Intel® RAID Web Console 3

Installation Guide

Installation instructions for the Intel® RAID Web 3 Console Utility

Rev 1.3

July 2021

Intel® Server Products and Solutions

<Blank Page>

Document Revision History

Date	Revision	Changes
December 2018	1.0	Initial release
July 2019	1.1	Instructions for installing on VMWare corrected.
February 2020	1.2	Supported OSs and language updated.
July 2021	1.3	Added “Setting the Firewall rules” section. Added “Configuring the Light Weight Monitor System” section. Added Language considerations (windows* OS) section. Added more explanation about the different installation types Fixed broken link for the VIB Package Updated Intel logo Modified the list of supported browsers Corrected minor typos

Disclaimers

Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software, or service activation. Performance varies depending on system configuration. No computer system can be absolutely secure. Check with your system manufacturer or retailer or learn more at intel.com.

You may not use or facilitate the use of this document in connection with any infringement or other legal analysis concerning Intel products described herein. You agree to grant Intel a non-exclusive, royalty-free license to any patent claim thereafter drafted which includes subject matter disclosed herein.

No license (express or implied, by estoppel or otherwise) to any intellectual property rights is granted by this document.

The products described may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request.

Intel disclaims all express and implied warranties, including without limitation, the implied warranties of merchantability, fitness for a particular purpose, and non-infringement, as well as any warranty arising from course of performance, course of dealing, or usage in trade.

This document contains information on products, services and/or processes in development. All information provided here is subject to change without notice. Contact your Intel representative to obtain the latest Intel product specifications.

Copies of documents which have an order number and are referenced in this document may be obtained by calling 1-800-548-4725 or by visiting www.intel.com/design/literature.htm.

Intel, the Intel logo, are trademarks of Intel Corporation or its subsidiaries in the U.S. and/or other countries.

*Other names and brands may be claimed as the property of others.

Table of Contents

List of Figures

List of Tables

1. Guide Organization

The Intel® RAID Web Console 3 Installation Guide contains the following sections:

Table 1. Guide organization

Section	Description
Intel® RAID Web Console 3 Overview	Provides an overview of the Intel® RAID Web Console 3 Software including monitoring and maintaining storage devices, and the required hardware and software to run the application.
Intel® RAID Web Console 3 Feature Comparison Matrix	Outlines the Intel® RAID Web Console 3 feature differences for MegaRAID®, iMegaRAID™, Syncro® (High Availability DAS), Software RAID, Integrated RAID (IR), and Initiator-Target (IT) controllers.
Installing Intel® RAID Web Console 3 Software	Provides information on Intel® RAID Web Console 3 Installers and steps to install and uninstall the Intel® RAID Web Console 3 software.
Performing Initial Setup	Provides certain initial setups that you need to perform before running the Utility.
Server Dashboard	Provides information about the Server Dashboard screen and its components.
Controller Dashboard	Provides information about the Controller Dashboard screen and its components.

2. Intel® RAID Web Console 3 Overview

Intel® RAID Web Console 3 (RWC3) software is a web-based application that performs monitoring, maintaining, troubleshooting and configuration functions for the Intel® RAID Products. The RWC3 graphical user interface (GUI) simplifies the viewing of an existing server hardware configuration, as well as creating and managing storage configurations.

2.1 Monitoring the Storage Devices

RWC3 software displays the status of the controller cards, virtual drives, and physical drives on the controller. Device status icons signal drive failures and other events that require immediate attention. Real-time email notifications (based on alert settings) about the status of the server may be sent to the user. The system errors and events are recorded in an event log file and are displayed.

2.2 Maintaining the Storage Devices

RWC3 software can perform system maintenance tasks, such as updating the controller firmware.

2.3 Troubleshooting the Storage Devices

RWC3 software signals critical issues of failed devices and provides recommendations for troubleshooting. Additionally, the software displays contextual links, which help locate the device and initiate troubleshooting, where the user can import or clear foreign configurations. The software also provides a diagnostic report including information for all the supported devices and their configurations, properties, and settings. This complete report is downloadable and can be sent to the Intel support team for further troubleshooting.

2.4 Personality Management

Personality Management allows switching the RAID controller between the different controller's personalities.

2.5 Hardware and Software Requirements

The following table provides the hardware and software requirements for the RAID Web Console 3 software:

Table 2. Hardware and software requirements

Requirements	Description
Controller	• Any 12 Gb/s Intel® RAID Module or controller (entry-level or full-featured or • Any mid-tier or Mainstream 6Gb/s Intel® RAID Modules or controllers or • Any Intel motherboard working with Intel ESRT2.
Supported operating systems	• Microsoft Windows* Server 2016 • Microsoft Windows* Server 2019 • Red Hat Enterprise Linux* 7.5 • Red Hat Enterprise Linux* 7.6 • Red Hat Enterprise Linux* 8.0 • SUSE Linux* Enterprise Server 12 SP2 • SUSE Linux* Enterprise Server 12 SP3 • SUSE Linux* Enterprise Server 12 SP4 • SUSE Linux* Enterprise Server 15 • SUSE Linux* Enterprise Server 15 SP1 • VMware* ESXi 6.5 Update 1 • VMware* ESXi 6.5 Update 2 • VMware* ESXi 6.5 Update 3

Requirements	Description
	• VMware* ESXi 6.7 Update 1 • VMware* ESXi 6.7 Update 2 • VMware* ESXi 6.7 Update 3 • VMware* ESXi 7.0 • VMware* ESXi 7.0 U1
Supported web browsers	• Web browser must support TLS 1.3 encryption • Windows* Internet Explorer® 11 and later (TLS 1.3 may need to be manually enabled) • Mozilla® Firefox® version 61 and later (version 63 enables TLS 1.3 by default). • Google Chrome® version 63 and later (version 70 enables TLS 1.3 by default).
Supported networks	• Internet Protocol versions 4 and 6 • Network Address Translation • Lightweight Directory Access Protocol (LDAP) • Domain • HTTP, HTTTPS
Supported languages	• English

3. Installing the Intel® RAID Web Console 3 Software

Intel® RAID Web Console 3 uses the Service Location Protocol to discover the different RWC3 nodes on a network and selects services and resources. The OpenSLP software is used and is bundled within the RWC3 installation package. While installing RWC3 ensure that you select the option to install OpenSLP.

The following are the different types of RWC3installations:

- Gateway
- StandAlone
- DirectAgent
- Lightweight Monitor (LWM)

The following table provides more information on each of these installers and their associated attributes:

Table 3. Types of installers and attributes

Feature	Gateway Installer	Standalone Installer	DirectAgent Installer	Lightweight Monitor
Permits discovery of other servers that run the Intel® RAID Web Console 3 software	Yes	No	No	No
Permits self-registration using OpenSLP and has interface for server discovery detection from the network	Yes	Yes **Note**: No interface for server discovery.	No	No
Allows to manage the servers from the list of discovered servers through the Graphical user interface.	Yes	No	No	No
Provides capability to configure LDAP information	Yes	Yes	No	No
Provides server monitoring capabilities and helps to monitor the health of the server and alerts the end-user of any issues with event logs and email notifications.	Yes	Yes	Yes	Yes
Provides a Graphical User Interface for monitoring the local server	Yes	Yes	No	No

3.1 Gateway Installer

The Gateway server is designed to have a single interface for monitoring all the RWC3 servers on the same network.
The Gateway installer has the following components:

- A backend with local agent and remote agent management capabilities.
- A monitor with remote monitoring capability.
- A client with remote and managed server capabilities.

The Gateway installer has the following features:

- Permits discovery of other servers that run the Intel® RAID Web Console 3 software.
- Permits self-registration using OpenSLP and has interface for server discovery detection from the network.
- Allows the user to manage the servers from the list of discovered servers through the user interface (UI).

Note: In order for the client's servers to be discovered and monitored, the appropriate firewall rules must be put in place on the client machines. RWC3 uses by default the TCP port 2463 (although this can be changed). OpenSLP uses the UDP port 427 for server discovery. Make sure the appropriate firewall rules are in place on the client or monitored RWC3 servers.

3.2 Standalone Installer

The Standalone server is designed to monitor and manage RAID configurations on the local server through a GUI, although this kind of installation can be monitored and managed from a Gateway server too.
The standalone installer has the following components:

- A back-end including a local agent (without remote agent management capability).
- A monitor (without remote monitoring capability).
- A client (without remote and managed server capabilities).

The standalone installer has the following features and limitations:

- Does not permit the discovery of other hosts that are running the Intel® RAID Web Console 3 software.
- Permits self-registration of the current host using OpenSLP, but will not have any interface for server discovery detection from the network.
- Provides capability to configure LDAP information.
- Does not allow to add managed servers through the user interface (UI).

3.3 DirectAgent Installer

This kind of installation only has the components required for remote managing and monitoring from the RWC3 Gateway server. There is no GUI available on the local server.
The direct agent installer has the following components:

- A back-end with local agent and a monitor component.
- A thin agent, which supports discovery (using SLP), authentication, and DCMD tunneling.

The standalone installer has the following features:

- Indirect agent (MegaRAID SMI-S provider)
- Direct agent

3.4 Lightweight Monitor

This kind of installation has only the minimum required for monitoring the local server's RAID configurations. There is no remote monitoring or managing capabilities or GUI available.
The lightweight monitor installer has the following benefits:

- Provides server monitoring capabilities.
- Light Weight Monitor (LWM) monitors the status of the controller cards, virtual drives, drives, and other devices on the server.
- Alerts you of any issues that require immediate attention with system logs and real-time email notifications (based on the alert settings).

3.5 Installing Intel® RAID Web Console 3 Software on the Microsoft Windows* Operating System (Interactive mode)

Perform the following steps to install the Intel® RAID Web Console 3 software:

1. Run the Intel® RAID Web Console 3 setup.exefile. The **InstallShield Wizard** dialog appears.

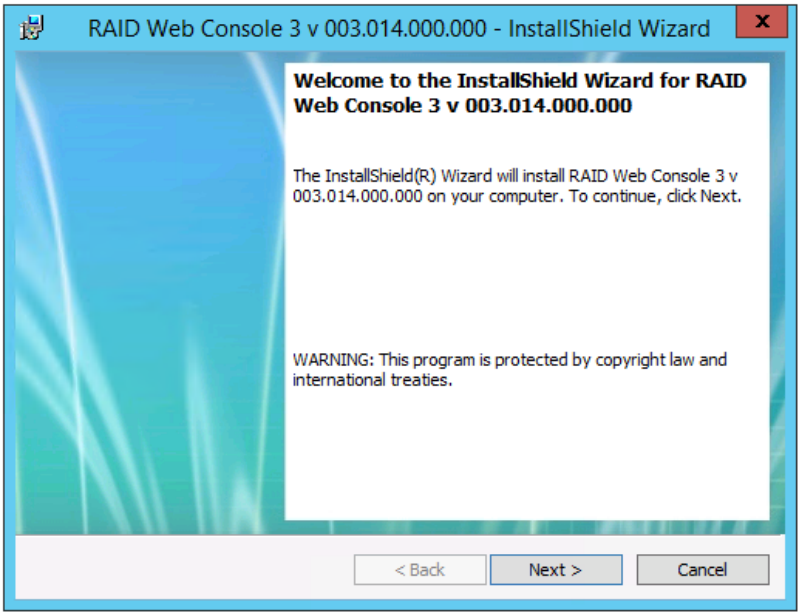


Figure 1. InstallShield Wizard dialog

2. Click **Next**. The **License Agreement** dialog appears.
3. Read the agreement and select **I accept the terms in the license agreement**, and click **Next**. The **Customer Information** dialog appears.
4. Enter your username and the relevant organization name, and click **Next**. The **Port Configuration Settings** dialog appears.

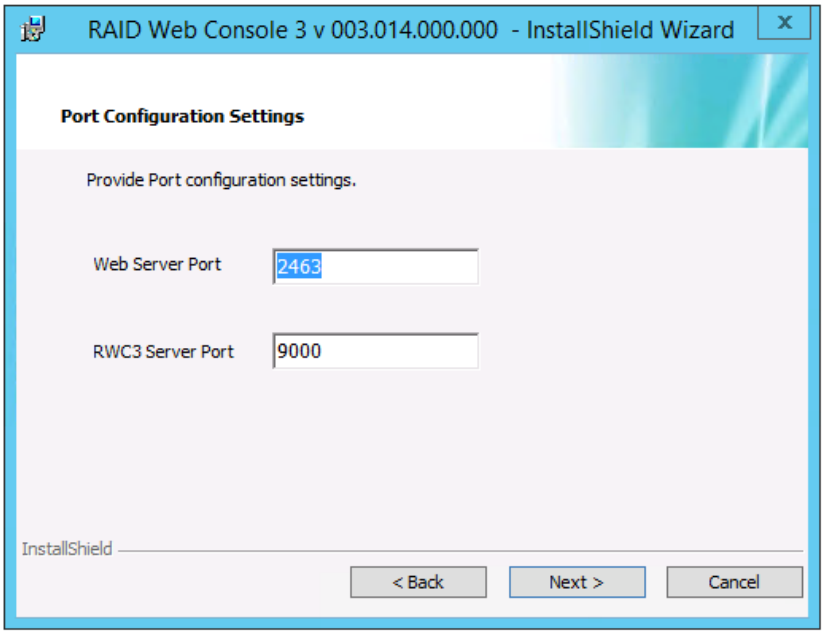


Figure 2. Port configuration settings dialog

5. Click **Next** if you want to proceed with the default port configuration settings. Otherwise, enter the port details in the **Web Server Port** field and the **RWC3 Server Port** field and click **Next**. Make sure that specified port numbers are available for use. You can edit this information after installation also. See sections Changing the Intel® RAID Web Console 3 Application Port Number and Changing the nginx Web Server Port Number. The **Destination Folder** dialog appears with the default file path.

Note: The Web Server port number selected here will be used for launching the RWC3 application.

6. (Optional) Click **Change** to select a different destination folder for the installation files.

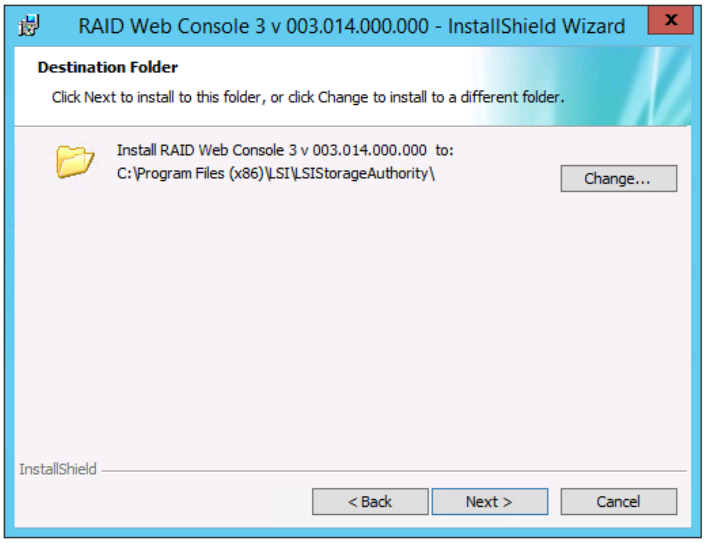


Figure 3. Destination folder dialog

7. Click **Next.**
8. The **Configure Range of Events to Generate Alert Notifications** dialog appears. You can configure alert notifications to get early notification of application or service issues/problem occurrences.

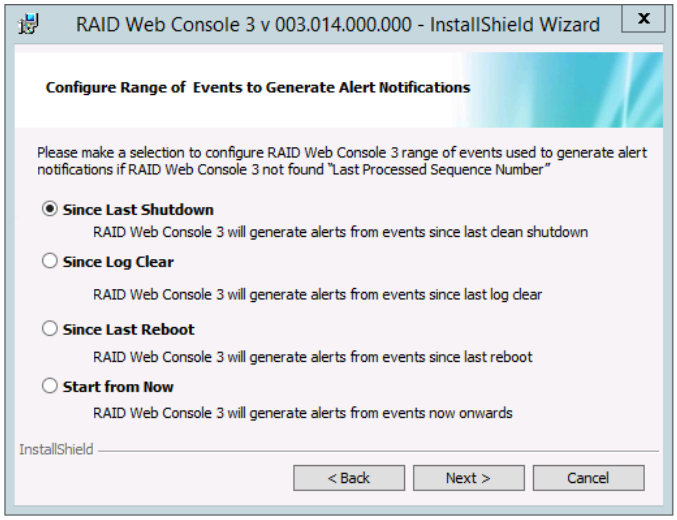


Figure 4. Configure range of events to generate alert notifications

The following configuration options are available:

- **Since Last Shutdown**: Select this option to retrieve events from the last clean shutdown.
- **Since Log Clear**: Select this option to retrieve events from the last log that was cleared.
- **Since Last Reboot**: Select this option to retrieve events from the last time the system was restarted.
- **Start From Now**: Select this option to retrieve events from now.

These configuration options may also be changed as per user requirement at any point in time by editing the lsa.conf file in the LSI Storage Authority/conf directory and choosing the required parameter.

For example, if **Since Last Shutdown** was selected at the time of installation and the user would like to change configurations to **Since Last Reboot**, go to:

Retrieve range of events used to generate alert notification, if LSA not found LastProcessedSeqNum section.
Change the "retrieve_range_of_events_since =" to 2

Note: You must restart the LSI Storage Authority service for the configuration changes to take effect.

9. Select a setup type that suits your needs. The following options are available:
   For more information on each of these installers and their associated advantages, refer to Table 3. Types of installers and attributes.
   - Gateway
   - StandAlone
   - DirectAgent
   - Lightweight Monitor (LWM)

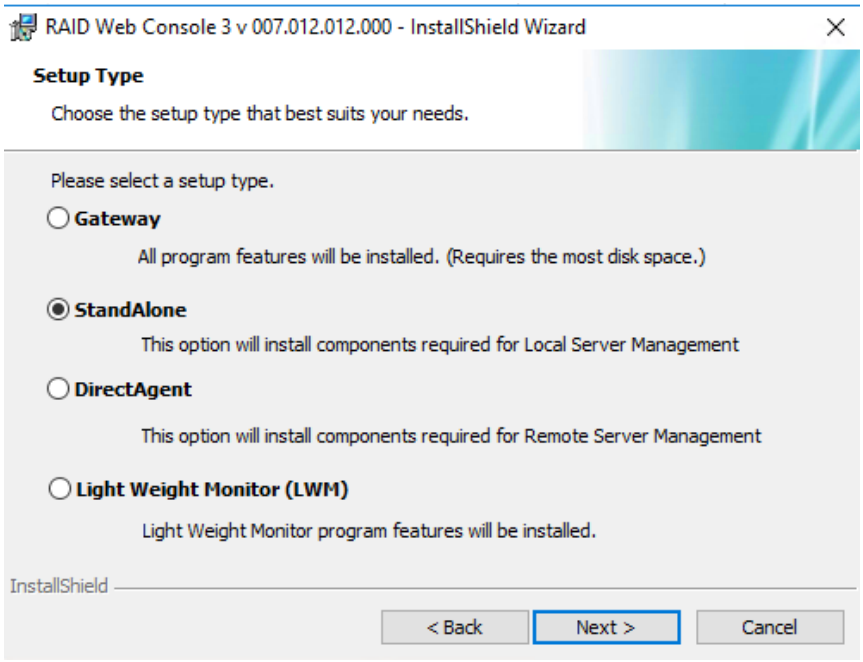
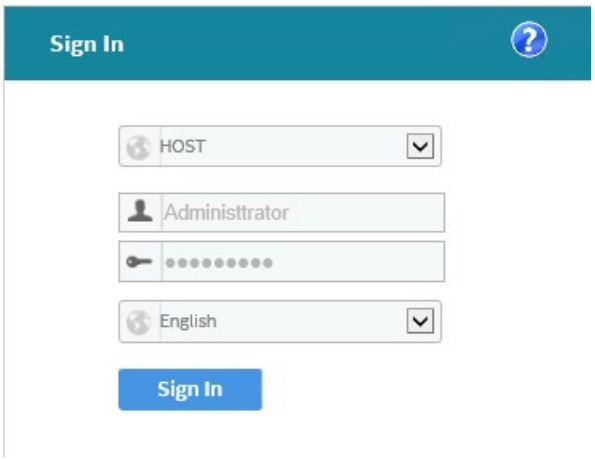


Figure 5. Setup type dialog

10. Click **Next**. The **Ready to Install the Program** dialog appears.
11. Click **Next**. Depending on the setup type selected, the **InstallShield Wizard Completed** dialog appears.
12. (Optional) Select the **Show the Windows* Installer log** check box to view the Windows* Installer log file. The log file (RWC3_install.txt) is created in the same folder from where setup.exeis installed.
13. Click **Finish**.
14. Launch **Intel® RAID Web Console 3** by opening a Web browser and typing: **http://localhost:<Web server port> i.e.** http://localhost: 2463

Note: The installer adds a direct access icon that can be double clicked on to launch the program.

15. Sign in using the appropriate credentials. Either an existing local account or a domain account.



16. Upon successful login, the **Select Controller** page appears.

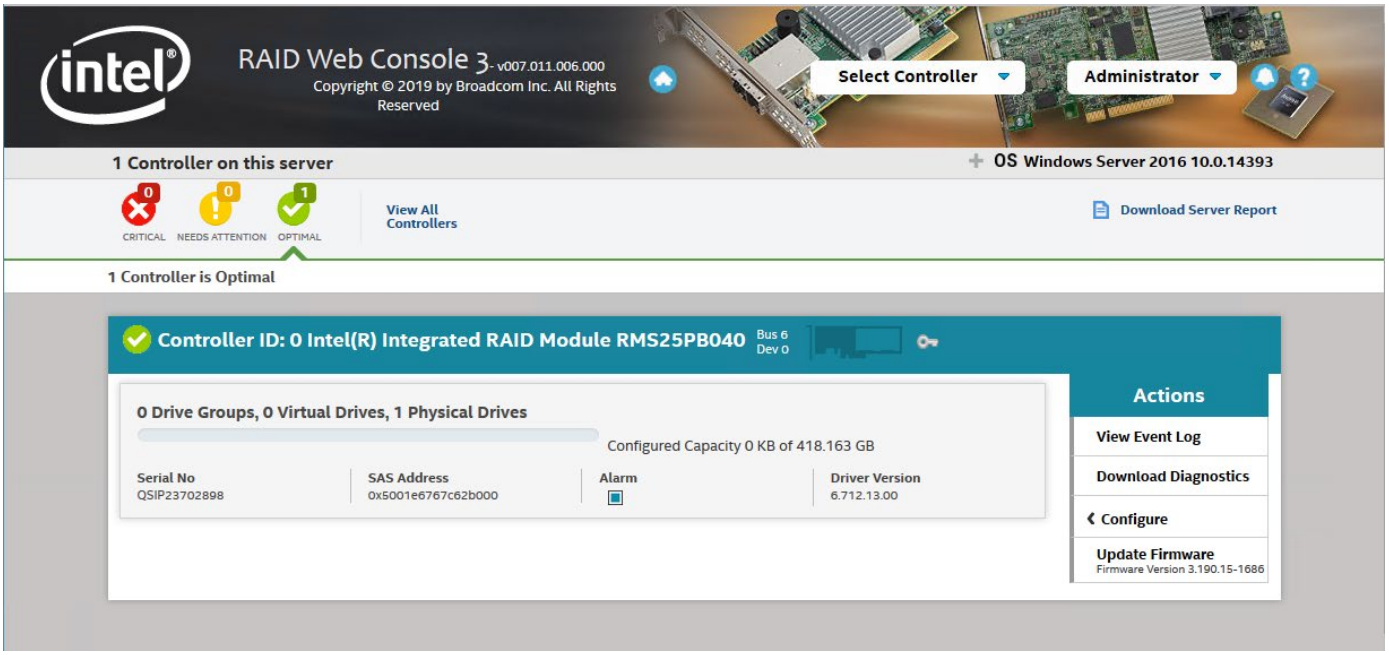


Figure 6. Intel® RAID Web Console 3 Select Controller page

The Select Controller page lists all the discovered RAID controllers on the server. From this page, the user can select the RAID controller to be managed.

3.6 Installing the Intel® RAID Web Console 3 Software on the Linux Operating System

The Intel® RAID Web Console 3 software supports both interactive and non-interactive modes of Linux installation.

3.6.1 Installing in Interactive Mode

Log in to the system with root privileges, or open the command prompt as root and run the installer through the command line.

Perform the following steps to install the Intel® RAID Web Console 3 Software in interactive mode:

1. Run the ./install.csh command from the installation disk or directory.

2. Read the license agreements for the software package. Agree to the terms of the entire license agreement and press Y. Otherwise, press N to exit the installation.

3. Select a setup type that suits your needs. The following options are available:

   - **Gateway**: Press the number 1. Selecting this option installs all the program features.
   - **StandAlone**: Press the number 2. Selecting this option installs components that are required for Local Server Management.
   - **DirectAgent**: Press the number 3. Selecting this option installs components that are required for Remote Server Management.
   - **Lightweight Monitor**: Press the number 4. Selecting this option installs the Lightweight Monitor program features.

4. The **Configure Range of Events to Generate Alert Notifications dialog** appears. The user may configure alert notifications to get early notification of application or service issues/problem occurrences. The following configuration options are available:

   - **Since Last Shutdown**: Select this option to retrieve events from the last clean shutdown.
   - **Since Log Clear:** Select this option to retrieve events from the last log that was cleared.
   - **Since Last Reboot:** Select this option to retrieve events from the last time the system was restarted.
   - **Start From Now:** Select this option to retrieve events from now.

   You can also change these configuration options as per your requirement at any point in time by editing the lsa.conf file in the LSI Storage Authority/conf directory and choosing the required parameter. You must restart the LSI Storage Authority service for the configuration changes to take effect.

5. Enter the nginx server port number. The port range is from1 to 65535. The default port number is 2463.

6. Enter the LSI Storage Authority Application port numbers. The port range is from 1 to 65535. The default port number is 9000.

   Ensure that the nginx_port number and the LSA_port number are in between the range, 1–65535 and /or different. If the nginx_port number and the LSA_port number are not specified in the command line, the default values are used.

By default, LSA communicates on Web Server Port 2463 and LSA Server Port 9000. Ensure that these ports are available to be used by LSA. Depending on your environment, if these ports are not available, specify the port details here. These port details may be edited after installation as well.

7. Turn off the Linux Firewall.

8. Extract the contents of the .zip file and install the appropriate package on the 32-bit Linux operating system or 64-bit Linux operating system. The LSA_Linux.zip file contents are as follows:

   - **x86:** Contains files for 32-bit platforms.
   - **x64:** Contains files for 64-bit platforms.

Note: Ensure that the Connect Automatically check box is selected. This is available under the Network Connections menu.

3.6.2 Installing in Non-interactive Mode

Log in to the system with root privileges, or open the command prompt as root and run the installer through the command line.

Perform the following steps to install the LSI Storage Authority software in the non-interactive mode:

1. Run the ./install.csh [-options] [nginx_port] [LSA_port] command from the installation disk. Where:

   - **Options:** Enter c for complete setup and m for monitor setup.
   - **nginx_port:** The nginx server port number.
   - **LSA_port:** The RWC3 Application port number.

   Ensure that the nginx_port number and the LSA_port number are between the range of 1-65535 and are different. If the nginx_port number and the LSA_port number are not specified in the command line, the default values (nginx default port 2463 and LSA default 9000) are used.

   Command Usage Examples:

   - **Gateway Installation with default ports**: ./install.csh -g
   - **StandAlone Installation with default ports:** ./install.csh -s
   - **DirectAgent Installation with default ports:** ./install.csh -d
   - **Light Weight Monitor Installation with default ports**: ./install.csh -l
   - **Gateway installation with different ports**: ./install.csh -g 1234 8000
   - **StandAlone installation with different ports:** ./install.csh -s 4321 7000
   - **DirectAgent installation with different ports**: ./install.csh -d 1254 8800
   - **Light Weight Monitor installation with different ports**: ./install.csh -l 4388 9900

2. Extract the contents of the zip file and install the appropriate package on the 32-bit Linux operating systems or the 64-bit Linux operating systems. The LSA_Linux.zip file contents are as follows:

   - **x86:** Contains files for 32-bit platforms.
   - **x64:** Contains files for 64-bit platforms.

Note: The RWC3 installation requires a prior installation of the OpenSLP software. This is an open source software and at the time of writing this guide there is no way to perform the installation of this software in a non-interactive mode

3.6.3 Uninstalling the Intel® RAID Web Console 3 Software on the Linux Operating System

Perform the following step to uninstall the Linux operating system:

1. Run the uninstaller.sh script (/opt/lsi/LSIStorageAuhority/uninstaller.sh).

Note: Alternatively, you can run the rpm -e <rpm_name> command to uninstall the RPMs from the target system.

3.6.4 Launch RWC3

Launch Intel® RAID Web Console 3 by opening a Web browser and typing: **http://localhost:<Web server port>** (i.e. http://localhost: 2463).

3.7 Support for the Intel® RAID Web Console 3 Software on the VMware* ESXi Operating System

This section outlines the pre and post-installation requirements needed to support the VMware* ESXi Operating System. The Intel® RAID Web Console 3 Software cannot be installed directly on the VMware* ESXi operating system. Management of the RAID controllers is performed through the RWC3 Software installed on a client Linux*/Windows* machine on the same subnet, however the SMI-S Provider needs to be installed on the host system in order to establish a communication path between the host system with the RAID controller installed and the client machine running the RWC3 software.

3.7.1 Network Communication Details

Network communication is a key element between the VMware* ESXi SMI-S Provider and the RWC3 management software. Ensure that the network settings are correct by making the following changes:

1. Provide a proper host name and an IP address while performing the initial configurations for the VMware ESXi host. By default, the host name is “Localhost” provide a meaningful name instead of leaving the default.
2. For networks with a DNS infrastructure, follow the next directions:
    - On the DNS server: Ensure DNS records are created in order to reach the ESXi host and the RWC3 client machine by name as well as by IP address. This means that both the “A” record and the pointer record (in the reverse lookup zone) need to be created. The records must have the FQDN for each machine.
    - On the ESXi host:
        a) Make sure the domain name is correct in the TCP/IP settings.
        b) Ensure the domain name appears as part of the host’s name on the ESXi host management web page or Virtual Center, in other words, the server name must appear as the FQDN.
        c) Make sure the DNS server’s IP address is correctly set in the “DNS configuration”.
        d) Make sure the DNS Suffixes are correctly set in the “Custom DNS Suffixes configuration”.
    - On the RWC3 client machine: Make sure the DNS suffixes are correctly set.

3. For networks that do not have DNS infrastructure, the hosts file on both, the ESXi host server and RWC3 client machine must be edited as follows:

- The /etc/hosts file on the ESXi host server should have an entry mapping the RWC3 client machine with its corresponding IP address, this way the client machine should be accessible from the ESXi host server by name.
- The hosts file on the RWC3 client machine should have an entry mapping the ESXi host server with its corresponding IP address, this way the ESXi host server should be accessible from the RWC3 client machine by name.
- For Windows* client machines, the default DNS server may need to be changed to 127.0.0.1 in order to use the entries in the hosts file.

Note: Both the Client and the Server should be in the same subnet.

3.7.2 SMI-S Provider Details

Deploy the SMI-S Provider on the ESXi host after setting the Network Communication on section 3.7.1

For VMware* ESXi 4.x, 5.x, and 6.x to work with RWC3, depending on the VMware* ESXi environment, the following SMI-S Provider must be installed:

Table 4. SMI-S Providers

VMWare ESXi Version	SMI-S Provider Version
VMware ESXi 4.x	VMware-ESX4-Provider.zip
VMware ESXi 5.4 and below	VMware-ESXi5.4-Provider.zip
VMware ESXi 5.5 and above	VMware-ESXi5.5-Provider.zip

Prerequisites:

1) Download the VIB package provided by Broadcom (license must be accepted to proceed at the Broadcom site)
2) Download the RAID controller's VMWare driver from the VMWare web site.

Note: this second step is required only if the ESXi host has not recognized the RAID controller. To find this out, using the VMCenter or the vSphere Client connect to the host, open the Configuration tab and select Storage Adapters. Notice that the RAID controller might appear named as a **MegaRAID SAS Controller**. If the ESXi installation was performed on a RAID controller's virtual drive, this step is not needed.

To deploy the MegaRAID SMI-S provider on an ESXi machine copy the VIB package as well as the driver file (in case needed) to the ESXi host, to a local path.

For example, using the vSphere Client, create a folder named RWC3 on data store “Datastore1”. Then copy the complete folder that was downloaded on prerequisite 1 (unzip the folder before the download)

Use the *esxcli command* to load the MegaRAID SMI-S provider, and run the following command for each VIB file:

ESXi# esxcli software vib install -v <VIB file> --force

(Make sure to include the complete file path)

Example:

```
[root@localhost:~] esxcli software vib install -v  /vmfs/volumes/datastore1/RWC3/LSI_Provider/vmware-esx-provider-lsiprovider.vi
b
b

Installation Result
   Message: The update completed successfully, but the system needs to be rebooted for the changes to be effective.
   Reboot Required: true
   VIBs Installed: LSI_bootbank_lsiprovider_500.04.V0.66-0002
   VIBs Removed:
   VIBs Skipped:
[root@localhost:~]
```

Note: A reboot is required after installing the SMI-S provider on VMware ESXi environment.

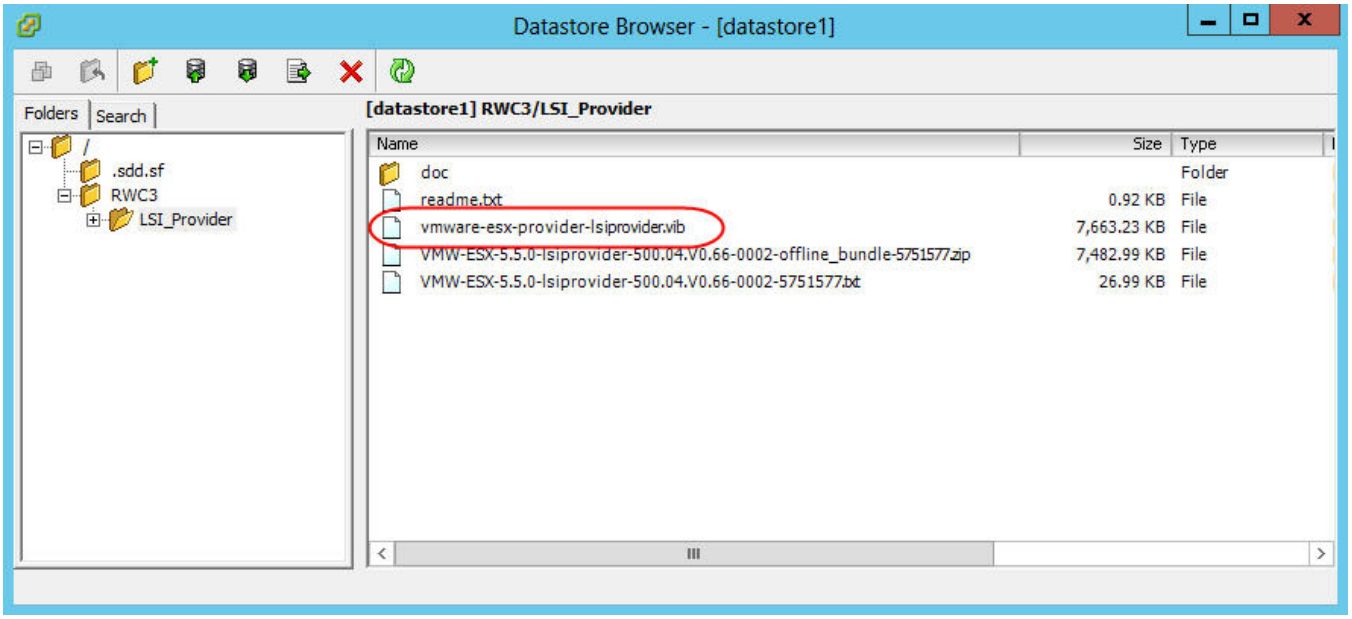
3.7.3 Firewall Details

Ensure that you run the following command after every reboot to disable the firewall, as it is enabled on every reboot:

esxcli network firewall unload

In a VMware* ESXi environment, to check whether the firewall is enabled, execute the following command:

esxcli network firewall get



3.7.4 Windows*/Linux* Client Steps

The following steps are required on the Windows*/Linux* Client:

1. Stop or disable the firewall on the client machine.
2. Install the latest RWC3 Client in a Gateway installation mode.
3. Launch RWC3. A certificate error may appear that can be ignored.
4. Ensure that ESXi host server is discovered.
5. Login to the newly discovered RWC3 server using the ESXi credentials. Logging in to the remote ESXi host for the first time may take 1–2 minutes.

Note: Disable the firewall on both the ESXi host and the RWC3 client machine.

Remote management of VMware* ESXi is supported only in a Gateway installation of RWC3 on the following operating systems:

- Microsoft* Windows Server
- RHEL
- SuSE Linux*

At this point, the RWC3 software should be able to manage the RAID controller(s) installed on the ESXi host server. Follow the next steps in case the server cannot be discovered.

3.7.5 Provider Services

Below are listed the SMI-S provider services, in case needed, ensure these services are up and running.

Run the following commands to ensure that provider services are up and running on VMware ESXi:

/etc/init.d/slpd status
/etc/init.d/sfcbd-watchdog status

3.7.6 Configuration Change Details

If there is any configuration change, ensure that the following actions are performed:

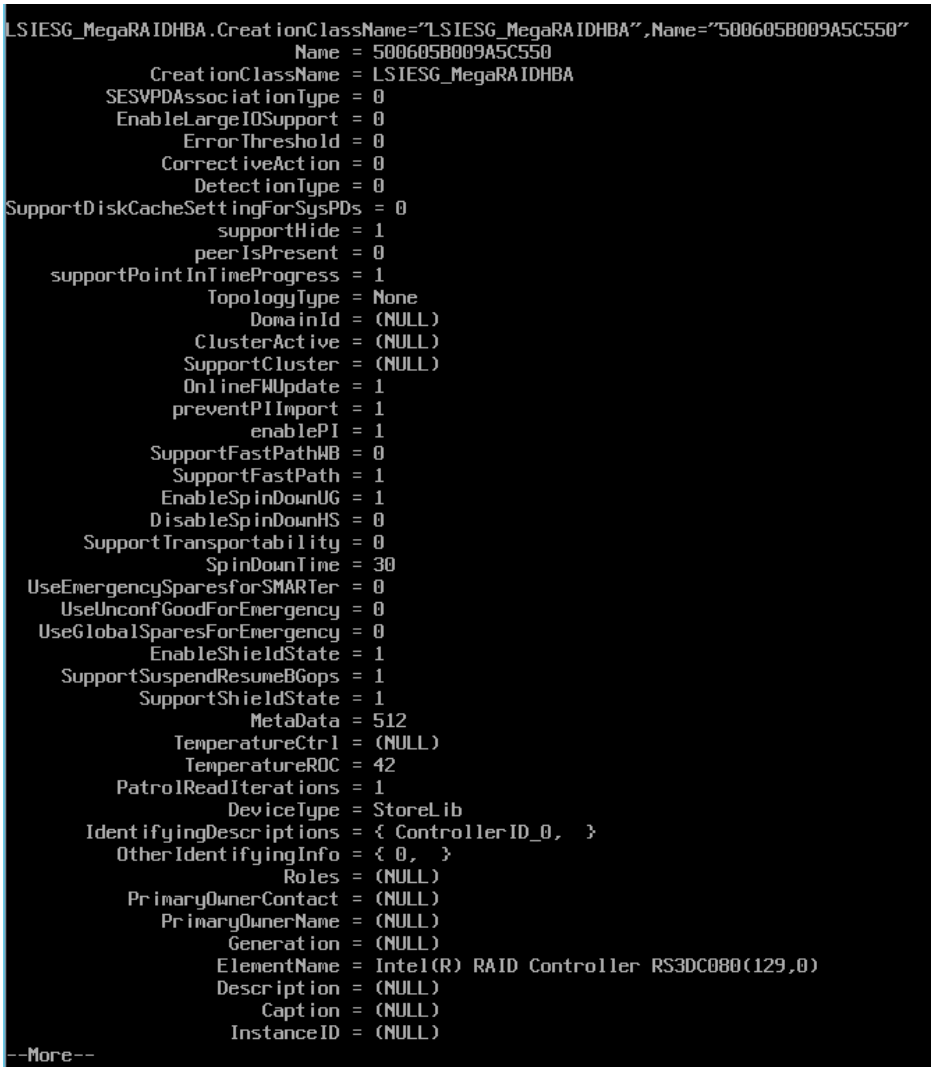
/etc/init.d/sfcb-watchdog stop
/etc/init.d/slpd stop
/etc/init.d/slpd start
/etc/init.d/sfcb-watchdog start

3.7.7 Storage Controller

Ensure that the storage controller on VMware* ESXi has the right configuration (Firmware/Driver) and is working as expected before connecting through LSA. The following command helps verify whether or not the controller is detected:

enum_instances cim_system lsi/lsimr13|more

Information pertaining to the RAID controller should be displayed.



3.7.8 Configuring the Network on VMware ESXi Environment

By default during the VMware ESXi Operating System installation, the IP and host name should be configured appropriately. If an already installed VMware ESXi Operating System is moved from one network to the other, and if the host name mapping isn't correct, follow the steps in the following link to configure the network and host name:
http://www.unixarena.com/2015/05/how-to-configure-the-network-on-vmware-esxi-6-0.html

3.7.9 Multi-subnet Configuration

When a gateway is part of multiple subnets, and the discovered VMware* server is part of one of these subnets, configuration for both the LSA gateway and the VMware gateway under the same subnet is required.

You can add an irrelevant IP address to the LSA configuration file (conf\LSA.conf -> private_ip_range=*) to avoid registering the wrong IP to the VMware gateway.

A CURL error in a CIMOM server results in a blocked AEN to the upper layer (CIMProvider-->LSA). This occurs when the servers are in different subnets or if there is any incorrect/incomplete AEN subscriptions. To avoid this error, both the client and the server must be in the same subnet. Any incomplete AEN subscriptions must be removed via CIMClient.

To view the existing subscriptions, enter:

host-ind -s

To remove an existing subscription, enter:

host-ind -d -k<*handler name*>

For example:

host-ind -d -k dhcp-x.y.z.k.dhcp.company.net_LSA_127.0.0.1

Note: It is recommended to either restart the sfcbservice or reboot the server after making any changes to the VMware* Server.

---

4. Performing the Initial Configuration

After successfully installing the Intel® RAID Web Console 3 Software, the following initial configurations must be set up.

4.1 Setting the Firewall Rules.

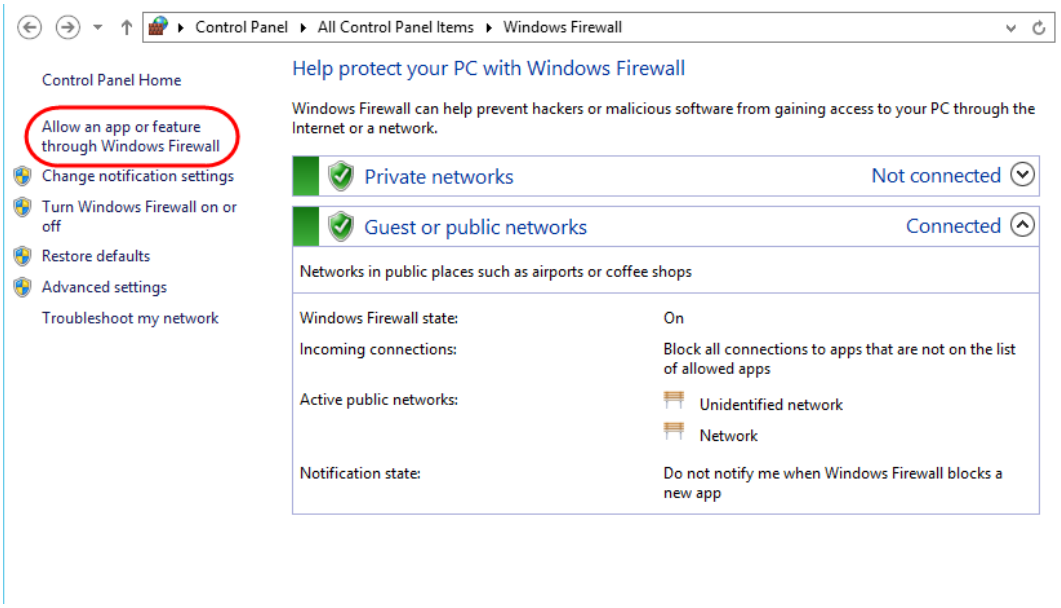
By default, RWC3 uses a TCP port 2463 for the communication among the different RWC3 servers on the network, although this port number can be different (See section 4.4 for instructions for changing the application port number). Also, OpenSLP uses UDP port 427 for server discovery. Both ports need to be allowed input traffic on the client RWC3 servers to allow the Gateway server to discover and manage them. See the following instructions to allow this traffic on the different Operating Systems.

4.1.1 Setting the firewall rules on Microsoft* Windows.

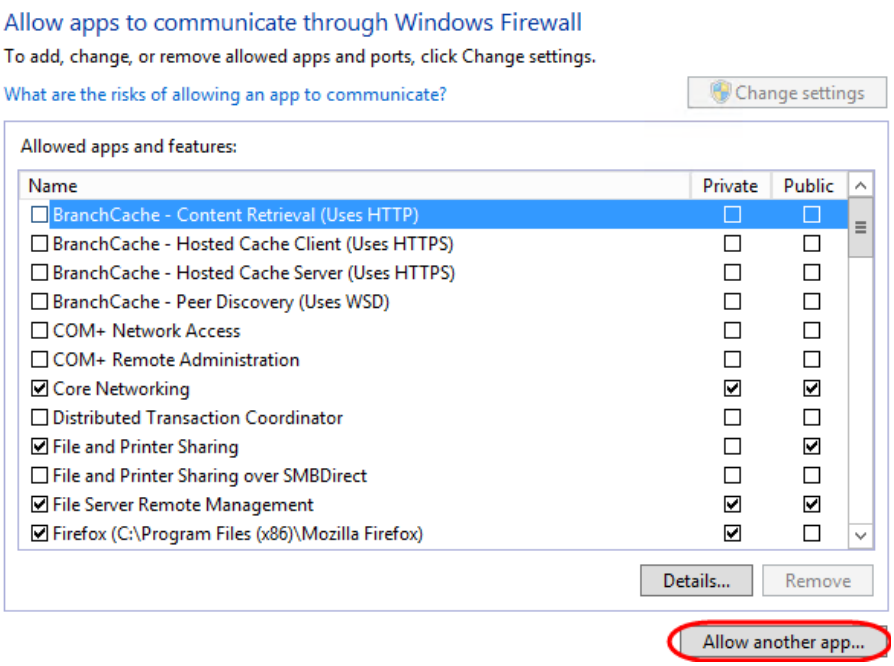
Experienced users may open the above-mentioned ports; however, this section shows an alternative and easier way to accomplish the same result.

The easiest way is to allow the **nginx** application to communicate through the Windows* Firewall.

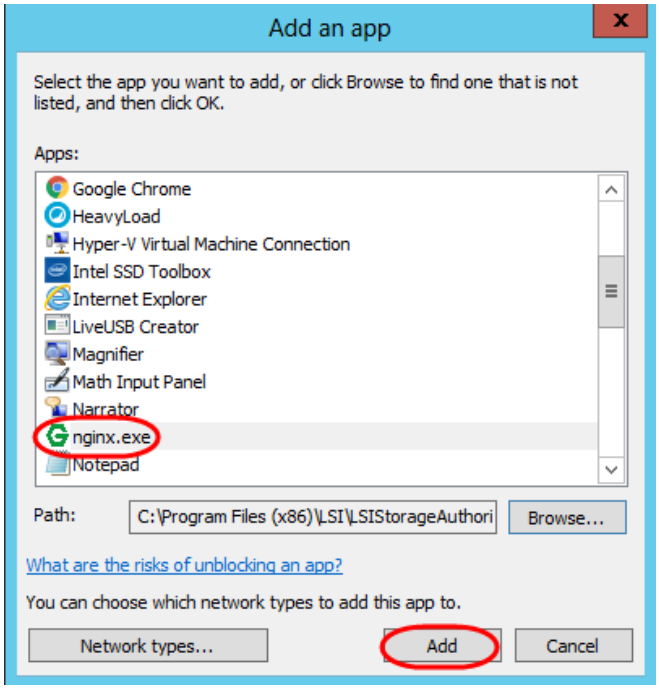
1. Open the Windows* Firewall.
2. Select **Allow an app or feature through Windows* firewall**



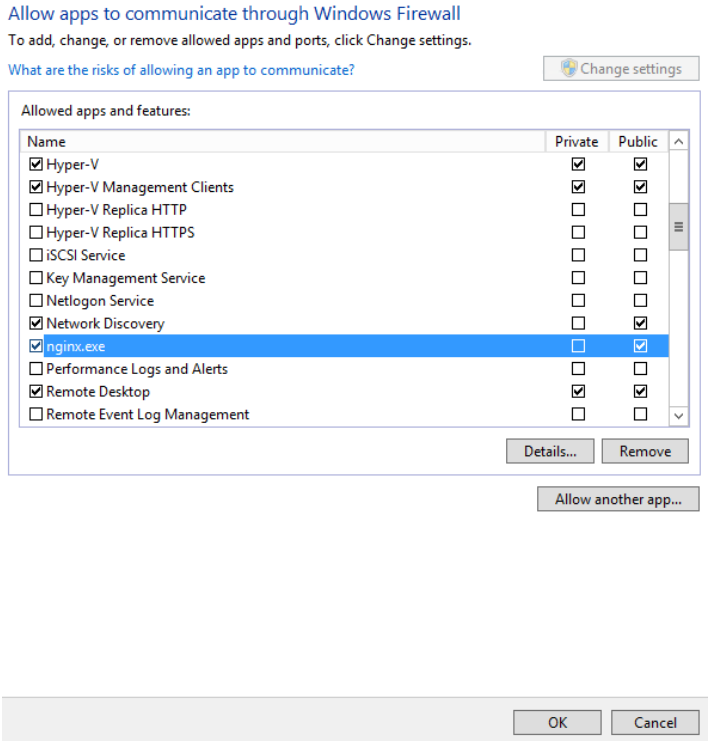
3. Select Allow another application.



4. Select **Browse** and navigate to the C:\Program files (x86)\ LSI\LSIStorageAuthority\server folder and look for the nginx.exe application. Select Add.



5. **nginx** will be added to the list of applications. Check mark on Private or Public depending on the network used for the RWC3 communication and click OK.



4.1.2 Setting the firewall rules on Linux*.

There are different ways to manage the Linux firewall, using the *firewall-cmd* command will be used on this guide as an example.

firewall-cmd -- get-active-zones provides details on the zone where the network interfaces are located. By default, the network interface, i.e. eno2, is on the "public" zone and most of the traffic is blocked. It is possible to change it to the "trusted" zone and allow all traffic, by issuing the command: **firewall-cmd --change-interface=eno2 --zone=trusted**.

```
[root@localhost ~]# firewall-cmd --get-active-zones
libvirt
  interfaces: virbr0
public
  interfaces: eno2
[root@localhost ~]# firewall-cmd --change-interface=eno2 --zone=trusted
success
[root@localhost ~]#
```

Being on the trusted zone, all traffic will be allowed without restrictions, however, this alternative is not feasible for all environments and the other alternative is not changing the zone but just opening the needed ports.
Type the next commands to open UDP port 427 and TCP port 2463 (The default port 2463 can be changed at the installation time or later, see section 4.4):
firewall-cmd --add-port=427/udp --zone=public --permanent
firewall-cmd --add-port=2463/tcp --zone=public --permanent

```
[root@localhost ~]# firewall-cmd --add-port=427/tcp --zone=public --permanent
success
[root@localhost ~]# firewall-cmd --add-port=2463/tcp --zone=public --permanent
success
[root@localhost ~]#
```

4.2 Using LDAP Authentication

To access the LDAP service, the RWC3 server must know some information about the LDAP server settings. Apart from the username and password details for the LDAP authentication, the RWC3 back-end must know some parameters to enable authentication.
Perform the following steps to configure these parameters in the **lsa.conf** file.

1. Open the **lsa.conf file** depending on the OS being used, see the corresponding file location.
   - Windows* OS: C:\Program Files(x86)\LSI\LSIStorageauthority\conf
   - Linux* OS: /opt/lsi/LSIStorageAuthority/conf
2. Enter a value for the ldap_mode field. If you set is as 0, the LDAP authentication using the RWC3 software is disabled. If you set it as 1, the LDAP authentication using the RWC3 software is enabled.
   Example:
   LDAP Login
   ldap_mode = 1
3. Enter the hostname of the LDAP server in the ldap_server field. This value is used to connect to the specific LDAP server for the user authentication.
   Example:
   # LDAP Server
   ldap_server = <Hostname of the LDAP server>
4. (Optional) Enter the LDAP protocol version in the ldap_protocol_version field. This value is used to define the protocol that is used to create an LDAP session.
   Example:
   # LDAP Protocol version
   ldap_protocol_version = v3

   Note: The default value is v3.

5. Enter the LDAP authentication mode in the ldap_bindingfield. In LDAP, the authentication is supplied through the Bind operation. LDAP supports three types of authentication modes:
   - **Anonymous:** When an LDAP session is created the authentication state of the session is set to the anonymous mode.
   - **BASIC (default)**: The simplest form of client authentication is to bind to the server using a clear-text password. This mechanism has security problems because the password can be read from the network.
   - **SECURE:** A more secure method is to use Simple Authentication and Security Layer (SASL) authentication mechanisms, such as DIGEST-MD5[4]. This is based on an encryption known to both the client and the server, allowing for a simple challenge-response scheme. The SASL authentication mechanism is also capable of negotiating data encryption to protect subsequent operations.

   Example:
   # LDAP_BINDING
   ldap_binding = BASIC

6. (Optional) Enter the LDAP server port number in the ldap_port_number field.

   Note: If a port number isn't specified, the standard LDAP port 389 is used for the BASIC authentication mode. For the SECURE authentication mode, the Port 636 is used

   Example:
   # LDAP Port Number
   ldap_port_number = 389

7. Enter the DN (distinguished name) details in the *dn_details field*. The format is as follows:

   Example:
   # LDAP_DN_DETAILSdn_details
   ={"DN":[{"key":"DC","values":["ldapdomain"]},{"key":"DC","values":["com"]},{"key"
   :"ou","values":["TEST"]}]}
   Where:
   - **DC:** This attribute contains the Domain Component type.
   - **ou:** This attribute contains the name of an organizational unit.
8. (Optional) Enter the LDAP user access privilege details in the readOnly field. The values follow:
9. 1 (default): Read only access.
10. 0: Full access
11. Restart the nginx Service and the RWC3 Service for the changes to take effect.

4.3 Accessing RWC3 Over Network Address Translation (NAT)

Network Address Translation (NAT) enables private IP networks that use unregistered IP addresses to connect to the internet. NAT operates on a router usually connecting two networks together, and translates the private addresses in the internal network into legal addresses.

To access the Intel® RAID Web Console 3 application over a NAT environment, the RWC3 server must know some information about the NAT server settings.

Perform the following steps to configure the parameters in the **lsa.conf** file in the **LSI Storage Authority/conf directory**:

1. Open the **RWC3.conf file** in the **Intel RAID Web Console 3/conf directory**.
2. Specify the public IP of nat_ipv4_ipv6.
   Example: if the public NAT IP address configured is 135.24.227.198, nat_ipv4_ipv6 = 135.24.227.198 must be specified.

Note: If you have multiple public NATs (for example, 135.24.227.198, 135.24.227.199, fe80::dc8d:e156:41e1:b06), nat_ipv4_ipv6 = 135.24.227.198, 135.24.227.199, fe80::dc8d:e156:41e1:b06 must be specified.

---

3. Restart the nginx service and the RWC3 Service for the changes to take effect.

4.4 Changing the Intel® RAID Web Console 3 Application Port Number

By default, RWCs listens on port 9000, perform the following steps to change the Intel® RAID Web Console 3 Application port numbers.

1. Open the **lsa.conf** file located on the following directories.
   For the Windows* OS: C:\Program Files (x86)\LSI\LSIStorageAutority\conf
   For the Linux* OS: /opt/LSI/LSIStorageAutority/conf
2. Enter the new port number in the listening_port field

   Note: Prior to assigning the port number, verify if the port is available for usage.

3. Save the **lsa.conf** file

4. Open the **nginx.conf** file located on the following directories:
   For the Windows* OS: C:\Program Files (x86)\LSI\LSIStorageAutority\server\conf
   For the Linux* OS: /opt/LSI/LSIStorageAutority/server/conf
5. Enter the new port number in the listening_port field
6. Replace all of the fastcgi_pass 127.0.0.1:9000 instances with fastcgi_pass 127.0.0.1:<new port number>
7. Save the **nginx.conf** file
8. Windows* OS only: Open the ***portconfig.properties*** file located on the C:\Program Files (x86)\LSI\LSIStorageAutority
   Enter the new port number in the <Client Port> <LSA Server Port> field
   Save the **portconfig.properties** file
9. Restart the nginx Service and the LSI Storage Authority Service
   Windows* OS:
   a) Open a Command prompt window as Administrator.
   b) Type Net stop NginxService.
   c) Type Net start NginxService.
   d) Type Net stop LSAService.
   e) Type Net start LSAService
   f) Close the Command prompt window.

   Linux* OS:
   a) At the Linux* prompt, type systemctl restart nginx
   b) At the Linux* prompt, systemctl restart lsa

4.5 Changing the nginx Web Server Port Number

By default, the nginx application listens on port 2463, perform the following steps to change the Intel® RAID Web Console 3 Web Server port number.

Perform the following steps to change the nginx web server port numbers.

1. Open the **lsa.conf** file located on the following directories.
   For the Windows* OS: C:\Program Files (x86)\LSI\LSIStorageAutority\conf
   For the Linux* OS: /opt/LSI/LSIStorageAutority/conf
2. Enter the new port number in the client_listening_port field

   Note: Prior to assigning the port number, verify if the port is available for usage.

3. Save the **lsa.conf** file
4. Open the **nginx.conf** file located on the following directories:
   For the Windows* OS: C:\Program Files (x86)\LSI\LSIStorageAutority\server\conf
   For the Linux* OS: /opt/LSI/LSIStorageAutority/server/conf
5. Enter the new port number in the listening_port field
6. Replace the listen 2463 instances with the new port number
7. Save the **nginx.conf** file
8. Windows* OS only: Open the ***portconfig.properties*** file located on the C:\Program Files (x86)\LSI\LSIStorageAutority
   Replace the 2463 in the <Client Port> field with the new port number
   Save the **portconfig.properties** file

9. Restart the nginx Service and the LSI Storage Authority Service
   Windows* OS:
   g) Open a Command prompt window as Administrator.
   h) Type Net stop NginxService.
   i) Type Net start NginxService.
   j) Type Net stop LSAService.
   k) Type Net start LSAService
   l) Close the Command prompt window.

   Linux* OS:
   c) At the Linux* prompt, type systemctl restart nginx
   d) At the Linux* prompt, systemctl restart lsa

4.6 Language considerations (Windows* OS)

When using native German, French, Spanish or Russian OSs, login errors may happen due to the different way that Windows* names the “Administrator” local group. In order to solve this issue, follow the next steps:

- Stop LSAService in Windows* Services on the local server using these languages.
- Edit LSA.conf located on the C:\Program Files(x86)\LSI\LSIStorageAuthority\conf folder
- Look for this line: full_access_groups = Administrators
- Change the key word Administrators to Administrateurs for French language, Administratoren for German, Administradores for Spanish and Администраторы or Administratory for Russian.
- Restart the LSAService

Note: In case of an LDAP network, no changes are required on the domain Controller, just on the local servers running RWC3.

---

5. Performing the Initial Setup

After successfully logging onto the Intel® RAID Web Console 3 software, perform the following initial setup tasks before proceeding.

5.1 Managing Servers from the Server Discovery Page on the Gateway Server

The Intel® RAID Web Console 3 software allows you to set up a list of servers to monitor and manage when installed in Gateway mode. Perform the following steps to manage the servers:

1. Make sure the firewall rules are in place on the client or monitored RWC3 servers.
2. On the **Remote Server Discovery** page, click the **Go To - Manage Server Page** hyperlink. The **Gateway - Authenticate dialog** opens.

Figure 7. Gateway authenticate dialog

3. Enter the administrator credentials for the **Gateway server**.
    a. Select the **Domain** option from the drop-down list.
    b. Type the user name and the password in the **Domain\Username** and **Password** text fields, respectively.

Note: The gateway server retains the login credentials in an encrypted file.

4. Click **Sign In**. The **Remote Server Discovery** page switches to the **Managing Servers** page. The list of managed servers with their health status is displayed, and the user may now add and remove the managed servers from the list. For more information, see Adding Managed Servers and Removing Managed Servers.

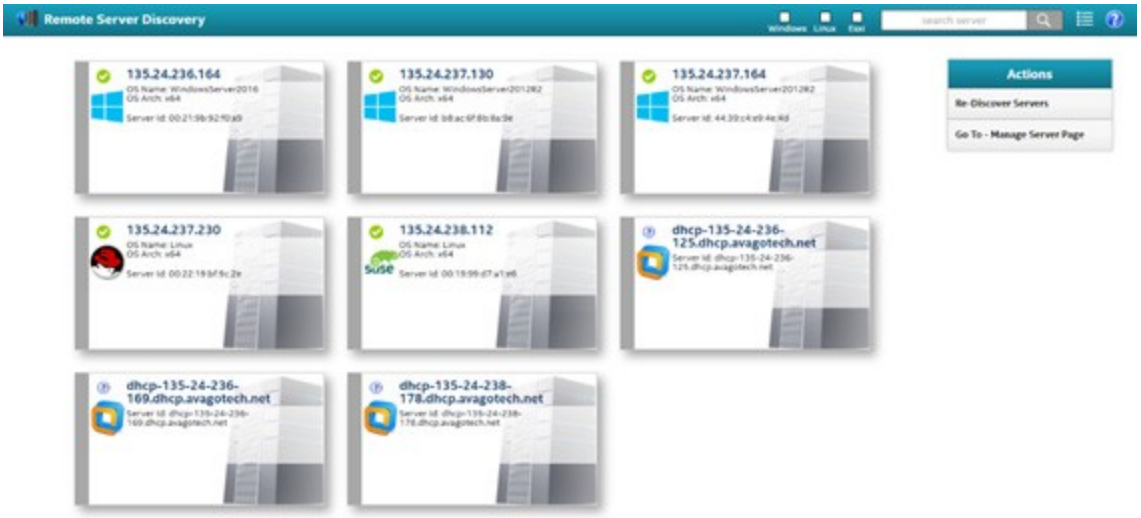


Figure 8. Managing server mode

5.2 Adding Managed Servers

Perform the following steps from the **Manage Servers** page to add the managed servers.

1. Select a server to add from the list of discovered servers, and click the **Manage** icon. The **Remote - Authenticate** dialog appears.

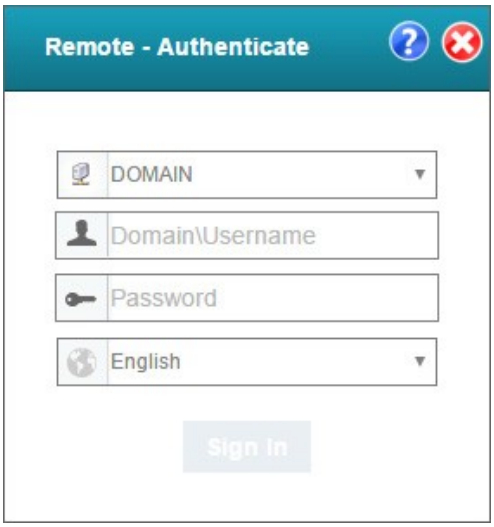


Figure 9. Remote - authenticate dialog

2. Enter the user credentials for the server you want to add.
    c. Select Host from the drop-down list.
    d. Type the user name and the password in the Username and Password text fields, respectively.
3. Click **Sign In**.

   The server is added to the list of managed servers. The  icon changes to  icon.
4. Click the server that you have added to the managed server list. The Server dashboard page for the server appears. See Server Dashboard.

5.3 Removing Managed Servers

Perform the following steps from the **Manage Servers** page to remove the managed servers:

1. Click the  icon. The host is removed from the list of managed servers. The  icon changes to the  icon.

5.4 Alert Settings

The **Alert Settings** tab,  , contains the following actions:

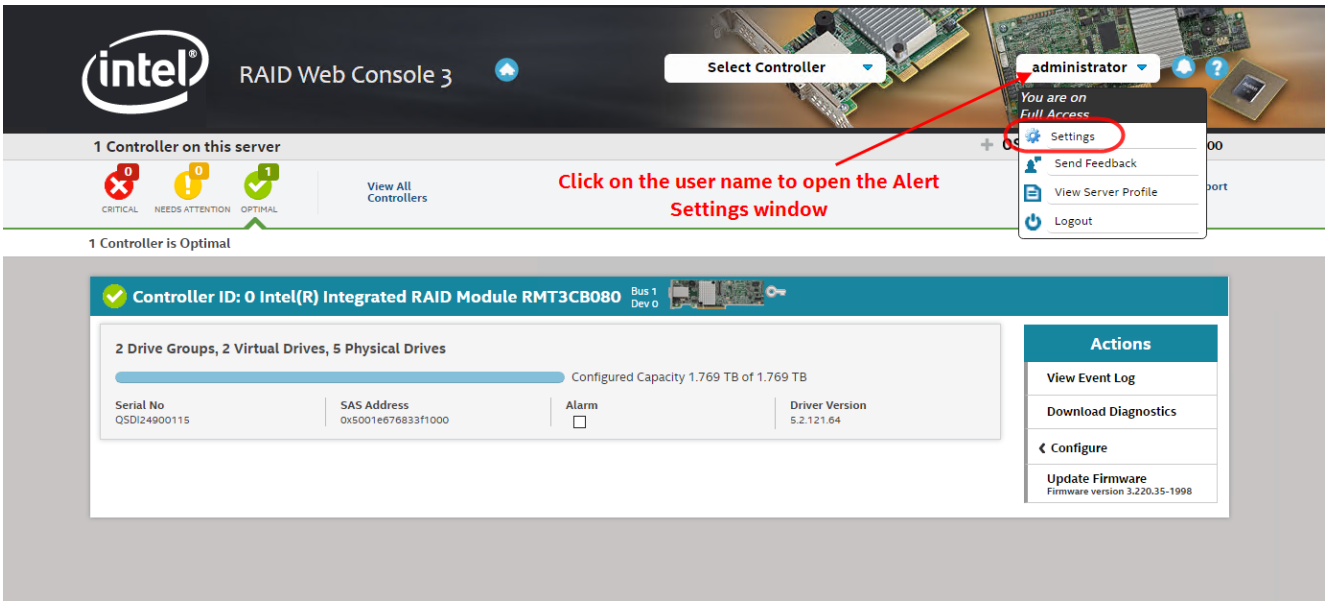
1. Changes to the alert delivery method for different severity levels.
2. Specifications to different alert delivery methods for inside and outside the application.
3. Defaulting back to default alert delivery methods and the default severity level of an individual event.
4. Ability to save the alert settings on the server.

Based on the severity level (Information, Warning, Critical, and Fatal), the default alert delivery methods change. By default, each severity level has one or more alert delivery methods configured for it. The different alert delivery methods are as follows:

1. **System Log:** By default, all of the severity events are logged in the local syslog. In the Windows* operating system (OS), the system log is logged in Event Viewer > Application. In the Linux* OS, the system log is logged in var > log.
2. **Event Log:** By default, all the severity events appear in the event log. Click View Event Log to view the event log. Each message that appears in this log has a severity level that indicates the importance of the event (severity), an event ID, a brief description, and a date and timestamp (when it occurred).
3. **System Messages**: By default, fatal and critical events are displayed as system messages. System messages are displayed in a yellow bar at the top of the Server dashboard and the controller dashboard. System messages let you view multiple events in a single location.
4. **Email:** By default, fatal events are displayed as email notifications. Based on the configuration, the email notifications are delivered to your inbox. In the email notification, besides the event's description, the email also contains system information and the controller's image details. Using this additional information, you can determine the system and the controller on which the fatal error occurred.

To change the alert delivery method for each severity level, perform these steps:

1. Click **Username > Settings** in the Server dashboard.
   The **Alert Settings** window appears, including the default alert delivery methods for each severity level.



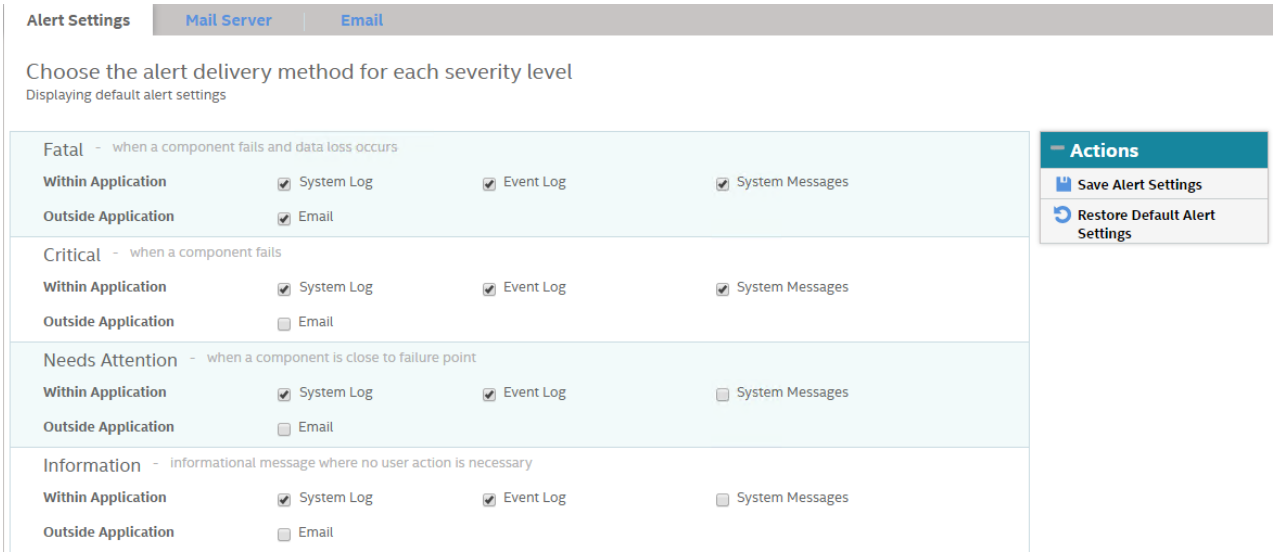


Figure 10. Alert settings windows

2. Select the desired alert delivery method for each severity level by clicking the required check box.
3. Click **Save Alert Settings** to save the settings on the server.

Note: Click **Restore Default Alert Settings** to revert back to the default alert delivery method settings.

5.5 Setting Up the Email Server

Perform the following steps to enter or edit the mail and SMTP server settings.

1. In the **Settings** window, click the **Mail Server** tab. The **Mail Server** tab appears and displays the current mail server settings.

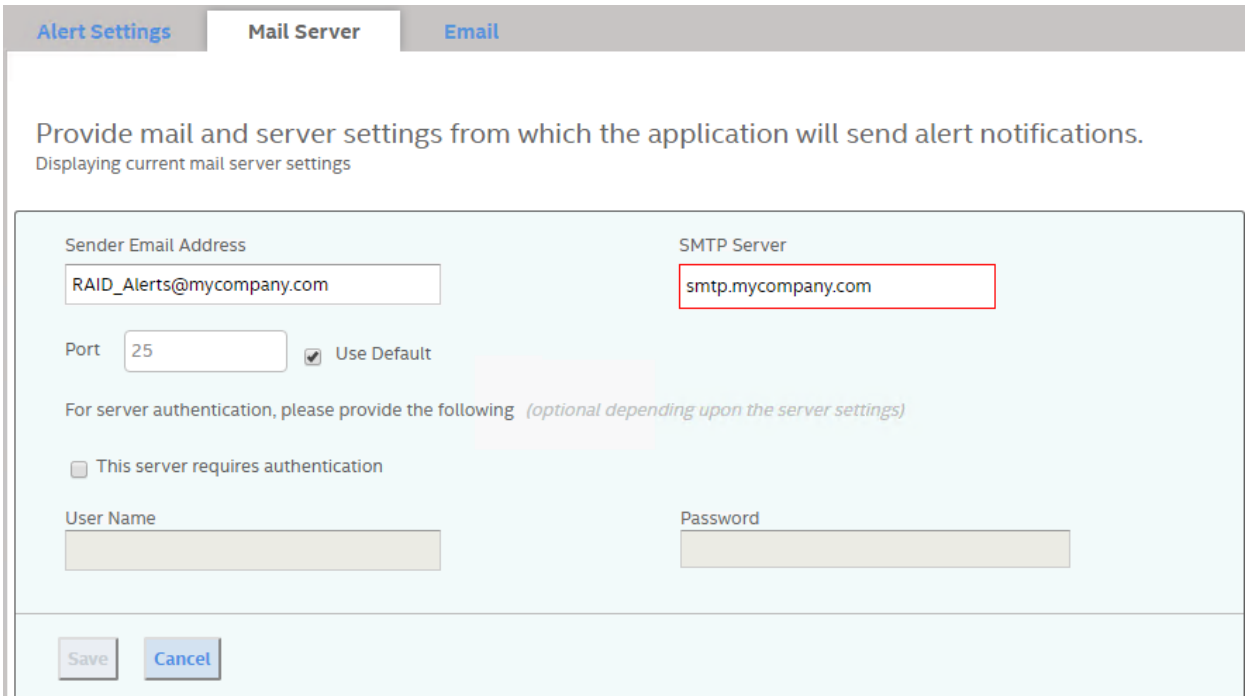


Figure 11. Mail server window

2. Enter a sender's email address in the **Sender Email Address** field, or edit the existing sender email address.
3. Enter the SMTP server name/IP address in the **SMTP Server** field, or edit the existing details.

4. Clear the **Use Default** check box to enter the desired port number in the **Port** field.
5. If on your SMTP server, the **Auth Login** feature is enabled or enabling this feature is needed on the Intel® RAID Web Console 3 software, enter the authentication details in the **User Name** and **Password** fields.
6. Click **Save**.

5.6 Adding Email Addresses of Recipients of Alert Notifications

Perform the following steps to add email addresses of recipients of the alert notifications.

1. In the **Setting** window, click the **Email** tab. The **Email** tab appears and displays the current email settings.

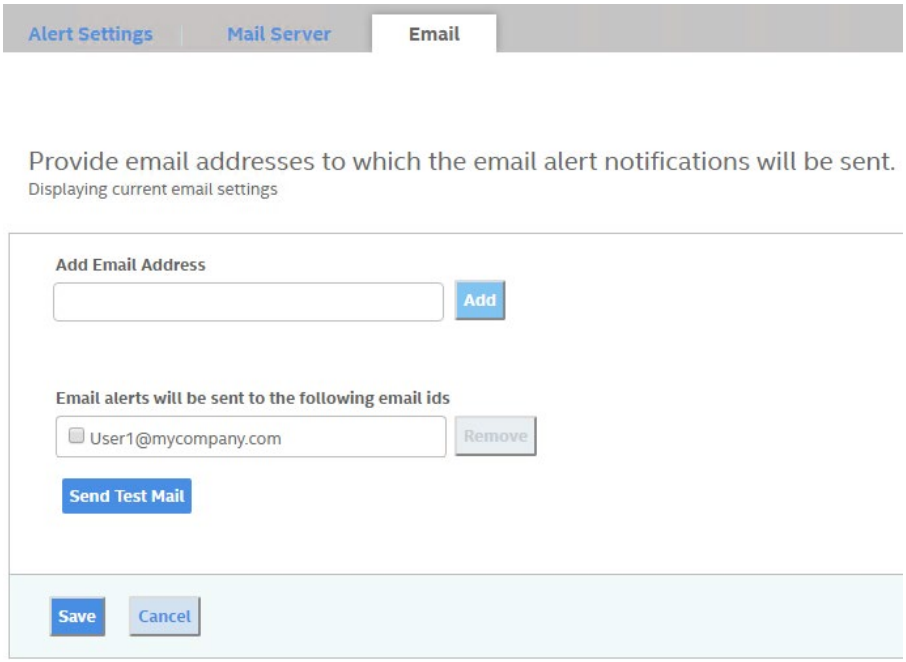


Figure 12. Email window

2. Enter the email address to add in the **Add Email Address** field.
3. Click **Add**. The new email address appears in the **Email alerts will be sent to the following email ids** field. Click **Remove** to delete the email addresses that are added.
4. Click **Send Test Email** to send a test message to the email addresses added for the recipients of alert notifications. A pop-up message indicates if the test message was successfully sent to the email address.
5. Click **Save** to save the email settings.

5.7 Configuring the Light Weight Monitor System

This section provides information on how to configure the Light Weight Monitor (LWM) agent.

Note: In order to configure the email server, alert settings, and system logs, the syslog.conf and config-current.JSON files must be edited. These files have the write permissions. Do not edit any other files in the package. If reverting back to the original settings is required, copy the contents of the config-default.JSON file to the config-current.JSON file. This action restores the configuration settings to its original state.

5.7.1 Setting Up the Email Server

Perform the following steps to configure the email server:

1. Open the config-current.JSON file in one of the following directories:
   Windows* OS: C:\Program Files (x86)\LSI\LSIStorageAuthority\conf\monitor.
   Linux* OS: /opt/lsi/LSIStorageAuthority/conf/monitor.

2. Make the following changes in the "email" sections of the files.

   Default Configuration:
   "email":
   {
   "isActive": true,
   "type": "EMAIL",
   "sender": "lsa-monitor@server.com",
   "server": "127.0.0.1",
   "to":
   [
   "root@localhost"
   ],
   "authentication":
   {
   "type": "NONE"
   }
   }

   Changes to Be Made: Edit the server field with the IP address of your SMTP server. For example, "server": "135.24.227.243"

3. If on your SMTP server, the Auth Login feature is enabled and if you want to enable this feature in the LWM agent, enter the following authentication details:

Default Configuration:
"email":
{
"isActive": true,
"type": "EMAIL",
"sender": "lsa-monitor@server.com",
"server": "127.0.0.1",
"to":
[
"root@localhost"
],
"authentication":
{
"type": "NONE"
}
}

Changes to Be Made: Enter the authentication details in the username and password fields, and make the

following changes in the "authentication" field.

"username": "Intel",
"password": "xxxx",
"authentication":
{
"type": "AUTH-LOGIN"
}

Where: Intel represents SMTP server's user name and xxxx represents the Base 64 converted SMTP configuration password.

4. Save the config-current.JSON file.
5. Perform the following steps to restart the Light Weight Monitor services for the changes to take effect.
   Windows* OS:
   Open a command prompt window.
   a) type the following command to stop the Light Weight Monitor service:
      sc stop LSAService
   b) type the following command to start the Light Weight Monitor service:
      sc start LSAService

   Linux* OS:
   Run the following command:
   /etc/init.d/LsiSASH restart

It is also recommended to restart the system log. To restart the system log, run the following command:
svcadm restart system-log

5.7.2 Adding the Email Addresses of Alert Notification Recipients

Perform the following steps to add email addresses of recipients of the alert notifications.

1. Open the config-current.JSON files in one of the following directories:
   Windows* OS: <ProgramFilesFolder>\LSI\LSIStorageAuthority\conf\monitor
   Linux* OS: cd /opt/lsi/LSIStorageAuthority/conf/monitor

2. Make the following changes in the following sections of the files.
   In the "email" section and "to" field, add your email ID. You can add multiple email addresses by separating
   them with commas. For example,
   "to": [xxx@xx.com, abc@zyz.com, ...]
   Where: xxx@xx.com or abc@zyz.com represents your email ID.
3. Save the config-current.JSON file.
4. Perform the following steps to restart the Lightweight Monitor services for the changes to take effect.
   Windows* OS:
   a) Start the command prompt.
   b) b. Type the following command to stop the Lightweight Monitor service:

      sc stop LSAService
      c. Type the following command to start the Lightweight Monitor service:
      sc start LSAService

      Linux* OS:
      Run the following command:
      /etc/init.d/LsiSASH restart

It is also recommended to restart the system log. To restart the system log, run the following command:
svcadm restart system-log

5.7.3 Configuring Alert Settings

5.7.3.1 Changing the Default Alert Delivery Method for Each Severity Level

Perform the following steps to change the default alert delivery methods for each severity level.

1. Open the config-current.JSON file in the following directories:
   Windows* OS: <ProgramFilesFolder>\LSI\LSIStorageAuthority\conf\monitor
   Linux* OS: cd /opt/lsi/LSIStorageAuthority/conf/monitor
2. In order to set the default alert delivery method for the warning severity level from the system log to both, the system log and email notification, make the following changes.
   {
   "warning": [
   "systemlog",
   "email"
   ]
   }
3. Save the config-current.JSON file.
4. Perform the following steps to restart the Light Weight Monitor services for the changes to take effect.
   Windows* OS:
   Open a command prompt window.
   c) type the following command to stop the Light Weight Monitor service:
      sc stop LSAService
   d) type the following command to start the Light Weight Monitor service:
      sc start LSAService

   Linux* OS:
   Run the following command:
   /etc/init.d/LsiSASH restart

5.7.3.2 Changing the Alert Delivery Method for a Specific Event

Perform the following steps to change the alert delivery method for a specific event.

5. Open the config-current.JSON file in the following directories:
   Windows* OS: <ProgramFilesFolder>\LSI\LSIStorageAuthority\conf\monitor
   Linux* OS: cd /opt/lsi/LSIStorageAuthority/conf/monitor
   Make the following changes to the events array.
   "events": [
   {
   "typeId": 4,
   "severity": "INFO",
   "actions": [
   "email"
   ]
   }
   ]
6. Save the config-current.JSON file.
7. Perform the following steps to restart the Light Weight Monitor services for the changes to take effect.

Windows* OS:
Open a command prompt window.

e) type the following command to stop the Light Weight Monitor service:
   sc stop LSAService
f) type the following command to start the Light Weight Monitor service:
   sc start LSAService

Linux* OS:
Run the following command:
/etc/init.d/LsiSASH restart

5.7.3.3 Changing the Severity Level for a Specific Event

Perform the following steps to change the severity level for a specific event.

8. Open the config-current.JSON file in the following directories:
   Windows* OS: <ProgramFilesFolder>\LSI\LSIStorageAuthority\conf\monitor
   Linux* OS: cd /opt/lsi/LSIStorageAuthority/conf/monitor
9. Make the following changes to the events array.

```
"events": [
{
"typeId": 4,
"severity": "CRITICAL",
"actions": [
"global"
]
}
]
```

10. Save the config-current.JSON file.
11. Perform the following steps to restart the Light Weight Monitor services for the changes to take effect.
    Windows* OS:
    Open a command prompt window.

g) type the following command to stop the Light Weight Monitor service:
   sc stop LSAService
h) type the following command to start the Light Weight Monitor service:
   sc start LSAService

Linux* OS:
Run the following command:
/etc/init.d/LsiSASH restart

6. Server Dashboard

The Server dashboard is the default landing page in the Intel® RAID Web Console 3 software. The Server dashboard displays the overall summary of the server and the devices attached to it. The user is able to troubleshoot, configure, maintain, and monitor the controllers from the Server dashboard. The following figure and table describe the three sections included in the Server Dashboard.

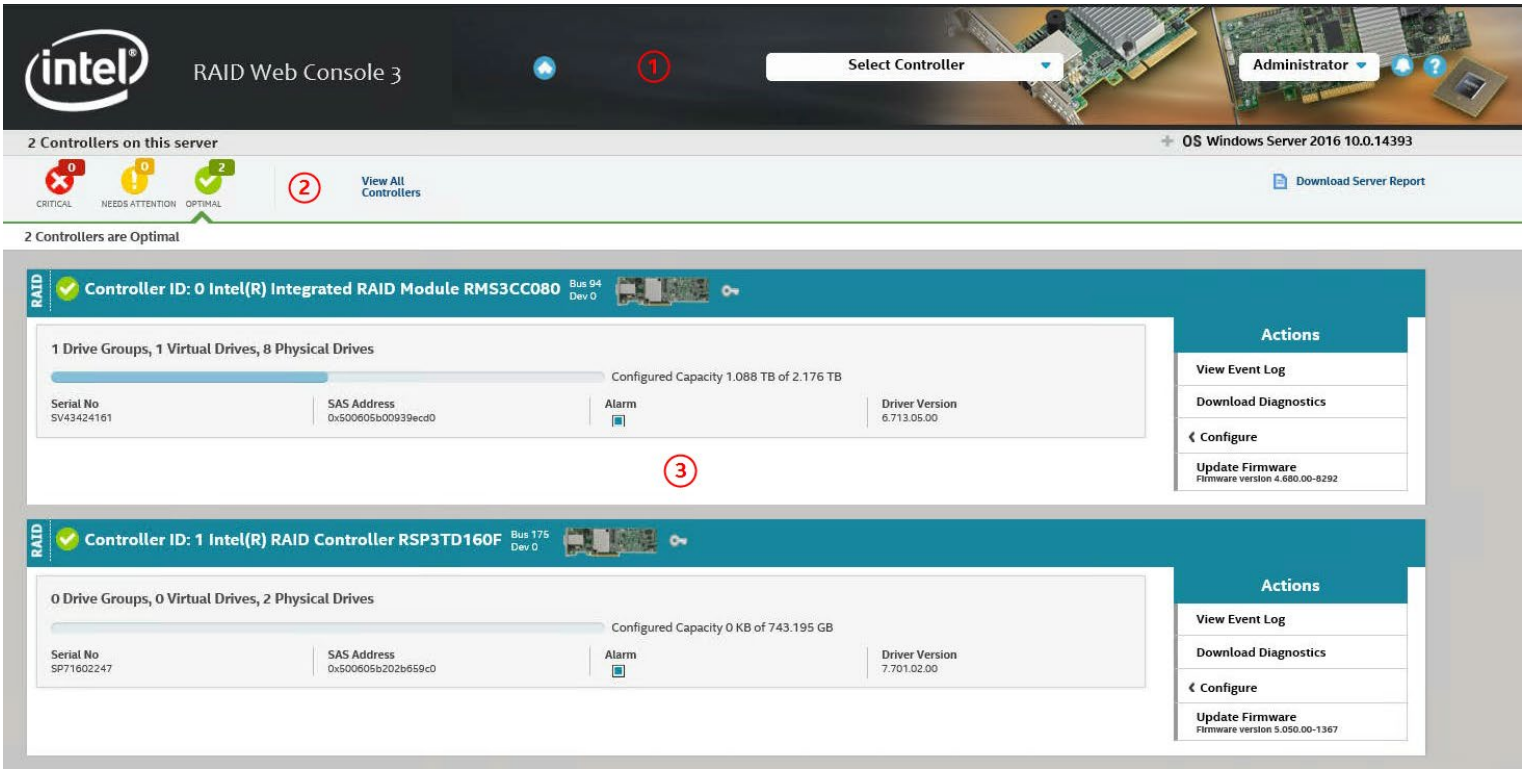


Figure 13. Server dashboard

Table 5. Server dashboard description

Section	Description
1	Main Navigation – Helps you to traverse among the various views. This navigation is available across all of the pages in the software. The description follows: The home symbol  helps you to navigate to the Server dashboard from any page in the software. Select Controllers: Lists the controllers that you are monitoring. The color-coded controller status icons (red, amber, and green) indicate the health status of all the controllers based on their criticality. Click a controller to navigate to its dashboard. Username: Displays the name of the user. Click @Settings to perform initial settings. Click Send Feedback to email your feedback to the Avago Technical Support using your Gmail or Microsoft Outlook accounts. Click View Server Profile and expand the + button to view the server configurations, such as the server IP, server name, OS Name, OS version, OS architecture, and the version of the Intel® RAID Web Console 3 software that is installed. You can also view the controller information, such as controller hardware, enclosure of the controller, and information on physical drives and virtual drives associated with the controller. Click Logout to exit from the software. The bell symbol  lets you enable or disable system messages The question mark symbol  displays the Intel® RAID Web Console 3 software context-sensitive hel

2	Controller Status – Description as follows: Displays the status of all of the controllers that are connected to the server. It displays the total number of controllers and status icons based on their criticality: Critical: Indicates that a critical error exists on the controller and the controller needs immediate attention. Needs Attention: Indicates that an error exists on the controller that needs attention, however, not immediately. Optimal: Indicates that the controller is operating in an optimal mode. Displays critical issues of failed devices and provides recommendations for troubleshooting. Additionally, you can see contextual links, which help you to easily locate the device and initiate troubleshooting. **Note**: Based on the criticality of a controller, the Intel® RAID Web Console 3 software displays information about that particular controller in the controller information pane. For example, if a controller is in the critical state, that controller is open by default. If you want to view information about other controllers, click the respective Controller Status icon. Click View All Controllers to view information about all of the controllers. Download Server Report: Enables you to download the server report, which contains consolidated information about the server and all of the devices connected to it. OS Information – Displays the server's operating system information.
3	Controller Info Displays information about the controller: Controller status. When multiple controllers are connected, the controllers are sorted based on the Bus device function. The controllers are indexed with numbers 0, 1, 2, and so on. Controller summary Controller properties Controller issues Controller event logs Lets you perform the following tasks: Configure the controllers. See Configuration Change Details Download diagnostics. Update the controller firmware. View, download, and clear event logs. Perform various operations on the controller. Navigate to any of the controllers to see its specific view by clicking on the appropriate controller.

7. Controller Dashboard

You can perform controller-related actions and view all the information pertaining to a controller from the Controller dashboard. The following figure and table describe this page.

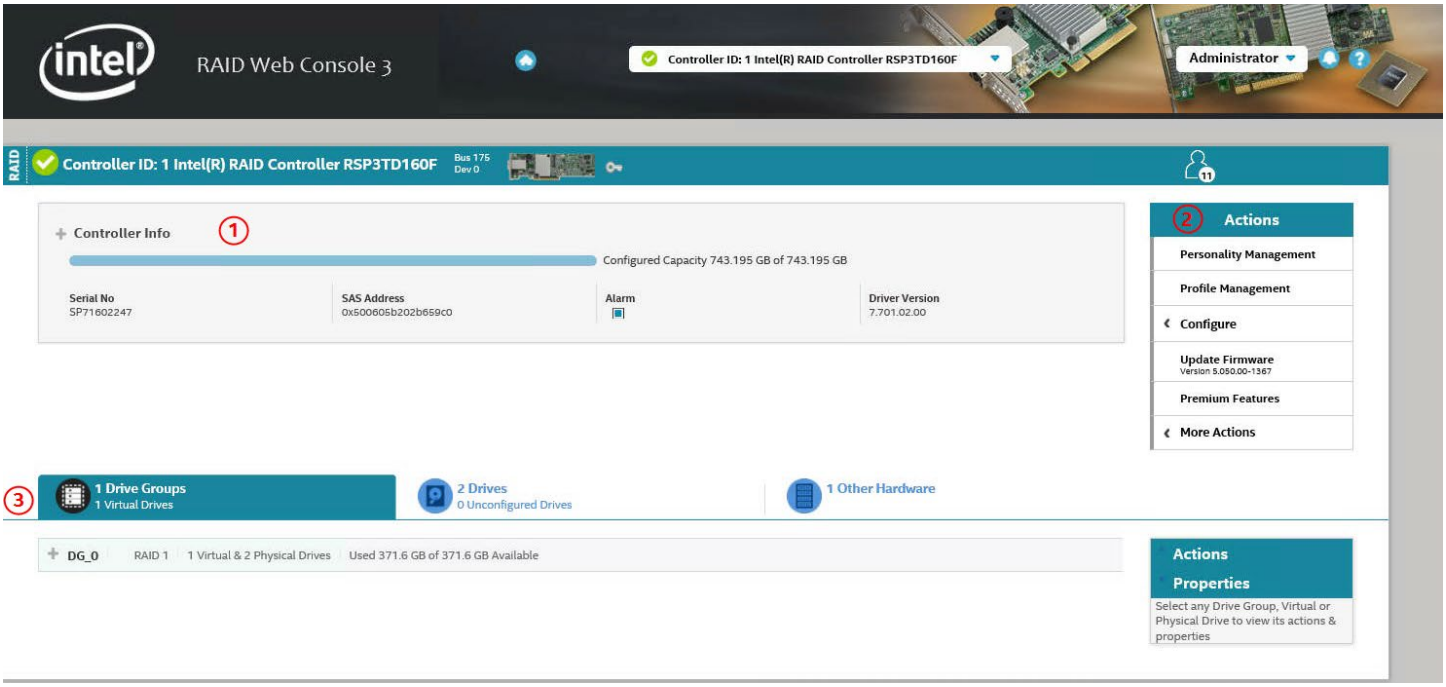


Figure 14. Controller dashboard

Table 6. Controller Dashboard Description

Section	Description
1	**Controller Summary**: Displays the name of the MegaRAID controller card. The color-coded icons indicate the status of the controller card. Displays the basic controller properties, such as the controller serial number, vendor ID, SAS address, driver version, device ID, host interface, and so on. **Note:** Click the + icon to view the advanced properties of the controller, such as the NVRAM details, data protection information properties, BIOS version, firmware properties, drive security properties, emergency spare properties, SSD Cache (Cachecade) properties, and so on.
2	**Controller Actions**: Lets you perform the following actions: 5. Create configuration 6. Clear configuration 7. Enable or disable an alarm 8. Update the controller firmware 9. Import or clear foreign configurations 10. View Premium features 11. View event log
3	**Controller Views**: Displays all of the configured drive groups, virtual drives, and physical drives associated with the selected controller card. It also displays the hardware, such as enclosures, backplanes, and the CacheVault associated with the controller. All these views are displayed as tabs. **Note**: Click the + icon to view detailed information about the device. Select any device from the expanded view to perform relevant actions and view device properties.