

---

Blade Manager 4.1

# Administrator's Guide

ClearCube Technology, Inc.



**Copyright © 2005, ClearCube Technology, Inc. All rights reserved.**

Under copyright laws, this publication may not be reproduced or transmitted in any form, electronic or mechanical, including photocopying, recording, storing in an information retrieval system, or translating, in whole or in part, without the prior written consent of ClearCube Technology, Inc.

This information is subject to change without notice and ClearCube shall not be liable for any direct, indirect, special, incidental or consequential damages in connection with the use of this material.

#### **Trademarks**

ClearCube™, C3 Architecture™, Blade Switching BackPack™, PC Blade™, and C/Port™ are trademarks of ClearCube Technology Inc. Product and company names mentioned herein are trademarks or trade names of their respective companies.

#### **Patents**

The ClearCube Architecture and its components described in this user manual are protected by numerous granted and pending U.S. and international patents.

Granted patents include: US06020839, US06012101, US05994952, US05966056, US05926172, US06167241, US06148182, US06119146, US06038616, US06385666, and US06037884. Inquiries regarding patented technology should be directed to ClearCube Corporate Headquarters.

# Contents

- Contents . . . . . i
- Figures . . . . . ii
- Blade Manager Client . . . . . 1
  - Packaging . . . . . 1
- Blade Manager Installation . . . . . 2
  - Installing Blade Manager . . . . . 3
- Using Blade Manager . . . . . 5
  - Launching Blade Manager . . . . . 5
- Viewing System Status . . . . . 7
  - System Management Views . . . . . 7
  - Out-of-Band Management . . . . . 9
  - Blade Management on a Network . . . . . 10
- Alert Features . . . . . 11
  - Adding Alerts . . . . . 11
  - SNMP Setup . . . . . 13
- Contacting Support . . . . . 15
  - ClearCube . . . . . 15
  - Active Perl . . . . . 15

# Figures

- Figure 1 ClearCube One-Click Installer ..... 3
- Figure 2 Launching Blade Manager ..... 5
- Figure 3 Logging In to Blade Manager ..... 6
- Figure 4 System Information View ..... 6
- Figure 5 Asset Management View ..... 7
- Figure 6 Alert Addition ..... 11
- Figure 7 Alert Addition Confirmation ..... 12
- Figure 8 Alerts View ..... 12
- Figure 9 Alert Deletion Confirmation ..... 13
- Figure 10 SNMP Setup ..... 13
- Figure 11 SNMP Configuration ..... 14

# Blade Manager Client

ClearCube's Blade Manager 4.1 Client provides PC Blade health monitoring and asset management on a one-to-one basis. This means that administrators can configure hardware and software thresholds to trigger email and/or SNMP Alerts, and perform other management tasks on each Blade. Every ClearCube Blade is shipped from the factory with the Blade Manager Client installed.

For larger implementations that require a central console to manage the Blade Manager Clients, visit [www.clearcube.com](http://www.clearcube.com) for information regarding ClearCube Control Center. Control Center is required to utilize the Alerting features of Blade Manager.

---

## Packaging

The Blade Manager 4.1 Client is shipped with an All-in-one installer application (see page 3) that automates the correct installation of the necessary software components (see page 2). Additionally, all these components are provided on the Blade Manager 4.1 Installation CD as independently installable applications. Blade Manager requires that these components be installed in a specific order prior to installing the application.

This manual is the most current version as of the initial release ship date for the Blade Manager 4.1 Client. For free updated manual versions, please visit the Tech Docs section at <http://support.clearcube.com>.

# Blade Manager Installation

Blade Manager 4.1 can be installed on client Blades running Windows 2000 or Windows XP. For Blade Manager to function properly, install the following software modules in the order listed before installing Blade Manager. The All-in-one installer does this for you. Additionally, each of these modules is provided on the Blade Manager 4.1 Installation CD. Installation requires administrator access privileges.

- **Java Runtime Environment version 1.4.2** – Blade Manager 4.1 requires JRE version 1.4.2\_03 or later. The correct Java version is provided on the Blade Manager 4.1 Installation CD shipped from ClearCube. The version of a previously installed Java package can be checked in **Add or Remove Programs** from the Control Panel, or by running the `Java -version` command at the DOS prompt, which returns the installed Java version. Versions previous to 1.4.2\_03 should be removed.

Version 1.4.2\_03 or later of the Java 2 Enterprise Edition 1.4 SDK, which adds support for EJBs, JSPs, XML, and Web Services APIs, can also be used.

- **ActiveState Perl 5.6.1** – Blade Manager 4.1 requires ActiveState Perl 5.6.1. The correct version of ActiveState Perl is provided on the Blade Manager 4.1 Installation CD shipped from ClearCube. The version of a previously installed ActiveState Perl can be checked in **Add or Remove Programs** from the Control Panel, or by running the `Perl -version` command at the DOS prompt to display the version of the currently installed Perl. Versions previous to 5.6.1 should be removed.

The ActiveState Repository has a large collection of modules and extensions in binary packages that are easy to install and use. To view and install these packages, use the Perl Package Manager (PPM) which is included with ActivePerl.

- **ClearCube Distributed Computing Infrastructure (DCI)**—Blade Manager 4.1 requires ClearCube DCI version 2.0.8. The correct version is provided on the Blade Manager 4.1 CD shipped from ClearCube. Before installing Blade Manager 4.1, please make sure that the current DCI is installed. The installed DCI version can be verified through **Add or Remove Programs** in the Control Panel. Versions previous to 2.0.8 should be removed prior to installing Blade Manager 4.1.
- **ClearCube Perl PlugIn**—Blade Manager 4.1 requires ClearCube Perl PlugIn version 1.1. The correct version is provided on the Blade Manager 4.1 Installation CD. The installed Perl PlugIn version can be verified through **Add or Remove Programs** in the Control Panel. Version 1.0 should be removed.

To use the Alerting features of Blade Manager, ClearCube Control Center is also required.

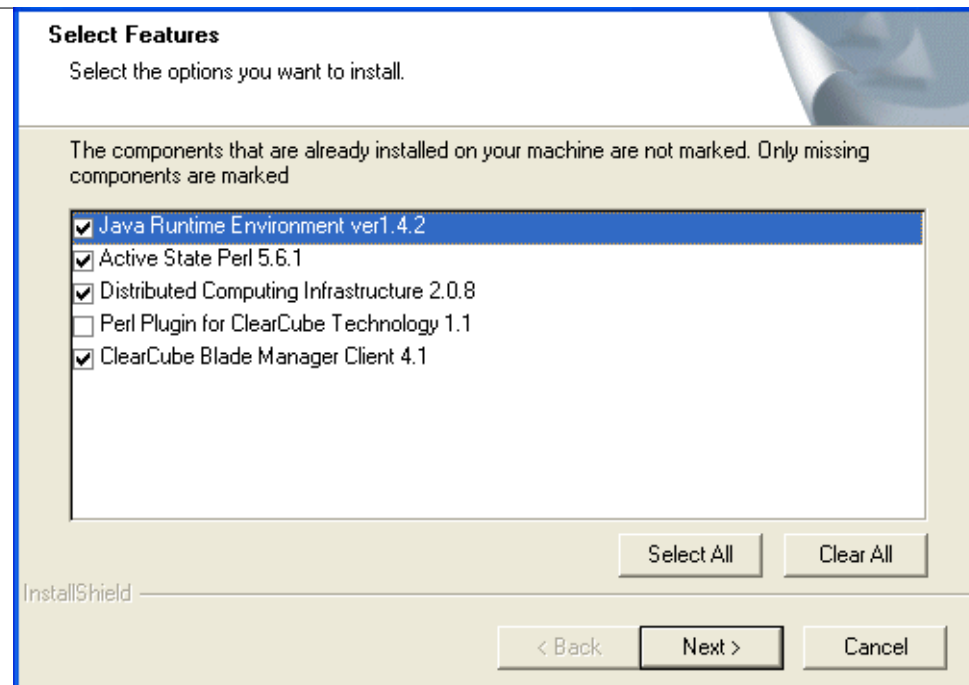
---

## Installing Blade Manager

The Blade Manager 4.1 All-in-one installer application checks for the necessary components, and installs all components not detected. In addition, separate installers for each application are provided on the Blade Manager 4.1 Installation CD.

Before installing Blade Manager, check the versions of the JRE, ActiveState Perl, ClearCube DCI, and Perl PlugIn (if these products are installed), and remove any previous versions. Previous versions of Blade Manager should also be removed.

The Blade Manager Installation CD provides an All-in-one installer for the Administration Console that simplifies the task of installation. See *Figure 1*.



*Figure 1 ClearCube One-Click Installer*

The installer displays all the required components for the Blade Manager installation. If a component needs to be installed, the box next to its name is checked. If it has already been installed, the box next to its name is empty. The installer then installs each component selected in the correct order. It is strongly recommended to use the All-in-one installer to determine the necessary components and their installation order, and to accept the settings of the installer.

**Note:** Verify the versions of your installed components, and uninstall outdated versions before beginning to install Blade Manager 4.1.

## ***Installation***

Installation requires administrator access privileges. In all cases, allow the installer adequate time to complete its operation. The ClearCube All-in-one installer appears to pause at several times during its execution, while showing no obvious activity. The installation resumes within several seconds, and displays a dialog box with information or more instructions.

To install Blade Manager, do the following:

1. To begin installation, launch the `setup.exe` file from the Blade Manager Client folder on the Blade Manager 4.1 Installation CD.
2. Choose the components to be installed from the Select Features window (see *Figure 1*). Press **Next**.
3. Follow the prompts as appropriate. If you are unsure of a prompt, use the default.
4. Once the installation is complete, restart your system.

## ***Uninstallation***

Uninstallation requires administrator access privileges. To install Blade Manager, do the following:

1. From the Control Panel, choose **Add or Remove Programs**.
2. Select **ClearCube Blade Manager 4.1 Client** from the list of programs.
3. Click the **Change/Remove** button.
4. Select the radio button for **Remove**. Click the **Next** button.
5. Once the removal is complete, click the **Finish** button.

The other components for Blade Manager can be uninstalled in a similar fashion.

**Note:** Components must be uninstalled in the following order, or system errors will occur.

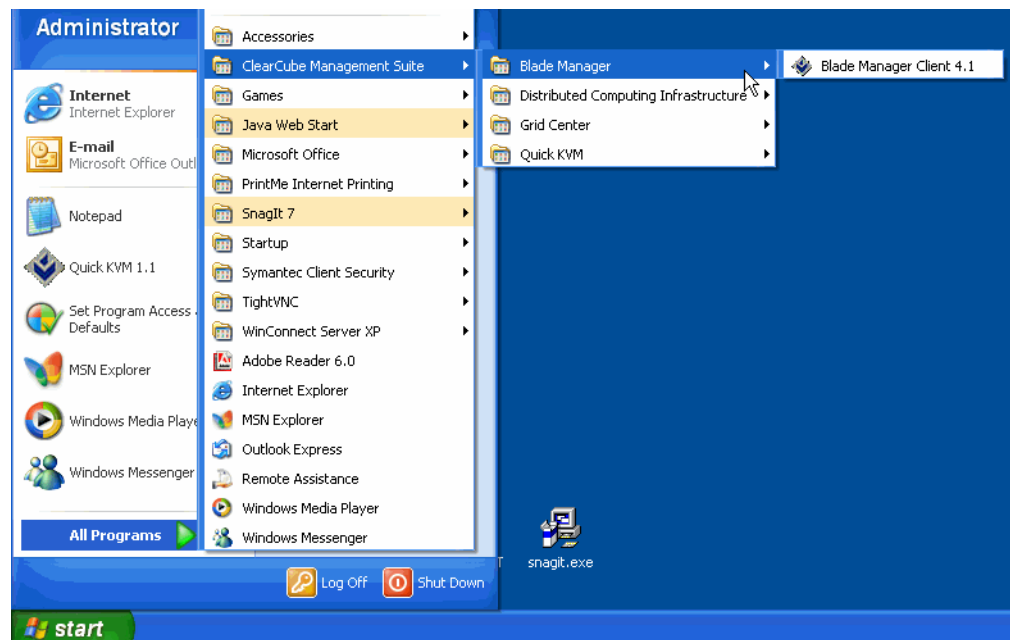
1. Blade Manager
2. ClearCube Perl PlugIn
3. ClearCube Distributed Computing Infrastructure (DCI)
4. ActiveState Perl
5. Java Runtime Environment



# Using Blade Manager

## Launching Blade Manager

Launch Blade Manager by selecting **Start Menu**→**All Programs**→**ClearCube Management Suite**→**Blade Manager**→**Blade Manager 4.1 Client**, as shown in *Figure 2*.



*Figure 2* Launching Blade Manager

The first screen in Blade Manager is the login screen. When logging in, there are two options for authentication:

- Local Authentication
- Domain Authentication

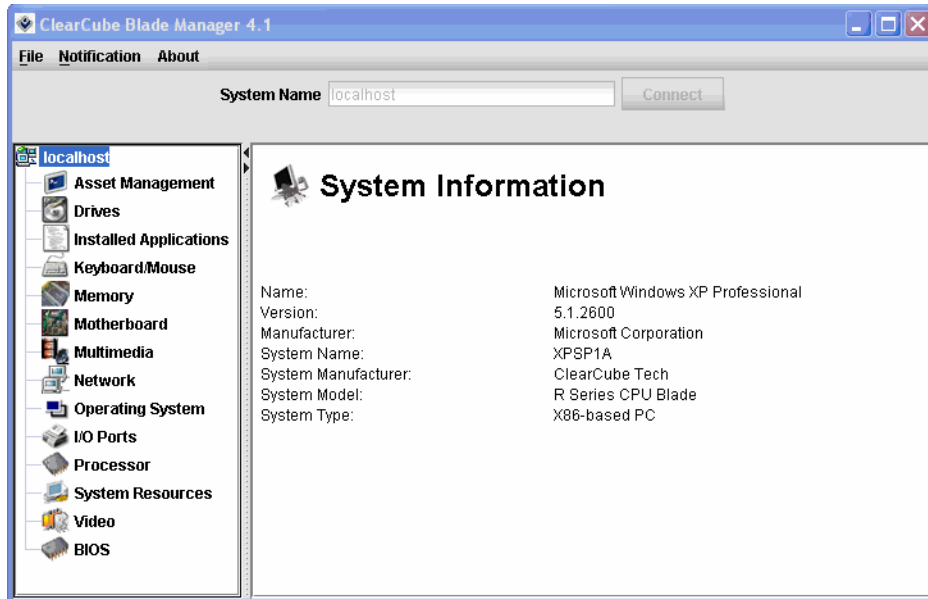
Blade Manager automatically detects the presence of a Domain Controller and populate the **Log on to** pull-down menu with the discovered domain(s), as well as the local machine name. By default, only a member of the Local Administrators group or the Domain Users group can log in to Blade Manager.

Once in Blade Manager, you can elect to perform authentication locally or with domain credentials by choosing **Authentication** from the **File** menu. Enter the username and password, and then choose the appropriate authentication mechanism by specifying the local machine or the domain from the **Log on to** pull-down menu. Click the **Submit** button to log in, as shown in *Figure 3*.



*Figure 3 Logging In to Blade Manager*

The Blade Manager Client displays information for the local machine in the System Information view, shown in *Figure 4*.



*Figure 4 System Information View*

The Blade Manager interface allows you to connect to other Blades to view Blade information or to configure Alerts. To connect to another Blade, enter the hostname in the **You are connected to** field at the top center of the screen and click the **Connect** button.

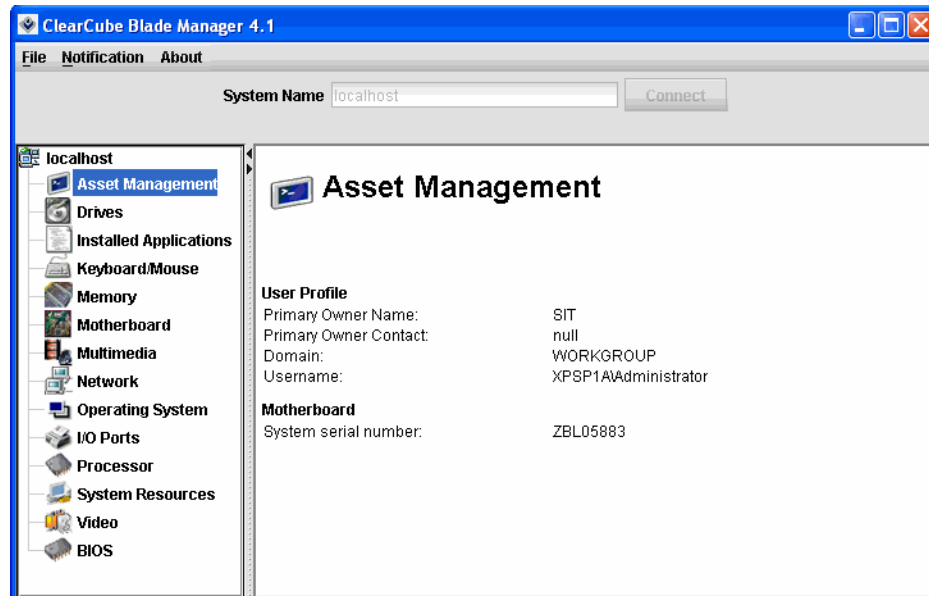
As a security measure, this function is accessible only if you are logged into Blade Manager using domain credentials. You must be a Domain Administrator and must be logged into the domain to connect to other machines. This prevents end users from accessing other machines.

# Viewing System Status

---

## System Management Views

The system management views allow the administrator to view information regarding a Blade's hardware, software, and firmware. This lets the administrator perform real time troubleshooting on each machine. Clicking an item in the left-hand pane displays detailed information in the right-hand pane, as shown in *Figure 5*.



*Figure 5 Asset Management View*

This example shows the information displayed when the Asset Management view is chosen. It includes Primary Owner Name, Primary Owner Contact, Domain, Username, and System Serial Number. This information is retrieved from the data entered when Windows was installed.

Table 1 shows the information displayed when each category is chosen.

*Table 1 System Information*

<b>Category</b>	<b>Available Information</b>
Asset Management	Primary Owner Name Primary Owner Contact Domain Username System Serial Number
Drives	Primary Drive Model Primary Drive Partitions Primary Drive Size Primary Drive Cylinders Primary Drive Sectors Primary Drive Total Heads Drive Letter (all local drives) File System Type (all local drives) Free Space (all local drives) Size (all local drives)
Installed Applications	Programs listed in Add/Remove Programs
Keyboard/Mouse	Keyboard Description Keyboard Layout Mouse Description Mouse Hardware Type
Memory	Total Visible Memory Size Free Virtual Memory Total Virtual Memory Module Bank Label Module Capacity Module Speed Module Device Locator
Motherboard	Manufacturer Model Max Supported CPU Speed Slot Description Slot Width
Multimedia	Device Manufacturer Device Name Product Name Version
Network	IP Address NIC Description MAC Address Subnet Default Gateway Preferred DNS Server Alternate DNS Server
Operating System	Operating System Type Version Service Pack Running Processes Environment Variables System Drivers

Table 1 System Information (Continued)

Category	Available Information
I/O Ports	Device ID (Communications Port) Maximum Baud Rate
Processor	Processor Type Description Processor ID Manufacturer Device ID CPU Current Clock Speed Load Percentage Max Clock Speed Status Blade Temperature (reported by RMC) Blade Fan Speed (reported by RMC) Blade Voltage (reported by RMC)
System Resources	IRQ Settings DMA Settings I/O Settings Memory Settings
Video	Video Card Manufacturer Video Card Type Driver Version Driver Date Installed Display Drivers Supported Resolutions & Refresh Rates
BIOS	Manufacturer Version Details SMBIOS version

---

## Out-of-Band Management

Blade Manager allows administrators to gather out-of-band information regarding the processor on each Blade. This is done by querying a Switch Manager console, which collects the information from the Remote Management Card (RMC). The RMC does not rely on a response from the operating system. Thus, even when an application or operating system is unresponsive, this information is still available. The information is displayed in the Processor System Management view (click **Processor** in the left tree).

To activate out-of-band information management, files must be added or modified in the Switch Manager file path. You must have access to the Switch Manager server to make the necessary changes for out-of-band management.

To activate out-of-band information management, do the following:

1. From the root level of the Blade Manager 4.1 Installation, navigate to the **RMC** folder.

This folder contains a README file with the instructions for adding/modifying the Switch Manager files. It also contains the files that must be added on the Switch Manager server for the out-of-band management to function properly.

2. Copy the **BM** folder to the following location:

```
..\webapps\SM\WEB-INF\classes
```

This contains the `readBMRMC.class` file.

3. Edit the `web.xml` file on the Switch Manager server to include the following:

```
<servlet>
<servlet-name>readBMRmc</servlet-name>
<servlet-class>BM.readBMRmc</servlet-class>
</servlet>

<servlet-mapping>
<servlet-name>readBMRmc</servlet-name>
<url-pattern>/readBMRmc</url-pattern>
</servlet-mapping>
```

These entries should be inserted at the appropriate places in the `web.xml` file.

The format and the location for these entries are essential for proper functionality of Blade out-of-bound health management values.

---

## Blade Management on a Network

If you configure a Blade using Blade Manager or the Control Center server as a member of a workgroup, move the system to a domain, and then move the system back to a workgroup (either the same workgroup or a new one), network connectivity is lost until the security settings are returned to their default. This is a known issue with Windows, and is documented in Microsoft's Knowledge Base as article 313222, found at:

<http://support.microsoft.com/?kbid=313222>

To reset the system to its default security setting, enter the following command at a command prompt:

```
secedit /configure /cfg %windir%\repair\secsetup.inf /db secsetup.sdb /verbose
```

Ignore the warning message that is issued after the command runs.

# Alert Features

---

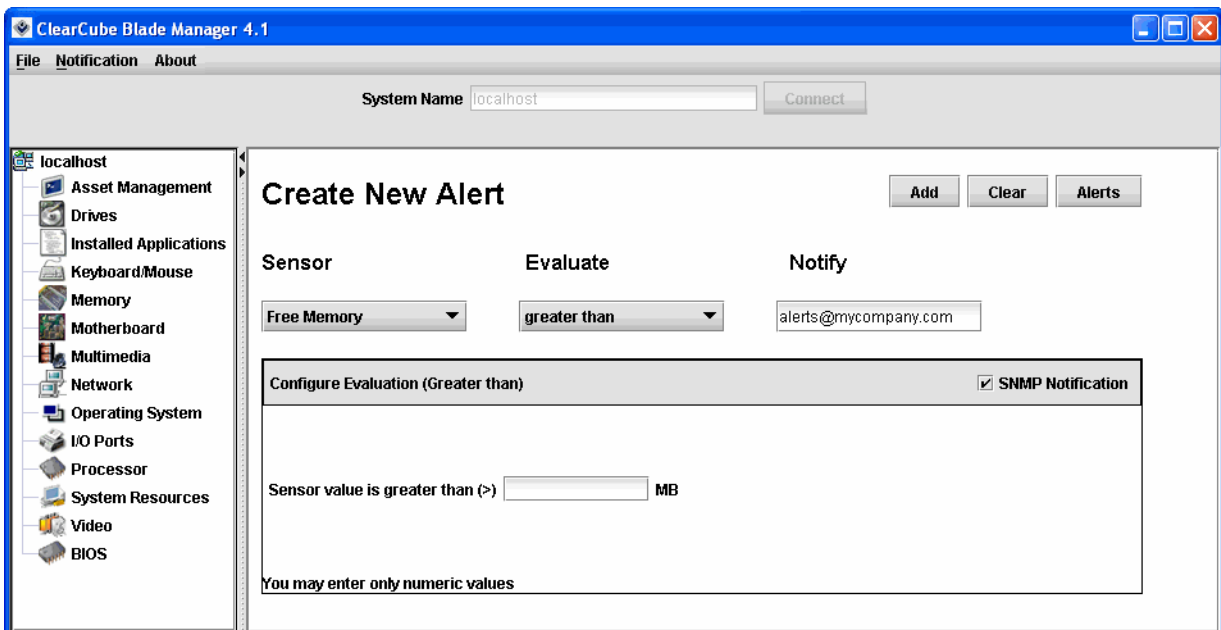
## Adding Alerts

Alerts can be created using configurable thresholds to notify administrators of specific Blade conditions or issues. When Alert conditions are met, Blade Manager sends an email to the configured email address and, if selected, sends an SNMP trap to a configured SNMP destination.

The Alerting feature cannot be enabled without a ClearCube Control Center console. Without access to Control Center, the Blade Manager Client can only be used for viewing Blade health and inventory information.

### *Creating New Alerts*

To create an Alert, select **Add Alerts** from the Notification pull-down menu. This displays the screen shown in *Figure 6*.



*Figure 6 Alert Addition*

Select the Sensor for the Alert to be created by using the **Sensor** pull-down menu. The Sensor is the component that is monitored for a specific condition.

Next, select an item from the **Evaluate** pull-down menu. The Evaluate option allows specifying the compare condition and threshold. After selecting the appropriate compare condition, enter the Sensor value (threshold) in the Configure Evaluation field at the bottom of the primary pane. The last step is to choose the Alert action(s). Enter the recipient's email address and/or check the SNMP checkbox. Click the **Add** button. The dialog shown in *Figure 7* is displayed. Click **OK** to continue.



Figure 7 Alert Addition Confirmation

## Viewing Alerts

From the Create New Alert screen, click the **Alerts** button. The view shown in *Figure 8* is displayed.

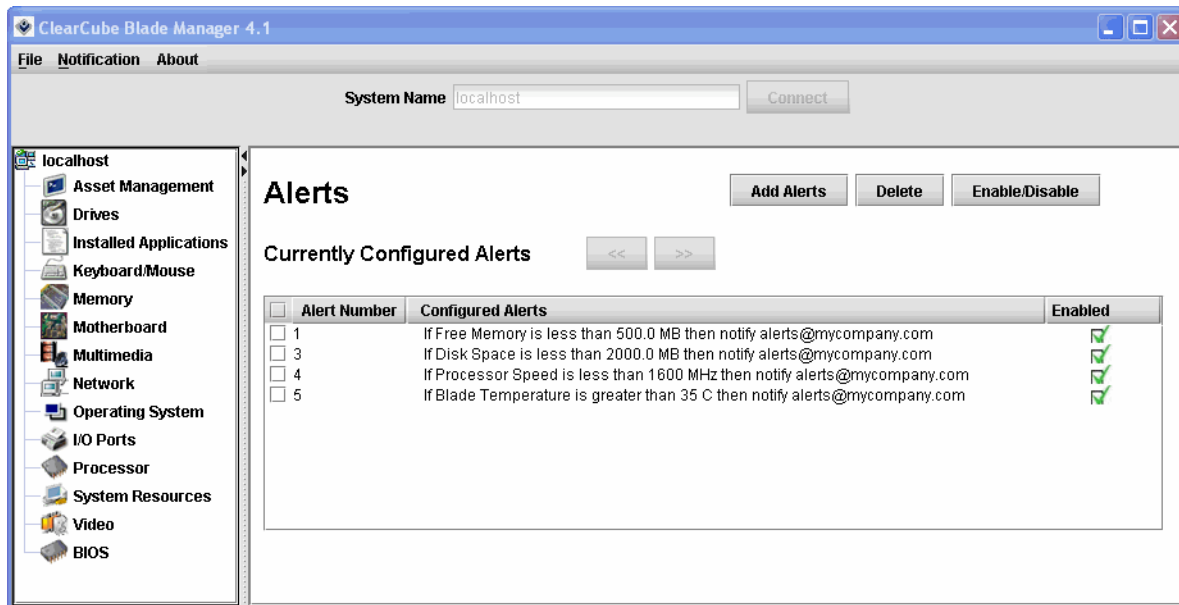


Figure 8 Alerts View

## Enabling/Disabling Alerts

When an Alert is created on a system, that Alert is automatically enabled. To selectively enable or disable individual Alerts, select or deselect its **Enabled**



checkbox in the Alerts view. When an Alert is not selected as enabled, no action is taken with respect to that Alert, even when the Alert's threshold is met. The **Enable/Disable** button (top right) also allows selecting a list of conditions by Alert number (left checkboxes) and enabled or disabled at once.

## Deleting Alerts

To delete an Alert, select its checkbox in the left column of the Alerts view, and click the **Delete** button. The dialog shown in *Figure 9* is displayed. Click the **OK** button to confirm.



*Figure 9 Alert Deletion Confirmation*

Multiple Alerts can be selected for simultaneous deletion.

---

## SNMP Setup

SNMP traps can be set up by selecting the SNMP checkbox when an Alert is created, in the Create New Alert view, as shown in *Figure 10*.



*Figure 10 SNMP Setup*

However, before SNMP can work, the `snmp.config` configuration file needs to be edited to provide the correct information for the receiver and sender machines. This file is located at the following location:

```
%CC_INSTALL_DIR%\BM4Client
```

where `%CC_INSTALL_DIR%` is the installation directory for the ClearCube DCI. The default location of this path is:

```
C:\Program Files\ClearCube Management Suite\DCI\BM4Client
```

Use a text editor such as Notepad to edit this file, as shown in *Figure 11*. In this example, `Computer1` is the hostname of the management server and `Computer2` as the hostname of this Blade Manager client.

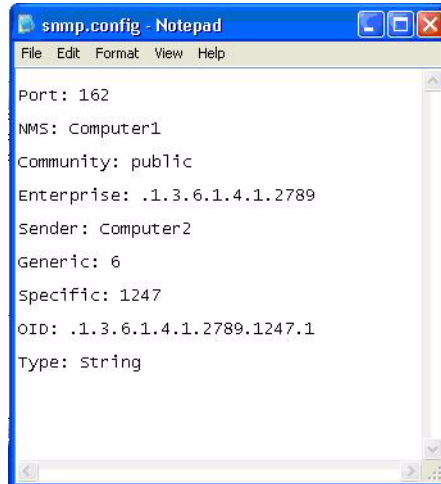


Figure 11 SNMP Configuration

Table 2 lists the fields in the `snmp.config` file. An in-depth explanation of SNMP is beyond the scope of this document. For most customers, only the NMS and Sender fields need to be configured. Enter the trap destination in the NMS field and the local hostname in the Sender field.

Table 2 SNMP Configuration

SNMP Field	Description
Port	Trap destination TCP Port.
NMS	Hostname or IP address of the Network Management Server (trap destination).
Community	Community string to be sent with trap. NMS can be configured to ignore traps without this string.
Enterprise	Vendor identification number for the management subsystem.
Sender	Hostname or IP address of machine sending the trap (local machine).
Generic	A number in the range 0-6 used when specific traps are not implemented.
Specific	Indicates specific trap sent. If a generic trap is used this value is ignored. This number is arbitrary; specific traps must be defined by the enterprise.
OID	Operation Identifier.
Type	Trap format type.

Customers who need detailed configurations specific to their environments can change the SNMP Port, Generic and Specific Trap Information, and the Trap Data Type.

# Contacting Support

---

## ClearCube

In the event you have any problems with your ClearCube software, please refer to our Web site or contact ClearCube Technical Support for guidance.

<a href="mailto:support@clearcube.com">support@clearcube.com</a>	Email address to ClearCube Technical Support
<a href="http://support.clearcube.com">support.clearcube.com</a>	ClearCube Support Website
(866) 652-3400	Direct line in the US
+1 (512) 652-3400	Direct line from outside the US

---

## Active Perl

ClearCube Blade Manager 4.1 utilizes ActiveState Perl technology. ActivePerl is the up-to-date, quality-assured Perl binary distribution from ActiveState. Current releases, and other professional tools for open source language developers are available at: <http://www.ActiveState.com/>

The ActiveState Repository has a large collection of modules and extensions in binary packages that are easy to install and use. To view and install these packages, use the Perl Package Manager (PPM) which is included with ActivePerl.

Commercial support for ActivePerl is available through ActiveState at: <http://www.ActiveState.com/Support/Enterprise/>

For peer support resources for ActivePerl issues see: <http://www.ActiveState.com/Support/>

### *Acknowledgements*

ClearCube Blade Manager 4.1 utilizes ActiveState Perl technology.

**ActiveState**

Dynamic Tools for Dynamic Languages

**ClearCube Technology, Inc.**

8834 Capital of Texas Highway North    Austin, Texas 78759    voice **512.652.3500**

**[www.clearcube.com](http://www.clearcube.com)**