "A class derived from DAPort representing a FIO drive.";
...
SystemName = "host";
...
State = 1;
...
Writability = 1;
ReducedWritabilityReason = NULL;
HealthLevel = 1;
HealthPercentage = 95;
```

```
...
FlashbackAvailability = TRUE;
...
WriteRegulationLevelActual = 1;
WriteRegulationLevelLifespan = 1;
WriteRegulationLevelPower = 1;
WriteRegulationLevelThermal = 1;
...
ConfiguredMinimumLifespanDate = "2015-07-03";
};
Query capacity and usage counters of a specific ioDimm (in this case fct0):
$ cimcli -n root/fio ei FIO_SSDStatistics
The output should look something like this (values may change as development
continues):
//Instance of FIO_SSDStatistics
instance of FIO_SSDStatistics
{
Caption = "SSD Statistics";
Description = "A class derived from StatisticalData representing the individual
statistics of a FIO drive.";
InstanceID = "FIO:fct0:stats";
ElementName = "Statistics for FIO drive fct0";
...
UsableDataMByteCapacity = 343597;
TotalLogicalMByteCapacity = NULL;
PhysicalMBytesRead = 3906848424;
PhysicalMBytesWritten = 1176325487;
ReadOperations = 1449386155;
WriteOperations = 958639238;
CurrentMByteRAMUsage = 18446744071796534236;
PeakMByteRAMUsage = 18446744072718038771;
};
```

Debugging

The Fusion-io CIM provider is equipped with an internal logging mechanism based on the `log4cxx` framework. By default, the logs are configured to only display *Informational, Warning,* and *Error* level messages. If more detailed output is desired, the logs can be configured with a debug mode that generates additional informtion. To enable debug logging, edit the logging configuration file (`logcfg_smis.properties`) and replace the line:

```
log4j.rootLogger=info, R
```

with the following:

```
log4j.rootLogger=debug, R
```

End User License Agreement

The following is a copy of the End User License Agreement that you are required to agree to in order to install and use ioSphere Management Solution:

FUSION-IO END-USER LICENSE AGREEMENT (11.9.12)

IMPORTANT - PLEASE READ CAREFULLY BEFORE INSTALLING OR USING THIS SOFTWARE PRODUCT: This end-user license agreement ("Agreement") is a legal agreement between you (either an individual or the entity you represent) ("you") and Fusion-io, Inc. ("Fusion-io") that governs your use of any general availability release of the software product in executable object code provided to you with this Agreement, as well as the related user guide, Utilities, and Documentation (collectively, the "Software") and your use of any beta release of a software product in executable object code provided to you with this Agreement, as well as the related, user guide, Utilities, and Documentation (collectively, "Beta Software"). The Software and Beta Software are interchangeably referred to in this Agreement as the "Product."

RIGHTS IN THE PRODUCT ARE OFFERED ONLY ON THE CONDITION THAT YOU AGREE TO ALL TERMS AND CONDITIONS OF THIS AGREEMENT. BY INSTALLING, COPYING, DOWNLOADING, OR OTHERWISE USING THE PRODUCT, YOU AGREE TO BE BOUND BY THIS AGREEMENT. IF YOU DO NOT ACCEPT THIS AGREEMENT, DO NOT INSTALL, DOWNLOAD, OR OTHERWISE USE THE PRODUCT.

1. DEFINITIONS

1.1 "Documentation" means the most current version of any documentation, in all forms, that formally describes the use, function, or technical details of the Product (e.g., reference manuals, user manuals, on-line help files, and training manuals) provided to you for use with the Product in accordance with this Agreement.

1.2 "Error" means a failure of the Software to perform substantially in accordance with the applicable material technical and functional specifications set forth in the Documentation, which failure is reproducible by Fusion-io on an unmodified copy of the most current Release of the Software (excluding faults in the Documentation itself).

1.3 "Maintenance Services" means the maintenance services described in Section 3.3.

1.4 "Release" means a Maintenance Release or a Major Release that is provided to you as part of the Maintenance Services in accordance with Section 3.3.

(a) "Maintenance Release" means a version of the Software that incorporates Error corrections or provides minor functional or performance improvements. Maintenance Releases do not include Major Releases.

(b) "Major Release" means a version of the Software that provides substantial functional or performance improvements. Fusion-io will determine in its sole discretion whether a modification to the Software is a Major Release or a Maintenance Release.

1.5 "Scope Limitations" means the limitations on the scope of the licenses granted to you under this Agreement that are specified in the user guide or the product installation guide for the Product.

1.6 "Unauthorized Use" means any use, possession, knowledge, viewing, inspection, examination, copying, disclosure, or other activity involving any part of the Product that is not expressly authorized under this Agreement or otherwise in writing by Fusion-io.

1.7 "Utilities" means the most current version of any utility file designed to operate with, supplement, optimize, configure, or maintain the Product that is made available to you for use with the Product.

2. LICENSE GRANTS

2.1 License to the Software. Subject to the terms and conditions of this Agreement, Fusion-io grants to you a limited, worldwide, non-exclusive, perpetual (subject to termination in accordance with the terms of this Agreement), non-transferable (except as permitted in Section 11.4) license, without right of sublicense to: (a) reproduce, without modification, executable object code copies of the Software; (b) install copies of the Software on computers operated by or for you; (c) internally use installed copies of the Software as described in the Scope Limitations; and (d) reproduce, without modification, and internally use a reasonable number of copies of the Documentation and Utilities solely in connection with use of the Software. Each of the rights granted in this Section 2.1 is subject to the Scope Limitations and contingent upon your compliance with the Scope Limitations. This Agreement applies to each Release unless Fusion-io provides other terms with the Release. In case of a conflict between this Agreement and such other terms, the other terms will prevail.

2.2 Evaluation License. If Fusion-io has provided you with a copy of the Software solely for internal evaluation to determine whether you will purchase a license or subscription to the Software, Fusion-io grants to you a limited, non-exclusive, non-transferable license, without right of sublicense, to internally use the Software, without modification, solely for evaluation purposes during the Evaluation Period ("Evaluation License"). The "Evaluation Period" means the 30 days following the date you initially download the Software unless Fusion-io agrees in writing to extend the period or otherwise to a longer Evaluation Period for a specified period of time. The Software may be used only by those of your employees that must have access to the Software in order to permit you to evaluate the Software. Your Evaluation License does not grant the rights provided for in Sections 2.1, 3.3, 3.4, 7.2(b), or 7.2(c).

2.3 License to Use Beta Software. If Fusion-io has provided you with Beta Software, Fusion-io grants you a non-sub-licensable, nontransferable, nonexclusive, limited license to: (a) use one copy of the Software; and (b) make

a single copy of the Software for backup or archival purposes only, as long as the copy contains all of the original proprietary notices ("Beta License"). Your Beta License does not grant the rights provided for in Sections 2.1, 3.3, 3.4, 7.2(b), or 7.2(c).

2.4 Third Party Software. The Product may contain or be distributed with third party software covered by an open source software license ("Open Source Software") or by a license other than that granted by this Agreement ("Third Party Software"). If Open Source Software is included, the terms and conditions of this license do not apply to the Open Source Software. If Third Party Software is included, the terms and conditions of this license may not apply to Third Party Software. Information concerning the inclusion of Open Source Software and Third Party Software, if any, and the notices, license terms, and disclaimers applicable to that software are generally contained in a corresponding license file identified with file names such as "notice," "license," "license.txt," "readme," "readme.txt," or "copying"; you should contact Fusion-io support if you cannot locate the Open Source Software or Third Party Software license for the Product. If, in a notice file, Fusion-io identifies code as "Modifiable Code", Fusion-io authorizes you to a) modify the Modifiable Code, and b) reverse engineer the Product modules that directly interface with the Modifiable Code, provided you do so only for the purpose of debugging your modifications to the Modifiable Code. If the Open Source Software licenses include a license that provides for the availability of source code (e.g., the GNU General Public License) and the corresponding source code is not included with the Product, check Fusion-io's product support pages to learn how to obtain such source code.

2.5 Reservation of Rights. The Product is licensed, not sold, by Fusion-io to you under this Agreement, and nothing in this Agreement will be interpreted or construed as a sale or purchase of the Product. You will not have any rights in or to the Product except as expressly granted in this Agreement. Fusion-io reserves to itself all rights to the Product not expressly granted to you in accordance with this Agreement. Fusion-io retains all copyright, patent, and other intellectual property rights in and to the Product. You acknowledge that the Product, all copies of the Product, any derivative works, compilations, and collective works of the Product, and any know-how and trade secrets related to the Product are the sole and exclusive property of Fusion-io and contain Fusion-io's confidential and proprietary materials.

3. KEYS, DEPLOYMENT, MAINTENANCE SERVICES, and support services

3.1 Delivery of Keys. Fusion-io has delivered, or will deliver to you a key to install and access the Product. You are responsible for the use of keys assigned to you. You may not share the keys with third parties. You may not use any key that is assigned to a third party. If this Agreement grants you an Evaluation License, your key or the Software may include disabling code, which may be used to disable the Software. Fusion-io may use such disabling code to ensure that you do not continue to use the Software longer than the term of your Evaluation License. Upon the expiration of your Evaluation License, and if Fusion-io has not granted you an extension, the Software may cease to function in

some or all respects and you may lose access to data made with or stored using the Software. You acknowledge that the disabling of the Software is a key feature of the Evaluation License rights and responsibilities covered by this Agreement.

3.2 Deployment Services. You are solely responsible for the deployment of the Product for operation, including installation, configuration, integration, and testing, unless you have contracted to have Fusion-io perform such deployment services in accordance with the terms of Fusion-io's professional services agreement.

3.3 Maintenance Services. Fusion-io will provide you with Maintenance Services for so long as you are current with your payment of the Maintenance Services subscription fees. Maintenance Services are provided under the following terms:

(a) Fusion-io will use reasonable efforts to correct (e.g., by providing a workaround or correction) verified Errors with a level of effort commensurate with the severity of the Error. Fusion-io is not, however, obligated to correct all Errors.

(b) Within a reasonable time after general commercial publication, Fusion-io will make available to you one copy of all Maintenance Releases and all corrections to the associated Documentation. You may purchase Major Releases for an additional fee.

(c) Fusion-io reserves the right, in its sole discretion, to create a Major Release of the Software. Fusion-io will support a Release of the Software for a period of six months from the first production ship date of the Major Release that supersedes it or from the discontinuation date, as applicable. Special support prices may apply for the support of outdated or discontinued Releases of the Software after the initial six-month period.

(d) Unless otherwise expressly agreed to in writing by Fusion-io, Fusion-io is not obligated to provide Maintenance Services related to: (i) your failure to implement all Releases and Error corrections and workarounds provided by Fusion-io; (ii) changes to the operating system or hardware environment on which the Software operates; (iii) modification of or addition to the Software; (iv) improper installation of the Software; (v) interconnection of the Software with third party software or hardware not furnished by Fusion-io or not specified in the Documentation for use with the Software; or (vi) use of the Software in a manner for which it was not designed or beyond the scope of the license set forth in the Agreement.

(e) Unless otherwise expressly agreed to in a separate agreement by Fusion-io, the Maintenance Services do not include: (i) visits to your site; (ii) any work with or relating to any third party equipment or software; (iii) any installation, configuration, integration, or setup of the Software; (iv) consultation with your end users, distributors, or manufacturers; or (v) any professional services associated with the Software, including without limitation

any custom development, training and knowledge transfer, or other services that may be covered in any service agreement with Fusion-io or any third party.

(f) You will provide Fusion-io with reasonable access to all necessary personnel to answer questions regarding Errors and other problems reported by you. You will promptly implement all Releases, Error corrections, and workarounds provided by Fusion-io. You must supervise, control, and manage the use of the Software. In addition, you are responsible for archiving your data to mitigate against losses that may be caused by Errors. In order to provide Error corrections, workarounds, and Releases, Fusion-io may require you to upgrade, at your own cost, your hardware and software systems to Fusion-io's then-current supported versions of system components.

(g) The provision of the Maintenance Services by Fusion-io is contingent upon your performance of your obligations under this Agreement. Fusion-io reserves the right, in addition to other remedies that are available, to suspend its provision of the Maintenance Services for so long as you are not current with your obligations.

3.4 Support Services. Fusion-io will provide you with Support Services for so long as you are current with your payment of the Support Services subscription fees. "Support Services" means Fusion-io's provision of telephone and email support consisting of (a) assistance related to questions on the operational use of the Software; (b) assistance with identifying and verifying causes of suspected Errors; and (c) providing workarounds for verified Errors when reasonably available to Fusion-io.

4. LICENSEE OBLIGATIONS

4.1 General Restrictions. Except as otherwise explicitly provided in this Agreement or as may be expressly permitted by applicable law, you will not, and will not permit or authorize third parties to: (a) reproduce, modify, translate, enhance, decompile, disassemble, reverse engineer, or create derivative works of the Product; (b) rent, lease, or sublicense the Product; (c) use the Product on a service bureau or application service provider basis; (d) provide, divulge, disclose, or make available to, or permit the use of the Product by any third party; nor (e) circumvent or disable any technological features or measures in the Product.

4.2 Proprietary Rights Notices. You will neither alter nor remove any copyright notice or other proprietary rights notices that may appear on any part of the Product. In addition, when reproducing any part of the Product in accordance with this Agreement, you must include all copyright and other proprietary rights notices as are currently contained on each part of the Product.

4.3 Compliance with Laws. You will at all times comply with all applicable laws, statutes, ordinances, and regulations in connection with your use of the Product, and refrain from any unethical conduct or any other conduct that tends to damage the reputation of Fusion-io or the Product. You will inform Fusion-io of any requirements of laws, statutes, ordinances, rules, and regulations of all

governmental authorities that directly or indirectly affect your use of the Product.

4.4 Government Restricted Rights. If the Product is licensed for use by the United States or for use in the performance of a United States government prime contract or subcontract, the Product is delivered as: (a) "commercial computer software" as defined in DFARS 252.227-7014 Rights in Noncommercial Computer Software and Noncommercial Computer Software Documentation (Feb. 2012); (b) as a "commercial item" as defined in FAR 2.101; or (c) as "restricted computer software" as defined in FAR 52.227-14(a), Rights in Data--General (Dec. 2007); whichever is applicable. The use, duplication, and disclosure of the Product by the Department of Defense shall be subject to the terms and conditions set forth in this Agreement as provided in DFARS 227.7202 (Dec. 2011). All other use, duplication and disclosure of the Product by the United States shall be subject to the terms and conditions set forth in this Agreement and the restrictions contained in subsection DFARS 252.227-7013(b)(3)(i), Rights in Technical Data and Computer Software (Feb. 2012), and FAR 52.227-19(b), Commercial Computer Software--Restricted Rights (Dec. 2007). As used in FAR and DFARS, contractor/licensor is Fusion-io, Inc. 2855 E. Cottonwood Parkway, Suite 100, Salt Lake City, UT 84121.

4.5 Export. The Product may be subject to United States export control laws, including the U.S. Export Administration Act and its associated regulations, and may be subject to export or import regulations in other countries. You must comply strictly with all such regulations that are now or later in effect and acknowledge that you have the responsibility to obtain licenses to export, re-export, or import the Product. You represent that: (a) you are not a citizen, national, or resident of, and you are not under the control of, the government of Cuba, Iran, Sudan, Iraq, Libya, North Korea, Syria, nor any country to which the United States has prohibited export; (b) you will not download or otherwise export or re-export the Product, directly or indirectly, to the above mentioned countries nor to citizens, nationals or residents of those countries; (c) you are not listed on the United States Department of Treasury lists of Specially Designated Nationals, Specially Designated Terrorists, and Specially Designated Narcotic Traffickers, nor are you listed on the United States Department of Commerce Table of Denial Orders; (d) you will not download or otherwise export or re-export the programs, directly or indirectly, to persons on the above mentioned lists; and (e) you will not use the Product for, and will not allow the Product to be used for, any purposes prohibited by United States law, including, without limitation, for the development, design, manufacture or production of nuclear, chemical or biological weapons of mass destruction.

4.6 No Warranties. You will not make or publish any representations, warranties, or guarantees on behalf of Fusion-io concerning the Product without Fusion-io's specific prior written approval.

4.7 Protection against Unauthorized Use. You acknowledge that the Product furnished to you by Fusion-io involve valuable proprietary rights of Fusion-io. You will take appropriate steps and precautions for the protection of the Product. Without limiting the generality of the foregoing, you will use your

best efforts to prevent any Unauthorized Use and immediately notify Fusion-io in writing of any Unauthorized Use that comes to your attention. In the event of any Unauthorized Use by anyone who obtained access to the Product directly or indirectly through you or any of your employees, agents, representatives, or contractors, you will take all steps reasonably necessary to terminate such Unauthorized Use and to retrieve any copy of the applicable Product in the possession or control of the person or entity engaging in such Unauthorized Use. You will provide to Fusion-io such cooperation and assistance related to any such Unauthorized Use as Fusion-io may reasonably request.

4.8 Restrictions on Use of Beta Software. You may not use Beta Software in a live production environment or in conjunction with revenue bearing traffic.

4.9 Feedback. If Fusion-io has provided you with a copy of Beta Software in order to help Fusion-io prepare the Beta Software for commercial release, you will provide feedback to Fusion-io concerning the functionality and performance of the Beta Software, including identifying potential errors and improvements ("Feedback"). If Fusion-io grants you an Evaluation License, you may provide such Feedback to Fusion-io regarding your use of the Software. You hereby assign to Fusion-io all right, title, and interest in and to the Feedback you provide. Fusion-io may use the Feedback, free of charge, without obtaining your consent.

4.10 Confidentiality Required Under Beta License and Evaluation License. Beta Software has not been made available to the public and Fusion-io desires to maintain the confidentiality of the Beta Software until it is commercially released. If Fusion-io has provided you with Beta Software or has provided you with the Software solely for evaluation purposes, you will take reasonable steps to maintain the confidentiality of and not disclose to any third party: (a) the terms of this EULA, (b) all non-public information disclosed by Fusion-io to you under this EULA, and (c) all Feedback, performance data, and other information obtained through your testing and evaluation.

5. FEES AND PAYMENT

5.1 Fees and Payment Terms

(a) You will pay Fusion-io the license fees, Maintenance Services subscription fees, Support Services subscription fees, and any other amounts owing under this Agreement, plus any applicable sales, use, excise, or other taxes, as specified in your quote or order form.

(b) Any amount not paid when due will be subject to finance charges equal to 1.5% of the unpaid balance per month or the highest rate permitted by applicable usury law, whichever is less, determined and compounded daily from the date due until the date paid. You will reimburse any costs or expenses (including, but not limited to, reasonable attorneys' fees) incurred by Fusion-io to collect any amount that is not paid when due. Fusion-io may accept any check or payment in any amount without prejudice to Fusion-io's right to recover the balance of the amount due or to pursue any other right or remedy. Amounts due from you under this Agreement may not be withheld or offset by you against amounts due to you for any reason. Unless otherwise specified in your quote or

order form, all amounts payable under this Agreement are denominated in United States dollars, and you will pay all such amounts in United States dollars.

5.2 Taxes. Other than state net income taxes and federal net income taxes imposed on Fusion-io by the United States, you will bear all taxes, duties, and other governmental charges (collectively, "taxes") resulting from this Agreement. You will pay any additional taxes as are necessary to ensure that the net amounts received by Fusion-io after all such taxes are paid are equal to the amounts which Fusion-io would have been entitled to in accordance with this Agreement as if the taxes did not exist.

5.3 Audit. During the term of this Agreement and for three years thereafter, you will keep current, complete, and accurate records regarding the reproduction and use of Product. You will provide such information to Fusion-io and certify that you have paid all fees required under this Agreement within five business days of any written request, so long as no more than four requests are made each year. You will, after reasonable prior notice from Fusion-io, provide Fusion-io reasonable access to your premises, records, and personnel so that Fusion-io may audit and confirm that you comply with this Agreement. If an audit reveals any reproduction, use, or distribution of the Product that is not compliant with this Agreement, you will promptly comply with this Agreement and make an additional payment as contemplated in this Agreement, plus interest at the rate specified in Section 5.1(b). If the amount of the underpayment is 5% or greater, you will promptly reimburse Fusion-io for its reasonable costs of conducting such audit.

6. TERM AND TERMINATION

6.1 Term. This Agreement will commence upon your acceptance of this Agreement and continue until terminated in accordance with this Agreement.

6.2 Notice of Material Breach or Default. If either party commits a material breach or default in the performance of any of its obligations under this Agreement, then the other party may give the defaulting party written notice of the material breach or default (including a statement of the facts relating to the material breach or default, the provisions of this Agreement that are in material breach or default, and the action required to cure the material breach or default) and of the non-defaulting party's intention to terminate the Agreement pursuant to Section 6.3 if the material breach or default is not cured within 30 days after the defaulting party's receipt of such notice (or such later date as may be specified in such notice). Without limiting the foregoing, any failure by you to timely pay to Fusion-io any amounts owing under this Agreement will constitute a material breach of this Agreement.

6.3 Notice of Termination. If the defaulting party fails to cure a material breach or default specified in any notice under Section 6.2 within 30 days after receipt of such notice (or such later date as may be specified in such notice), then the non-defaulting party may terminate this Agreement by giving the defaulting party written notice of termination. If you fail to timely pay any Maintenance Services subscription fees or Support Services Subscription fees, Fusion-io may, without limitation to any of its other rights or remedies, suspend

performance of Maintenance Services and the Support Services until it receives all amounts due.

6.4 Termination of Evaluation License. If Fusion-io grants you an Evaluation License under this Agreement, this Agreement will terminate upon the earliest of: (a) the conclusion of the Evaluation Period; (b) your breach of any of provision of this Agreement, or (c) your return, destruction, or deletion of all instances and copies of the Software in your possession.

6.5 Termination of Beta License. If this Agreement grants you a Beta License, this Agreement will terminate immediately upon the earliest of: (a) six months after a "generally available" version of the Beta Software is released; (b) one year after your initial download of the Beta Software; (c) your failure to comply with any term of this EULA; or (d) your return, destruction, or deletion of all instances and copies of the Beta Software in your possession.

6.6 Post-Termination Obligations. If this Agreement or any licenses in this Agreement are terminated for any reason, (a) you will pay to Fusion-io any fees, reimbursable expenses, compensation, or other amounts that have accrued prior to the effective date of the termination, (b) any and all liabilities accrued prior to the effective date of the termination will survive, and (c) you will immediately discontinue all use of the Product, uninstall the Product from your systems, destroy or return to Fusion-io all copies of the Product within five days of such termination, and immediately thereafter, if requested by Fusion-io, provide Fusion-io with a written certification signed by an authorized representative certifying that all copies of such Product have been destroyed and all use of such Product has been discontinued. Sections 1, 2.5, 3.1, 4, 5, 6, 7, 9, 10, and 11 survive termination or expiration of this Agreement and the licenses granted herein.

7. WARRANTIES AND DISCLAIMER

7.1 Mutual Warranties. Each party represents and warrants to the other that: (a) this Agreement has been duly executed and delivered and constitutes a valid and binding agreement enforceable against such party in accordance with its terms; (b) no authorization or approval from any third party is required in connection with such party's execution, delivery, or performance of this Agreement; and (c) the execution, delivery, and performance of this Agreement does not violate the laws of any jurisdiction or the terms or conditions of any other agreement to which it is a party or by which it is otherwise bound.

7.2 Performance Warranty

(a) Unless you have been granted an Evaluation License or a Beta License, Fusion-io warrants to you that the Software will perform without Errors during the 90-day period following delivery to you of the license key to the Software ("Warranty Period"). Software governed by an Evaluation License or a Beta License is provided "as is" and Fusion-io does not warrant that the Software or Beta Software will operate without error or interruption.

(b) If any portion of the Software fails to conform to the warranty in Section 7.2(a), your exclusive remedy, and Fusion-io's entire liability in

contract, tort, or otherwise, will be to use commercially reasonable efforts to provide a correction or workaround for any Error that is (a) reported to Fusion-io during the Warranty Period and (b) reproducible by Fusion-io on an unmodified copy of the most current Release of the Software. If after repeated efforts, Fusion-io is unable to provide a correction or workaround for a reported Error, then your exclusive remedy, and Fusion-io's entire liability in contract, tort, or otherwise, will be to terminate this Agreement and receive a refund of all license fees paid by you for the Software upon your return of the original and all copies of the Software in your possession, together with your certification that you have ceased all use, reproduction, and distribution of the Software.

(c) The warranty and remedies set forth in Sections 7.2(a)and 7.2(b) will not apply to the extent that a reported Error is caused in whole or in part by: (i) any defect in any portion of any third party software or hardware not furnished by Fusion-io or not specified in the Documentation for use with the Software; (ii) any modification or enhancement made to the Software by anyone other than Fusion-io; (iii) the failure of you to follow the most current instructions promulgated by Fusion-io with respect to the proper use of the Software; (v) the negligence of you or any third party; or (vi) Unauthorized Use of the Software. If Fusion-io determines that any warranty claim reported by you falls within any of the foregoing exceptions, you will pay Fusion-io for its services at Fusion-io's hourly rates then in effect.

7.3 Disclaimer. EXCEPT FOR THE EXPRESS REPRESENTATIONS AND WARRANTIES STATED IN THIS SECTION 7, FUSION-IO MAKES NO ADDITIONAL REPRESENTATION OR WARRANTY OF ANY KIND WHETHER EXPRESS, IMPLIED (EITHER IN FACT OR BY OPERATION OF LAW), OR STATUTORY, AS TO ANY MATTER WHATSOEVER. FUSION-IO EXPRESSLY DISCLAIMS ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR YOUR PURPOSE, QUALITY, ACCURACY, TITLE, AND NON-INFRINGEMENT. FUSION-IO DOES NOT WARRANT THAT THE PRODUCT IS ERROR-FREE OR THAT OPERATION OF THE PRODUCT WILL BE SECURE OR UNINTERRUPTED.

7.4 Risks of Using Beta Software. Fusion-io has not commercially released Beta Software, and Beta Software has not yet been tested like other commercially released software that you may use. Therefore, it is likely that Beta Software will contain errors, including errors that may cause the Beta Software or your computer or device to malfunction or cause a loss of data. If you do not wish to accept the risk of errors in the Beta Software, please do not install or use the Beta Software. Furthermore, Fusion-io is not obligated to correct errors, correct the effects of errors (e.g., fix your computer or recover lost data), or provide any technical support related to use of the Beta Software.

8. INTELLECTUAL PROPERTY INFRINGEMENT

8.1 Infringement Defense. Fusion-io will defend you from any actual or threatened third party claim that the Software infringes or misappropriates any U.S. patent issued as of the date you first accept this Agreement or any copyright or trade secret of any third party during the term of this Agreement if: (a) you give Fusion-io prompt written notice of the claim; (b) Fusion-io has full and complete control over the defense and settlement of the claim; (c) you

provides assistance in connection with the defense and settlement of the claim as Fusion-io may reasonably request; and (d) you comply with any settlement or court order made in connection with the claim (e.g., relating to the future use of any infringing materials).

8.2 Infringement Indemnification. Fusion-io will indemnify you against: (a) all damages, costs, and attorneys' fees finally awarded against you in any proceeding under Section 8.1; (b) all out-of-pocket costs (including reasonable attorneys' fees) reasonably incurred by you in connection with the defense of such proceeding (other than attorneys' fees and costs incurred without Fusion-io's consent after Fusion-io has accepted defense of such claim); and (c) if any proceeding arising under Section 8.1 is settled, all amounts to any third party agreed to by Fusion-io in settlement of any such claims.

8.3 Mitigation of Infringement Action. If your use of the Software is, or in Fusion-io's reasonable opinion is likely to become, enjoined or materially diminished as a result of a proceeding arising under Section 8.1, then Fusion-io will either: (a) procure you the continuing right to use the Software; (b) replace or modify the Software in a functionally equivalent manner so that it no longer infringes; or if, despite its commercially reasonable efforts, Fusion-io is unable to do either (a) or (b), Fusion-io will (c) terminate the licenses with respect to the Software subject to the infringement claim and refund to you an amount equal to the depreciated license fees paid by you (calculated on a straight line basis over a three-year life).

8.4 Exclusions. Fusion-io will have no obligation under this Section 8 for any infringement to the extent that it arises out of or is based upon: (a) the combination, operation, or use of the Software with third party software or hardware not furnished by Fusion-io or not specified in the Documentation for use with the Software if such infringement would have been avoided but for such combination, operation, or use; (b) use of the Software outside of the scope of the license granted to you; (d) your failure to use the latest Release of the Software or to comply with instructions provided by Fusion-io, if the alleged infringement would not have occurred but for such failure; (e) any modification of the Software not made by Fusion-io where such infringement would not have occurred absent such modification; or (f) Unauthorized Use of the Software. You will reimburse Fusion-io for any costs or damages that result from these actions.

8.5 Exclusive Remedy. This Section 8 states Fusion-io's sole and exclusive liability, and your sole and exclusive remedy, for the actual or alleged infringement of any third party intellectual property right by the Software.

9. LICENSEE INDEMNIFICATION

9.1 Defense. You will defend Fusion-io from any actual or threatened third party claim arising out of or based upon the your or a third party's use of the Product or your breach of any of the provisions of this Agreement if: (a) Fusion-io gives you prompt written notice of the claim; (b) you has full and complete control over the defense and settlement of the claim; (c) Fusion-io provides assistance in connection with the defense and settlement of the claim as you may

reasonably request; and (d) Fusion-io complies with any settlement or court order made in connection with the claim.

9.2 Indemnification. You will indemnify Fusion-io against: (a) all damages, costs, and attorneys' fees finally awarded against Fusion-io in any proceeding under Section 9.1; (b) all out-of-pocket costs (including reasonable attorneys' fees) reasonably incurred by Fusion-io in connection with the defense of such proceeding (other than attorneys' fees and costs incurred without your consent after you has accepted defense of such claim); and (c) if any proceeding arising under Section 9.1 is settled, you will pay any amounts to any third party agreed to by you in settlement of any such claims.

9.3 Exclusions. You will have no obligation under this Section 9 to the extent that Fusion-io is obligated under Section 8.1 to defend you against such third party claim. Fusion-io will reimburse you for any costs or damages that result from any such actions.

10. LIMITATIONS OF LIABILITY

10.1 Disclaimer of Consequential Damages. NOTWITHSTANDING ANYTHING TO THE CONTRARY CONTAINED IN THIS AGREEMENT, FUSION-IO WILL NOT, UNDER ANY CIRCUMSTANCES, BE LIABLE TO YOU FOR CONSEQUENTIAL, INCIDENTAL, SPECIAL, OR EXEMPLARY DAMAGES ARISING OUT OF OR RELATED TO THE TRANSACTION CONTEMPLATED UNDER THIS AGREEMENT, INCLUDING BUT NOT LIMITED TO LOST PROFITS OR LOSS OF BUSINESS, EVEN IF FUSION-IO IS APPRISED OF THE LIKELIHOOD OF SUCH DAMAGES OCCURRING.

10.2 Cap on Liability. UNDER NO CIRCUMSTANCES WILL FUSION-IO'S TOTAL LIABILITY OF ALL KINDS ARISING OUT OF OR RELATED TO THIS AGREEMENT (INCLUDING BUT NOT LIMITED TO WARRANTY CLAIMS), REGARDLESS OF THE FORUM AND REGARDLESS OF WHETHER ANY ACTION OR CLAIM IS BASED ON CONTRACT, TORT, OR OTHERWISE, EXCEED THE TOTAL AMOUNT PAID BY YOU TO FUSION-IO UNDER THIS AGREEMENT (DETERMINED AS OF THE DATE OF ANY FINAL JUDGMENT IN AN ACTION).

10.3 Independent Allocations of Risk. EACH PROVISION OF THIS AGREEMENT THAT PROVIDES FOR A LIMITATION OF LIABILITY, DISCLAIMER OF WARRANTIES, OR EXCLUSION OF DAMAGES IS TO ALLOCATE THE RISKS OF THIS AGREEMENT BETWEEN THE PARTIES. THIS ALLOCATION IS REFLECTED IN THE PRICING OFFERED BY FUSION-IO TO YOU AND IS AN ESSENTIAL ELEMENT OF THE BASIS OF THE BARGAIN BETWEEN THE PARTIES. EACH OF THESE PROVISIONS IS SEVERABLE AND INDEPENDENT OF ALL OTHER PROVISIONS OF THIS AGREEMENT. THE LIMITATIONS IN THIS SECTION 10 WILL APPLY NOTWITHSTANDING THE FAILURE OF ESSENTIAL PURPOSE OF ANY LIMITED REMEDY IN THIS AGREEMENT.

11. GENERAL

11.1 Notices. Any notice required or permitted to be given in accordance with this Agreement will be effective if it is in writing and sent by certified or registered mail, or insured courier, return receipt requested, to the appropriate party at the address set forth in your quote or order form and with the appropriate postage affixed. Either party may change its address for receipt of notice by notice to the other party in accordance with this Section. Notices are deemed given two business days following the date of mailing or one business day following delivery to a courier.

11.2 Governing Law. This Agreement will be interpreted, construed, and enforced in all respects in accordance with the local laws of the State of Utah, U.S.A without reference to its choice of law rules and not including the provisions of the 1980 U.N. Convention on Contracts for the International Sale of Goods. Each party hereby irrevocably consents to the exclusive jurisdiction and venue of the federal, state, and local courts in Salt Lake County, Utah, in connection with any action arising out of or in connection with this Agreement.

11.3 Consent to Use of Data. Fusion-io may collect technical information relating to your use of the Product and Fusion-io products. To the extent you select the applicable option when installing the Product, you grant Fusion-io and its contractors a perpetual, irrevocable right to use and disclose non-identifiable information relating to your use of the Product, as long as any disclosed information does not include a key or other mechanism that would enable the information to be re-identified.

11.4 Assignability. You may not assign your rights, duties, or obligations under this Agreement without Fusion-io's prior written consent, which consent will not be unreasonably withheld. If consent is given, this Agreement will bind your successors and assigns. Any attempt by you to transfer its rights, duties, or obligations under this Agreement except as expressly provided in this Agreement is void. Fusion-io may freely assign its rights, duties, or obligations under this Agreement without your prior written consent, including by operation of law or in connection with a merger, acquisition, reorganization, or sale of all or substantially all of its assets.

11.5 Commencing Legal Action. An action for breach of this Agreement or any other action otherwise arising out of this Agreement must be commenced within one year from the date the right, claim, demand, or cause of action first occurs or be barred forever.

11.6 Waiver. The waiver by either party of any breach of any provision of this Agreement does not waive any other breach. The failure of any party to insist on strict performance of any covenant or obligation in accordance with this Agreement will not be a waiver of such party's right to demand strict compliance in the future, nor will the same be construed as a novation of this Agreement.

11.7 Severability. If a court of competent jurisdiction holds any provision of this Agreement to be illegal, unenforceable, or invalid, the provision will be enforced to the maximum extent permissible and the remaining portions of this Agreement will remain in full force and effect. If any limitation or restriction on the grant of any license to you under this Agreement is found to be illegal, unenforceable, or invalid, the license will immediately terminate.

11.8 Interpretation. The parties have had an equal opportunity to participate in the drafting of this Agreement and the attached exhibits, if any. No ambiguity will be construed against any party based upon a claim that that party drafted the ambiguous language. The headings appearing at the beginning of several sections contained in this Agreement have been inserted for identification and reference purposes only and must not be used to construe or interpret this Agreement. Whenever required by context, a singular number will

include the plural, the plural number will include the singular, and the gender of any pronoun will include all genders.

11.9 Entire Agreement. This Agreement contains the complete agreement between the parties with respect to the subject matter hereof, and supersedes all prior or contemporaneous communications, agreements, and understandings relating to the Product, whether oral or written. Any varying or additional terms contained in any purchase order or other written notification or document issued by you in relation to the Product licensed under this Agreement will be of no effect.

Please direct all questions concerning this Agreement to: Fusion-io, Inc., 2855 E. Cottonwood Parkway, Suite 100, Salt Lake City, UT 84121; Attention: Legal Department.

Fusion Powered Support

We offer Fusion Customer Services and Support by phone, e-mail and on the Web. For the most up-to-date contact information, visit: http://support.fusionio.com

E-Mail

Our support e-mail address is: support@fusionio.com

E-mail is the fastest way to get simple questions answered. Please give a detailed description of your problem with your complete contact information (name, phone number, e-mail address, location address).

Warranty Support

Warranty Support is available via support@fusionio.com and http://support.fusionio.com.

Telephone Support

ioFX Support

North America: (855) 322-5767

Enterprise Support

North America: (877) 816-5740

Country Numbers

For product support outside of North America, please use the number for the country/region closest to you from the table below. If that is not possible, please contact North America at (801) 424 5474.

Country	Phone Number
Australia	(02) 8278 1489
Belgium	02 700 74 86
China	40-08866109
Denmark	4331 4999
Finland	097 251 9979
France	01 57 32 48 90
Germany	(069) 17 07 76 790

Country	Phone Number
Hong Kong	3071 3587
Italy	02 23331509
Japan	(03) 6743-9765
Luxembourg	(224) 87 19 84
Mexico	01 882 816 5740
Netherlands	070 7703993
Norway	23 02 49 99
Singapore	6818 5692
South Korea	02 3483 6689
Sweden	08 593 663 99
United Kingdom	(020) 3564 9935

Web

Go online to find tips, FAQs, and troubleshooting help, or download the latest user guides, software, and support packages at: http://support.fusionio.com

Glossary

C

CIM
Common Information Model

CIMOM
Common Information Model Object Manager

CMPI
Common Manageability Programming Interface

D

DA
Direct Attached

DHCP
Dynamic Host Configuration Protocol

DMTF
Distributed Management Task Force

DNS
Domain Name System

H

HBA
Host bus adapter

I

IOPS
Input/Output Operations Per Second

iSCSI
Internet Small Computer System Interface

L

LDAP
Lightweight Directory Access Protocol

LED
Light-emitting diode

M

MiB
Mebibyte

P

PBW Endurance
Petabytes Written Rating

PCI
Peripheral Component Interconnect

S

SAN
Storage Area Network

SAS
Statistical Analysis System

SCSI
Small Computer System Interface

SDK
Software development kit

SMI-S
Storage Management Initiative – Specification

SMTP
Simple Mail Transfer Protocol

SNIA

Storage Networking Industry Association

SSD

Solid-state drive

U

UPS

Uninterruptible power supply

V

VSL

Virtual Storage Layer

W

WBEM

Web-Based Enterprise Management

Index

R

S

T

U

V

W

Z