Flash Management Console 3.15.0

User Guide

Table of Contents

Introduction

Welcome to the Flash Management Console, where you can easily manage High IOPS and io3 Flash Adapterss across multiple servers throughout a data center. This manual describes Flash Management Console's controls and functionality.

Flash Management Console runs on both Windows and Linux platforms. Flash Management Console can manage hosts running Windows, and Linux. Visit http://www.ibm.com/support/entry/portal/docdisplay?lndocid=MIGR-65723 (follow that link and then select *High IOPS or io3 Flash Adpapters software matrix*) for the latest list of supported systems.

NOTE-

All operating systems must be 64-bit architecture to support High IOPS and io3 Flash Adapters.

Getting Started

For detailed instructions to install Flash Management Console, see the *Flash Management Console 3.15.0 Installation Guide.*

First Time Setup, New Install

NOTE-

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

1. Enter, and re-enter, a password for user Admin.
2. 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).
3. Enable **Remote Access** (optional).This setting is unchecked by default. Check this box to allow remote access to this Flash Management Console server.
4. Enable **Advertise Using Zeroconf** (optional). This allows Agents to automatically discover and connect to Flash Management Console (requires Avahi on Linux or Bonjour on Windows).
5. The Host Name field should be populated. It is a best practice to use a fully qualified host name for the server. If you want to use a different name click the drop-down arrow or enter the alternate name in the Host Name field.
6. The Port field is set to 9051 by default; You have the option of entering a different port here.
7. Unless you have your own custom SSL certificates and key, click **Pre-configured SSL Certificate**.

Attention!

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

8. Click **Save Changes**.

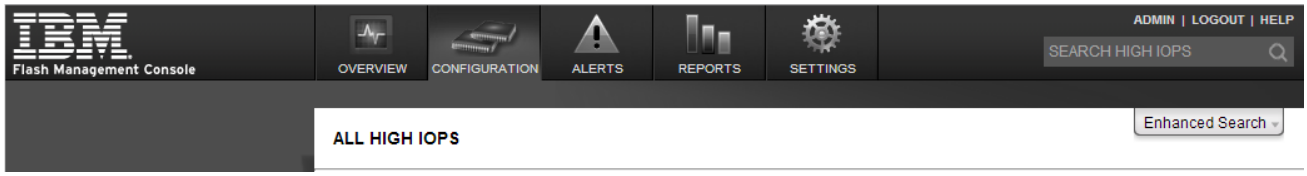
Flash Management Console restarts and displays the login page.

Top-Level Tabs

The Flash Management Console application is divided into five top-level tabs:

- Overview
- Configuraiton
- Alerts
- Reports
- Settings

These tabs are static and appear at the top of the window regardless of the page you are viewing.

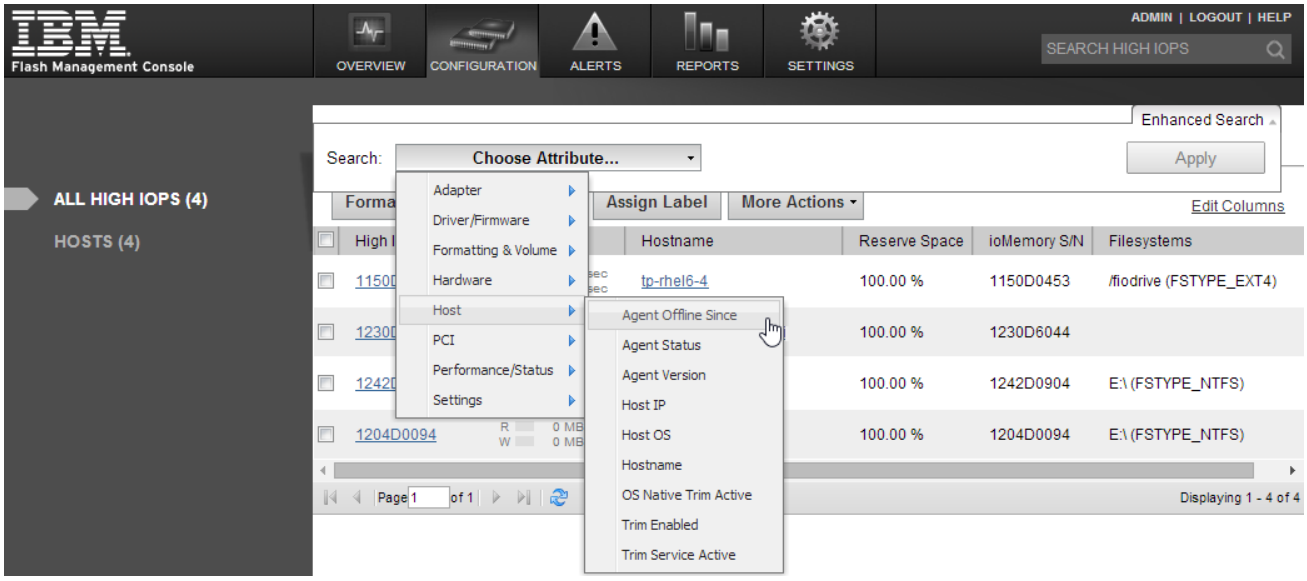


To the right of the top-level tabs are the following title bar links:

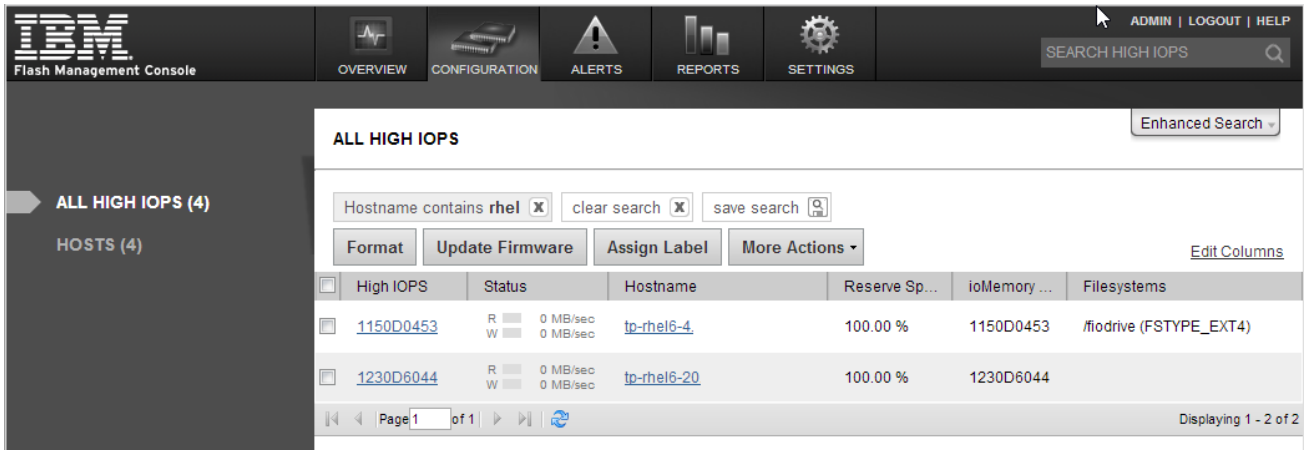
- Admin—This is only visible when logged in as an administrator.
- Logout
- Help—This will provide links to Lenovo support and the online Knowledge Base.

A search box is available below the title bar links when using the Configuration, Alerts, or 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:



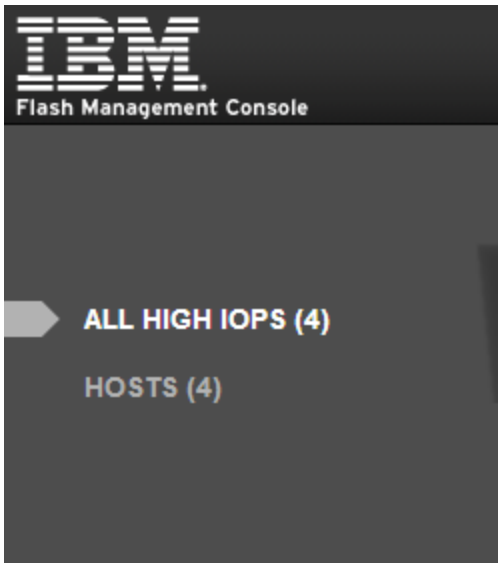
If a current search criteria is applied on any of the pages where the Search box is active, you will see that criteria displayed above the grid. Use Enhanced Search to add additional search criteria to the search. (Additional search criteria are evaluated as a logical AND, where all search criteria must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



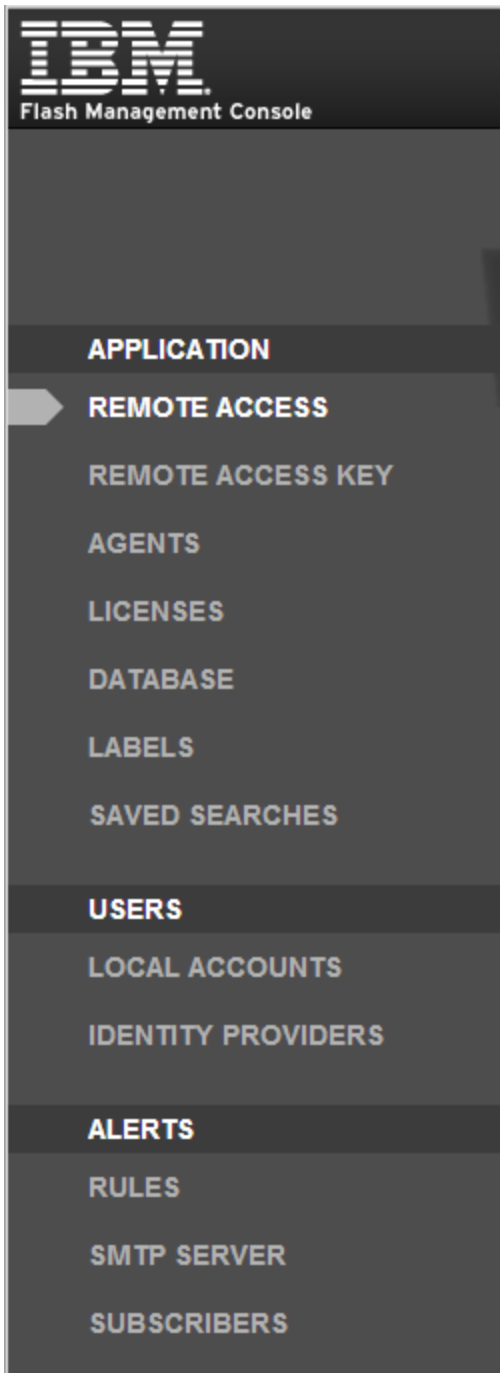
Click the criteria itself to remove an item from the search criteria, or click **clear search** to clear all search filters.

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.

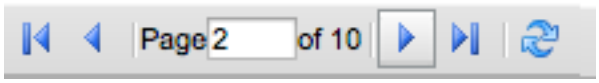


For the Settings tab, the following options are provided:


IBM
Flash Management Console
APPLICATION
REMOTE ACCESS
REMOTE ACCESS KEY
AGENTS
LICENSES
DATABASE
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:



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

Attention!

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.

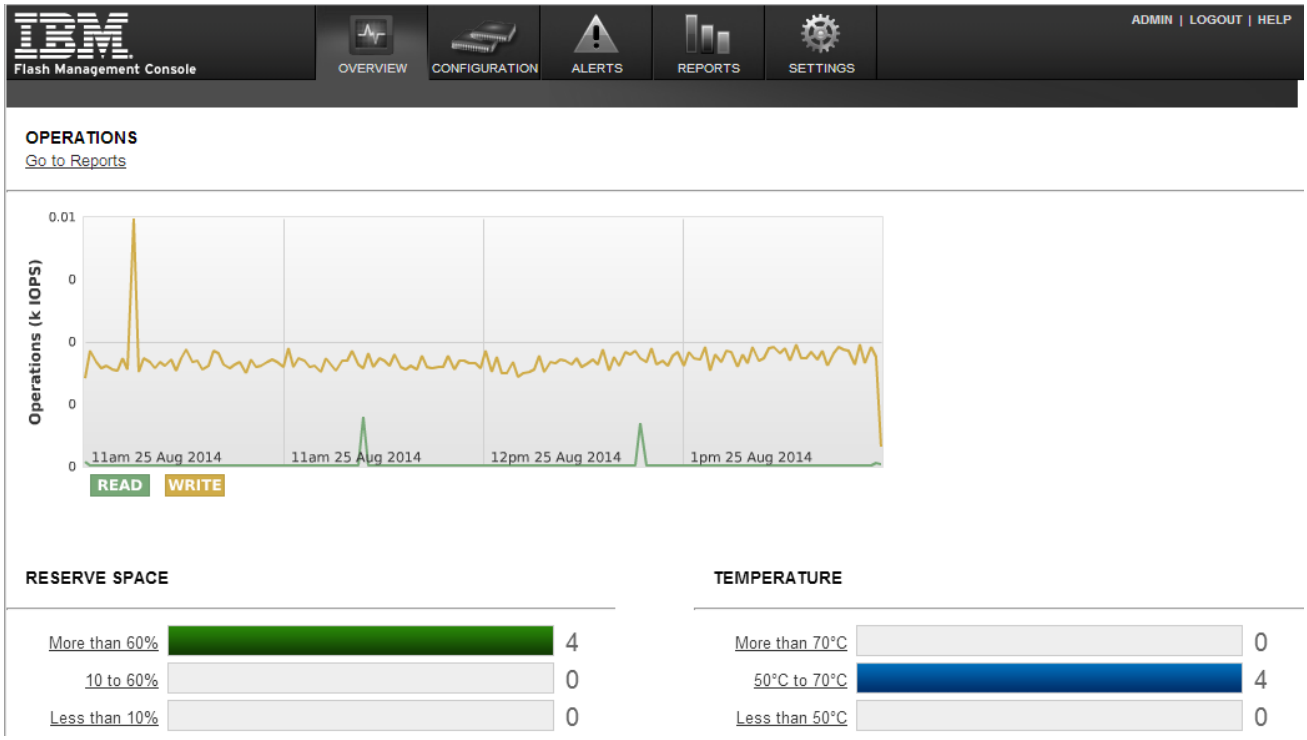
The Flash Management Console Feature Set

This section describes the controls and features of the Flash Management Console.

Overview Tab

The Overview tab summarizes key information gathered from all High IOPS and io3 Flash Adapterss, including

- IOPS
- Reserve Space
- Temperature



Operations

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

Read 

and Write 

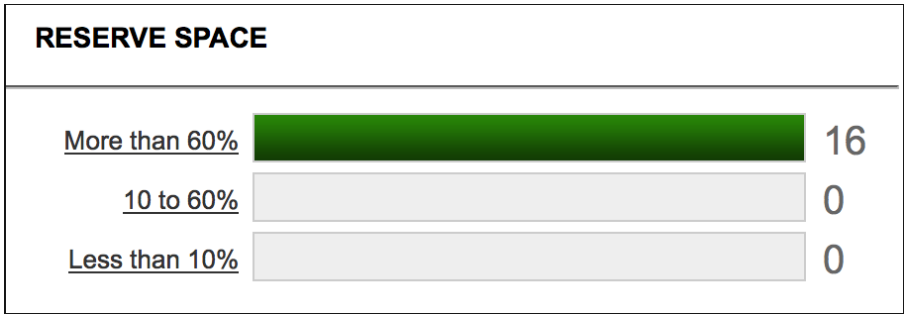
buttons at the bottom of the graph allow you to toggle between the display of Read and Write data of the Operations report.

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 See Reports Tab on page 22.

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.



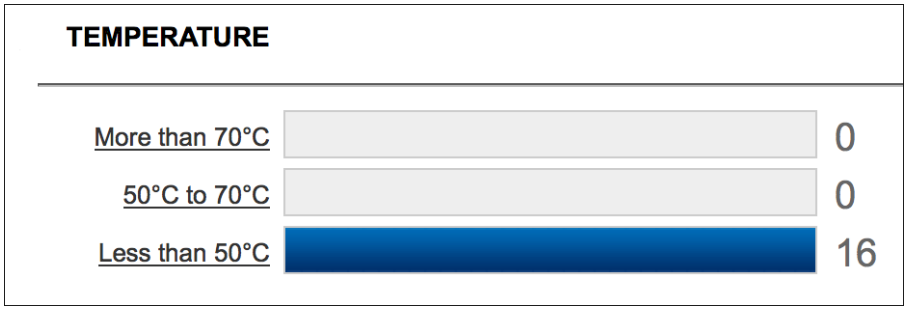
An early warning message is sent by the driver when the amount of reserve is close to reaching the 10%-available threshold. If the reserve space decreases to 0% of its original size, the device enters write-reduced mode (degraded) in order to prolong the lifespan of the device. Sometime after the reserve 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 High IOPS and io3 Flash Adapters 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 High IOPS and io3 Flash Adapterss are within preset temperature ranges.



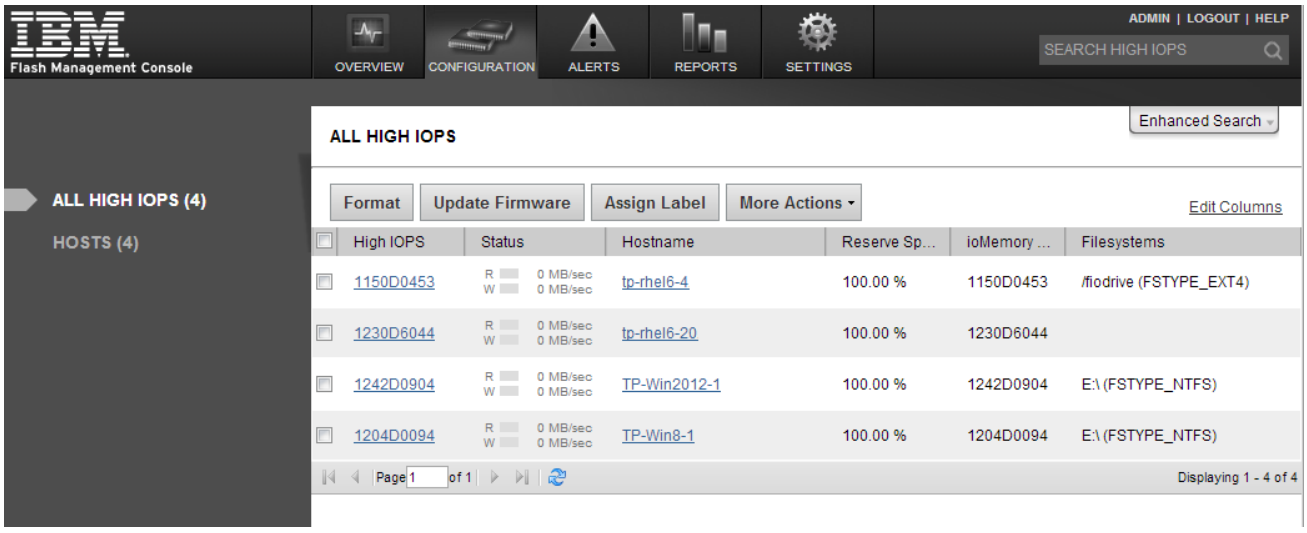
The links on the left of the reports are links that will take you to the **Configuration** tab with an Enhanced Search filter set that matches the label. For example, clicking on the "Less than 50°C" link will take you to the **Configuration** tab where an "FPGA Temperature is less than 50" filter only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

Normal operating temperature for devices vary. However, as device temperature rises 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

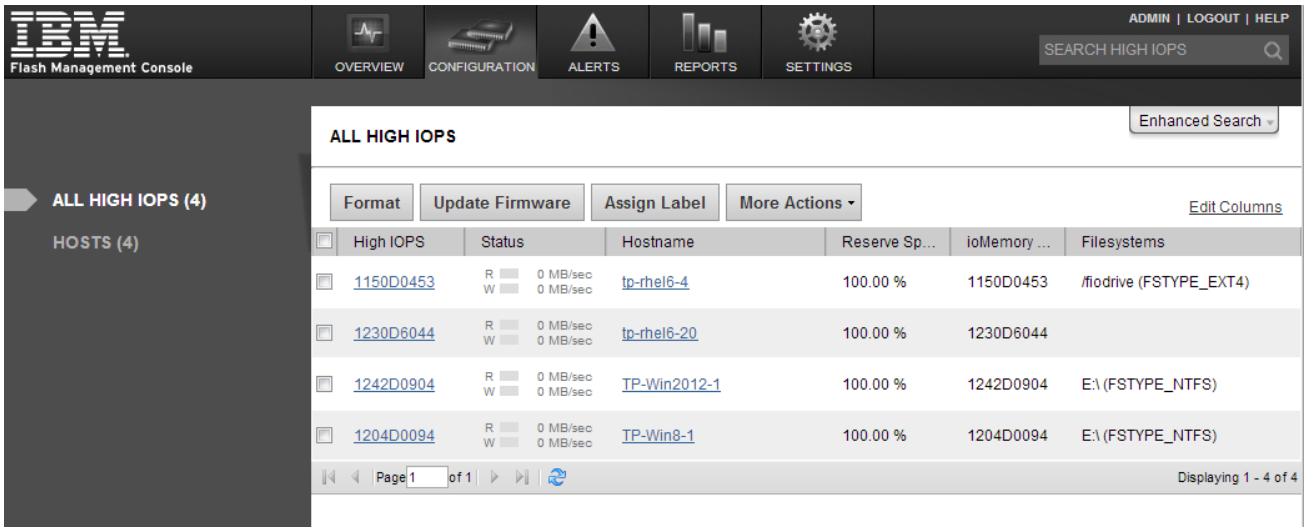
This page provides a central location where you can configure and manage your devices.



Click **More Actions** button to access the **Attach** device and **Detach** device options. See See More Actions on page 18 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 itemioMemory.



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 See Device Page on page 49 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.

Attention!

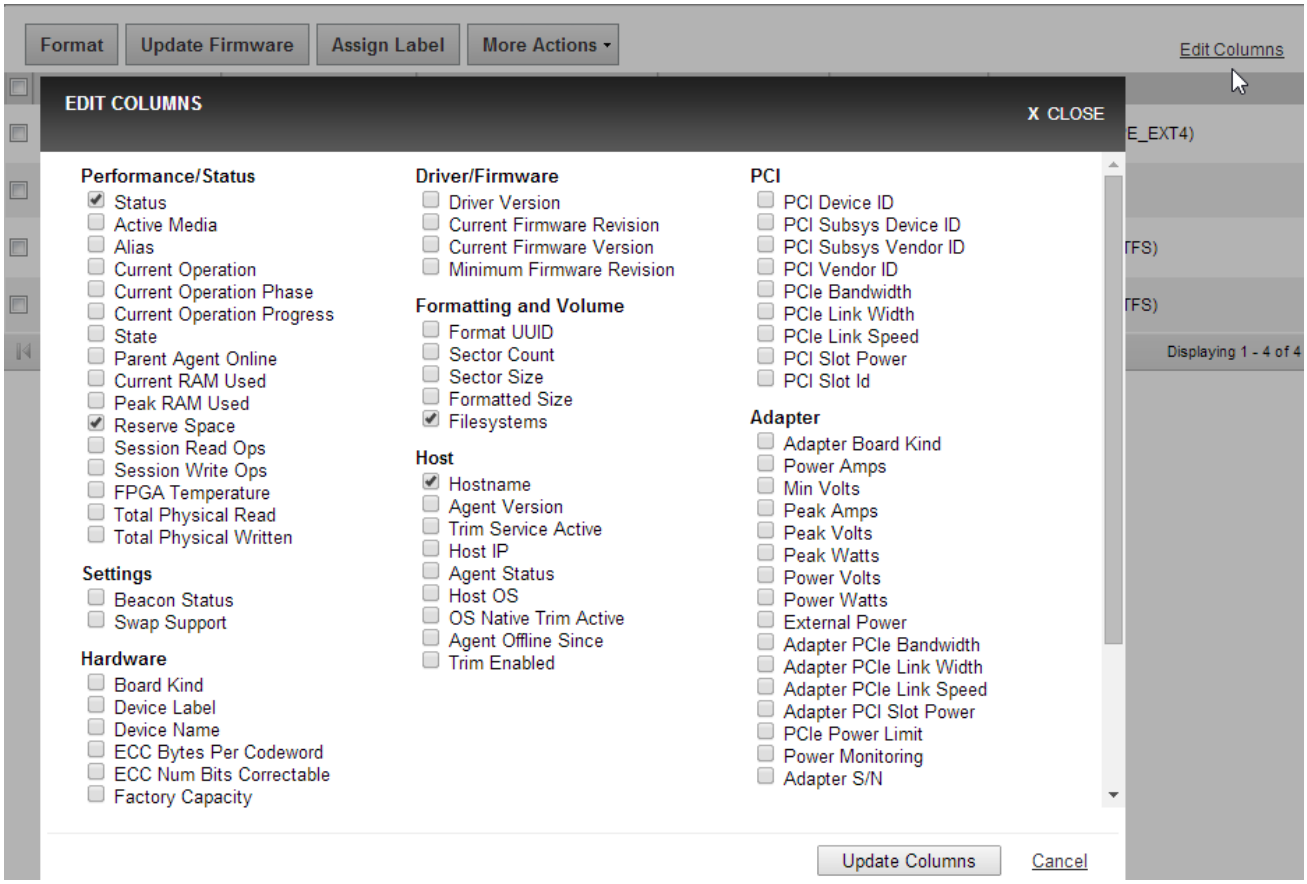
Do not Update Firmware across multiple devices simultaneously. Update firmware on one device at a time. A Duo card should be treated as two logical devices and each half should be updated separately.

Attention!

In the image above, the All High IOPS filter has been selected in the sidebar. Flash Management Console 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

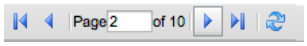
Click **Edit Columns** to specify what device data you want displayed in the device grid.



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.



High IOPS

The High IOPS screen displays a list of High IOPS and io3 Flash Adapterss 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 See Configure Device Tab on page 50)

On the High IOPS 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 See Device Page on page 49

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.

Attention!

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

Attention!

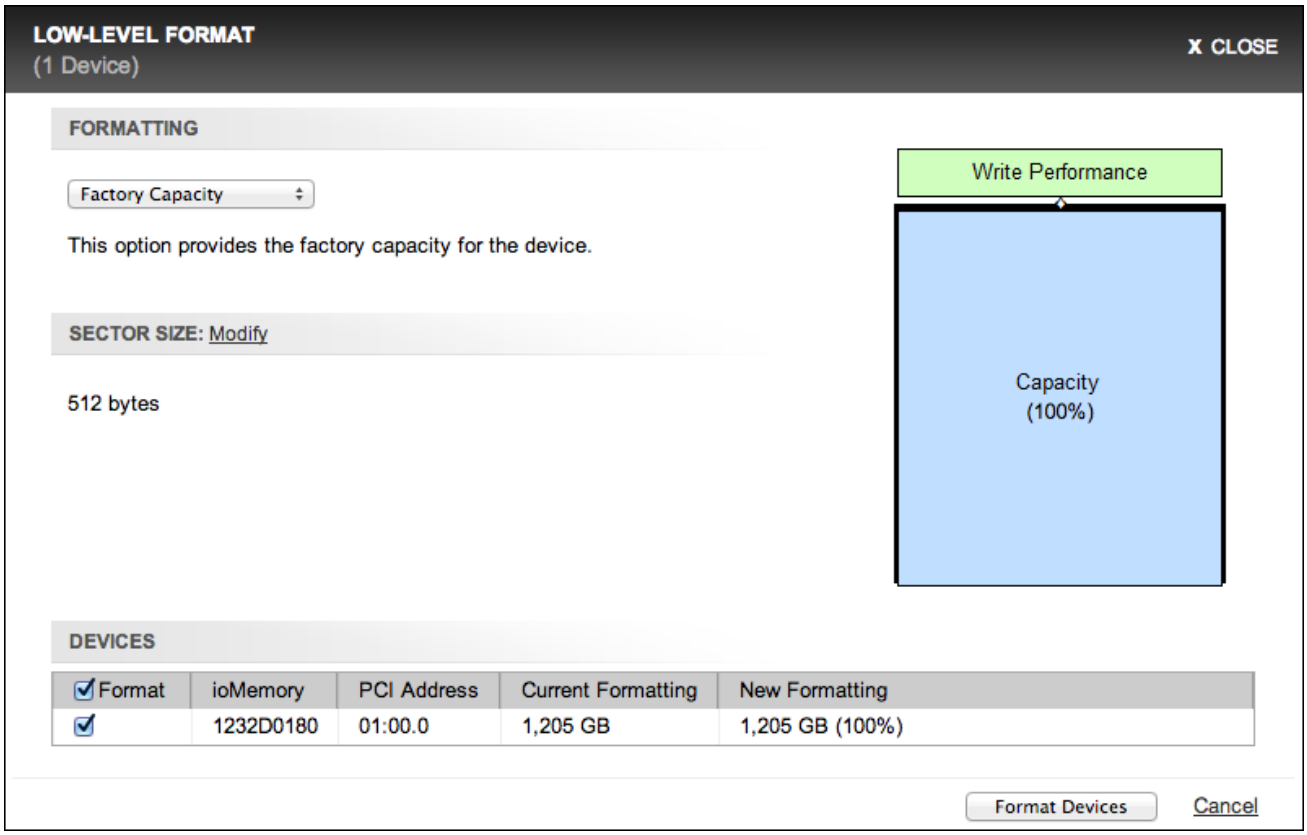
Formatting a device will destroy any data still remaining on it. Please be sure to back up your data before proceeding.

Your High IOPS and io3 Flash Adapters come 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 Customer Support.

Flash Management Console 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 High IOPS and io3 Flash Adapters on the Flash Management Console page to format simultaneously.

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

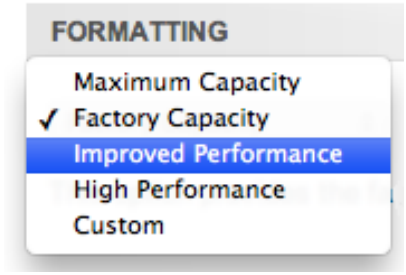


Attention!

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.

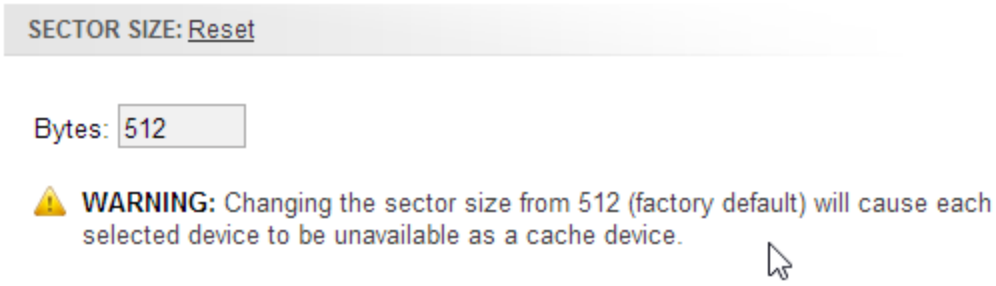
Here you can set the ratio of "Write Performance to Capacity." You can increase write performance by decreasing the High IOPS and io3 Flash Adapters's capacity--the reverse is also true. You can select from a drop-down list of preset ratios

- Maximum Capacity
- Factory Capacity
- Improved Performance
- High Performance

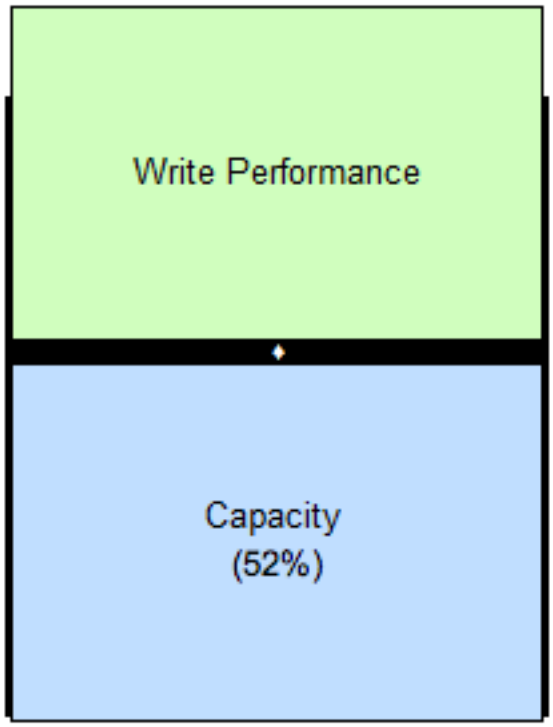


You can customize the Write ratio with the Custom selection (from the drop-down menu) or by dragging the line between Write Performance and Capacity in the graphic.

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.



Attention!

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

The selected High IOPS and io3 Flash Adapters(s) appear below the Write Performance/Capacity graphic. Check the corresponding checkbox to perofrm the desired action on the selected device or devices.

NOTE-

If an High IOPS and io3 Flash Adapters 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 High IOPS and io3 Flash Adapters, click **Format Devices**.

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 See Appendix B - Software Updates on page 65.

Update Firmware

Updating High IOPS and io3 Flash Adapters involves two procedures: updating the ioMemory VSL (driver) on the host machine, and updating the firmware on the High IOPS and io3 Flash Adapters. Refer to See Appendix B - Software Updates on page 65 for more information.

Attention!

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:
Fusion ioMemory VSL software 3.x `C:\Program Files\Fusion-io ioMemory VSL\Firmware`
Fusion ioMemory VSL software 4.x `C:\Program Files\SanDisk\Fusion 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 High IOPS and io3 Flash Adapters's firmware. You should upgrade the firmware if:

- Flash Management Console 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 High IOPS and io3 Flash Adapters stops working.
- You are instructed to do so by Customer Support.

NOTE-

In most cases, if you upgrade the High IOPS and io3 Flash Adapters firmware, you must also upgrade the High IOPS and io3 Flash Adapters driver. Most support issues arise from mismatched firmware and drivers.

Upgrading the firmware may take some time. Monitor the progress using Flash Management Console.

Attention!

Back up the data on your High IOPS and io3 Flash Adapters(s) prior to performing the upgrade.

Attention!

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.

Attention!

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 **Update Firmware**, 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 High IOPS and io3 Flash Adapters(s) appear below the Update firmware drop-down menu. Check the corresponding checkbox to perofrm the desired action on the selected device or devices.

NOTE-

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 High IOPS and io3 Flash Adapters's firmware, click **Update Firmware**. Or, to exit the Update Firmware dialog without updating any devices, click **Cancel**.

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 See Appendix B - Software Updates on page 65.

Assign Label

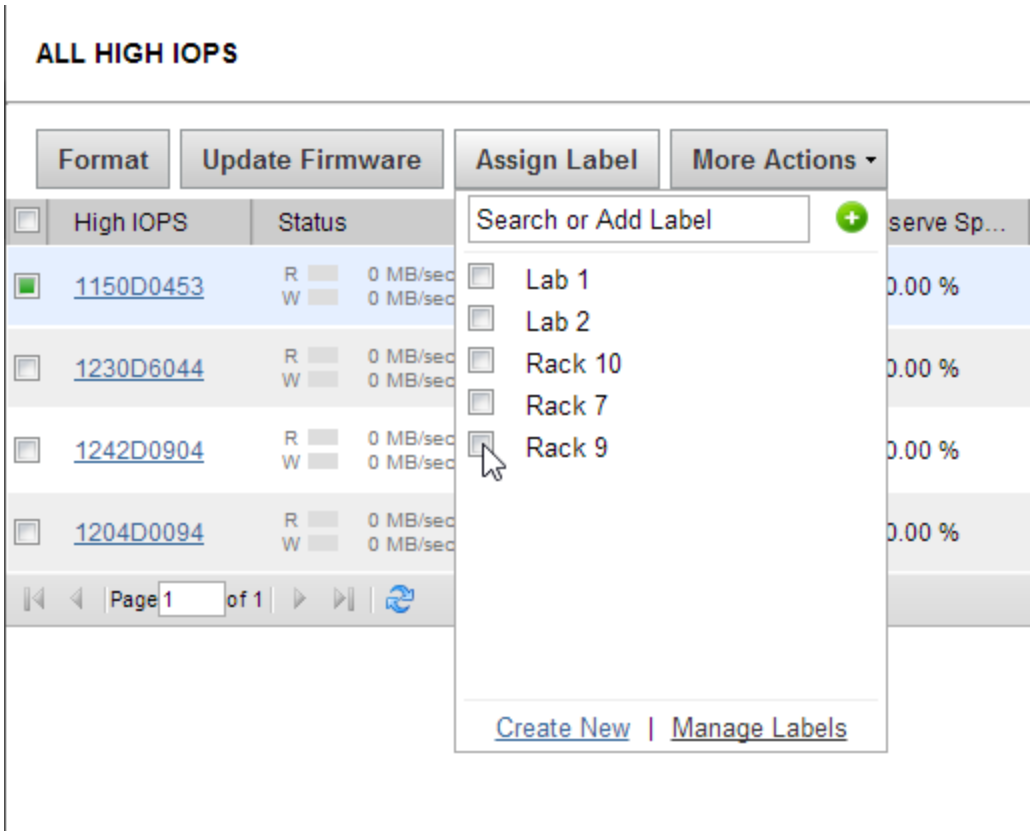
Assign Label lets you organize your High IOPS and io3 Flash Adapterss into categories or groups.Clicking on the label will quickly display all High IOPS and io3 Flash Adapterss belonging to that group.

NOTE-

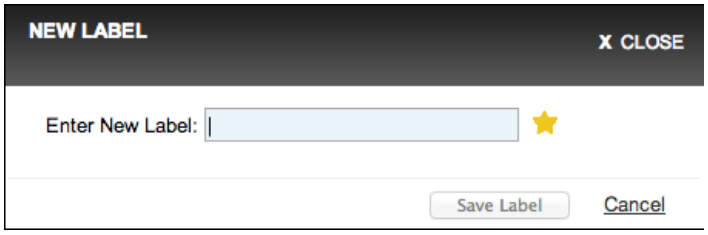
When you create a new label, you can mark it as a Favorite by selecting the star icon. For more information about Labels, see See Labels on page 29.

NOTE-

You can also create new labels on the Settings tab.



To create a new label, select one or more High IOPS and io3 Flash Adapterss on the Flash Management Console page and click **Assign Label**, then click the green plus button. The New Label drop-down appears.



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

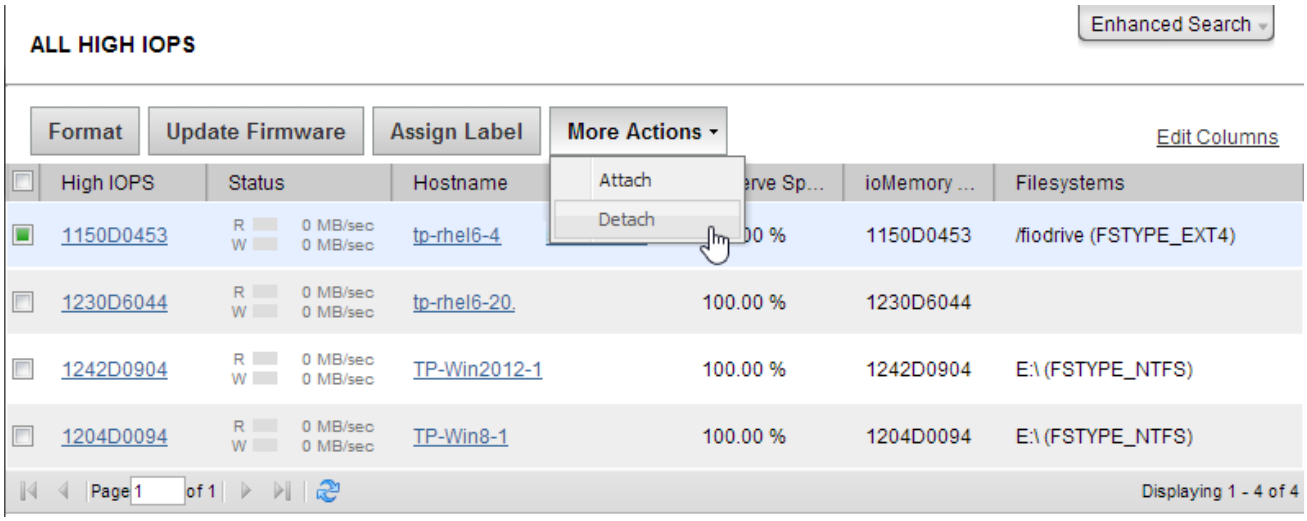
The New Label dialog will close after you save the label. Alternately, you can close the window with the Cancel link or by clicking **Close** in the upper right corner.

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 High IOPS and io3 Flash Adapterss.



The Attach device operation creates a link, so the High IOPS and io3 Flash Adapters 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 when you manually detach an High IOPS and io3 Flash Adapters (that is, to perform a low-level format).

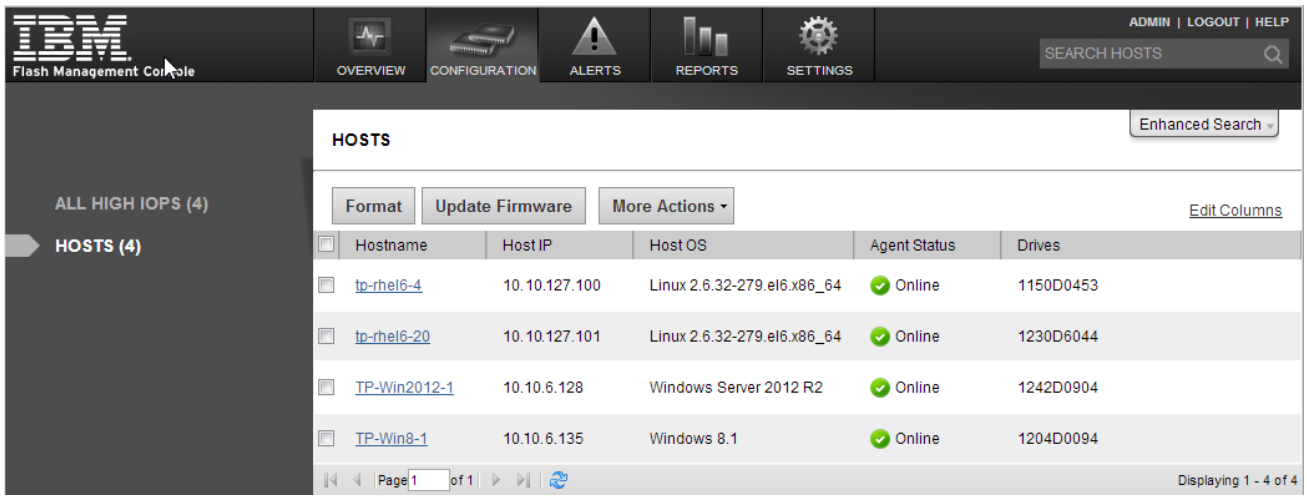
Detach device disconnects your High IOPS and io3 Flash Adapters from the operating system. Once detached, the device is not accessible to users or applications. (You need to use Attach to make it accessible.) You will not need to use this action because Flash Management Console automatically detaches when performing an update or format from the UI.

Hosts

The Flash Management Console Hosts Screen displays when the user clicks a Hosts link in the interface.

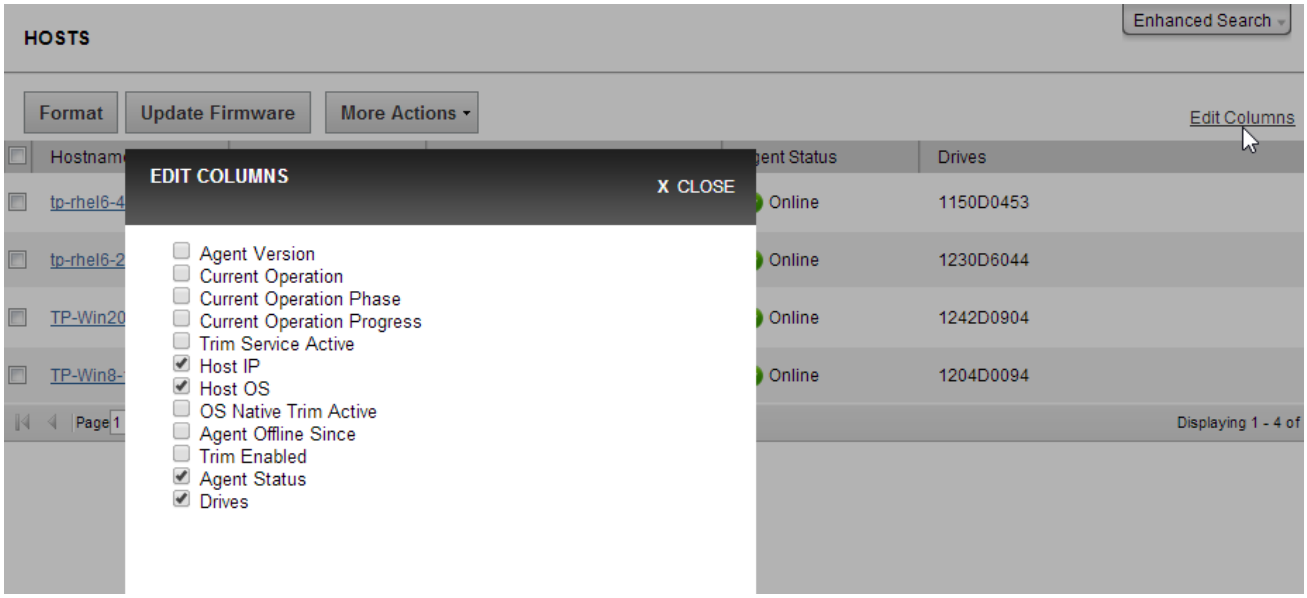
When you select Hosts from the sidebar, the host page displays information about the hosts that contain High IOPS and io3 Flash Adapterss. By default, the hosts grid shows

- Hostname
- Host IP
- Host OS
- Agent Status
- Drives
- 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**.

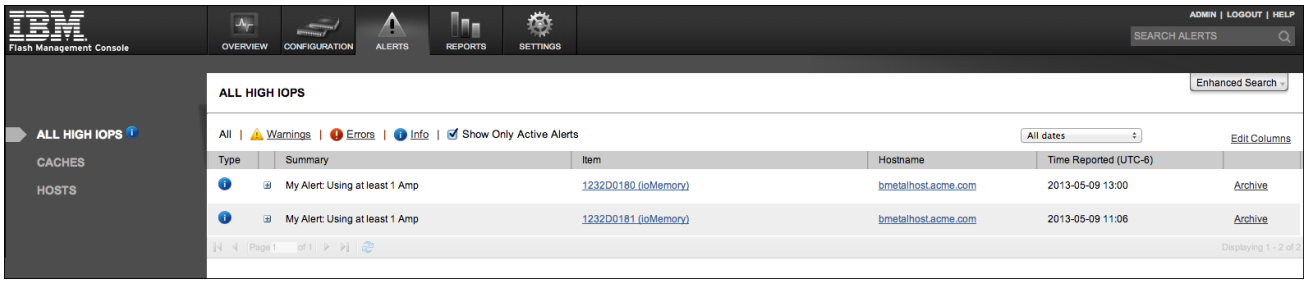
Alerts Tab

This page lists current and historical alerts for High IOPS and io3 Flash Adapterss and cache instances. Alerts are for recording or notification purposes.

> **Attention!**
>
> 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



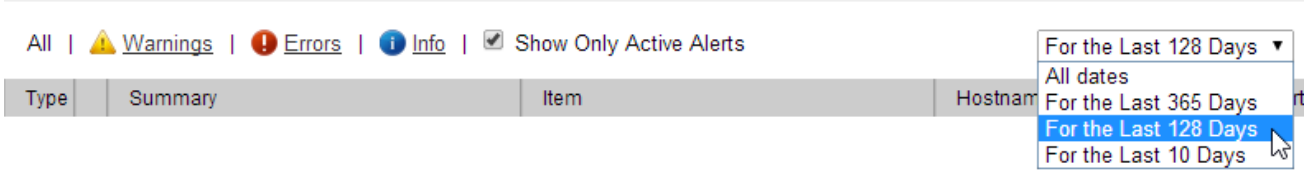
Active Alerts

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.

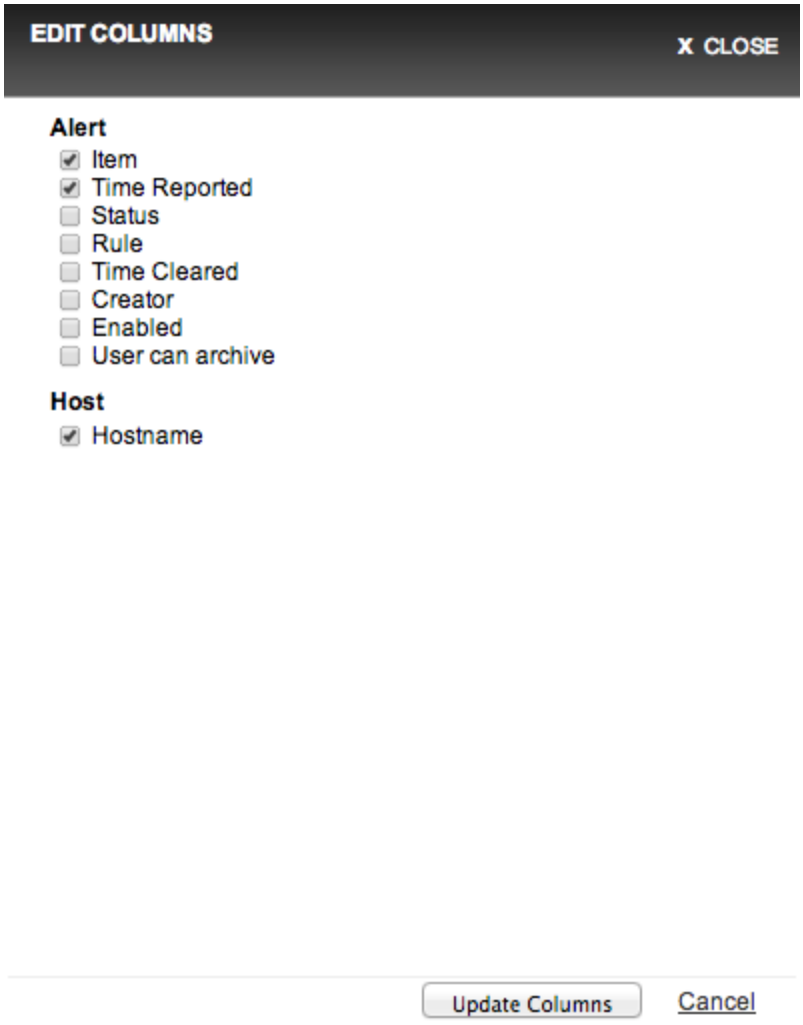
For the Last _____ Days

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.



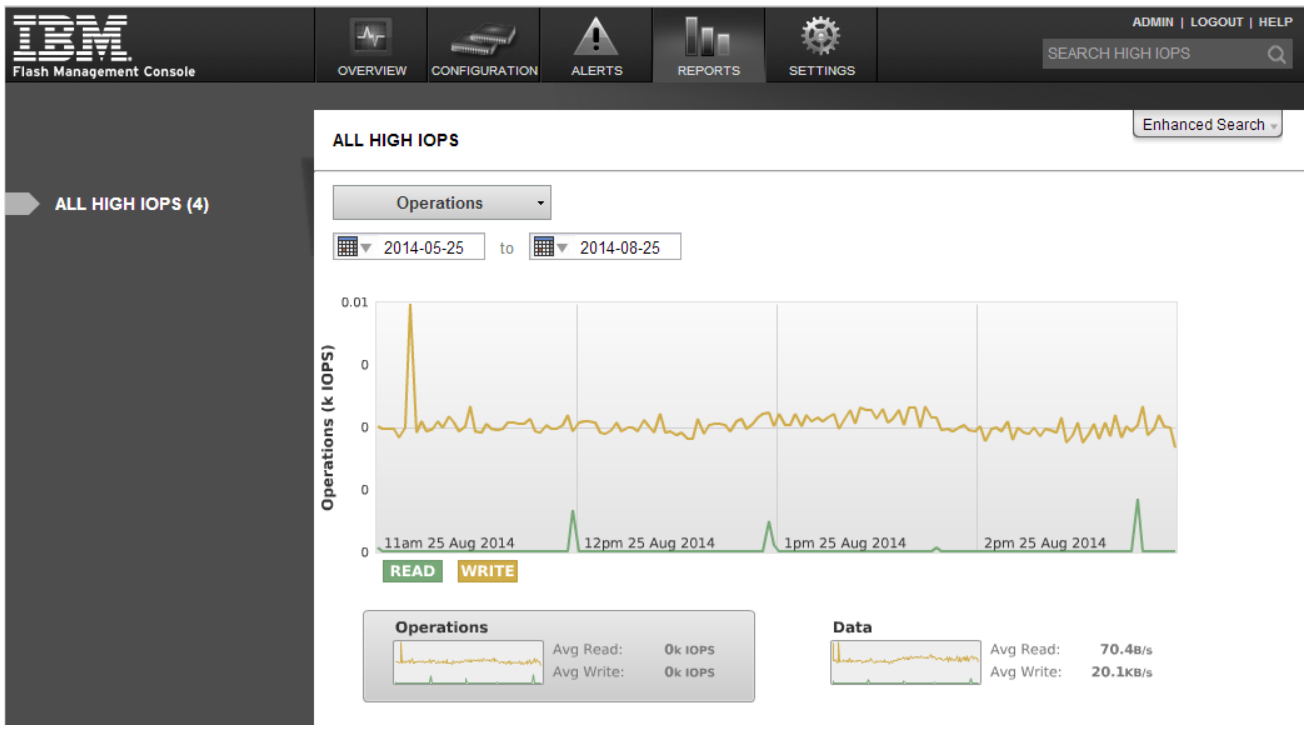
Select the columns you want to display, then click ***Update Columns***.

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

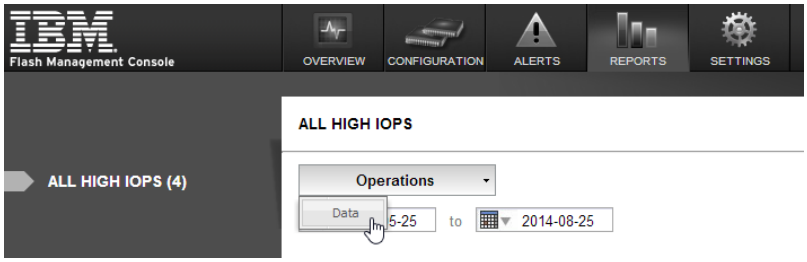
This page reports the Operations and the Data information for High IOPS and io3 Flash Adapterss.



For more information on the specific graphs available, see See Reports Device Tab on page 52.

Operations - Data Drop-Down

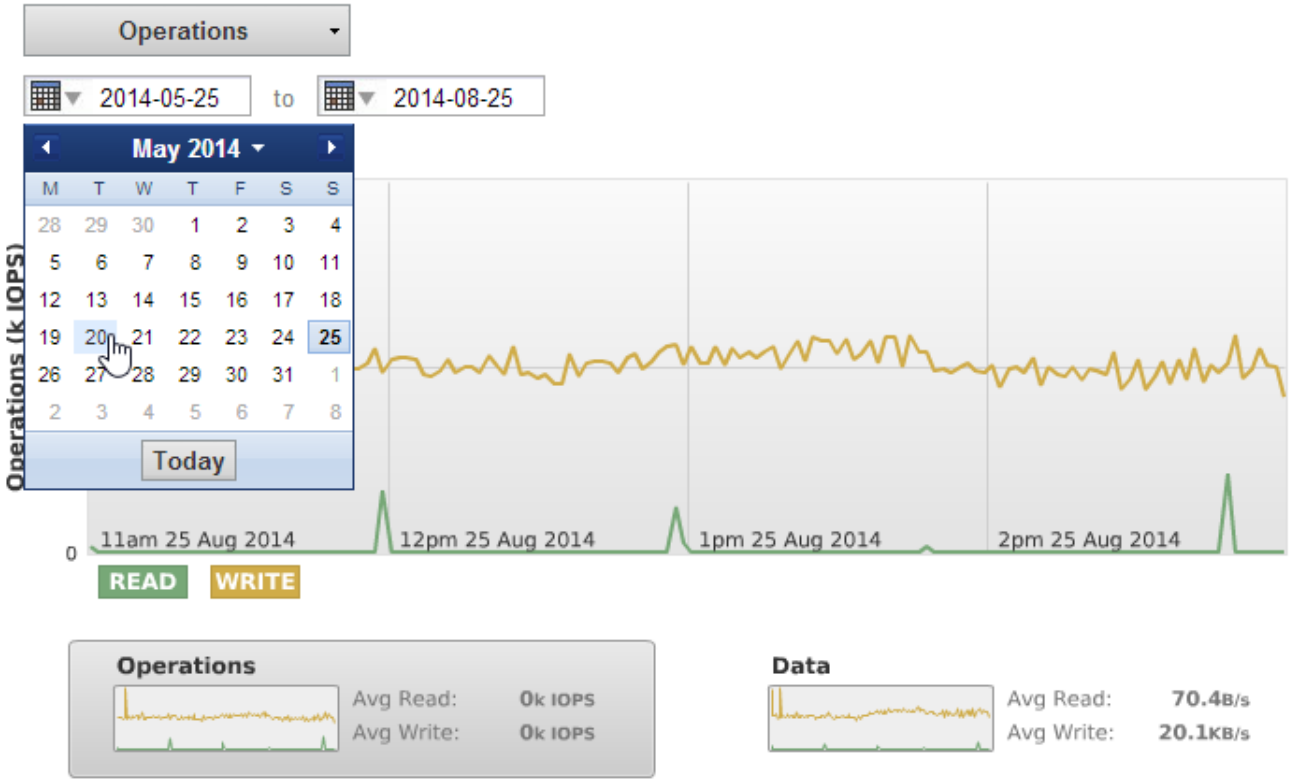
Click to display information about Operations (IOPS) or data volume.



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

Date Range

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

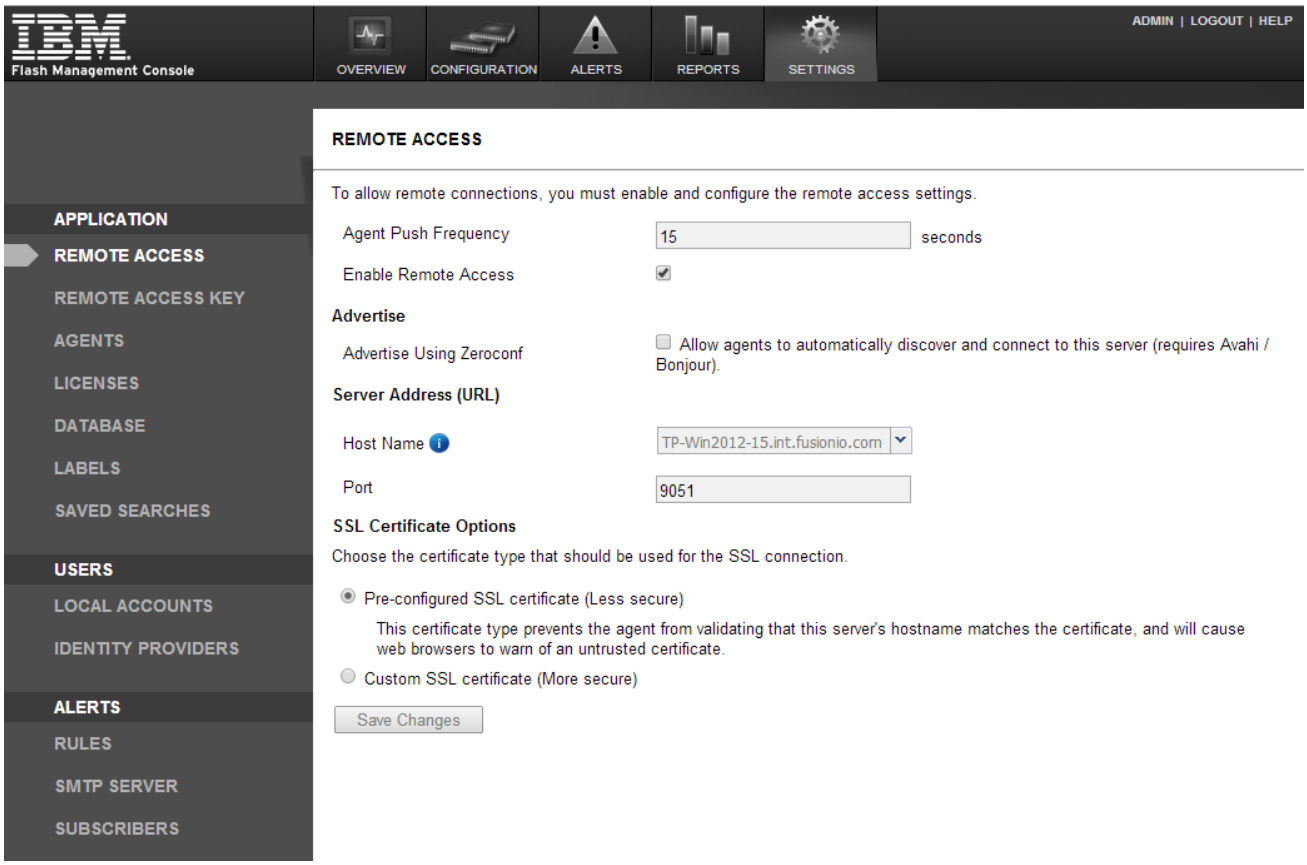


Read and Write Buttons

Click **Read** READ or **Write** 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, High IOPS and io3 Flash Adapters labels, and saved searches.



Attention!

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).

Attention!

Increasing this number above 600 displays this message:
"A high push frequency will potentially result in data being out of date in the Flash Management Console."

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.

> **Attention!**
>
> Do not disable remote access from within the VMWare VCenter plugin. Doing so will cause vSphere clients to fail to connect to Flash Management Console.

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.

> **Attention!**
>
> 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.

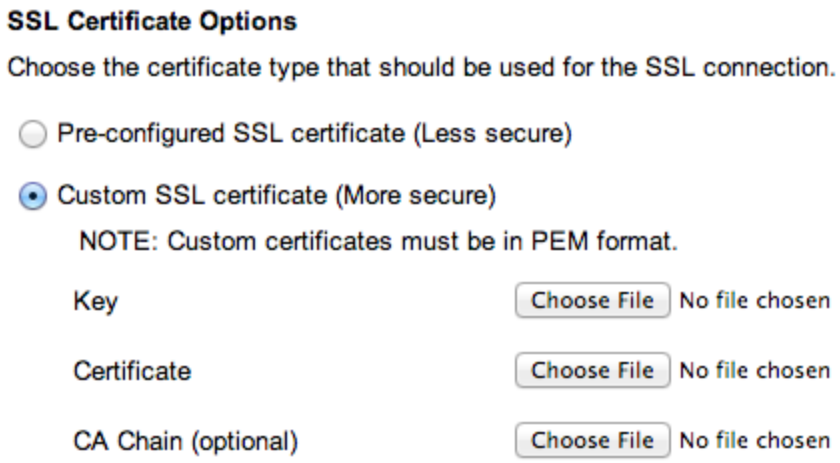
Port

By default, the port is set to 9051, which is reserved for Flash Management Console 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 Flash Management Console 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 Flash Management Console: 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.

Attention!

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 directory:

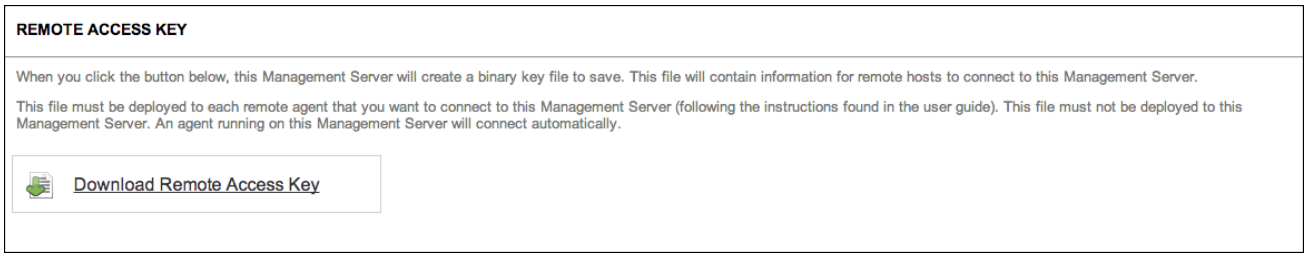
Windows

```
C:\ProgramData\fio\agent_keys
```

Linux

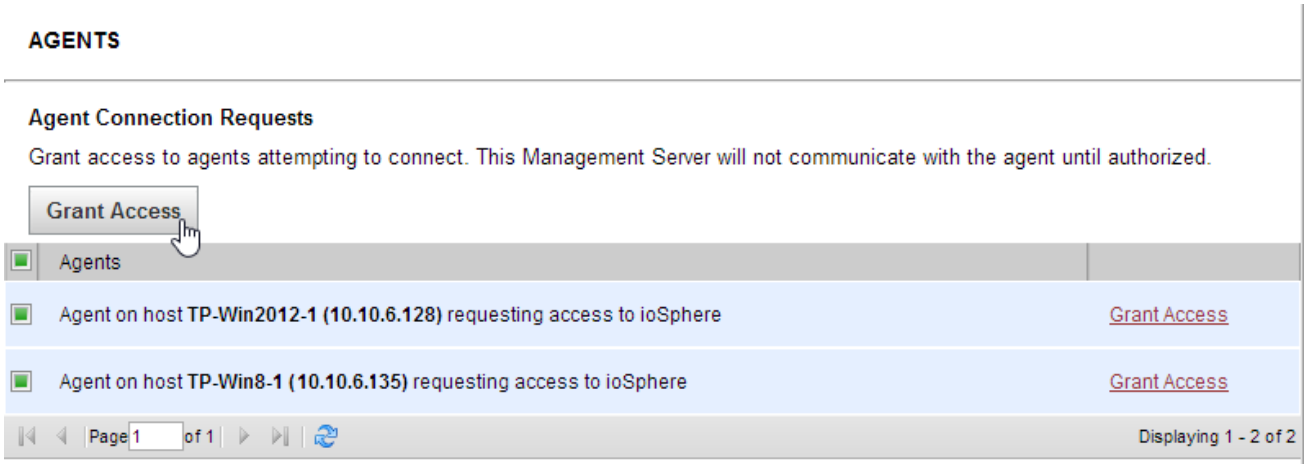
```
/var/lib/fio/agent_keys/
```

Once copied, the Agent should connect within 15 seconds.



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.

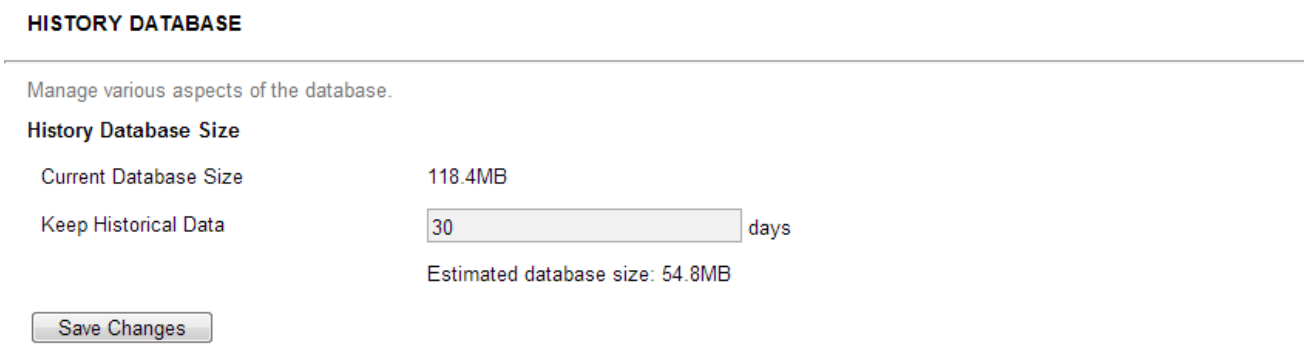


Licenses

The Licenses option in the Flash Management Console is provided for managing licensed products like caching. See the installation guide of the license product you want to use for information on licensing.

Database

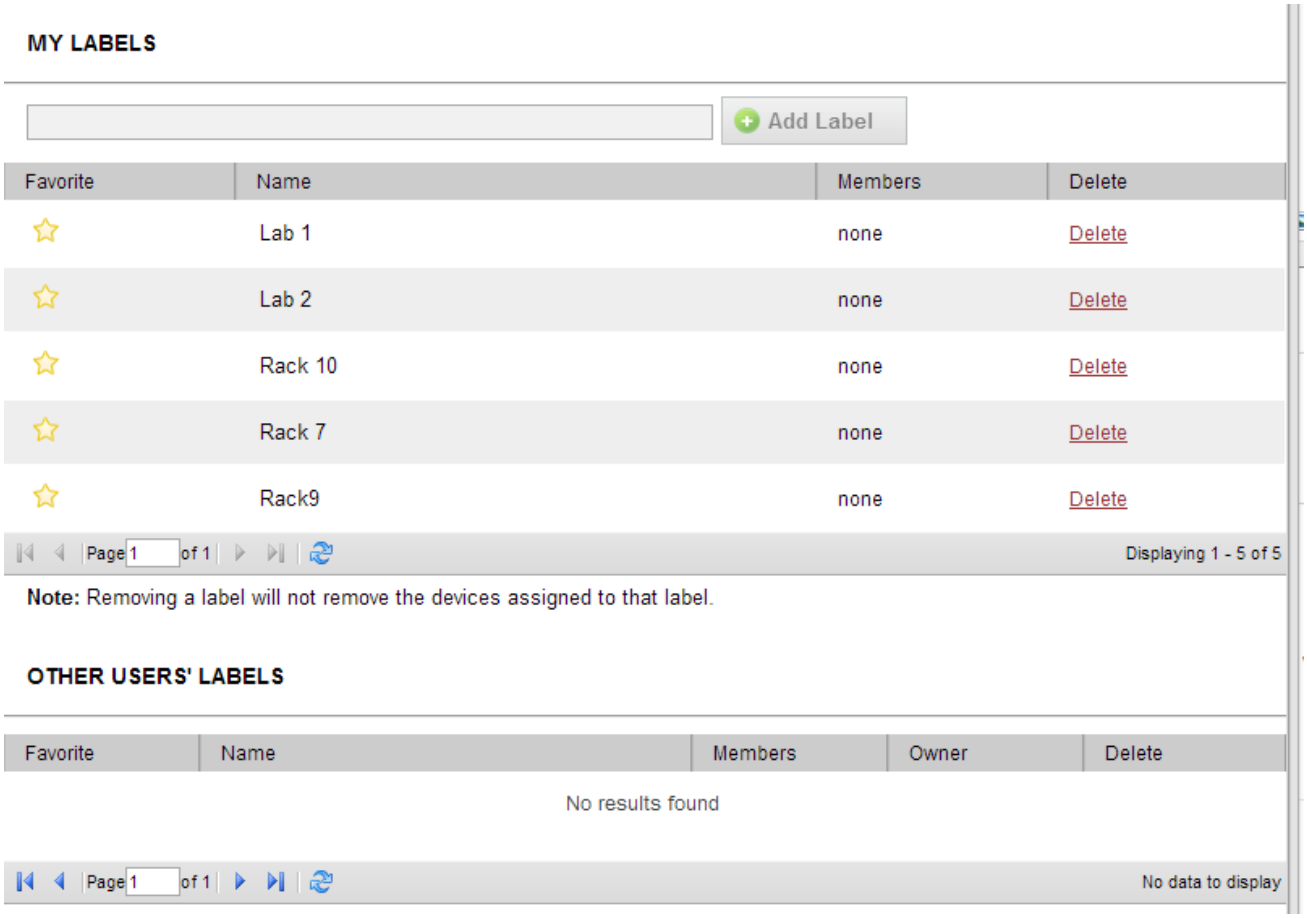
Here you can adjust the size of your history database by specifying how many days to include in the historical data. Click **Save Changes** after you have made any changes.



By default, Flash Management Console keeps the last 30 days of data. This can be modified to store up to 10 years.

Labels

Labels are used to organize your High IOPS and io3 Flash Adapterss 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 See Configuration Tab on page 9 for more information about creating labels.



NOTE-

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

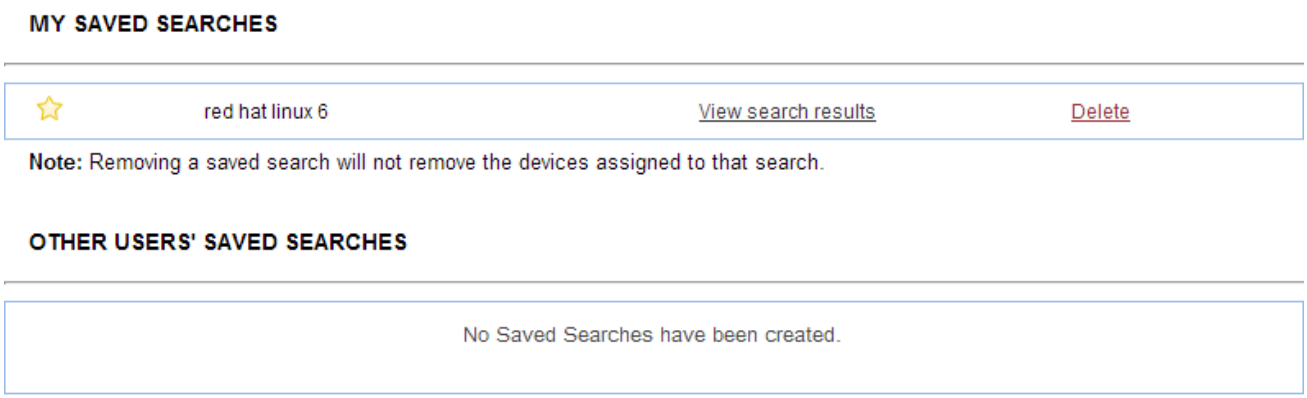
To change the Favorite settings of a label, click the star icon next to the label name. A yellow star means it is a favorite, a faded star means it is has not been marked as a favorite.

Delete

To delete a label, click **Delete** 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 See Alerts Tab on page 21)or Reports tab (see See Reports Tab on page 22), you can come here to rename it, mark it as a favorite, or delete it.



To view the results of a saved search, click **View Search Results**. 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 **Delete** next to the name.

NOTE-

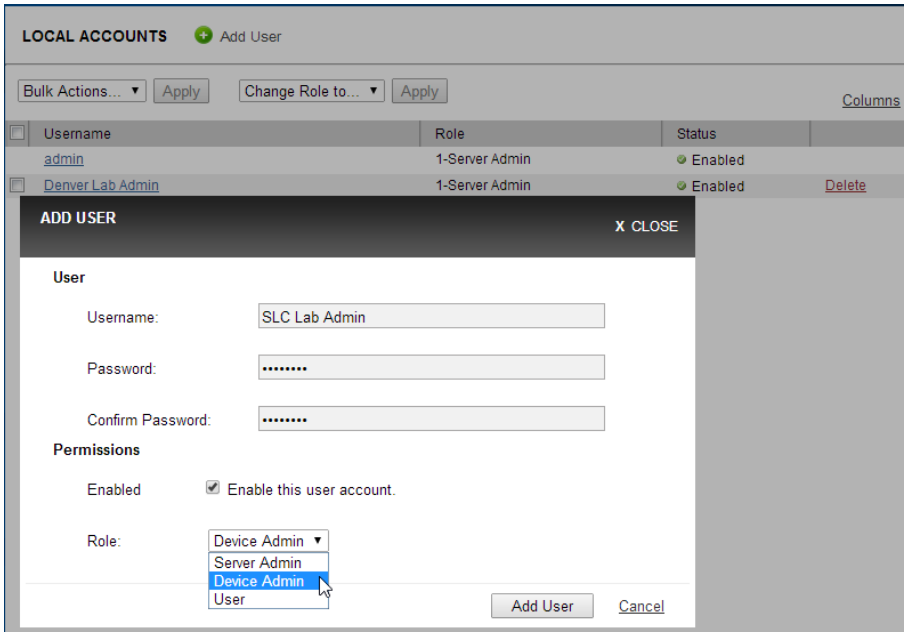
Other Users' Saved Searches: While only an admin can edit saved searches created by other users, anyone can add another user's saved search to their favorites.

Local Accounts

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

Add User

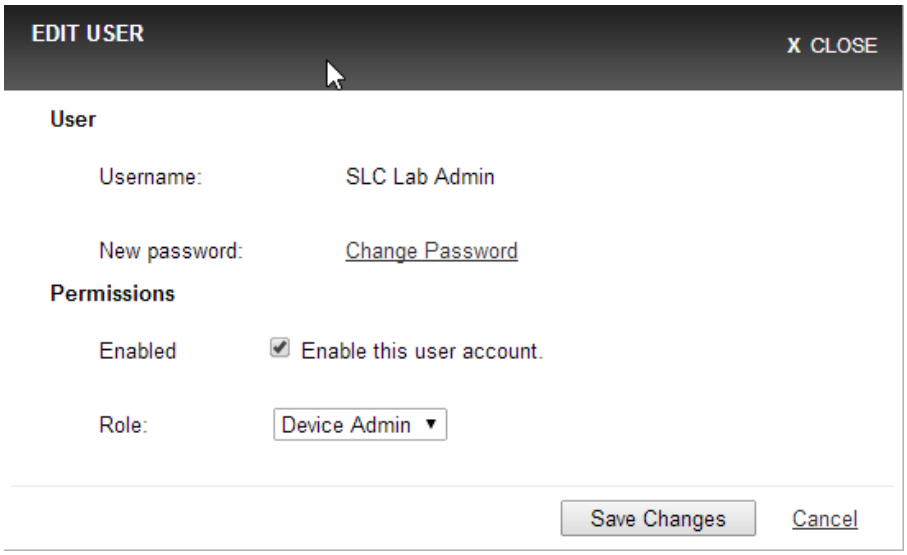
To add a new user, click **Add User**. 



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.



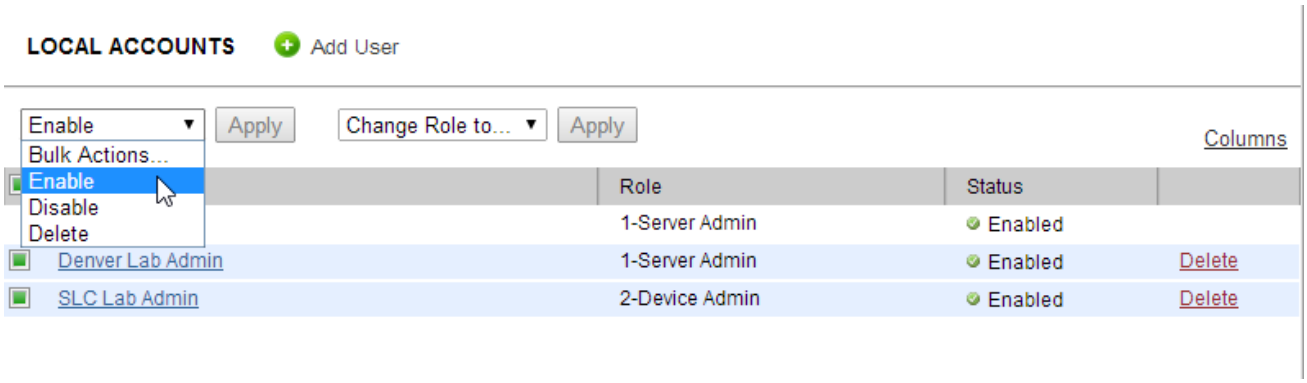
To change a user's password, see See Changing Passwords on page 33.

Delete User

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

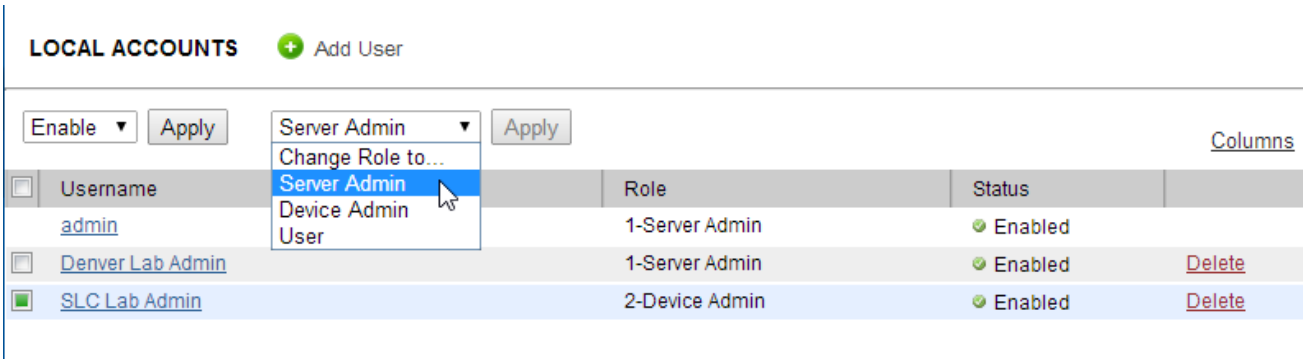
Bulk Actions

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:



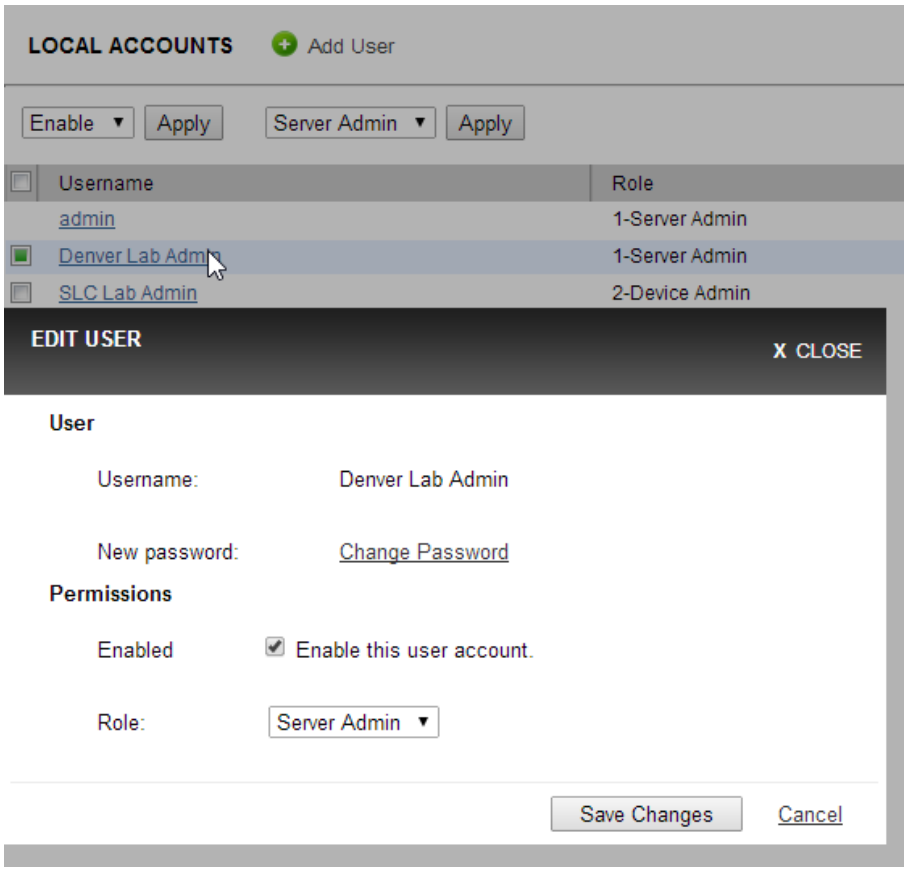
Then click **Apply.**

The available roles are:

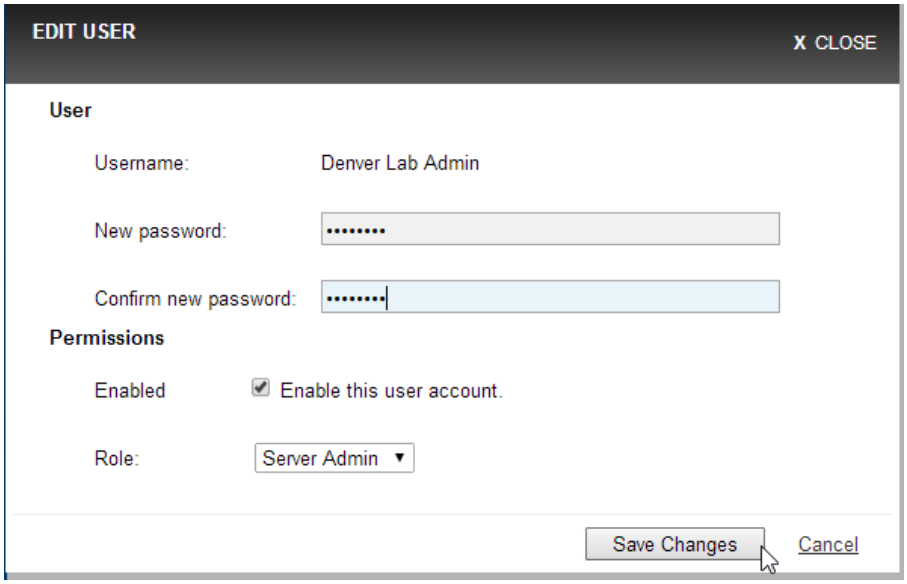
- Server Admin - The Server Admin role can administer the server and change configuration and settings on the server and the ioMemory devices attached to the server.
- Device Admin - The Device Admin role can administer and configure the ioMemory devices attached to the server, but cannot make changes to the server.
- User - The User role has read-only privileges to the server and devices attached to the server, but cannot make changes to either of them.

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.

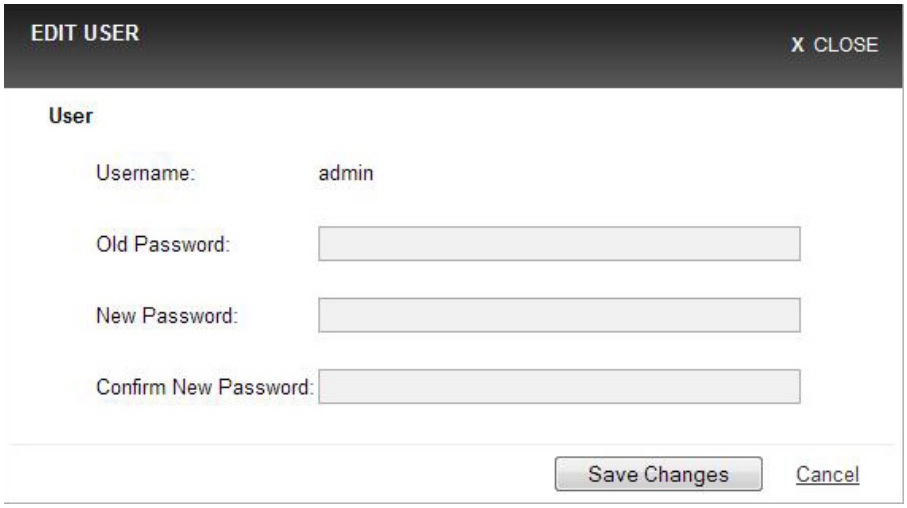


Enter the new password information, then click **Save Changes.**

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 High IOPS and io3 Flash Adapters 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 **`ibm-flash-management-console-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:

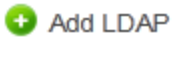
- Set the Search Base DN field to the user's entry: **`${dn}`**
- Set the Search Filter: **`(objectclass=*)`**
- Set the Scope to Base level
- Set the Role to User

Identity Providers

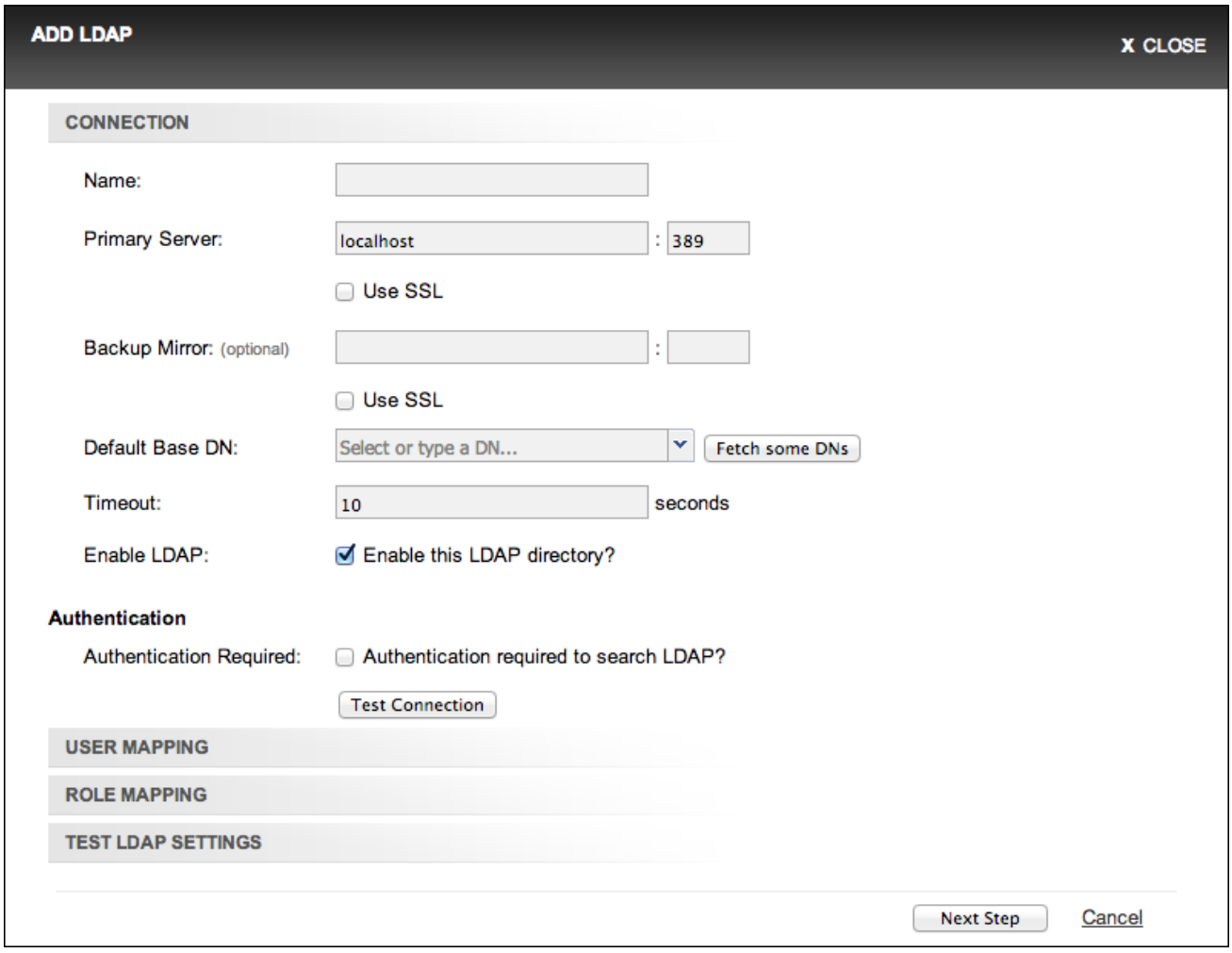
Currently the Flash Management Console only supports LDAP identity providers.

For more information about LDAP settings, refer to See Appendix A - Adding and Editing LDAP Providers on page 56

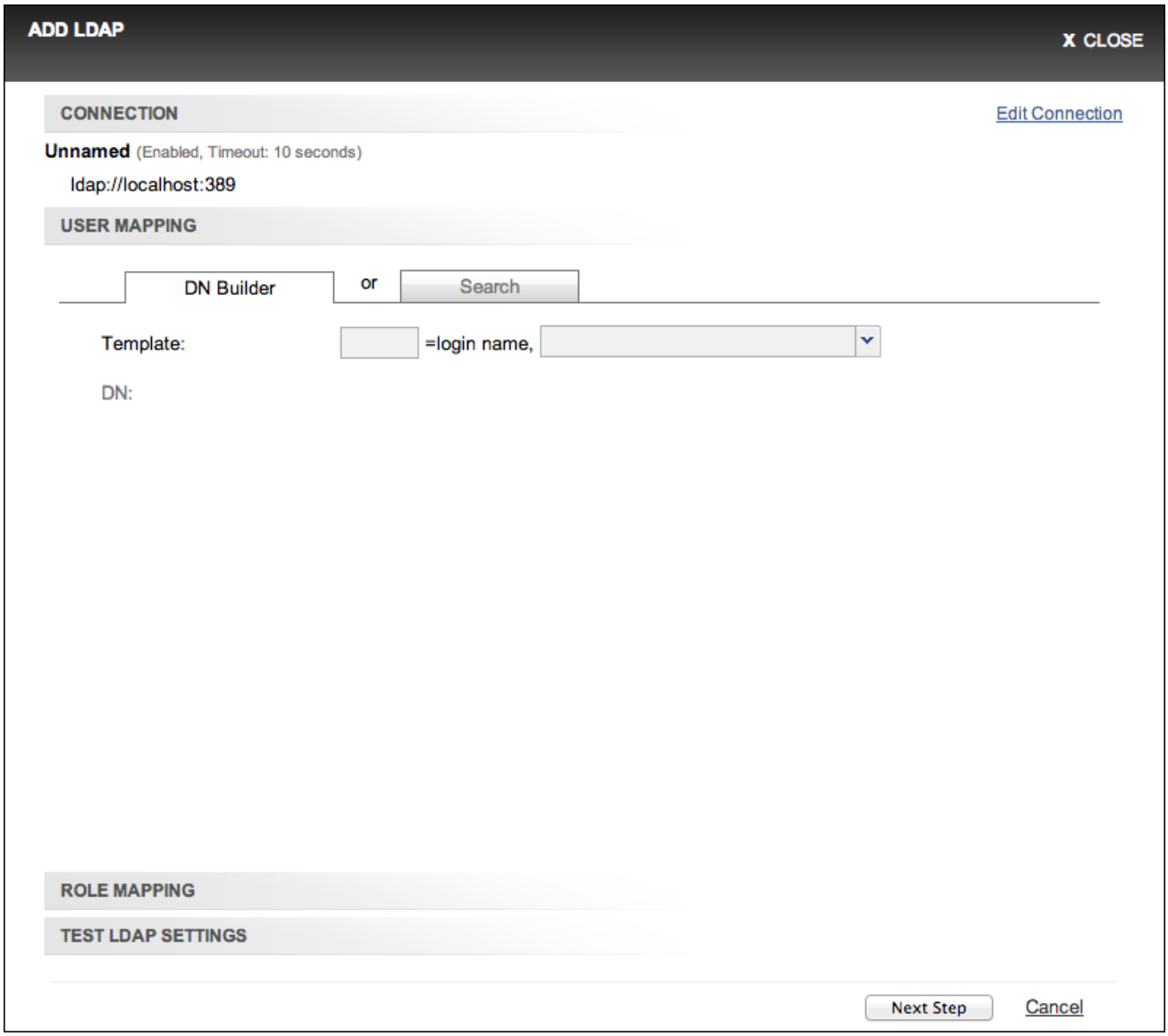
Add LDAP

Click the **Add LDAP** 

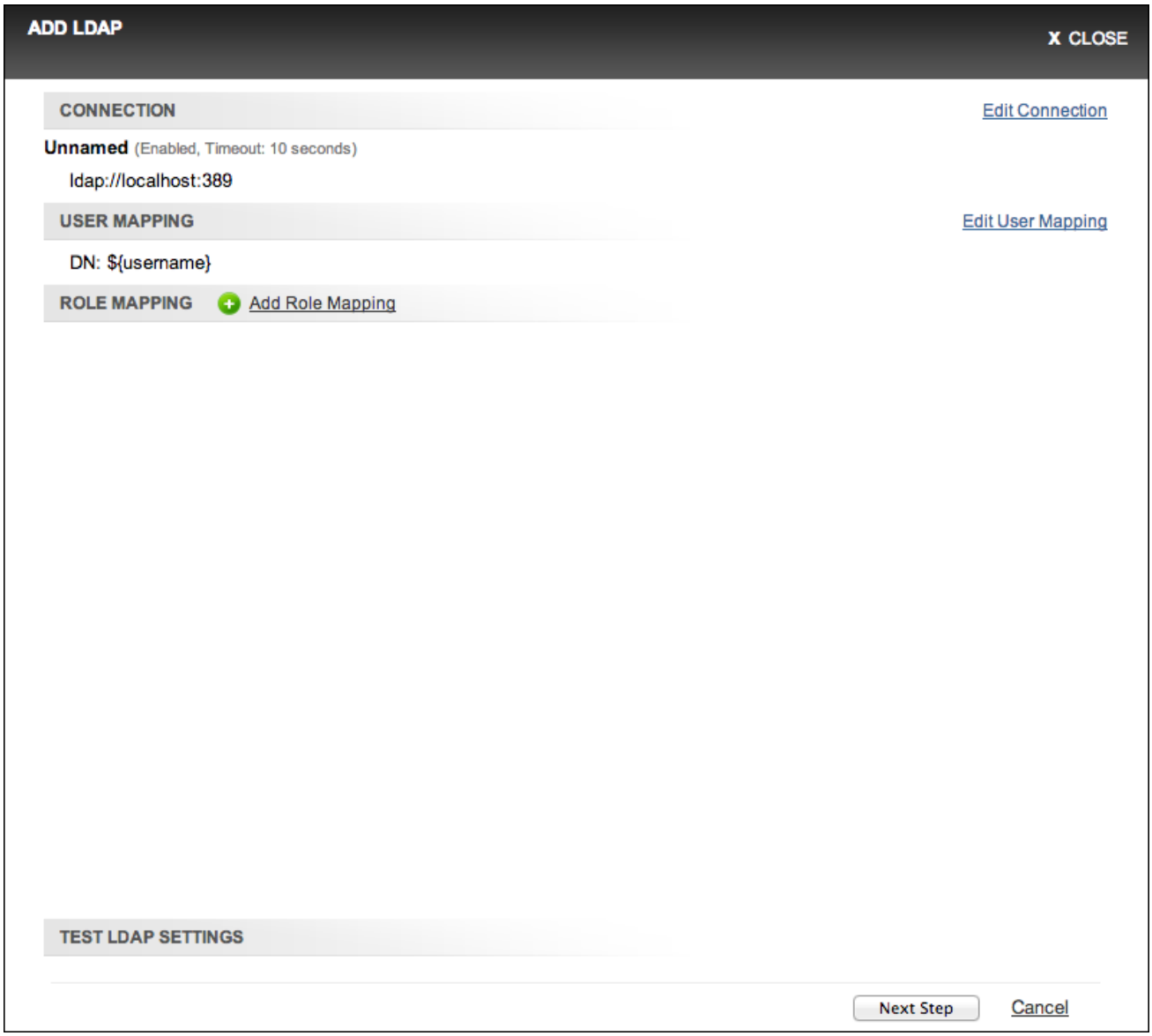
link to open the Add LDAP wizard, where you can configure the LDAP connection, User Mapping, Role Mapping, test LDAP settings, and add additional LDAP configurations.



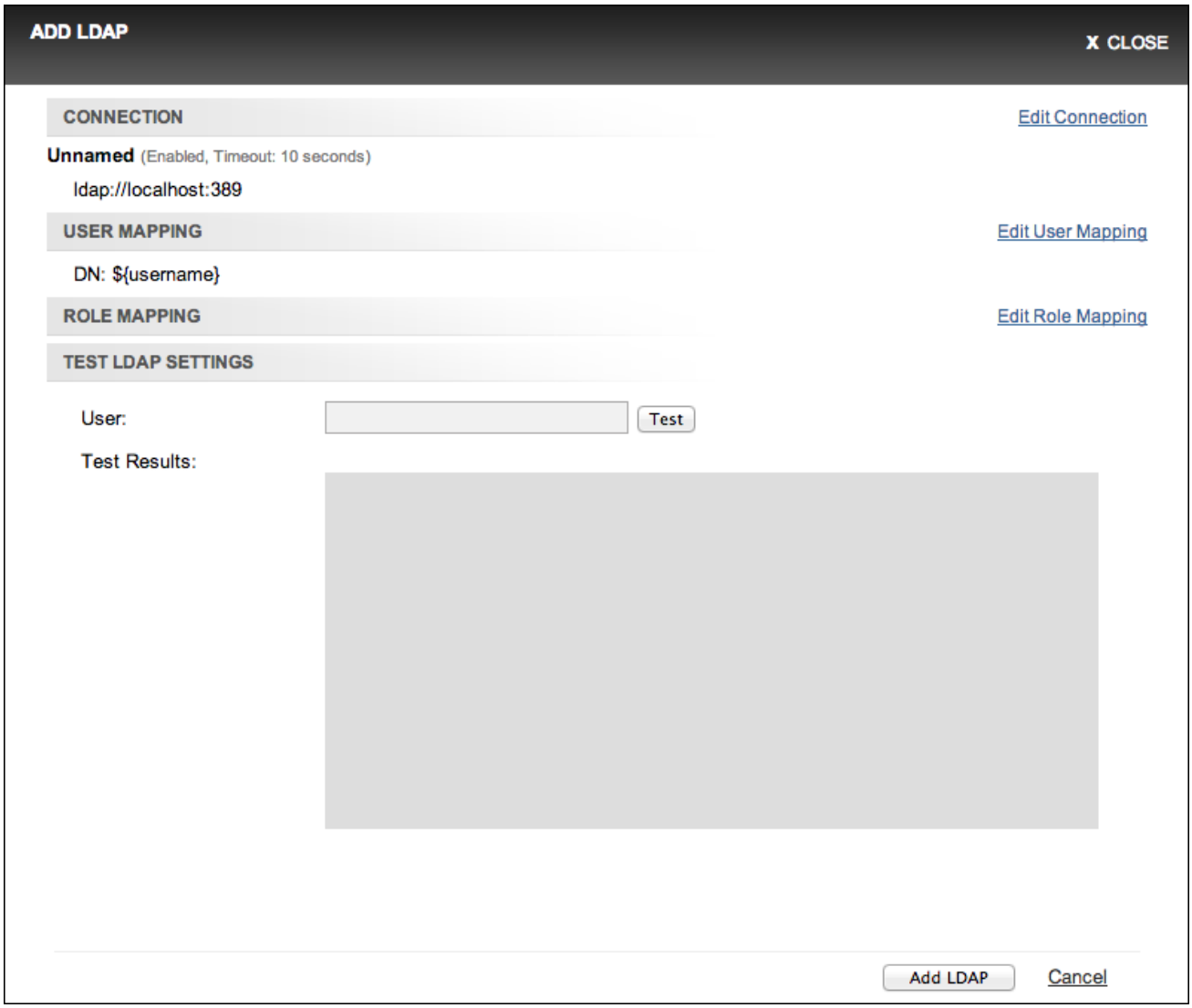
Enter the LDAP connection information, then click **Next Step.**



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

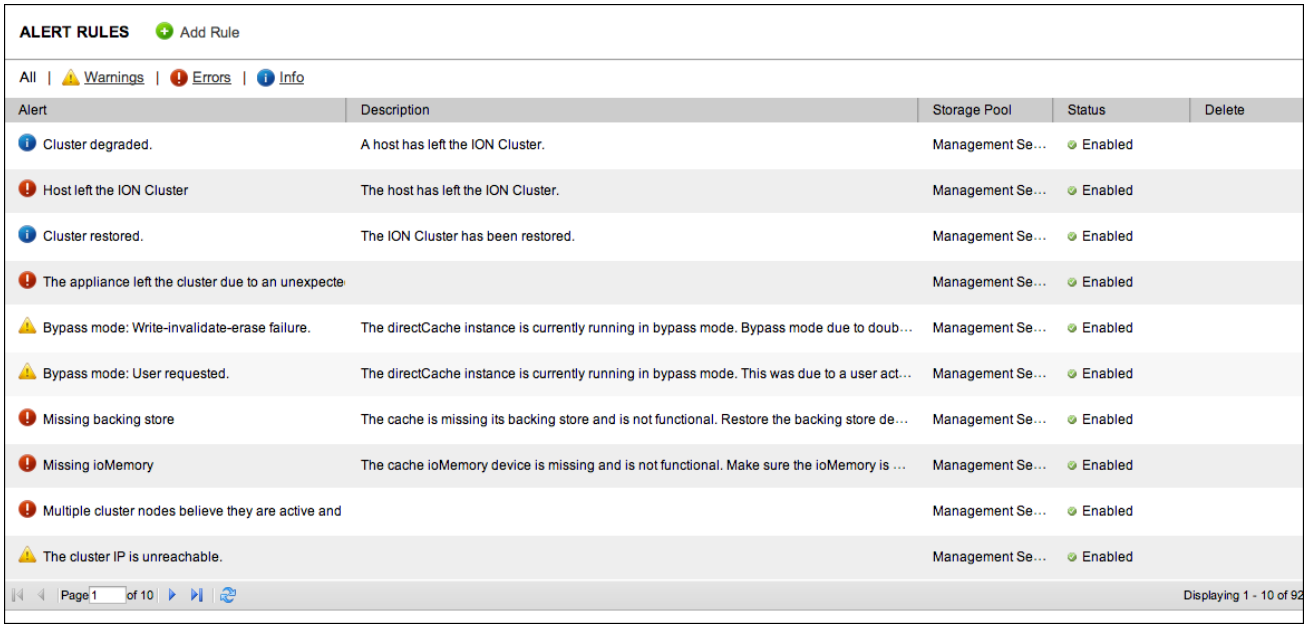
To edit an LDAP entry, click on the Provider link.

Delete LDAP

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

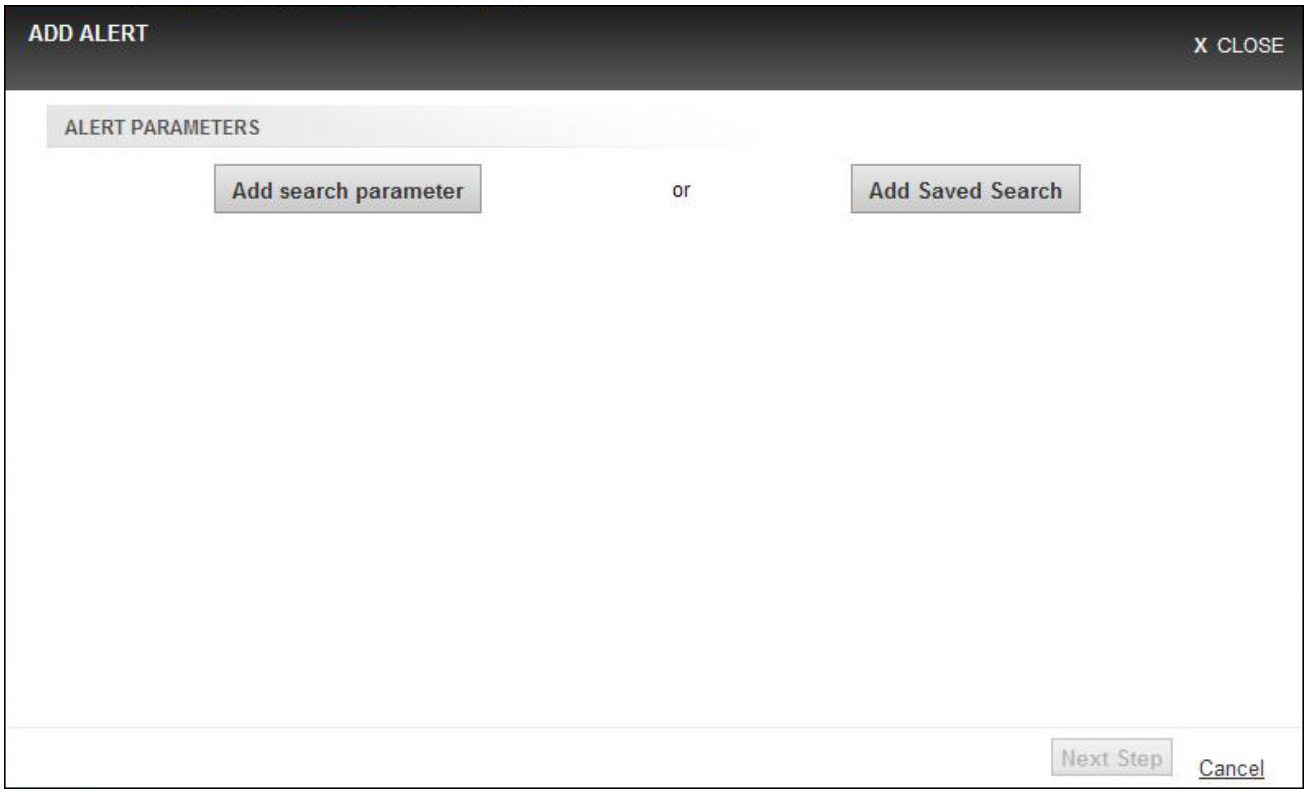
Rules

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

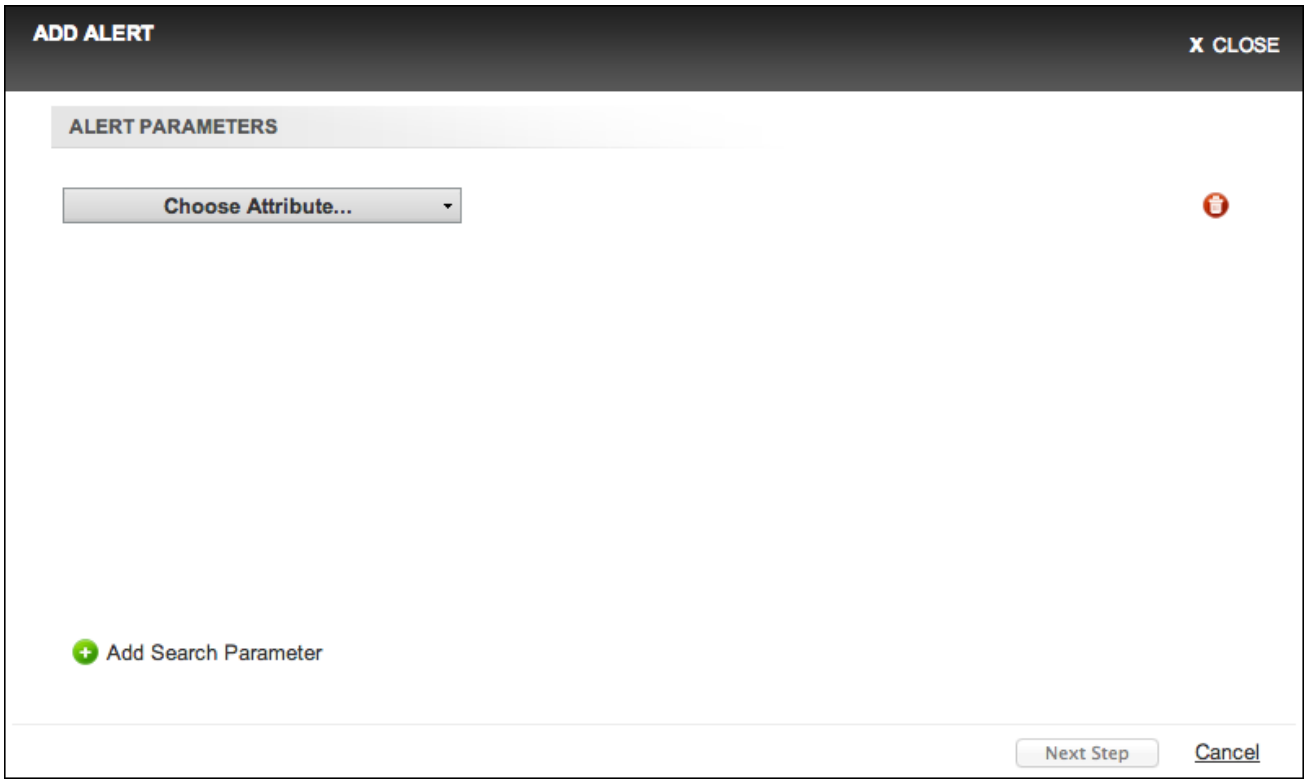


Add Rule

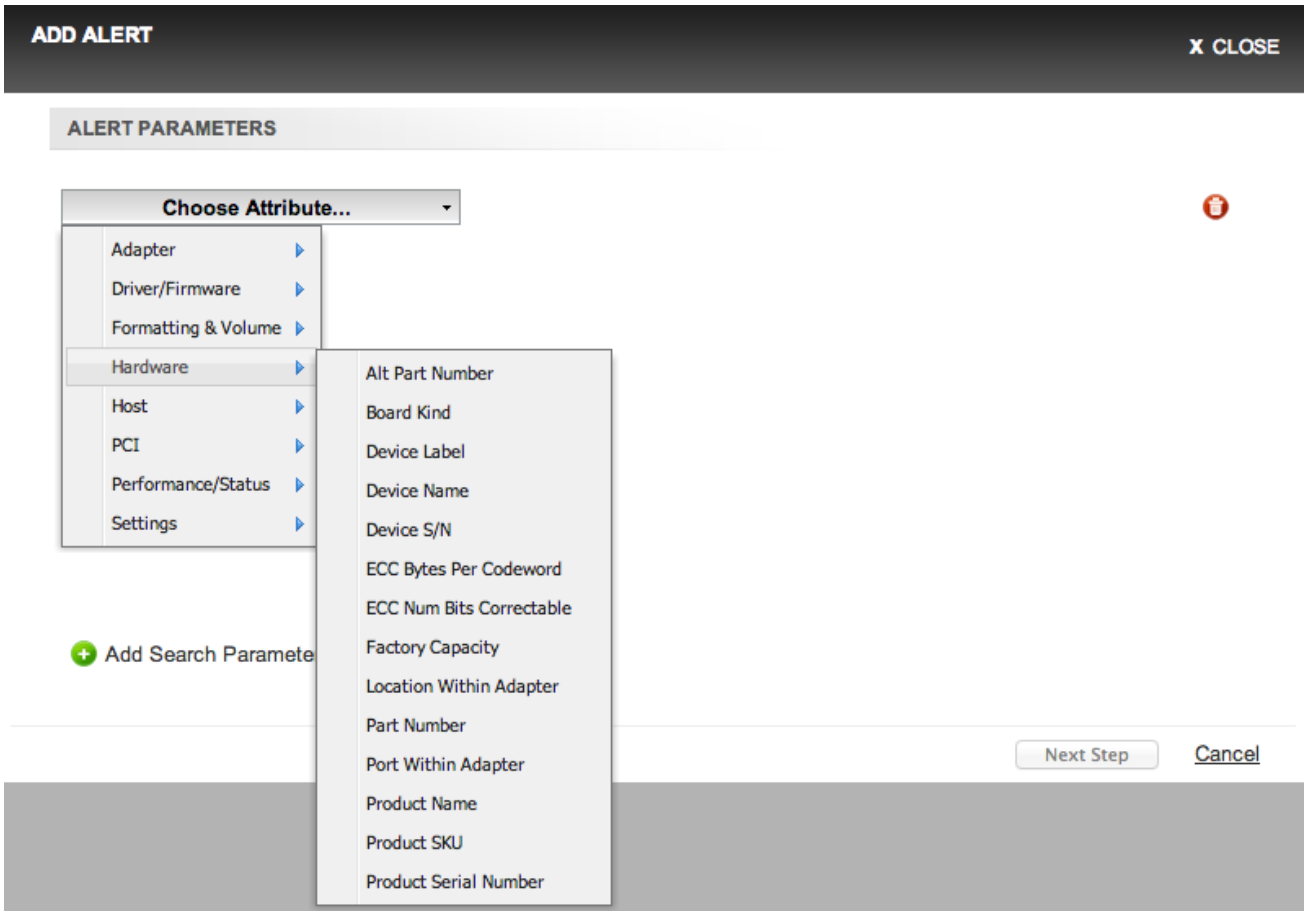
Click the Add Rule link to open the Add Alert dialog, where you can create a custom filter that will trigger an alert.



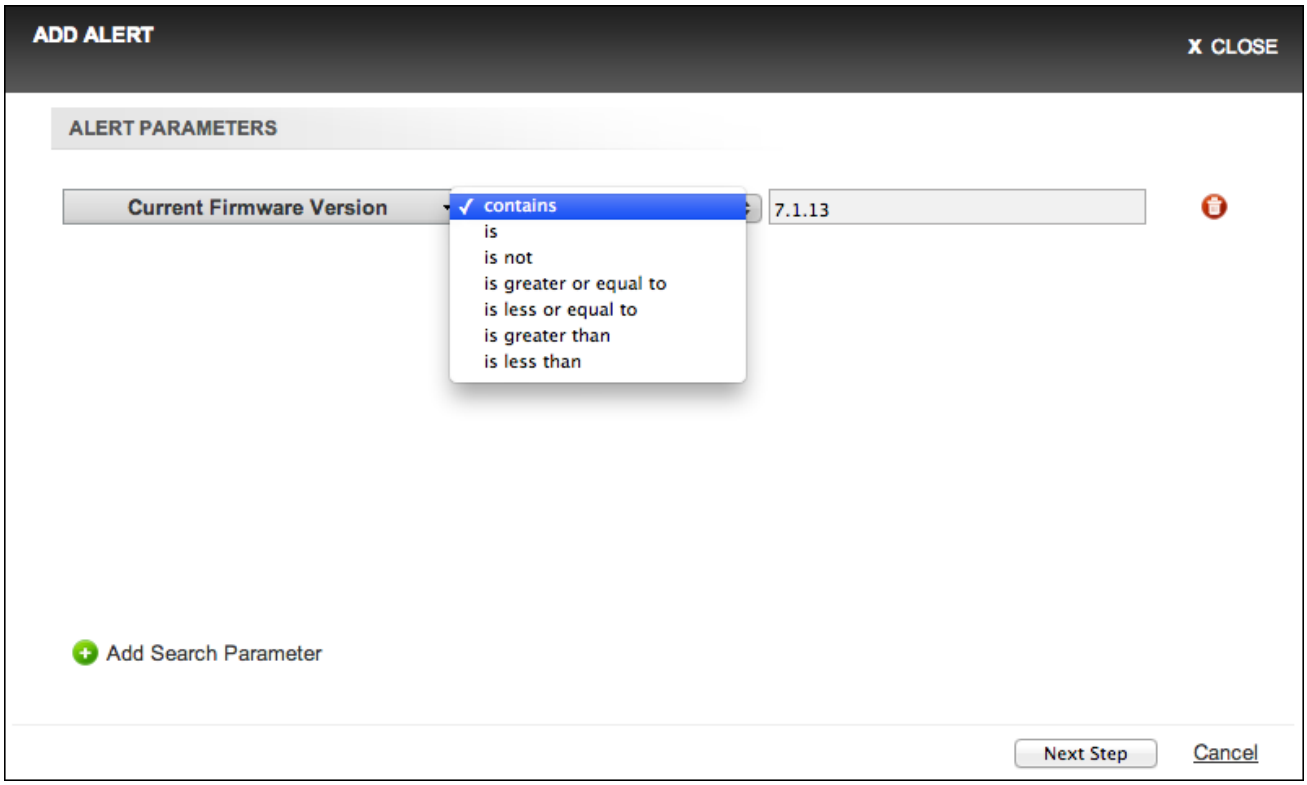
In the Add Alert dialog, click **Add search parameter** or (if you have one or more saved searches) the **Add Saved Search** button. When you add a saved search, its parameters are automatically added to the new Alert.



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



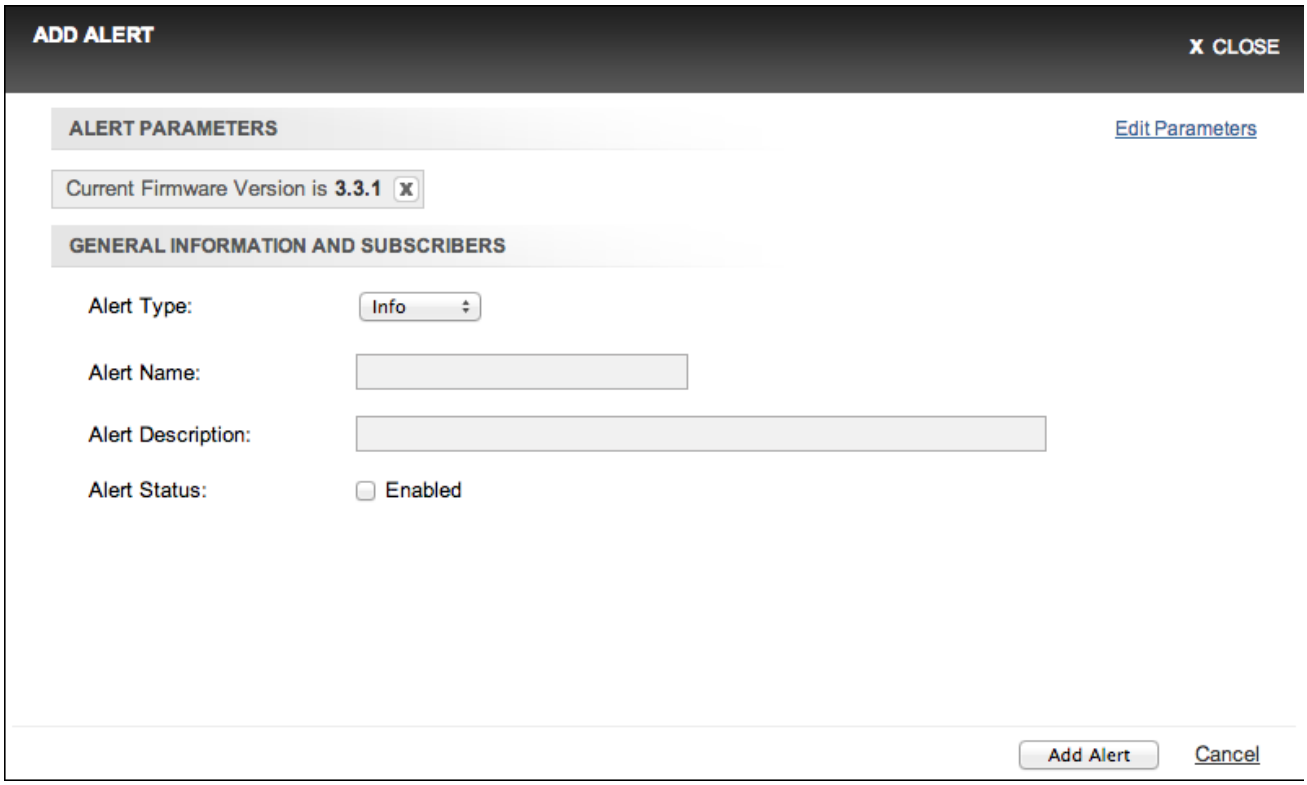
Enter the Rule parameters for the chosen attribute.



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

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

Click **Next Step** 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 **Add Alert** 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

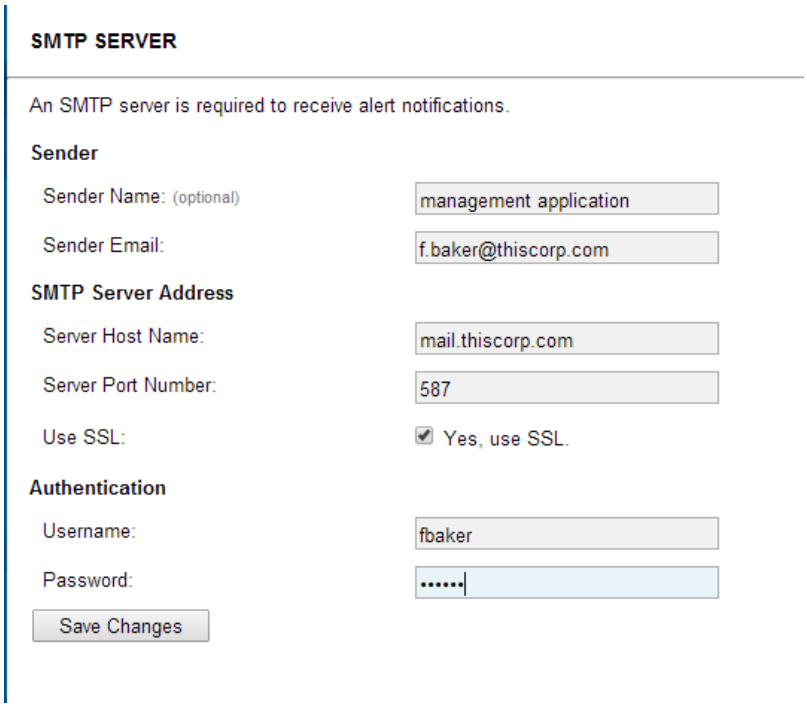
To delete a custom rule entry, click on the **Delete** link next to the **Rule.**

NOTE-

Only custom rules can be modified and deleted.

SMTP Server

In order for the Flash Management Console 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.

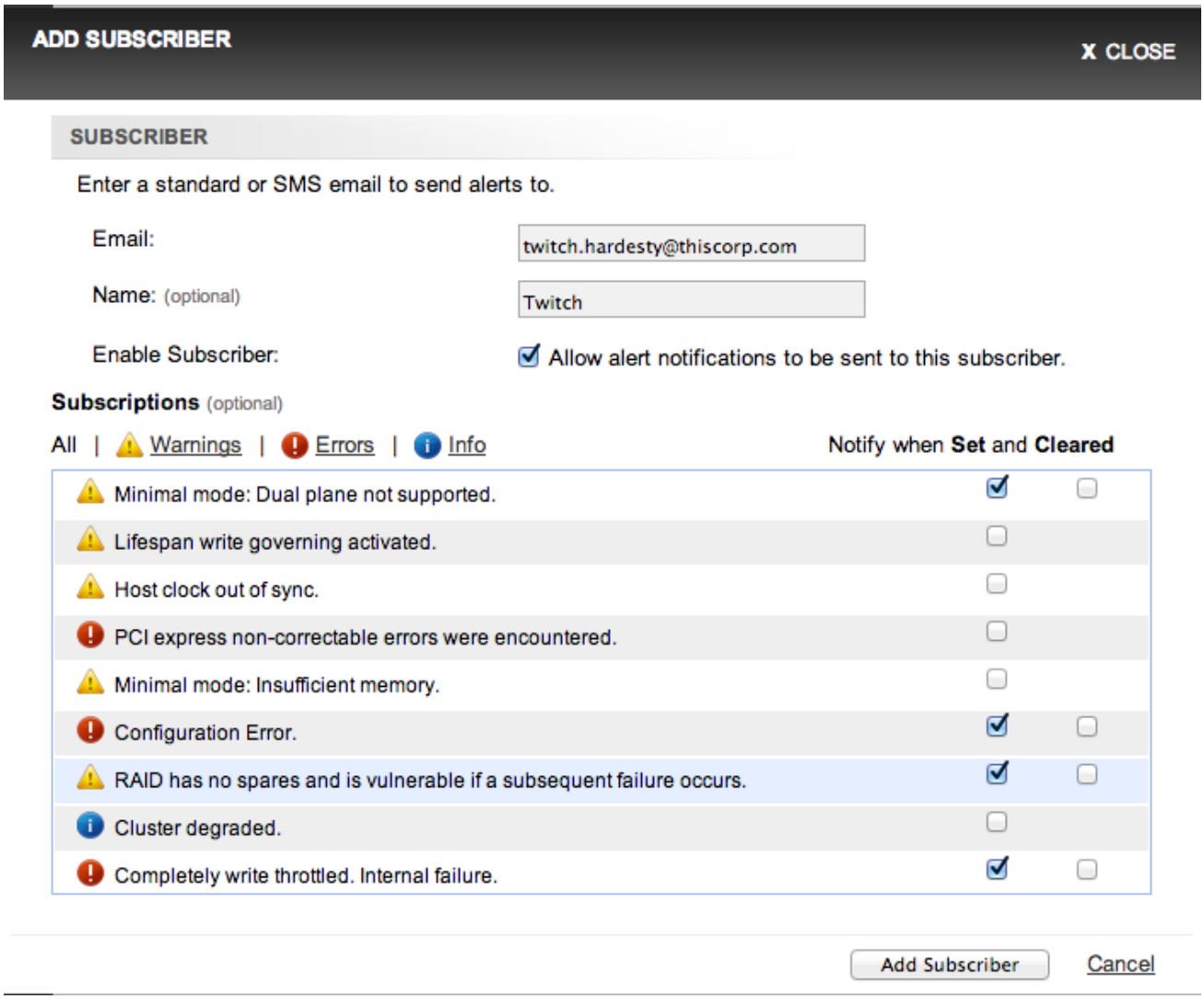


Subscribers

The Flash Management Console Management Solution can send email alerts to an 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 an 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.

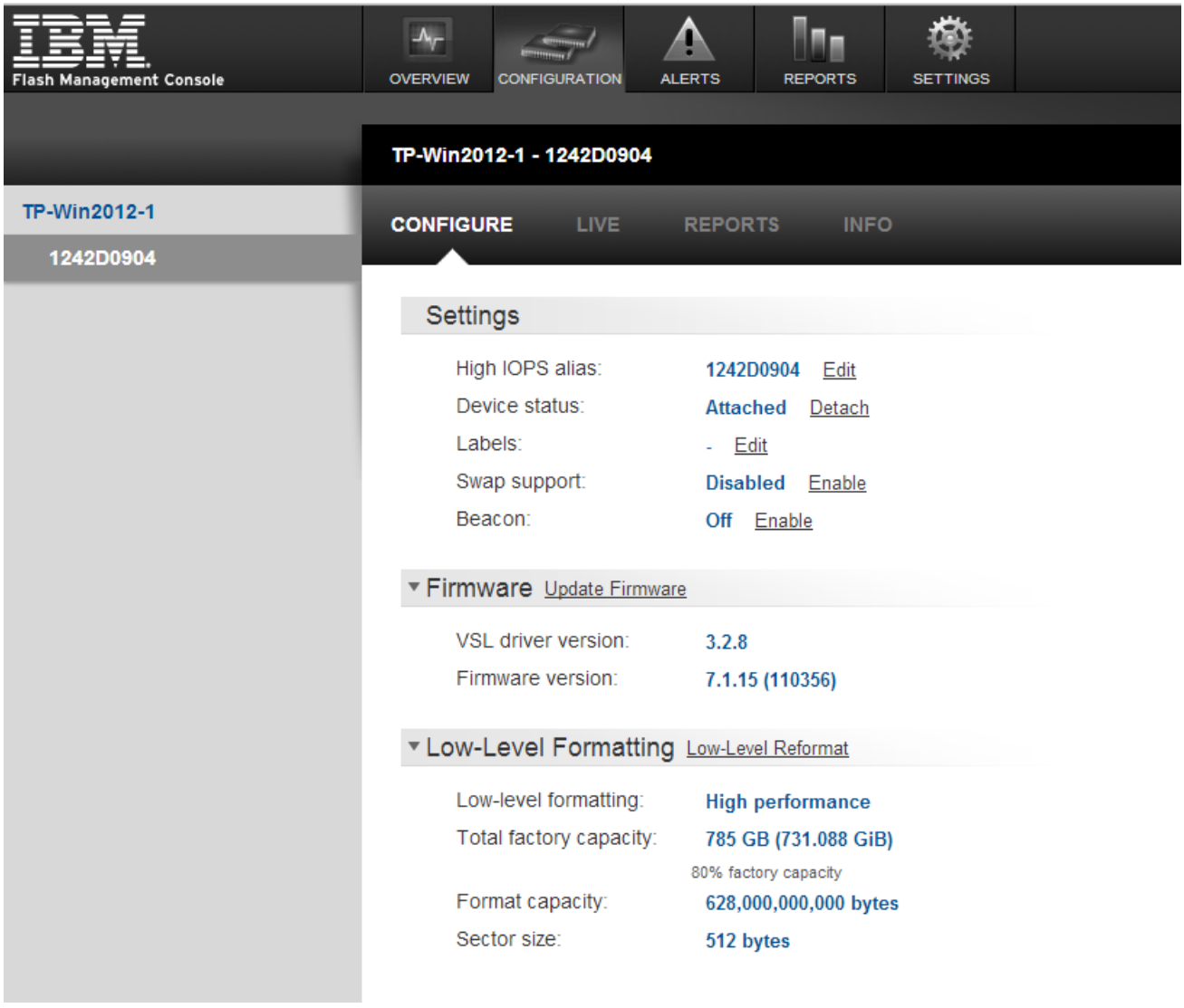
Delete Subscriber

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

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 Flash Management Console
- Click an High IOPS and io3 Flash Adapters link name link from any table in Flash Management Console.



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 High IOPS and io3 Flash Adapters installed in that server, and a tab panel on the right monitors and lets you perform configuration tasks.

Configure Device Tab

Here you can edit the following settings:

- High IOPS and io3 Flash Adapters Alias (Name, by default the serial number is used)
- Device Status (Attach/Detach)
    - The Attach Device operation creates a link so the High IOPS and io3 Flash Adapters interacts with the operating system. In most cases, the operating system driver automatically attaches the installed High IOPS and io3 Flash Adapters(s) at boot time, so you only need to use Attach Device when you manually detach an High IOPS and io3 Flash Adapters (such as to perform a low-level format).
    - Detach Device disconnects your High IOPS and io3 Flash Adapters 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 High IOPS and io3 Flash Adapters to perform a low-level format or a firmware upgrade.
- Labels/Change Labels link
- Swap Support (Enable/Disable)
  High IOPS and io3 Flash Adapters 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.

Attention!

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.

Attention!

You must have 400MB of free RAM per 80GB of ioMemory device capacity (formatted to 4KB block size) to enable an High IOPS and io3 Flash Adapters 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 High IOPS and io3 Flash Adapters's LEDs to blink, making it easier to find among several devices.

You can also update firmware (see See Appendix B - Software Updates on page 65 for more information) and perform a low-level reformat.

Live Device Tab

The Live tab lets you monitor important information for one or several High IOPS and io3 Flash Adapterss in real time. The Live tab displays IOPS Read/Write when Operations is selected, MB/Second when Data is selected. The following table describes the information displayed in the various graphs on the High IOPS and io3 Flash Adapters Live Performance screen.

Item	Description
Data	A histogram of average megabytes per second being read or written to the Cache devices.
Operations	A histogram of average operations per second (shown in KIOPS) being performed on the Cache devices.
Combined Read/Write	Overlapping histograms of actual reads and writes to the Cache devices. The histogram is updated every second.
Temperature	The temperature of the FPGA on the High IOPS and io3 Flash Adapters. Operating temperatures of devices vary, but throttling on older devices may occur after 78° C.
Current RAM	The current RAM being consumed on the host by the driver.
Peak RAM	The peak amount of RAM that has been consumed since power on by the driver.
PBW Performance	This value reflects the amount of wear experienced by the High IOPS and io3 Flash Adapters. Values of 100% represent no wear on the device, or, that the device has 100% of its endurance left.
Reserve Space	As the High IOPS and io3 Flash Adapters retires bad memory locations it moves the data at those bad locations to reserved space. This value reflects the amount of reserve space still available.

Reports Device Tab

The **Reports** tab shows from three to five history graphs for a single High IOPS and io3 Flash Adapters:

- Operations
- Data & Endurance
- Temperature
- Cache Hit Requests (available only when the device is being used as a cache)
- Cache Latency (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 High IOPS and io3 Flash Adapters 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 High IOPS and io3 Flash Adapters, 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).

Info Device Tab

The **Info** tab provides details about a single High IOPS and io3 Flash Adapters.

About VMware Support

There is no agent that runs on vCenter or ESX/ESXi servers. Flash Management Console support for vCenter and ESXi is provided through the IBM FlashCache Storage Accelerator. Download and deploy IBM_FCSA_Virtual-2.2.3.•••.ova from your vCenter to intall the plug-in for the VMware environment.

Maintenance and Troubleshooting

The following items provide information on troubleshooting issues with Flash Management Console.

Location of Flash Management Console Logs

On Linux, Flash Management Console logs can be found in the following directory:

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

On Windows, Flash Management Console logs can be found in the following folder:

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

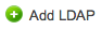
Changing a Management Server's Host Name

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

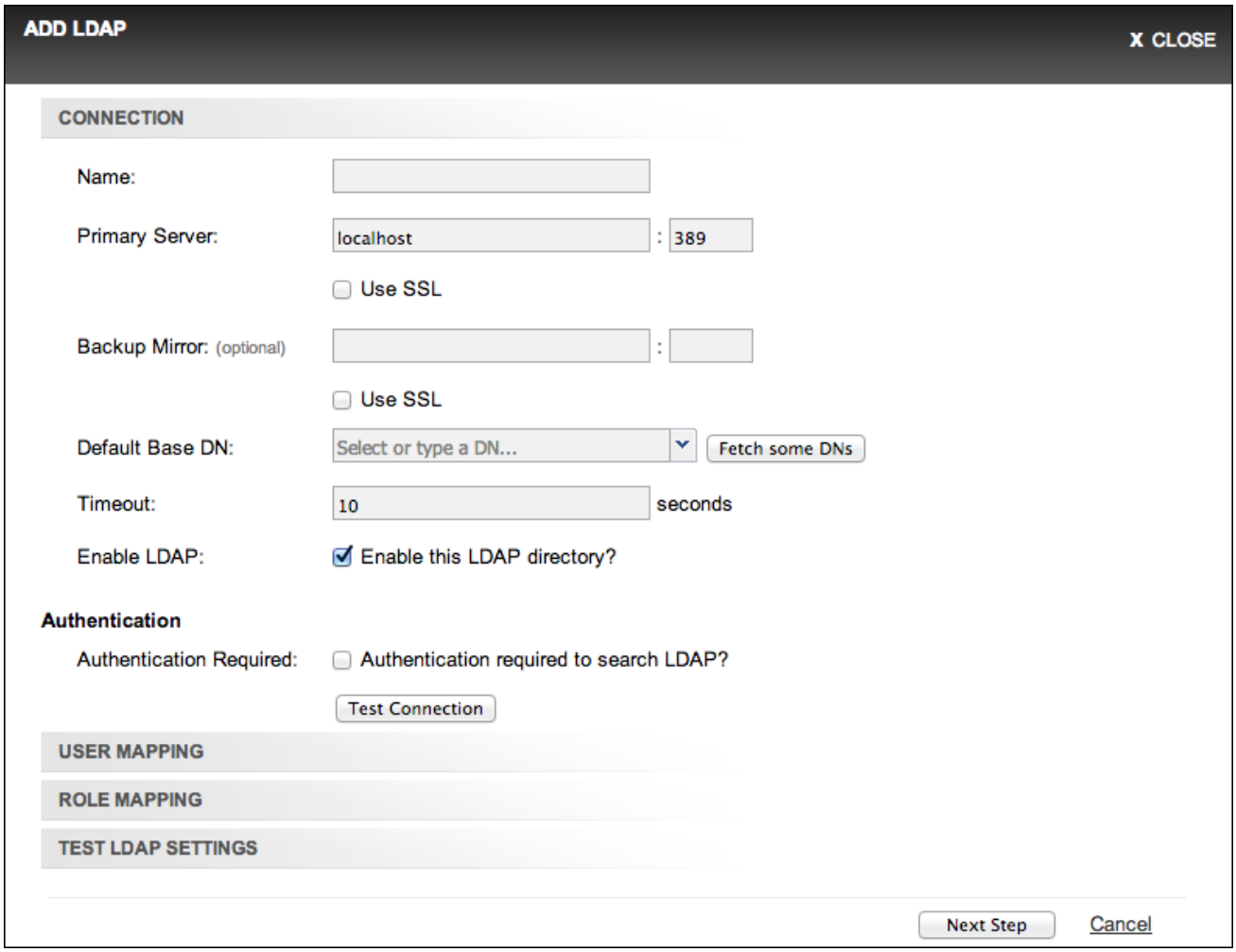
1. Open a browser to the management server UI (for example: **`https://new-host-name`**), login and navigate to the **Settings > REMOTE SETTINGS** screen.
2. Select the host name or IP address you would like the management server to use from the host name drop-down.
3. Update custom certificate and key 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.

NOTE-

The Flash Management Console 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.

NOTE-

The Flash Management Console 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.

NOTE-

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.

NOTE-

The Auth DN and Password are securely stored in the Flash Management Console, 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

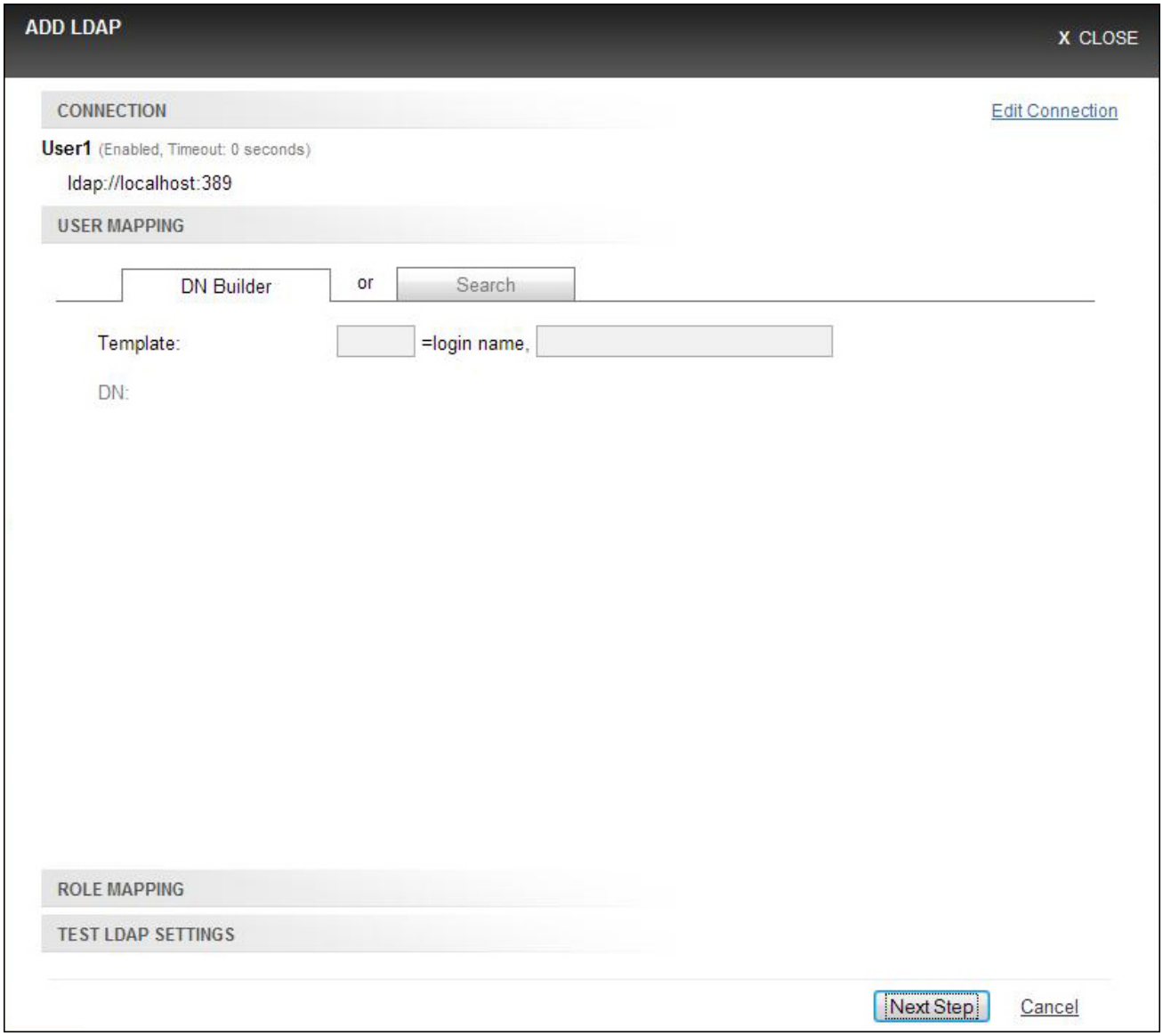
Any errors encountered are displayed at the top of the dialog.

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.

Flash Management Console 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).

NOTE-

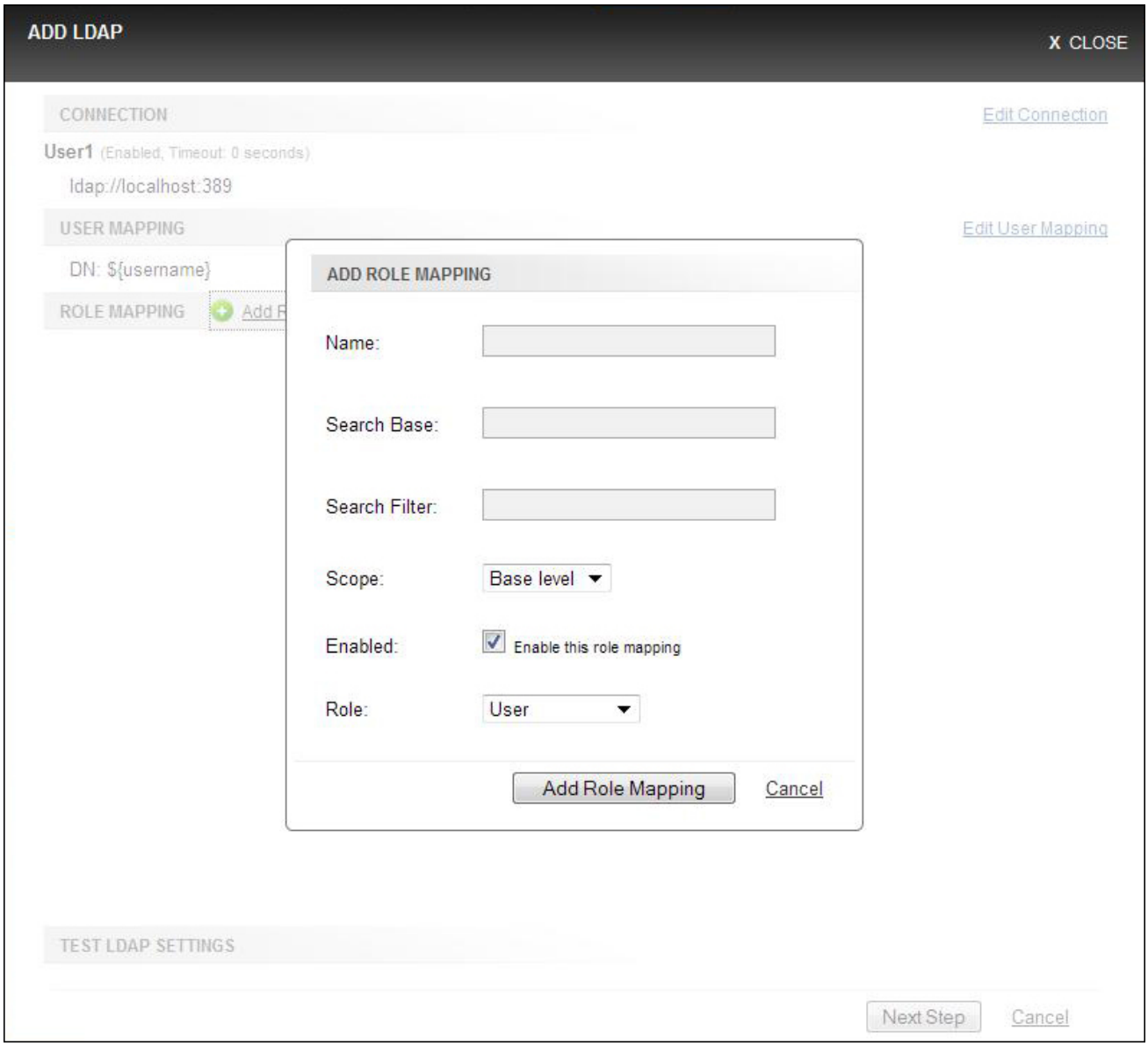
The special token "$\{username\}" is replaced with the name the user is attempting to log in with when Flash Management Console performs the authentication.

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 Flash Management Console: 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

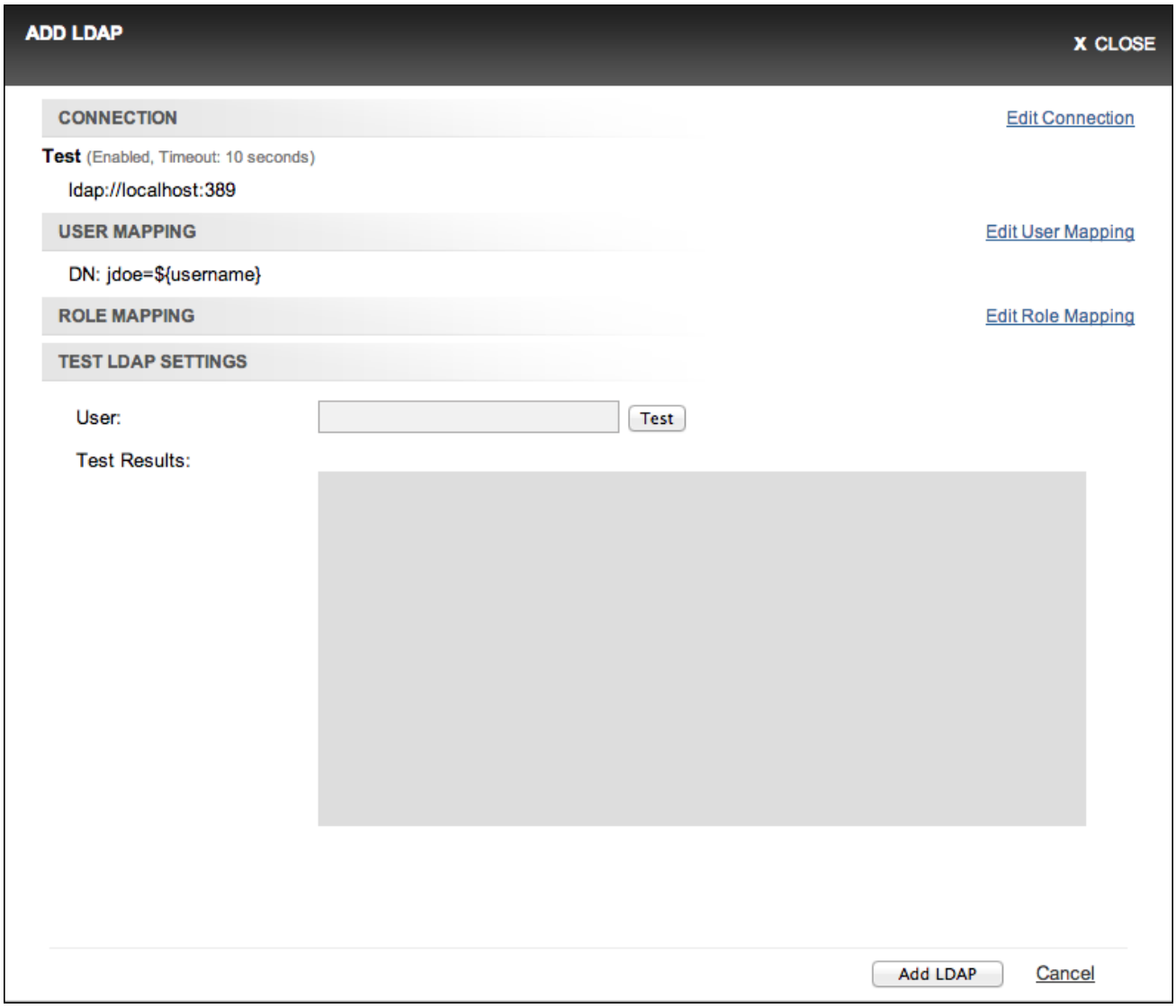
Grant the User role to everyone who is able to authenticate

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 High IOPS and io3 Flash Adapterss involves two procedures: updating the High IOPS and io3 Flash Adapters VSL (driver) on the host machine, and updating the firmware on the High IOPS and io3 Flash Adapters.

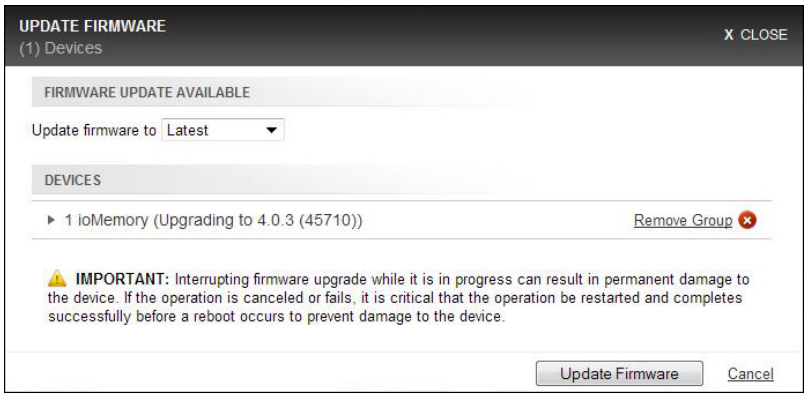
To update the High IOPS and io3 Flash Adapters VSL on the host machine:

1. Get the latest High IOPS and io3 Flash Adapters VSL files and documentation.
2. Follow the instructions in the *High IOPS and io3 Flash Adapters VSL User Guide* to install the High IOPS and io3 Flash Adapters VSL on the host machine.
3. 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:
   Fusion ioMemory VSL software 3.x **`C:\Program Files\Fusion-io ioMemory VSL\Firmware`**
   Fusion ioMemory VSL software 4.x **`C:\Program Files\SanDisk\Fusion 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 High IOPS and io3 Flash Adapterss:

1. Open the Flash Management Console.
2. If you are using Flash Management Console, 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. 

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

Config History - Flash Management Console

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 High IOPS and io3 Flash Adapters 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 Legacy High IOPS Adapter 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 Lenovo.

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

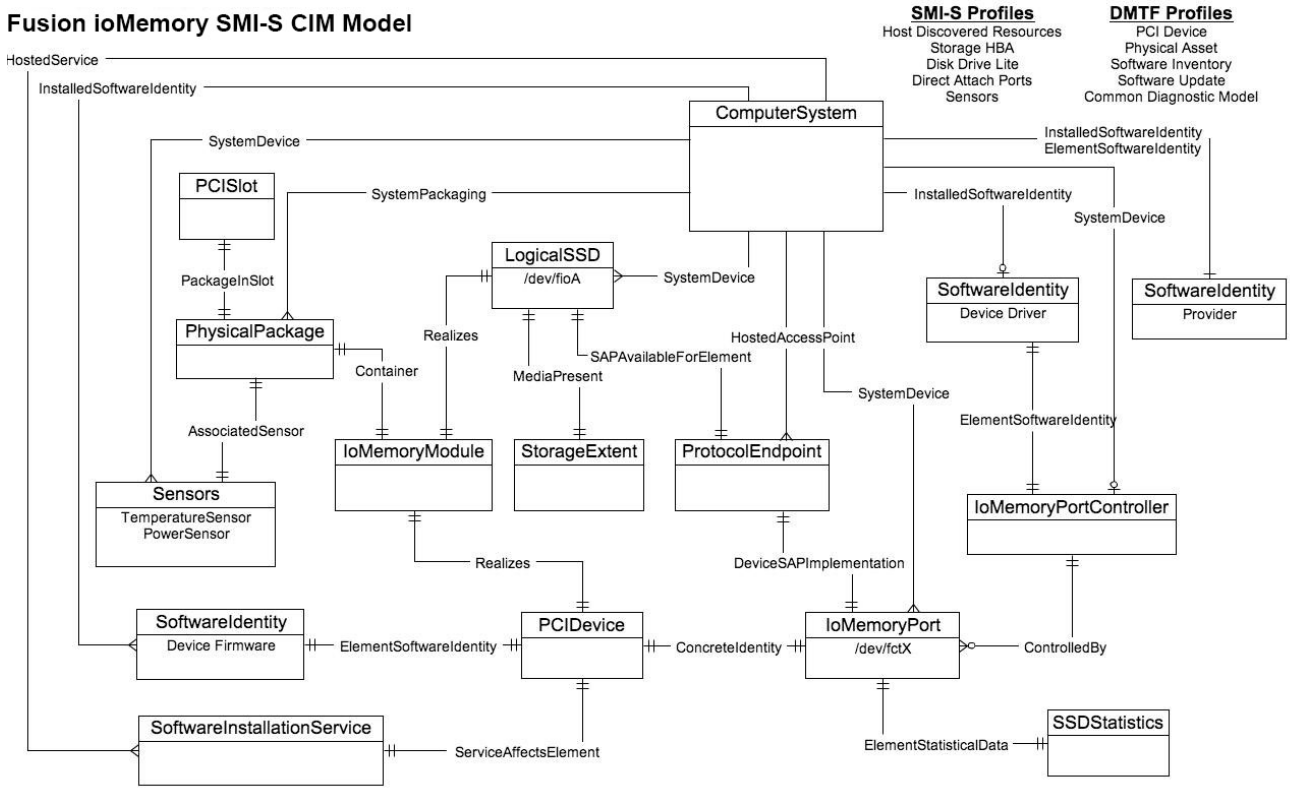
SMI-S v1.4 Common Diagnostic Model
http://www.dmtf.org/standards/mgmt/cdm/

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 Lenovo.

The Lenovo Legacy High IOPS Adapter 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 Legacy High IOPS Adapter 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.



The central instance of the model is an instance of the High IOPSPort class, a logical representation of the High IOPS and io3 Flash Adapters module and associated PCI adapter. It supports the extrinsic methods necessary to provision the drive. An instance of PCIDevice and High IOPSPort exists for each Lenovo High IOPS and io3 Flash Adapters module installed in the system and they are associated with an instance of ConcreteIdentity. An instance of SSDStatistics is associated to each High IOPSPort by an ElementStatisticalData association and contains important performance and capacity data pertaining to the associated drive. High IOPSPort is scoped by an instance of the ComputerSystem class. The SystemDevice aggregation aggregates ioMemory modules within the containing ComputerSystem.

An instance of High IOPSPortController represents the functional driver used to control the High IOPS and io3 Flash Adapters modules installed in the host system. High IOPSPortController specializes CIM_ PortController. It aggregates High IOPSPorts with the ControlledBy aggregation. The driver version and vendor information are represented by the SoftwareIdentity instance associated to High IOPSPortController 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 High IOPSPort 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 High IOPSPort 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 High IOPSPort using SAPAvailableForElement association and to the scoping ComputerSystem using the SystemDevice aggregation.

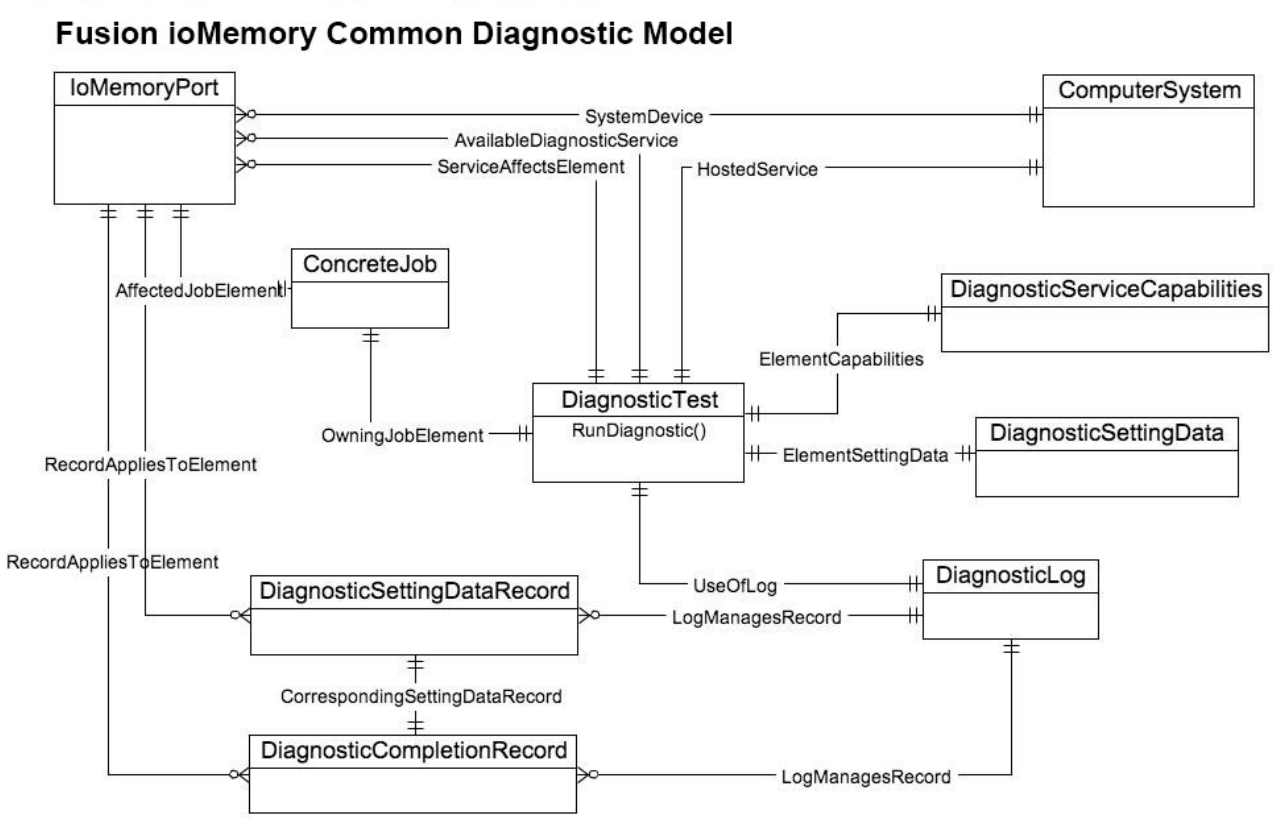
The High IOPS and io3 Flash Adapters module, being a PCI-E device, is also represented by an instance of the PCIDevice class. High IOPSPort is an alternate representation of the PCIDevice and its associated control device. It is associated to it by the ConcreteIdentity association.

Firmware installed on the High IOPS and io3 Flash Adapters 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 High IOPS and io3 Flash Adapters 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 High IOPS and io3 Flash Adapters 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 High IOPS and io3 Flash Adapters is installed is represented by an instance of the Slot class, which is associated to the PhysicalPackage class using the PackageInSlot association.

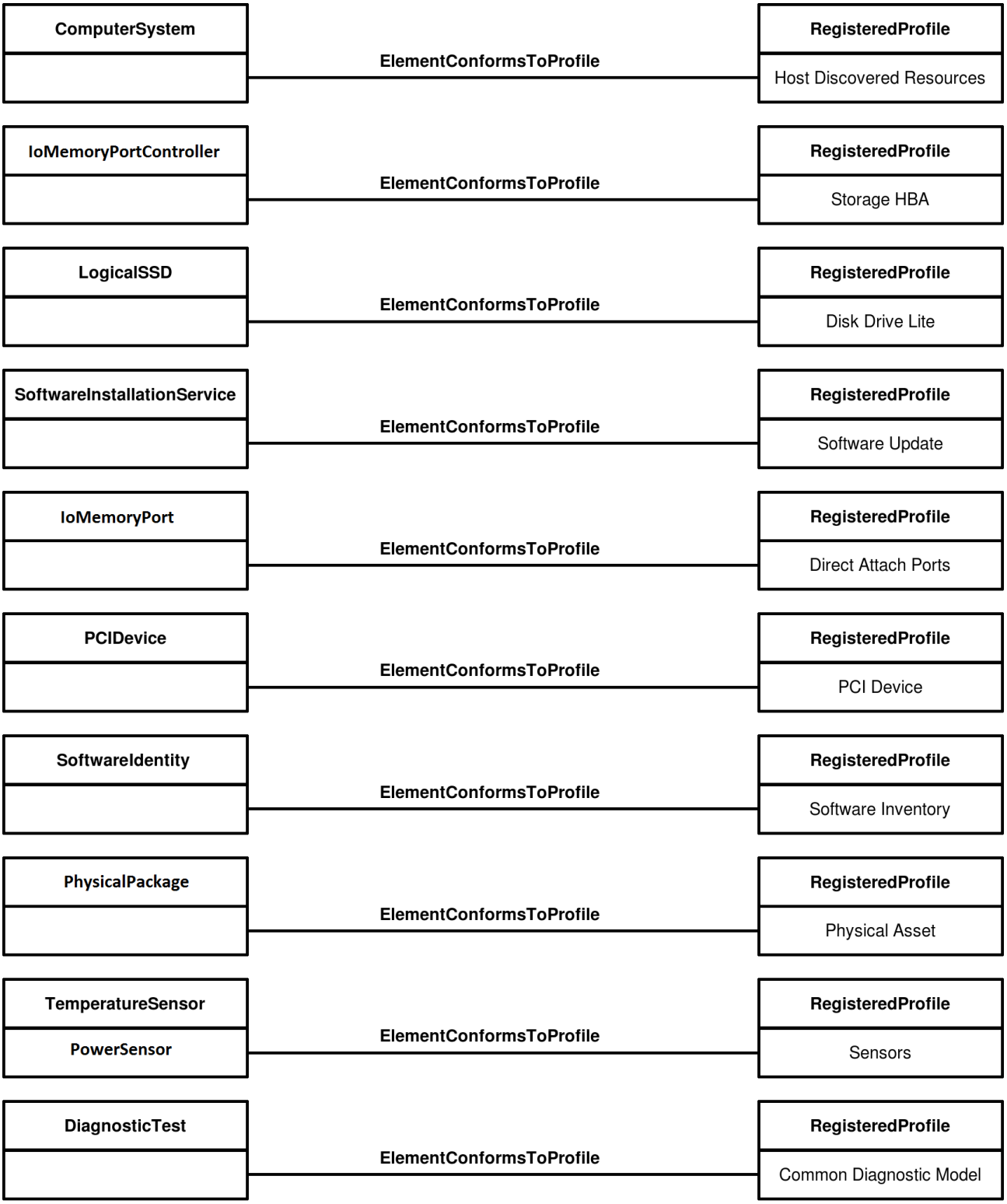
The following figure shows the details of the Common Diagnostic Model for Fusion-io drives.



The central class is DiagnosticTest. An instance is always be available by associations to ComputerSystem and each High IOPSPort. After a test is run using the RunDiagnostic method specifying the target High IOPSPort, 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 Lenovo 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 Lenovo device CIM model. Not all class properties are described in detail. Consult the CIM schema for detailed description of all properties.

Data Model Classes

High IOPSPort

One instance of High IOPSPort exists for each Lenovo High IOPS and io3 Flash Adapters 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 High IOPS and io3 Flash Adapters 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.

High IOPSPorts are aggregated by High IOPSPortController via the ControlledBy aggregation. High IOPSPorts are associated to their corresponding PCIDevice with the ConcreteIdentity association. High IOPSPorts 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.

High IOPSPorts is aggregated by **High IOPSPortController** via the **ControlledBy** aggregation. **High IOPSPorts** are associated to their corresponding PCIDevice with the ConcreteIdentity association. **High IOPSPorts** 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 High IOPS and io3 Flash Adapters modules. Logically, it looks just like two Legacy High IOPS Adapters. The **High IOPSPort** class is extended to

include information about the carrier card type, serial number and external power connection. This way, both the Legacy High IOPS Adapter and the ioDuo is supported.

SSDStatistics

One instance of SSDStatistics exists for each **High IOPSPort** 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 **High IOPSPort** is *Attached.*

High IOPSPortController

Only one instance of **High IOPSPortContoller** exists, representing the driver software used to control **High IOPSPorts**. **High IOPSPortController** specializes **CIM_PortController.**

High IOPSPortController is aggregated to the scoping **ComputerSystem** using the **SystemDevice** aggregation. **High IOPSPortController** 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 **High IOPSPort** and is associated to the **High IOPSPort** using the **DeviceSAPImplementation** association and **LogicalSSD** using the **SAPAvailableForElement** association. Since an High IOPS**Port** represents both the initiator and target ports, only one **ProtocolEndpoint** per **High IOPSPort** is needed to model the connection between **High IOPSPort** and **LogicalSSD.**

LogicalSSD

One instance of **LogicalSSD**, a subclass of **CIM_DiskDrive**, exists for each block device(**`/dev/fioX`**) exposed by a Lenovo 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 **High IOPSPort,** 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. **LogicallSSDs** are associated to their **ProtocolEndpoints** via **SAPAvailableForElement** association. If the **High IOPSPort** 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 High IOPS and io3 Flash Adapters 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 Lenovo

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 Lenovo 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 **High IOPSPort,** its alternate logical representation, using the **ConcreteIdentity** association. **PCIDevice** is also associated to **PhysicalPackage,** representing the physical aspects of the High IOPS and io3 Flash Adapters module, via the **Realizes** association.

PCISlot

One instance of **PCISlot** exists for each High IOPS and io3 Flash Adapters. 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 High IOPS and io3 Flash Adapters 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 **High IOPSPort.** The diagnostic run is synchronous and runs instantaneously.

The resulting **ConcreteJob** object associates to the originating **DiagnosticTest** instance and the respective **High IOPSPort** instance that was specified (for more information, see See Description on page 67). 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 High IOPS and io3 Flash Adapters 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 See Description on page 67). 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 High IOPS and io3 Flash Adapters. The Lenovo 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 **Lenovo 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

Property	Value
EventID	Not used
OwningEntity	“Fusion-io”
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 **Lenovo 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 **High IOPSPort** 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 High IOPS and io3 Flash Adapters 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 **High IOPSPort** health percentage reports 0% health. The reason for reduced writability can be found in the **ReducedWritabilityReason** property of the **High IOPSPort** 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 **High IOPSPort** health percentage continues to report 0% health when this happens.

Property	Value
IndicationIdentifier	<mfr>:<hostname>:read_only
PerceivedSeverity	Degraded/Warning (3)
ProbableCause	Other(1)

Property	Value
MessageID	FIO_0006
MessageFormatString	“Device <Device ID> is not allowing write operations”

Temperature indications

The High IOPS and io3 Flash Adapters 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 High IOPS and io3 Flash Adapters 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 Lenovo High IOPS and io3 Flash Adapters 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 High IOPS and io3 Flash Adapters 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 High IOPS and io3 Flash Adapters 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 High IOPS and io3 Flash Adapters 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 High IOPS and io3 Flash Adapters 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 Lenovo High IOPS and io3 Flash Adapters 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 Lenovo SMI-S provider implements a standard WBEM interface based on DMTF and SNIA standards for remote management of Lenovo 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 Lenovo High IOPS and io3 Flash Adapters CIM provider requires the following software to be installed and functioning properly:

- Lenovo High IOPS and io3 Flash Adapters VSL driver (2.x, 3.x or 4.x series driver)
- Lenovo High IOPS and io3 Flash Adapters VSL SDK (version must match driver)
- Package **`libfio`** for 2.x driver on Linux
- Package **`libvsl`** for 3.x driver on Linux
- Package **`libvsl`** for 4.x driver on Linux
- Included in Windows driver installation
- Must match the architecture (32/64-bit) of the Lenovo 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 Lenovo CIM provider, but it requires linking dynamically to the libraries at runtime:

- **`libuuid`**

- **`libblkid`**

Hardware support

The Lenovo High IOPS and io3 Flash Adapters CIM provider supports all Lenovo High IOPS and io3 Flash Adapterss. The CIM provider works with any 2.x, 3.x, or 4.x series Lenovo VSL driver, and has no requirement on minimum firmware versions of connected devices. Each version of the Lenovo 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

Attention!

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
```

Attention!

Lenovo CIM provider updates cached data from Lenovo 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.

NOTE-

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 Lenovo 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
```

Appendix D:
Flash Management Console Simulator

The Flash Management Console is a simulated version of the Lenovo VSL SDK. This simulator is a useful tool to test the your system in ways and situations that cannot be done under normal working conditions.

Using the Simulator, you can test error conditions that you would otherwise not be able to,because you can not force the system into that error condition. You can simulate errors you are unavailable to replicate in a live system setup.

Simulator Prerequisites

NOTE-

All of the following software modules can be downloaded from their respective company's website.

Install the following software modules:

- MySQL (See See MySQL Setup on page 90.)
- Python 2.6, including python-dev
- Django 1.3.1
- libmysqlclient-dev

Attention!

You may need to download **django** from their website, rather than using **apt-get** or **yum**. On **ubuntu**, the version you get with **apt-get** is 1.1.)

First Time Installation

1. Once you have successfully installed the necessary software, open a python interactive shell and enter **`import django`** to confirm a successful installation.
2. Install the **`python-mysqldb`** extensions using **easy_install MySQL-python**. This is required for **django** to communicate with the **mysql** database.

Attention!

If you're using **easy_install**, the other packages you may want to install are:

easy_install pip
easy_install yolk

You must complete the steps outlined for periodic maintenance before running the simulator for the first. See See Periodic Maintenance on page 90 for more information.

MySQL Setup

1. Download and install **MySQL** from your preferred OS package manager or the main website.
   - Ubuntu 10.04: https://help.ubuntu.com/10.04/serverguide/mysql.html
   - CentOS: http://dev.antoinesolutions.com/mysql
2. Upon installation, you will be prompted to enter a root user password. Enter "fusionio". (This is currently hardcoded in **settings.py** for **django** to connect to **mysql.**
3. Install **mysql-python** extensions using **easy_install** or your OS package manager.
4. Create a file in your **HOME** directory called ".my.cnf" to allow **mysql** CLI commands to automatically log in and not have to be entered every time. Its contents should be as follows:
   - [client]
   - user = "root"
   - password = "fusionio"
5. For Windows, place this file at MySQL Server 5.5\my.cnf in the install directory for MySQL.

Attention!

For better performance, edit your system /etc/mysql/my.cnf file and add "skip-sync-frm=OFF" to the [mysqld] section and restart the service

Periodic Maintenance

You must perform these actions before running the simulator for the first time. Navigate to the simulator's install directory (**/usr/share/fio/FioMgmtSim**).

1. Create the database for the **django** project. To do this, run the following script:

```
> cd /usr/share/fio/FioMgmtSim
> ./reset_db.py
```

NOTE-

You will need to reset the database after updating to a new version of the simulator.

2. Once the database is created, it needs populated. Run the script found in the **FioMgmtSim** folder called **populate_db_vsl_only.py** that will populate the database with a small set of default data.

```
> ./populate_db_vsl_only.py
```

Customizing the Database

You can write your own python scripts to populate the database with your own data, or you can run the included script, then run your own after. This modifies the scripts and stores them. You can also open the **sqlite** database and edit it,

Attention!

You will lose any edits whenever you run reset_db.py.

Use **populate_db_vsl_only.py** to populate the database with SAFT information. **populate_db.py** accepts a single argument that is the path to a JSON file containing values that override the defaults. This allows you to customize the data populated into the database.

You can customize the following values:

Key	Description	Default
serial_base	Base serial number	1232D018
host_hostname	Host name	Current machine name
host_os_name	Host OS	Current machine OS
host_ip_address	Host IP address	Current machine IP address
host_is_cluster_master	Cluster master flag	1
cluster_name	Cluster name	clu1
cluster_ip_address	Cluster IP address	Current machine IP address

Running the Simulator

To run the simulator, run the following:

```
> cd /usr/share/fio/FioMgmtSim
> python manage.py runserver 0.0.0.0:9052
```

You can choose to listen on loopback by replacing 0.0.0.0 with localhost

Port 9052 is the default simulator port. You can change this, but when you run **fio-agent**, you will have to supply additional command line parameters for it to find the simulator.

For the **fio-agent -f -s**[host:port], the default, **-s** assumes localhost:9052. If you want to connect to another person's simulator, you can run **fio-agent-sothermachine:9052**

> **NOTE-**
> 127.0.0.1 may run faster than localhost on Windows.

Errors

- If you get the following output while trying to run **fio-agent -s:**

```
2011-10-27 19:35:50,089 [0x000004a8] ERROR vsl_product - Failed to
initialize SDK:
Failed to read from or write to the device.
2011-10-27 19:35:51,093 [0x000004a8] ERROR vsl_dc_product - Failed to
initialize
direct cache SDK: Failed to read from or write to the device.
```

you need to run the simulator before starting the agent. If you are running your simulator, check the port.

- If Flash Management Console reports that not all my hosts are online, double-check your command-lines for the simulators and agents. If there is no **/var/lib/fio2/fio-agent-uuid** file, you might have forgotten the '-t' when pointing the **fio-agent** at **/var/lib/fio2.**
- If you see the error message "EnvironmentError: mysql_config not found", run **apt-get** to install **libmysqlclient-dev**.
- If you see the error message "missing Python.h" or similar errors, run **apt-get** to install **python2.6-dev.**

Simulating Errors and Warnings

To trigger an error or warning in an application using the simulator, you must inject error values into the simulator database. Once this is done, the next time the application queries for the latest data, it will see an error or warning condition and flag it as an alert appropriately.

In the simulator, there are four fields on the iom object that will cause Flash Management Console to show alerts:

- current_errors
- current_warnings
- write_throttling_state
- write_throttling_reason
- minimal_mode_reason

current_errors

This field is a bitset enumeration indicating the active errors on the High IOPS and io3 Flash Adapters. Each enum value corresponds to a set bit in a uint64 value, and these values may be bitwise OR'd together to simulate multiple errors active at the same time. To get the actual integer value of the given error, it is 2 raised to the <bit> power. So bit 0 = 2^0 = 1, bit 1 = 2^1 = 2, bit 2 = 2^2 = 4, and so on.

- Bit 0 - Device has entered failed state
- Bit 1 - Slot bandwidth incompatible
- Bit 2 - Partial Write Throttling (Note that Flash Management Console uses the write_throttling_ state/reason to detect this error, so setting this bit alone will not trigger the alert)
- Bit 3 - Complete Write Throttling (Note that Flash Management Console uses the write_throttling_ state/reason to detect this error, so setting this bit alone will not trigger the alert)
- Bit 4 - Temperature at critical threshold
- Bit 5 - Temperature surpassed critical threshold
- Bit 6 - VccInt Failure
- Bit 7 - VccAux Failure
- Bit 8 - Flashback

current_warnings

This field is a bitset enumeration indicating the active warnings on the High IOPS and io3 Flash Adapters. Each enum value corresponds to a set bit in a uint64 value, and these values may be bitwise OR'd together to simulate multiple warnings active at the same time. To get the actual integer value of the given error, it is 2 raised to the <bit> power. So bit 0 = 2^0 = 1, bit 1 = 2^1 = 2, bit 2 = 2^2 = 4, and so on.

- Bit 0 - Temperature at warning levels
- Bit 1 - Close to wearout
- Bit 2 - Slot bandwidth suboptimal
- Bit 3 - Errors on PCIe bus.
- Bit 4 - Power loss protection disabled
- Bit 5 - Power write governing
- Bit 6 - Thermal write governing
- Bit 7 - Lifespan governing
- Bit 8 - Minimal mode
- Bit 9 - Over power budget alarm
- Bit 10 - Missing LEB map
- Bit 11 - Media upgrade in progress
- Bit 12 - Reserves depleted

write_throttling_state

This field is an enumeration indicating the write throttling state of the device.

- 0 - Not write throttling
- 1 - Partial write throttling
- 2 - Complete write throttling

write_throttling_reason

This field is an enumeration indicating the reason for write throttling of the device.

- 0 - No reason given
- 1 - User forced
- 2 - Out of index space
- 3 - Out of available memory
- 4 - NAND chip hardware failure
- 5 - Close to wearout
- 6 - Adapter power cable isn't connected
- 7 - Internal failure
- 8 - ioMemory exceeds PCIe power specification
- 9 - Groomer could not free enough blocks to continue

minimal_mode_reason

This field is a bitset enumeration indicating why the High IOPS and io3 Flash Adapters is in minimal mode. Each enum value corresponds to a set bit in a uint64 value, and these values may be bitwise OR'd together to simulate multiple reasons active at the same time. To get the actual integer value of the given error, it is 2 raised to the <bit> power. So bit 0 = 2^0 = 1, bit 1 = 2^1 = 2, bit 2 = 2^2 = 4, and so on.

- Bit 0 - Firmware not compatible
- Bit 1 - Supplemental power required
- Bit 2 - Dual plane not supported
- Bit 3 - User forced
- Bit 4 - Internal error
- Bit 5 - Card limit exceeded
- Bit 6 - Unsupported OS
- Bit 7 - Not enough memory to load driver
- Bit 8 - SMP is in bootloader mode

- Bit 9 - Missing midprom data
- Bit 10 - Unsupported NAND

Modifying Error State

If you look at the JSON output from the simulator by hitting it in a browser, you will see these fields and their values:

```
http://localhost:9052/vsl/iom/1232D19050

{
...
"current_errors" : 0,
"current_warnings" : 0,
...
"write_throttling_reason" : 0,
"write_throttling_state" : 0
}

Similarly for a cache instance:
http://localhost:9052/vsl_dc/cache_instance/
{ ... "bypass_mode": null, ...
"cache_instance_current_errors": 0,
"cache_instance_current_warnings": 0, }
```

Each of these fields can be set to different values to cause errors or warnings to occur within Flash Management Console (or SNMP, SMI-s, etc. when they start using the simulator). The way you modify these values is by using curl and doing a PUT command to the appropriate resource URL. For example:

```
.tespey@dcropolis:~/hgroot/management/src/util/simulator/FioMgmtSim$ curl
-H
"Content-Type: application/json" -X PUT -d
'{"write_throttling_state":1,"write_throttling_reason":1}'
localhost:9052/vsl/iom/1232D19050
{
"retval": 0
}
```

The above example causes a partial write throttling warning on High IOPS and io3 Flash Adapters 1232D19050 with the reason of "User Initiated".

In general, you will use commands like the above to modify the values in the database to simulate the different error cases.

Other Examples

Activate two error conditions **- vccint** and **vccaux** on High IOPS and io3 Flash Adapters 1232D19050

```
user@system:~/hgroot/management/src/util/simulator/FioMgmtSim$ curl -H
"Content-Type: application/json" -X PUT -d '{"current_errors":192}'
```

```
localhost:9052/vsl/iom/1232D19050
{
"retval": 0
}
```

Activate overpower warning and overtemperature error conditions on High IOPS and io3 Flash Adapters 1232D19050

```
user@system:~/hgroot/management/src/util/simulator/FioMgmtSim$ curl -H
"Content-Type: application/json" -X PUT -d
'{"current_errors":32,"current_warnings":512}'
localhost:9052/vsl/iom/1232D19050
{
"retval": 0
}
```

Activate minimal mode (reason: user initiated) and close to wearout warning on High IOPS and io3 Flash Adapters 1232D19050

```
user@system:~/hgroot/management/src/util/simulator/FioMgmtSim$ curl -H
"Content-Type: application/json" -X PUT -d
'{"current_warnings":258,"minimal_mode_reason":8}'
localhost:9052/vsl/iom/1232D19050
{
"retval": 0
}
```

Clear all errors and warnings, write throttling state and minimal mode, reset to good state

```
user@system:~/hgroot/management/src/util/simulator/FioMgmtSim$ curl -H
"Content-Type: application/json" -X PUT -d
'{"current_errors":0,"current_warnings":0,"minimal_mode_reason":0,"write_
throttling_
state":0,"write_throttling_reason":0}' localhost:9052/vsl/iom/1232D19050
{
"retval": 0
}
```

Simulator Enable/Disable in SNMP/SMI-S

SMI-S

Windows:

1. Create new registry key "simulator-enable" in HKLM/SOFTWARE/Fusionio/fiosmis/CurrentVersion and set the value to one of the following:
    - **TRUE**
    - **ENABLED**
    - **ON**
2. Create new registry key "simulator-endpoint" and set endpoint value.
3. Restart winmgmt(WMI) service.

Linux

1. In smis.conf, set the value to one of the following:
    - **TRUE**
    - **ENABLED**
    - **ON**
2. Set SIMULATOR:ENDPOINT to simulator endpoint
3. Start/restart sfcb daemon

SNMP

Linux:

1. Run fio-snmp-agentx -S <endpoint>

Windows:

1. Create new registry key "simulator-enable" in HKLM/SOFTWARE/Fusion-io/fio-snmp-win/CurrentVersion and set value to 'on'.
2. Create new registry key "simulator-endpoint" and set endpoint value.
3. Restart SNMP service

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

S

T

Part Number: D0003052-009_5
Printed in the USA